ATTACKS AGAINST BUILDINGS:

Threats, Vulnerabilities and Risk Assessment

Marco Carbonelli

CISINT
OSSISNa

C I S I N T

Centro Italiano di Strategia e Intelligence

Marco Carbonelli

ATTACKS AGAINST BUILDINGS:

Threats, Vulnerabilities and Risk Assessment

Prefazione di Angelo Tofalo e Andrea Malizia

CISINT
OSSISNa

(2023) CISINT – Centro Italiano di Strategia e Intelligence
Associazione culturale non a scopo di lucro.
www.cisint.org - info@cisint.org

ISBN: 979-12-210-4808-7
Prima edizione dicembre 2023

To my parents, Anna and Franco, reliable and generous references.

To my wife Giovanna, always by my side, and to our precious children Stefano, Daniele and Francesca.

To my sister Laura, prematurely departed, her brave husband Gerry, and my beloved grandchildren Pablo, Alicia and Esteban.

To the research group of the Faculty of Industrial Engineering, University of Rome Tor Vergata, to Pasquale Gaudio, Andrea Malizia, Riccardo Quaranta, Mariachiara Carestia, Daniele Di Giovanni for their support in the study carried out together in recent years.

To the nonprofit association CISINT – Centro Italiano di Strategia e Intelligence, its president Federico Sesler and research coordinator Claudio Todaro, for their willingness to engage in discussion and technical insight, for their sincere passion and enthusiasm in finalizing this book and many other scientific publications.

To those who have been loyal and cooperative with me in almost four decades of work and activities in the field.

* * *

Ai miei genitori, Anna e Franco, riferimenti affidabili e generosi.

A mia moglie Giovanna, sempre al mio fianco, e ai nostri preziosi figli Stefano, Daniele e Francesca.

A mia sorella Laura, prematuramente dipartita, al suo coraggioso marito Gerry e ai miei amati nipoti Pablo, Alicia ed Esteban.

Al gruppo di ricerca della Facoltà di Ingegneria Industriale dell'Università di Roma Tor Vergata, a Pasquale Gaudio, Andrea Malizia, Riccardo Quaranta, Mariachiara Carestia, Daniele Di Giovanni per il supporto nello studio svolto insieme nei recenti anni.

All'associazione no-profit CISINT - Centro Italiano di Strategia e Intelligence, al suo presidente Federico Sesler e al coordinatore di ricerca Claudio Todaro, per la disponibilità al confronto e all'approfondimento tecnico, per la passione sincera e l'entusiasmo con cui si sono impegnati per la finalizzazione di questo libro e di tante altre pubblicazioni scientifiche.

A chi è stato leale e collaborativo con me in quasi quattro decenni di lavoro e attività sul campo.

Roma, dicembre 2023 *Marco Carbonelli*

Table of Contents

Foreword ... **13**

1 Introduction ... **17**

2 Statistics of Terrorist attacks on soft targets, hard targets and buildings ... **22**

2.1 General description of GTD ... 23

2.2 GTD structure, available information and statistical results from 2000 to 2019 ... 25

2.2.1 GTD analysis for geographical regions ... *26*

2.2.2 GTD analysis for preferred targets ... *33*

2.2.3 GTD analysis of building attacks and used weapons ... *40*

2.3 Terrorist attacks in Europe in 2020 ... 45

2.4 Conclusion on statistical analysis for terrorist events ... 47

3 Institutional approach on risk assessment for terrorist attacks and natural disasters ... **48**

3.1 Risk definition introduction ... 48

3.2 USA DHS approach to the risk assessment for natural disaster and terrorist attacks ... 50

3.3 United Nations approach on disaster risk assessment ... 52

3.4 European approach on disaster risk assessment ... 55

3.5 Comparison among the different approaches ... 57

4 Building threat assessment and ranking ... **59**

4.1 Introduction ... 59

4.2 Building Threats Assessment Method ... 60

4.2.1 Step 1 – List of the possible sites/buildings ... *64*

4.2.2 Step 2 – List of the possible threats ... *64*

4.2.3 Step 3 - Parameters for evaluating attractiveness and terrorist capability indexes ... *67*

4.2.4 Step 4 – Evaluation and ranking of the general attractiveness index ... *74*

4.2.5 Step 5 – Evaluation of the terrorist capability index ... *76*

4.2.6 Step 6 – Evaluation of the threat probability level ... *76*

4.3 Unmanned Aircraft System as a new vector for CBRe threats ... 78

5 Building vulnerability assessment: criticality analysis and vulnerability evaluation ... **80**

5.1 Introduction ... 80

5.2 Building Vulnerability Assessment Method ... 80

5.2.1 Step 1: Building Criticality Analysis ... *81*

5.2.2 Step 2: Characterization of specific threats for the vulnerability analysis ... *91*

5.2.3 Step 3: Evaluation of the Vulnerability Level for the building ... *91*

6 Building Exposure Assessment ... **94**

7 Risk assessment for buildings ... **97**

7.1 Multi-Risk Assessment Method characteristics ... 97

7.2 Building Risk Assessment Method ... 99

7.3 BRAM, Internal-External Vulnerability and Vulnerability Reduction Factor ... 106

8 Case studies and discussion of obtained results ... **109**

8.1 BTAM application to three different Case Studies ... 109

8.1.1 BTAM practical application ... *111*

8.2 BVAM application to a Case Study ... 115

8.2.1 Building Criticality Analysis (BVAM Step 1) ... *115*

8.2.2 Characterization of specific threats (BVAM Step 2) ... *126*

8.2.3 Evaluation of vulnerability level (BVAM Step 3) ... *132*

8.3 Discussion of results ... 132

9 Conclusions and future developments 134

10 Appendix A: Building Criticality Analysis 138

10.1 Site characteristics 138
10.1.1 Surrounding structures/facilities 138
10.1.2 Terrain characteristics 139
10.1.3 Curb Lane Parking characteristics 140
10.1.4 Perimeter barriers for pedestrian access 140
10.1.5 Vehicles access points 141
10.1.6 Pedestrian Access Control 141
10.1.7 Private Vehicle Access Control 141
10.1.8 Shipping/Delivery Vehicle Access Control 142
10.1.9 Alternative Potential Access 143
10.1.10 Anti-ram devices 143
10.1.11 Site lighting in the external area 144
10.1.12 External connection to the building 144

10.2 Architecture 145
10.2.1 Mixed tenant building 145
10.2.2 Receptacles to hide explosive devices 145
10.2.3 Public and critical points in the building 146
10.2.4 Equipment for access control and screening 147
10.2.5 Reinforced walls and doors 147
10.2.6 Roof access control 148
10.2.7 Building critical assets 148
10.2.8 Separation of critical assets and loading docs/shipping areas 149
10.2.9 Mailroom space and equipment 150
10.2.10 Debris generation limitation 150

10.3 Structural Systems 151
10.3.1 Construction characteristics 151
10.3.2 Structural and Non-Structural Components 152
10.3.3 Progressive collapse 153
10.3.4 Floor of loading dock 154
10.3.5 Mailroom explosion mitigation 154
10.3.6 In-ground structural systems 155
10.3.7 Underground water presence 156

10.4 Building Envelope 156
10.4.1 Envelope protection level 156
10.4.2 Envelope fenestration balance 157
10.4.3 Glazing characteristics 158
10.4.4 High external pressure resistance 158
10.4.5 Envelope and window glazing external condition 159

10.5 Utility systems and internal distribution infrastructures 160
10.5.1 Domestic water service 160
10.5.2 Security of water entry points 161
10.5.3 Water for the fire suppression system 161
10.5.4 Sewer System 162
10.5.5 Fuel storage for continuity operations 162
10.5.6 Electrical service redundancy 163
10.5.7 Security of electrical entry points 164
10.5.8 ICT services 164

10.6 Mechanical systems - HVAC 165
10.6.1 Air intakes and exhaust louvers 165
10.6.2 Roof access 165
10.6.3 Air filtration 166
10.6.4 Air CBR sensors 167
10.6.5 Air intakes and exhaust closure 167

10.6.6 Air-handling systems zoning 168
10.6.7 Air intakes and exhaust system security 169
10.6.8 Air pressurization 169
10.6.9 Smoke evacuation systems 170
10.6.10 HVAC maintenance 170
10.7 Infrastructure and systems of internal essential services 171
10.7.1 Domestic water distribution 171
10.7.2 Hot water management 171
10.7.3 Gas distribution 172
10.7.4 Gas storages 172
10.7.5 Electrical rooms and panels 173
10.7.6 Security system wiring 173
10.7.7 Emergency power distribution 174
10.7.8 Fire alarm system 175
10.7.9 Communication system rooms 175
10.7.10 ICT disaster recovery 176
10.7.11 Mass notification system 176
10.8 Security Systems 177
10.8.1 Perimeter and internal security 177
10.8.2 Video signal quality 178
10.8.3 Video recording continuity 178
10.8.4 Intrusion detection system and alarms 179
10.8.5 Emergency call buttons and boxes 179
10.8.6 Security control equipment and scanners 180
10.8.7 Safe mail handling 181
10.8.8 Security Control Room 181
10.9 Emergency, security and operation continuity plans 182
10.9.1 Security plan 182
10.9.2 Security plan testing 183
10.9.3 Risk analysis activity 183
10.9.4 Emergency plan 183
10.9.5 Operational continuity plan 184
11 Glossary 185
12 References and Publications 186

Foreword

By Angelo Tofalo and Andrea Malizia

Angelo Tofalo

The importance of protecting buildings, critical infrastructure and, even more generally, the assets that enable essential services to be secured from possible terrorist attacks constitutes one of the main objectives of national security policies and the protection of a nation's citizens. Today's complex international geopolitical situation, with recent conflicts in the heart of Europe and the Middle East, amid significant and generalized political instabilities in various countries and on different continents, unfortunately makes the terrorist threat even more relevant.

The study conducted by Dr. Marco Carbonelli in this book entitled "*Attacks Against Buildings: Threats, Vulnerabilities and Risk Assessment*" starts from this last statement, and substantiates it in the first part of the work with a robust analysis of the international data made available by the important Global Terrorism Database managed by Mariland University and the START consortium. An analysis that shows, from the year 2000 to the present day, the absolute relevance of explosive terrorist attacks worldwide and also the presence of chemical, biological and radiological attacks.

In its central part, the book focuses on describing innovative methods for assessing the terrorist threat, vulnerability and exposure of possible targets, consistently drawing on both the important studies initiated by the U.S. Department of Homeland Security and the most recent studies also conducted within the European Union on the protection of buildings from the terrorist threat.

Very relevant are the author's recent publications, collected and discussed in great detail in the book, on the topics of security and risk management. These publications span the five-year period from 2018 to 2022 and lead to the introduction of the innovative BRAM (Building Risk Assessment Methodology) methodology, which represents - from a technical point of view - the final result proposed by the book.

BRAM is, therefore, an end point for the book, but also a starting point for further studies in this area, considering the useful purpose that the methodology can also take on at an institutional level when applied for the planning stages of investments in terrorist risk reduction. A valuable and

internationally relevant work which, in today's situation of widespread conflict, takes on a very significant importance.

Angelo Tofalo is civil engineer, former deputy of the Italian Republic, Undersecretary of State for Defense and member of Copasir. He is also Director of the Scientific Committee of CISINT – Centro Italiano di Strategia e Intelligence.

* * *

Andrea Malizia

In an era marked by rapid urbanization and societal progress, the security and integrity of our built environment are under constant threat from various sources. This book, "*Attacks Against Buildings: Threats, Vulnerabilities, and Risk Assessment*" provides a comprehensive examination of the multifaceted challenges faced by buildings, encompassing intentional acts of violence, structural vulnerabilities, and the crucial aspect of risk assessment.

Nowadays we live in the intricate dance between human progress and architectural marvels, buildings stand as iconic symbols of our civilization's achievements. However, this prominence comes at a cost, as the guardians of our collective history and aspirations face an ever-evolving spectrum of threats.

The threats against buildings are as diverse as the structures themselves. At the forefront are intentional acts of violence, manifesting as terrorism and acts of aggression. As societies grapple with geopolitical uncertainties, the motivations behind such attacks become increasingly complex.

Marco Carbonelli's book navigates through the high-stakes realm of terrorism, scrutinizing its tactics, motives, and impact on the architectural fabric that shapes our urban landscapes through an analysis of the statistics of the events in the past and a deep elaboration of the case studies and lessons learned. Simultaneously, the vulnerabilities intrinsic to the design and construction of buildings unfold as a critical aspect of threat analysis.

From the silent erosion of environmental factors to the visible scars of structural deficiencies, understanding these vulnerabilities becomes paramount in fortifying our structures against adversities.

The vulnerabilities embedded in critical infrastructures are a pivotal section of this exploration. An examination of the vulnerabilities present in the very design and construction as well as the working destination of buildings is crucial to understanding and addressing potential weaknesses. This section considers many factors such as architectural flaws, outdated outdoor and indoor designs,

and inadequate maintenance and training practices that contribute to the overall vulnerability of structures.

As the unpredictable landscape of threats unfolds, the book shifts focus to the critical arena of risk assessment. Cutting-edge technologies, such as artificial intelligence, surveillance systems, new detection and protection technologies, and emergency management systems, emerge as stalwart defenders in this contest. Simultaneously, community engagement takes center stage, emphasizing the importance of a collective commitment to security and preparedness.

By examining methodologies and technologies, the book reports solutions for enhancing the resilience of buildings against multifaceted threats.

The book concludes by drawing insights from real-world incidents, offering valuable lessons to inform future security measures. Recommendations encompass a holistic approach, advocating for interdisciplinary collaboration, continuous risk assessments, and the integration of innovative technologies.

In the face of an ever-changing threat landscape, this book serves as a compass, guiding us towards a future where our buildings not only stand tall as testaments to human achievement but also stand resilient against the challenges that seek to test their mettle.

As we collectively navigate this dynamic terrain, the pursuit of safeguarding our built environment remains imperative for the preservation of our shared history and the sustenance of our future.

Andrea Malizia is professor and coordinator of the International Master Courses in “Protection Against CBRNe events” at the University of Rome Tor Vergata. He is also member of the Scientific Committee of CISINT – Centro Italiano di Strategia e Intelligence.

1 Introduction

The events that in the last decades marked a real fracture in the global comprehension of terrorism are, without any doubt, the attacks to the New York World Trade Center and to the Pentagon orchestrated by religiously-inspired al Qaeda on September 11, 2001, which are popularly referred to as 9/11 attack. As pointed out by many academics, this event, as well as its impact and consequences, opened a new era in the terrorist attacks against buildings [Ers1].

With regard to what happened after the 9/11 attack at international level, it should be noted that while the motivations behind terrorist activities have remained very varied – ranging from political to ideological and religious – the targets chosen by terrorists and the way in which attacks have been conducted have significantly changed if compared with the characteristics of the pre-9/11 ones.

It is essential to point out that recent terrorist activities have been no longer focused exclusively on institutional buildings or high-value targets, but there has been an increase in the number of attacks against *easy-to-hit* targets. Whereas before 9/11 terrorist actions were logistically complex and often aimed at hostage-taking or mass casualties at high-value sites, this phenomenon has evolved into a more dynamic one. The new trend in terrorist attacks following 9/11 has been characterized by a strong focus on logistically *easy-to-hit* sites, but the lethality of attacks has remained substantially high [End1].

Another important aspect in the analysis of terrorist events is related to the nature of the attackers: the last period has seen an increase in the number of *single individuals* that set-in place terrorist attacks, while in the past they were almost exclusively orchestrated by centralized terrorist organisations [Gau1].

In this scenario the *protection of buildings* from terrorist attacks has become one of the most important components of the defence strategy adopted firstly by USA after the 9/11 event and, in recent years, by European Countries. This is because *buildings* can represent one of the preferred targets of terrorists, being the central venue of a country's economic life and the embodiment of its wealth and culture.

For the reasons described above, a comprehensive approach to assessing the risk of buildings against terrorist attacks has become a key issue in these last years at both institutional and academic levels. Specifically, the focus of activities in this issue is on introducing technical methods and approaches that are applicable to building protection design, aiming to protect people and properties by enforcing the security of the external part of the site, of the building perimeter and of its internal functions.

As discussed in many references [FEM1, FEM2, FEM3, EuC4, Car1], the evaluation of terrorist risk is characterized by great uncertainties due to the difficulty to evaluate its components, so a full *quantitative* risk assessment [ISO1, ISO2] is generally very difficult to apply to the three fundamental quantities defined in the literature [Car1] as *threat*, *vulnerability* and *exposure*. This is especially true for *terrorist threats*, which are by nature very volatile and unpredictable. Identifying all the possible ways in which a variety of aggressors could harm a building or a site may require a very complicated and detailed analysis of every possible type of attack.

In a practical case, the building risk assessment is usually focused at institutional level on specific targets and on a limited number of probable and destructive attack types, mainly those using various

explosive devices, or *CBR* (Chemical, Biological, Radiological) *agents*, as for the case of USA DHS (Department of Homeland Security) approach [FEM1, FEM2, FEM3].

For these kinds of weapons, in a first analysis effort it could be useful to provide reliable *semi-quantitative* methods for the building risk assessment [ISO, ISO2] which, in combination with risk *qualitative* approaches, may decrease the subjectivity of the analysis often based solely on *judgement of risk experts*.

The final aim of the building risk analysis is to reduce the impact due to hazards and threats that may cause building damages and thereby harm occupants, or passers-by, impair critical functions, and inflict economic and other losses. Therefore, building design or requalification must rely on the best available information about prevailing risks and the best protective measures that can be deployed against these risks.

Taking into account all these first introduced elements, the *objective of this book* is to outline methods and approaches for:

- identifying the principal components of building *risk*, i.e., *threat*, *vulnerability* and *exposure*;
- characterizing the building *threats* for the case of *explosive* or *CBR* weapons;
- highlighting the building *criticalities* that can be exploited as *vulnerabilities* for a terrorist attack with the selected weapons;
- assessing the building *risk* level for different considered cases in a wide geographical area, ranking, at the end of the analysis, the risks according to their relevance;
- reducing building risk levels by introducing *countermeasures* and manipulating the three risk components, in particular the *vulnerabilities*.

The fundamental hypothesis underlying this work is that an *Assessment Team* - a group of professionals including engineers, architects, risk managers, CBR advisers and other technical experts - is involved in this *risk assessment process* to ensure that the obtained results are met with *sound* protective measures that will increase the capability of the building to resist potential terrorist attacks. In fact, building collapse or failure of other building functions can have a severe effect on all sectors of the economy and key resources of the hit country, and can result in significant loss of life.

For these considerations, modern buildings design might integrate the traditional code guidelines for hazards (i.e. earthquakes, floods, fires, etc.) with safety and security countermeasures related to terrorist possible attacks, as well as other environmental and economic considerations.

The research discussed in this book has been carried out since 2018 by the author in a researcher group operating at University of Rome Tor Vergata, Industrial Engineering Department: the fundamental results obtained and discussed in this work has been published on technical magazines or presented at conferences, as summarized in tab.1.1.

Tab.1.1 – Original publications in the period (2018-2022) referred and discussed in the book.

Num.	Authors	Title	Published on/Presented to	book Reference
1	M. Carbonelli	Terrorist Attacks and Natural/Anthropic Disasters	Aracne CBRNe Book Series, ISBN 978-88-255-2565-6, Rome (Italy), 2019	[Car1]
2	M. Carbonelli, A. Iannotti, A. Malizia	Disaster Management of a Major CBRN Accident	J. Masys (ed.), Handbook of Security Science, 6 February 2021, Springer Nature Switzerland AG	[Car2]
3*	M. Carbonelli, M. Carestia, R. Quaranta	Threat assessment method for buildings in case of terrorist attacks	International Journal of Safety and Security Engineering IJSSE, Vol. 11, No. 4, pp. 285-294. August 2021	[Car3]
4*	M. Carbonelli, L. Gratta	A general multi-risk assessment method for natural disasters and CBRNe attacks	International Journal of Safety and Security Engineering IJSSE, Vol. 11, No. 4, pp. 345-352. August 2021	[Car4]
5	M. Carbonelli, M. Carestia, R. Quaranta	Risk Assessment institutional approaches for disaster management: US, UN and EU cases	2nd Scientific International Conference on CBRNe - SICC Series Conference, 12 December 2020, Rome	[Car5]
6**	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, Risk safe 2022, pp.97-111, edition 2022 WIT Press, 13 December 2022	[Car6]

* This paper has been presented, before the publication, at the *2nd Scientific International Conference on CBRNe - SICC Series Conference*, December 2020, Rome.

** This paper has been presented, before the publication, at the RISK/SAFE 2022 - 13th Conference on Risk Analysis, Hazard Mitigation and Safety and Security Engineering, 12-14 October 2022, Rome.

In *Section* 2 of this book, with the aim of introducing a statistical characterization for terrorist attacks to buildings as the base of this study, a wide analysis on 20 years of terrorist attacks [Car2, Car7, Car8, Car9], specifically from 2000 to 2019, is carried out starting from the information made available by Global Terrorism Database (GTD). The evolution of the terrorist worldwide attacks and the economic areas of the world in which the attacks have been conducted in the period of interest are illustrated in the first part of the section and, after that, the focus is placed on the type of targets preferred by the terrorists and the number per year of attacks to buildings. As a fundamental result of the analysis, it will be demonstrated that a greater number of attacks have been oriented, in the last years, against *simple* public and private buildings, facilities and areas to target and kill individuals, typically civilians. In recent years, such kind of *simple* targets has been denoted in the literature as *soft targets*, in opposition of the term *hard targets* or *hardened structures* related to government, military, police and intelligence buildings and sites. In this section a specific definition of *soft target* and *hard target* is proposed with reference to GTD fields of information and a statistical comparison between the two attack categories, *soft targets* and *hard targets*, in the period 2000-2019 is described in depth. Furthermore, an analysis on the detailed target items, such as *houses*, *apartments*, *marketplaces*, *schools*, *universities*, *restaurants*, *theatres* and other *specific locations* are considered

and statistically analysed. Finally, the issue of building terrorist attacks is faced, characterizing 20 years of building attacks in term of used weapon, focusing in particular on the investigation of *explosive* an *CBR agent* weapons.

In *Section 3*, starting from the results discussed in [Car5] an analysis of the different institutional approaches used for the risk definition and evaluation in the field of disaster management is proposed. In particular, the definitions and approaches proposed by the United States of America, by the United Nations and finally by the European Union are considered and compared. The analysis provided shows that the concept of risk in this specific area of the disaster management implicitly refers to other fundamental quantities: the first ones we discuss in this work are *threat* and *hazard*. A further quantity of interest in the analysis is related to the possible criticalities, the *vulnerability*, that characterizes the *assets/exposures* and makes them susceptible to the damaging effects of a *threat/hazard*. Finally, the practical negative evidences of the *risk* effect are described by the two quantities *consequence* or *impact*. The comparison of the three different approaches proposed for the risk evaluation will provide important evidence of different practical application that makes the values of the *evaluated level of risk* conceptually different in the Institutions considered. These evidences will be useful to define specific models for *threat*, *vulnerability*, *exposure* and *risk* in the next sections of the book.

In *Section 4*, the essential features of an original *Threat Assessment Method* [Car3] for sites and buildings in case of terrorist attacks with *explosive/CBR* agents are described. 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 one or more sites/buildings. 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 ranking 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. Furthermore, a **threat probability scale of 7 levels** is proposed for the Assessment Team support: this scale will be the first fundamental component of the risk assessment method proposed in Section 7. Finally, the topic of Unmanned Aircraft System (UAS), commonly referred to as '*drone'*, is briefly introduced at the end of the section. In fact, the fast proliferation of UAS has raised security concerns, since they can be used as a powerful *weapon vector* by malicious actors, including terrorists.

In *Section 5* an original *Building Vulnerability Assessment Method* - based on the results published in [Car6] - is illustrated in detail taking the clue on the checklist developed by the USA Department of Veterans Affairs [FEM3] and on the risk analysis model presented in [Car1]. The method proposed for the vulnerability assessment is structured in *three different steps* and provides an analytical procedure based on *76 different items* organized in *9 topics* for identifying the building *criticalities*. These criticalities are detailed in **Appendix A** of the work and a **software prototype has been developed** for helping the Assessment Team in the *criticality analysis*, as presented in some results shown in Section 8 for the Case Studies. In the second step of the Building Vulnerability Assessment Method, specific *threats* applicable to the building under analysis are fixed and detailed.

Finally, in the third step the method provides the Assessment Team a **Vulnerability Scale of 7 levels** to specify, for the buildings and the threats analyzed, the different levels of *vulnerability*.

In *Section 6* the issue of *Building Exposure Assessment* is analysed following an approach discussed in [Car1]. The assessment here described for the building *exposure* is focused on *direct* and *tangible* effects on *assets* and the characterization of the exposure of a building is divided into the following two asset categories: *population capacity* in the building or in the surrounding area, and *economic values* of the building and of the business related to the building and to the surrounding area. Three different **Exposure Scales of 7 levels** are introduced and discussed to provide a further practical tool for the risk assessment stage discussed in Section 7.

In *Section 7* an original *Risk Assessment Method* for buildings is described on the base of the results published in [Car4]. The proposed method can be adopted in any operating scenario, and in presence of any threat discussed in this work, and can provide a sufficiently accurate estimate of the risk in a simple fashion based on **Scales of 7 levels** for *threat*, *vulnerability* and *exposure* introduced in the previous sections. The method allows to manage the different kinds of risk related to the threats analyzed and provides useful results 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 the buildings.

In *Section 8* a detailed analysis and several results of different **Case Studies** are provided, applying the *methods* proposed in this book. In particular, the attention is focused on the application of the *threat* assessment method and the *vulnerability* assessment method discussed in section 4 and 5, respectively. For the *threat assessment*, three different existing buildings will be taken into account and three different threats are applied to the buildings in the analysis. For the *vulnerability assessment* the method will be applied to a single case study, a *commercial center*, in order to show the different aspect to consider in the assessment when different *threats* are applied. The results of considered Case Studies will show the practical application and the results of the original methods described in the present work, providing real examples of threat and vulnerability assessments.

Lastly in closing, Section 9 contains an analysis of the findings and provides a description of future developments on the addressed issues.

2 Statistics of Terrorist attacks on soft targets, hard targets and buildings

One of the first aspects to verify in facing the issue of terrorist attacks against *buildings* is to analyze the statistical relevance of these kinds of attacks. In particular, it could be of real interest to verify on a long period of time, for example the last 20 years, the evolution of the terrorist attacks, the economic areas of the world in which the attacks have been conducted, the type of target - government sites, public commercial sites, public cultural areas and buildings, and so on - the number per year of attacks to buildings and weapon preferred by the terrorists in the attacks (explosive, non-conventional CBR attacks, incendiary, ballistic attacks and so on).

To answer these issues, in this second section of the book the attention is focused on the analysis of the most important database on terroristic events, denoted in the following by the acronym GTD (Global Terrorism Database) [GTD1]. All the original statistical analysis herein provided has been processed in the *respect of terms of use of GTD,* **National Consortium for the Study of Terrorism and Responses to Terrorism** (START), (2021), **Global Terrorism Database™, University of Maryland** [GTD1].

The breadth and richness of specific data of this international database is below briefly described and a detailed analysis of the GTD is provided, showing statistical computations and graphical representations of obtained results for the last **20 years**. In particular, the evolution of the terrorist worldwide attacks, the economic areas of the world in which the attacks have been conducted, the type of targets preferred by the terrorists, the number per year of attacks to buildings and the weapons preferred for these attacks are analyzed and it will be demonstrated as a greater number of attacks were oriented against *simple* public and private buildings, facilities and areas to target and kill individuals, typically civilians. In the literature [Hes1, Hes2, EuC5, UN3, DHS2] this kind of *simple* targets has been in recent years denoted as *soft targets* in opposition of the term *hard targets* or *hardened structures* related to government, military, police and intelligence buildings and sites which, in general, would require for terrorist attacks better planning, larger support and funds, and where the chances of success could be lower.

For the European Commission [EuC5] the so-called *soft targets* represent "*vulnerable material or human assets which in principle should not be specifically protected*" against terrorist and other types of malicious extremist attacks. Such targets are often selected by terrorists in their effort to maximize casualties, inflict fear to the population and attain media coverage. In two Hesterman's publications [Hes1, Hes2] the following type of structures are considered *soft targets*: *schools, churches, sports and recreational venues, malls, transportation hubs and hospitals*.

A more institutional list of *soft target types* has been suggested by the European Commission Joint Researcher Center (JRC) [EuC5] in consideration of the terrorist attacks in Paris, Brussels and Barcelona in 2015, 2016 and 2017, respectively. The targets in this list are defined as: "*areas with high people concentration, metro and train stations, airports, means of mass transportation, stadiums, concert venues, shopping malls, pedestrian areas, etc.*" and the US Department of Homeland Security (DHS) in 2018 proposed a first *Security Plan Overview* for *soft targets* and *crowded places* [DHS2].

Considering these initial attempts of definition, we can observe that not all *soft targets* are directly related to *buildings* or *constructions*: in the analysis presented in this book, this aspect will

be well addressed and taken into account, and specific statistical results on general *soft target*s and the case of *buildings* (*hard* or *soft*) as a target, will be illustrated.

Finally, it is useful to stress that the author of this book proceeded in a continuative way on the GTD observation and analysis in the last three years. For this reason, some first partial results of this study were published in 2019 in a book devoted to terrorist attacks and natural disasters [Car1], in 2021 on the Handbook of Security Science published by Springer [Car2] and in 2022 with three papers on the Italian Safety & Security Magazine [Car7, Car8, Car9]. In this section 2 of the work, all the most relevant results of the GTD complete study on *soft & hard targets* and *buildings* are presented and detailed, answering to the issues introduced and discussed above.

2.1 General description of GTD

The Global Terrorism Database GTD is an open-source database including information on terrorist events that took place **from 1970 to 2019**. The database is updated annually and, at the time of this analysis, the last updated release to the year 2019 was available.

Unlike some other event databases, the GTD includes systematic *worldwide international terrorist incidents* that have occurred during this time period, fifty years of data devoted to describing and characterizing terrorist attacks.

The main characteristics of the last release available for the GTD are the following:

- information on more than 200,000 terrorist attacks;
- information on more than 95,000 bombings, 20,000 assassinations, and 15,000 kidnappings and hostage events since 1970;
- information on at least 45 variables for each case, with more recent incidents including information on more than 120 variables;
- more than 4,000,000 news articles and 25,000 news sources were reviewed to collect incident data from 1998 to 2019 alone.

For each GTD incident, at a minimum, information is available on the date and location of the incident, a brief description of the event, the weapons used, the nature of the target, the number of casualties, and, if identifiable, the responsible group or individual.

The statistical information contained in the Global Terrorism Database is based on reports from a variety of open media sources. Information, as declared by the database manager - the *National Consortium for the Study of Terrorism and Responses to Terrorism* (START) - is not added to the GTD unless and until it has been determined that the sources are credible.

The START makes the GTD available free of charge via an online interface in an effort to increase understanding of terrorist violence so that it can be more readily studied and defeated.

Together with the database, START provides a *codebook* [GTD2]. This codebook is divided into two broad areas.

The first part describes the origins of the GTD and the key decisions made during the development of the GTD. In particular, the codebook describes the GTD's *definition* of *terrorism*,

inclusion *criteria* and other definitional filtering mechanisms, and the current data collection methodology.

In the second part the *codebook* outlines the variables that constitute the GTD and defines the possible values of the variables. These variables include the GTD ID, incident date, incident location, incident information, attack information, target/victim information, perpetrator information, perpetrator statistics, claims of responsibility, weapon information, casualties and fatalities information, consequences, kidnapping/hostage taking information and other additional information.

In order to maximize the efficiency, accuracy, and completeness of GTD collection, the GTD team at START has been combining automated and manual data collection strategies since 2012. The data collection process has been developed at the *University of Maryland*: this process begins with a set of over one million media articles on any topic published worldwide daily in order to identify the relatively small subset of articles that describe terrorist attacks. This is accomplished by applying customized sophisticated keyword filters to media articles available in different languages. This filter isolates an initial pool of potentially relevant articles, approximately 400,000 per month.

These articles are then processed using further Natural Language Processing (NLP) and machine learning techniques to refine the results, remove duplicate articles, and identify articles that are likely to be relevant. The GTD team manually reviews this second subset of articles to identify the *unique events* that satisfy the GTD inclusion criteria and are subsequently researched and coded according to the specifications of the GTD Codebook.

Each month, GTD researchers at START review approximately 16,000 articles and identify attacks to be added to the GTD.

The coding strategy relies on different coding teams, each one specialized on a particular domain of the GTD Codebook. The domains include location, perpetrators, targets, weapons and tactics, casualties and consequences, and general information.

This approach guarantees that the information is coded and reviewed by someone who is closely familiar with the particular coding guidelines for the domain, as well as the relevant context.

As general policy, events that are only documented by distinctly biased or unreliable sources are not included in the database.

Fundamental to the analysis performed by the teams is the definition of *terrorism* and GTD *inclusion criteria*.

The GTD defines a **terrorist attack** as

"the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation".

In practice, this means that to consider an incident for inclusion in the GTD, **all three** of the following attributes must be present:

- *The incident must be intentional* – the result of a conscious calculation on the part of a perpetrator.
- *The incident must entail some level of violence or immediate threat of violence* -including violence against property as well as violence against people.
- *The perpetrators of the incidents must be sub-national actors*. The database does not include acts of state terrorism.

In addition, at **least two** of the following three **criteria** must be present for an incident to be included in the GTD:

- **Criterion 1**: *The act must be aimed at attaining a political, economic, religious, or social goal*. In terms of economic goals, the exclusive pursuit of profit does not satisfy this criterion. It must involve the pursuit of more profound, systemic economic change.
- **Criterion 2**: *There must be evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) than the immediate victims*. It is the act taken as a totality that is considered, irrespective if every individual involved in carrying out the act was aware of this intention. As long as any of the planners or decision-makers behind the attack intended to coerce, intimidate or publicize, the intentionality criterion is met.
- **Criterion 3**: *The action must be outside the context of legitimate warfare activities*. That is, the act must be outside the parameters permitted by international humanitarian law, insofar as it targets non-combatants.

The above inclusion criteria are evaluated for each case to determine if it should be added to the GTD: more details on additional filtering mechanism, plots, conspiracies, unsuccessful attacks and single incident determination, can be found on the last version 2021 of the *codebook* [GTD2].

In the following, all the events reported in the GTD, selected as above discussed thought the two filters related to terrorism definition and inclusion criteria have been considered for the statistical analysis. One last important general aspect to stress: the GTD does not include plots or conspiracies that are not enacted, or at least attempted. For an event to be included in the GTD, the attackers must be "out the door," en route to execute the attack. Planning, reconnaissance, and acquiring supplies do not meet this threshold.

2.2 GTD structure, available information and statistical results from 2000 to 2019

For a more analytical study, as previously described, it is necessary to download the full GTD Database that contains more than 200,000 terroristic events.

The complete database structure is organized in *nine* detailed sections, hereafter listed:

Database Information Sections

I. GTD ID and Date
II. Incident Information
III. Incident Location
IV. Attack Information
V. Weapon Information
VI. Target/Victim Information
VII. Perpetrator Information
VIII. Casualties and Consequences
IX. Additional Information and Sources

More details for any sections are described in the *codebook* [GTD2].

2.2.1 GTD analysis for geographical regions

A first interesting analysis can be focused on the section III 'Incident Location'.

Taking into account different wide-areas of the world denoted in the following as *regions*, the GTD fields allow to statistical characterize the number of terrorist events per *region*.

A division in 12 *regions* [GTD2] is proposed as follow:

1. North America
2. Central America & Caribbean
3. South America
4. East Asia
5. Southeast Asia
6. South Asia
7. Central Asia
8. Western Europe
9. Eastern Europe
10. Middle East & North Africa
11. Sub-Saharan Africa
12. Australasia & Oceania

The detailed association between *regions* and *national states* is described in [GTD2]. Note that the geo-political boundaries of many countries have changed over the last 50 years covered by the GDT data. In a number of cases, countries that represented the location of terrorist attacks no longer exist today. This situation includes, for example, West Germany, the USSR and Yugoslavia. In these cases, the country name for the year the event occurred is recorded.

A first result for the statistical data processing is shown in tab 2.1 and fig.2.1 where the number of terrorist events per *region*, over the period of time 2000-2019, is reported and graphically represented.

Tab.2.1 and fig.2.1 show that:

- in the last 20 years the number of worldwide terrorist events recorded by GTD is 131,350;
- about 36% of the terrorist attacks in the last 20 years are concentrated in the Middle East & North Africa;
- South Asia gathers more than 33% of the terrorist events of the last 20 years;
- more than 82% of the international terrorist attacks in the last 20 years are concentrated in only three regions: Middle East & North Africa, South Asia and Sub-Saharan Africa;
- the two regions in which Europe is divided are, when considered together, attacked by terrorists roughly nine times bigger than North America region.

Tab2.1 – Terrorist events per region in the period 2000-2019.

Region	Terrorist events in 20 years (2000-2019)	%
Middle East & North Africa	47018	35.80%
South Asia	43541	33.15%
Sub-Saharan Africa	17236	13.12%
Southeast Asia	11156	8.49%
Eastern Europe	4135	3.15%
Western Europe	3597	2.74%
South America	3102	2.36%
North America	888	0.68%
Central Asia	239	0.18%
East Asia	221	0.17%
Central America & Caribbean	119	0.09%
Australasia & Oceania	98	0.07%
Total events	**131350**	**100%**

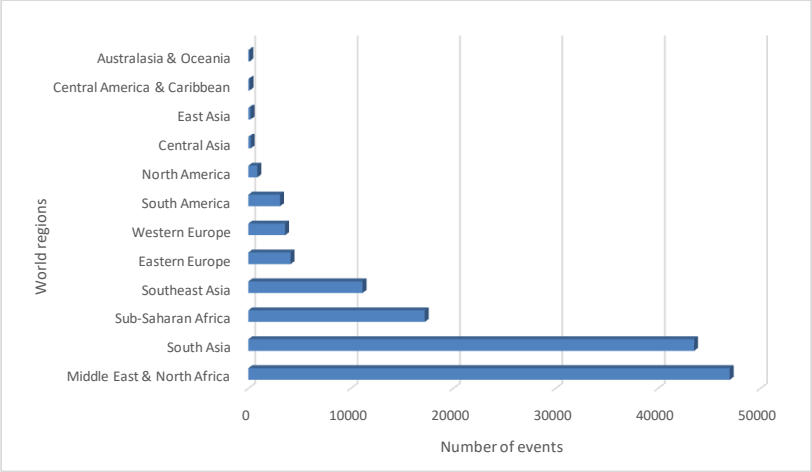

Fig.2.1 – Distribution of terrorist events in the world per region, period 2000-2019.

In particular, with the aim of punctually comparing the terrorist situation in the *North America* (Canada, Mexico, United States) region respectively with the *Western Europe* (Andorra, Austria, Belgium, Cyprus, Denmark, Finland, France, Germany, Gibraltar, Greece, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, United Kingdom, Vatican City) and *Eastern Europe* (Albania, Belarus, Bosnia-Herzegovina, Bulgaria, Croatia, Czech Republic, Czechoslovakia, Estonia, Hungary, Kosovo, Latvia, Lithuania, Macedonia, Moldova, Montenegro, Poland, Romania, Russia, Serbia, Serbia-Montenegro, Slovak Republic, Slovenia, Ukraine) regions, we can observe that in the last 20 years only 0.68% of the worldwide events took place in North America, and 3.15% and 2.74% in Eastern Europe and Western Europe, respectively.

Extending the analysis to the evolution over time, year per year, of the terrorist events per region, we can obtain the cumulative results described in tab.2.2.

Tab.2.2 - Evolution on the time, year per year, of the number of terrorist events per region.

Events/region/year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	Total
Australasia & Oceania	6	4	2	4			2	1	6	1	1			1	9	12	10	13	21	5	98
Central America & Caribbean	14	8	3	8	5	3	5	4		9	1	1	1	14	5	1	3	4	15	15	119
Central Asia	21	18	6	7	8	11	6	4	36	31	9	9	12	7	9	10	17	8	7	3	239
East Asia	19	19	4	6	4	2	1		25	8	1	4	4	15	43	28	8	7	6	17	221
Eastern Europe	234	252	112	100	45	76	70	62	209	165	261	198	173	166	963	685	136	112	72	44	4135
Middle East & North Africa	272	361	324	310	492	882	1186	1384	1535	1361	1463	1663	2402	4570	6996	6194	6557	4181	2737	2148	47018
North America	51	54	33	34	12	22	15	18	31	17	24	12	39	32	37	63	79	102	109	104	888
South America	150	229	162	117	42	49	50	47	144	159	148	106	136	185	283	176	165	179	301	274	3102
South Asia	356	385	334	353	369	604	938	984	1759	1945	1981	2138	3806	4612	4997	4586	3640	3432	3285	3037	43541
Southeast Asia	256	186	110	145	94	204	272	365	514	561	473	356	588	1188	1083	1072	1077	1024	874	714	11156
Sub-Saharan Africa	191	162	121	73	34	60	114	302	380	283	331	494	1167	1001	2320	1971	2082	2000	2210	1940	17236
Western Europe	253	234	119	121	59	104	98	76	162	182	133	95	193	254	214	335	272	296	203	194	3597
Total	**1823**	**1912**	**1330**	**1278**	**1164**	**2017**	**2757**	**3247**	**4801**	**4722**	**4826**	**5076**	**8521**	**12045**	**16959**	**15133**	**14046**	**11358**	**9840**	**8495**	**131350**

The total number of events in the world per year is shown graphically in fig.2.2.

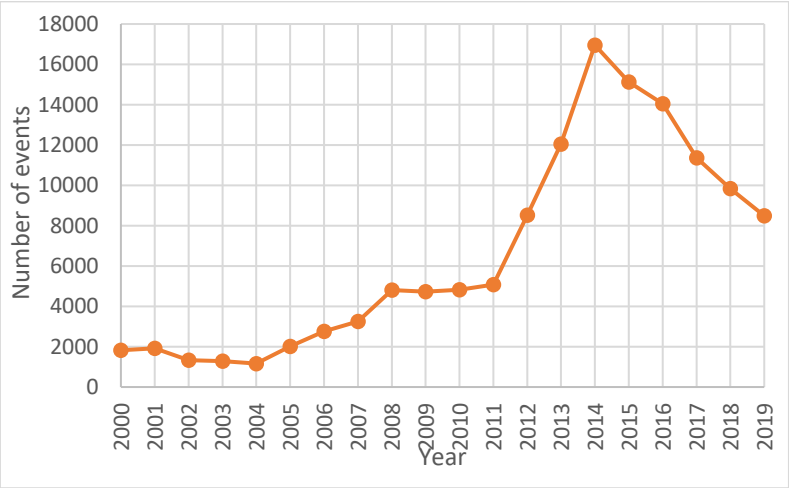

Fig.2.2 – Number of terrorist events in the world per year, period 2000-2019.

The analysis of the fig.2.2 highlights the very significant growth of the annual number of events in the years 2012-2017, corresponding to the effects of Middle East crisis, Syrian war, the international intervention against the ISIS (Islamic State of Iraq and Syria) and the first Crimea crisis between Russia and Ukraine. The maximum number of terrorist attacks per year is obtained in 2014 with 16,959 events.

Fig.2.3 shows the results obtained for the Eastern and Western Europe regions in terms of number of terrorist events per year in the period 2000-2019. It is easy to recognize for Eastern Europe in 2014 the maximum of around 1000 terrorist events mainly due to the first Crimea crisis. For Western Europe, the number of events oscillates around 200 attacks per years, with a peak of 335 terrorist events in 2015.

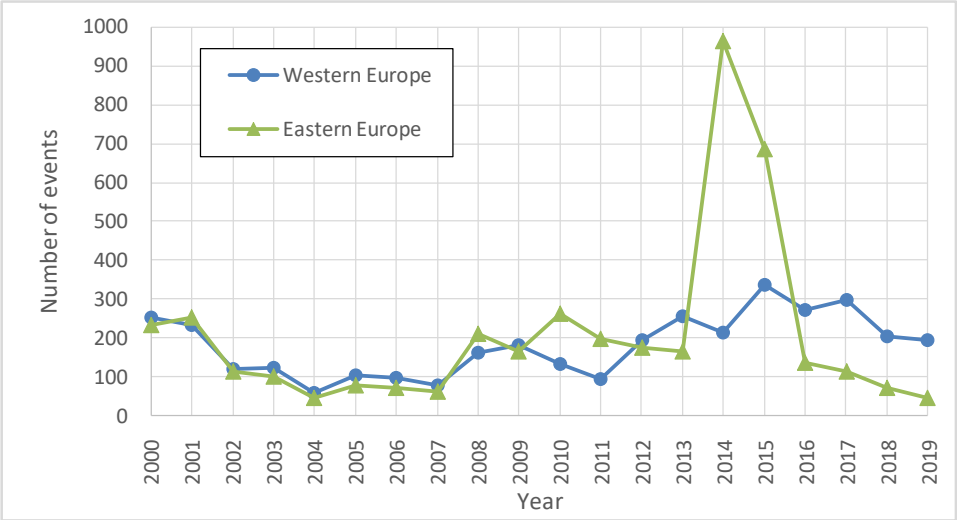

Fig.2.3 – Comparison of the number of terrorist events in Western and Eastern Europe per year, in the period 2000-2019.

In fig.2.4 a comparison between the number of terrorist events in Western Europe and North America is shown for the period 2000-2019. The illustrated trends show a clear prevalence of terrorist events in Europe compared to North America, with the ratio of attacks for European countries ranging from 2 to 5 times the annual value for North America.

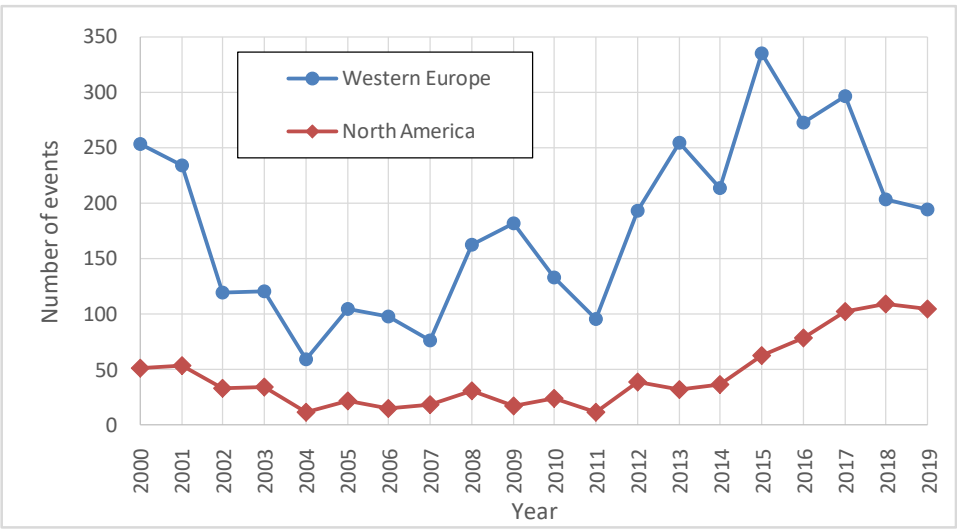

Fig.2.4 – Comparison of the number of terrorist events in Western Europe and North America per year, in the period 2000-2019.

Another fundamental information regarding the terrorist events is provided by the number of fatalities and casualties worldwide recorded per year in the period considered. In tab.2.3, column 3 and 4, respectively, the number of fatalities and casualties per year are reported for the period 2000-2019. To make a clearer comparison and analysis possible, in column 2 the number of terrorist events is reported as well.

Tab.2.3 – Number of worldwide terrorist events, fatalities and casualties per year, in the period 2000-2019.

Year	Num. of Events	Num. of Fatalities	Num. of Casualties
2000	1823	4394	5797
2001	1912	7727	28137
2002	1330	4797	7079
2003	1278	3317	7384
2004	1164	5716	11976
2005	2017	6343	12961
2006	2757	9316	15470
2007	3247	12825	22531
2008	4801	9157	18998
2009	4722	9277	19147
2010	4826	7829	15953
2011	5076	8246	14662
2012	8521	15494	25446
2013	12045	22280	37690
2014	16959	44524	41177
2015	15133	38993	44204
2016	14046	35236	40576
2017	11358	26892	25487
2018	9840	23290	20607
2019	8495	20329	18714
Total	**131350**	**315982**	**433996**

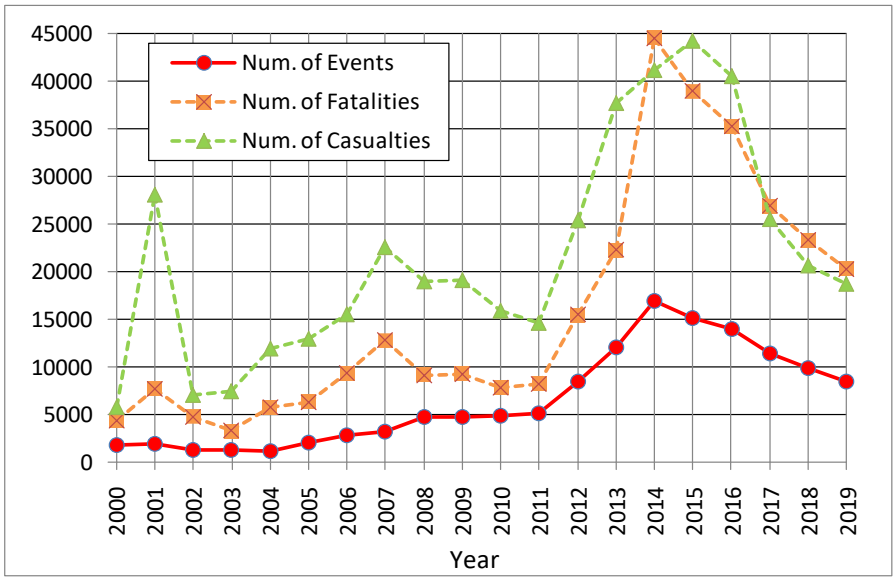

Fig.2.5 – Graphical representation of the worldwide number of terrorist attacks (events), fatalities and casualties per year, in the period 2000-2019.

All these data are graphically represented in fig.2.5, which shows:

- a first clear peak in the 2001 for the number of casualties, more than 28,000, and fatalities, more than 7,000, due mainly to the 11th September USA Twin Towers attacks. The countries affected in 2001 by deaths in terrorist events are illustrated graphically in fig.2.6;

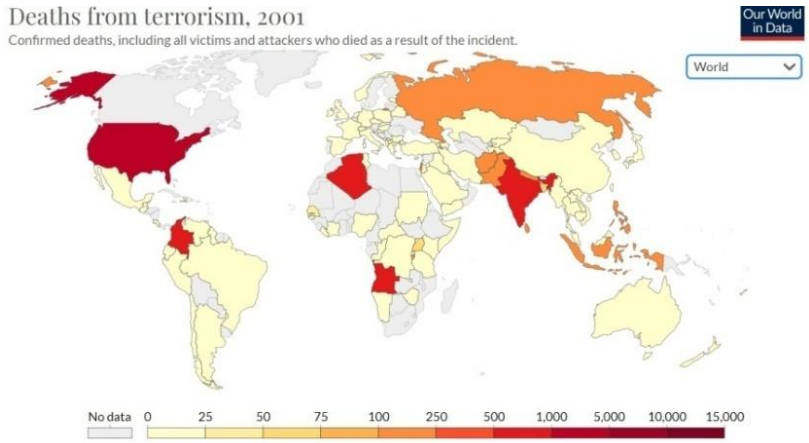

Fig.2.6 – Graphical representation of the countries interested by fatalities due to terrorist attacks in the 2001 (source https://ourworldindata.org/terrorism).

- a second peak in 2007 for the number of fatalities (12,825) and casualties (22,531) due to terrorist events, related to several areas of crisis mainly in Asia (Iraq, Afghanistan, Pakistan, India, Sri Lanka), as shown in fig.2.7;

Fig.2.7 – Graphical representation of the countries interested by fatalities due to terrorist attacks in the 2007 (source https://ourworldindata.org/terrorism).

- a third peak in 2014-2015 for the number of fatalities (44542 in 2014) and casualties (44204 in 2015) due to terrorist events, related to several areas of crisis mainly in the Middle East (Syria and Iraq), Africa (Nigeria), Ukraine and Asia (Afghanistan, Pakistan, India and China) as shown in fig.2.8.

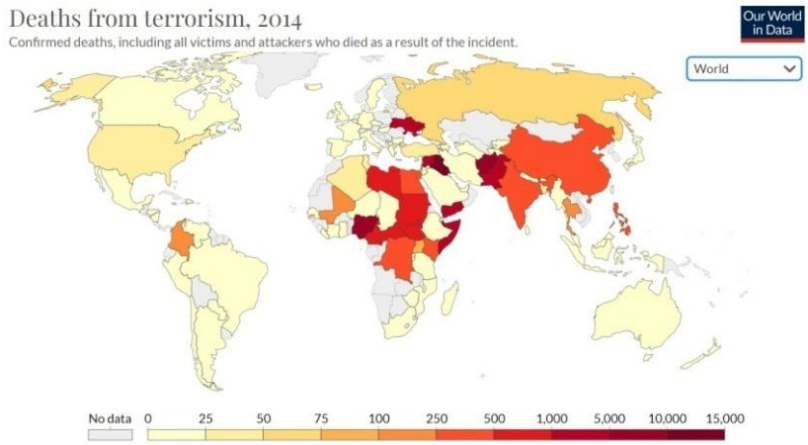

Fig.2.8 – Graphical representation of countries interested by fatalities due to terrorist attacks in the 2014 (source https://ourworldindata.org/terrorism).

Another important viewpoint is, as for the case of the number of events, the comparison between the number of fatalities per year for North America and Europe, both Eastern and Western. In tab.2.4 the detailed results obtained for the number of fatalities due to terrorist events per year in North America, Western and Eastern Europe, in the period 2000-2019 are presented.

Fig.2.9 makes it easy to compare the different behavior over the years, highlighting for the US the peak of fatalities in the 2001 due to the 11/9 attack and for the Eastern Europe the peak due to the Crimea Crisis in the Ukraine internal conflict.

The total final numbers reported in tab.2.4 show that Eastern Europe presents many more fatalities per event with respect to Western Europe and that, excluding the fatalities of the dramatic 9/11 event, the number of residual deaths in North America in 20 years (roughly 600) is even smaller than the Western Europe figure of 978.

Tab.2.4 – Number of fatalities due to terrorist events per year in North America, Western and Eastern Europe, period 2000-2019.

Year	Num. of Fatalities Western Europe	Num. of Fatalities North America	Num. of Fatalities Eastern Europe
2000	42	13	402
2001	40	3027	294
2002	9	4	518
2003	5	2	337
2004	196	0	584
2005	60	2	158
2006	6	8	59
2007	17	25	57
2008	3	23	101
2009	15	24	143
2010	5	4	235
2011	83	0	174
2012	12	24	179
2013	8	70	151
2014	6	34	1468
2015	171	63	791
2016	170	73	112
2017	83	127	101
2018	25	81	41
2019	22	77	34
Total	**978**	**3681**	**5939**

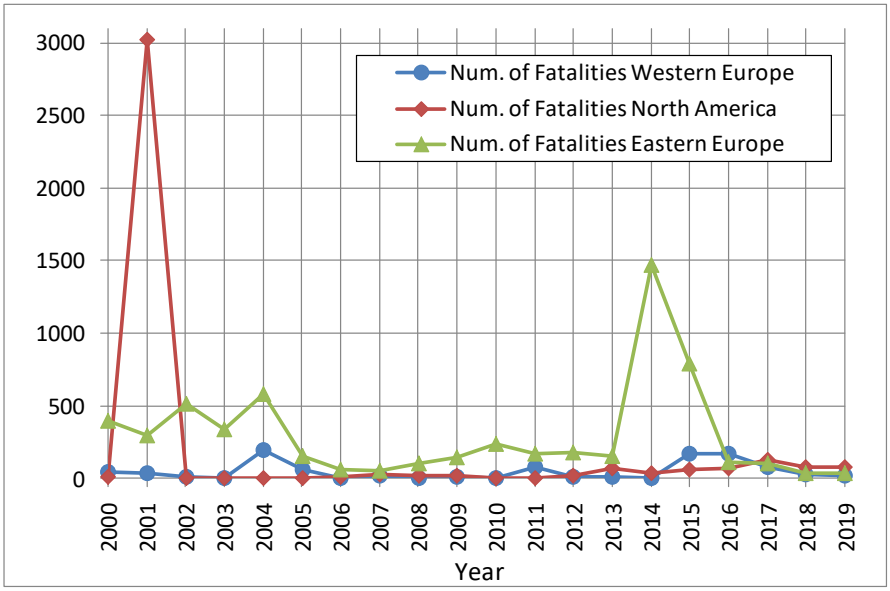

Fig.2.9 – Graphical representation of the number of fatalities per year due to terrorist events in North America, Western and Eastern Europe, in the period 2000-2019.

2.2.2 GTD analysis for preferred targets

A second interesting analysis applied to GTD can be focused on section VI "Target/Victim information". In particular, taking into account the definition of two categories *soft* and *hard targets* presented above in the introduction of this section, it is of fundamental interest to understand the behaviours of these two categories of complementary targets along the years.

Adopting the definitions proposed in GTD *codebook* [GTD2] and there detailed, we introduce 22 *sub-categories* of *target* listed in the following tab.2.5. For each sub-category we apply the definitions of *soft target* (ST) and *hard target* (HT) illustrated in the introduction of this section - applied to individuals, organizations, facilities, buildings and sites - and, after a careful evaluation of the sub-category definitions [GTD2], we assign the specific sub-category only to one of ST and HT categories, otherwise we assign the category "*Not Applicable"* (NA).

In tab.2.5 the possible 14 sub-categories related to *soft target* have been highlighted in yellow and the 4 sub-categories related to *hard targets* have been highlighted in light blue. Only for 4 other sub-categories it is not possible to assign a position in the ST or HT sets *a priori* and for this reason they have been assigned as "*Not Applicable*".

In tab.2.6 a first statistical analysis for the terrorist preferred targets is proposed, describing, for each of the 22 sub-categories of target introduced in tab.2.5, the associated number of terrorist attacks (events) recorded in GTD in the period 2000-2019, and the relative percentage of occurrence of the sub-category in the 20 years.

Tab.2.5 – Assignment of sub-categories of target to *soft* and *hard targets* categories.

Sub-category of Target	Soft Target	Hard Target	Not Applicable
Private Citizens & Property	✓		
Military		✓	
Police		✓	
Government (General)		✓	
Business	✓		
Religious Figures/Institutions	✓		
Transportation	✓		
Educational Institution	✓		
Terrorists/Non-State Militia			NA
Utilities	✓		
Journalists & Media	✓		
Government (Diplomatic)		✓	
Violent Political Party			NA
NGO	✓		
Telecommunication	✓		
Airports & Aircraft	✓		
Tourists	✓		
Food or Water Supply	✓		
Maritime	✓		
Abortion Related	✓		
Other			NA
Unknown			NA

The analysis of this first results for the period 2000-2019 at worldwide level shows that:

- the *soft targets* (yellow cells, 14 sub-categories) correspond to 63,629 terrorist events (48.44% of the total);
- the *hard targets* (light blue cells, 4 sub-categories) correspond to 57,516 terrorist events (43.79% of the total);
- the "Not Applicable" cells (4 sub-categories) correspond to 10250 terrorist events (7.77% of the total).

These first worldwide results, shown graphically in fig.2.10, highlight the prevalence of terrorist events against the *soft target* category over the *hard target* one in the last 20 years, confirming as first cumulative evidence, the opportunity to delve into greater depth on this issue introduced in recent technical literature [Hes1, Hes2, EuC5, UN3, DHS2].

Tab.2.6 – Target Sub-categories ranking in terms of worldwide number of terrorist events, in the period 2000-2019.

Sub-category of Target (period 2000-2019)	Number of events	%
Private Citizens & Property	36594	27.86%
Military	22529	17.15%
Police	19430	14.79%
Government (General)	14106	10.74%
Business	10097	7.69%
Unknown	5976	4.55%
Religious Figures/Institutions	3563	2.71%
Transportation	3423	2.61%
Educational Institution	3285	2.50%
Terrorists/Non-State Militia	2753	2.10%
Utilities	2531	1.93%
Journalists & Media	1673	1.27%
Government (Diplomatic)	1451	1.10%
Violent Political Party	1329	1.01%
NGO	766	0.58%
Telecommunication	707	0.54%
Airports & Aircraft	407	0.31%
Tourists	194	0.15%
Food or Water Supply	178	0.14%
Maritime	177	0.13%
Other	147	0.11%
Abortion Related	34	0.03%
Total	**131350**	**100%**

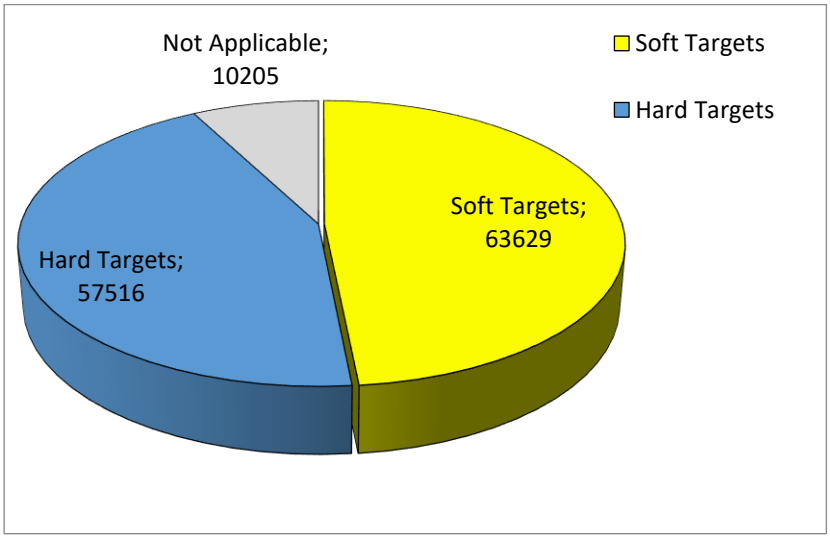

Fig.2.10 – Graphical representation of the worldwide percentage among *soft targets*, *hard targets* and *Not Applicable* cases, period 2000-2019.

To gain more insight on the behaviour over time of these two complementary target categories, an analysis of the annual events related to the two categories has been carried out and is reported in tab.2.7. and in fig,2.11, where the results obtained are shown graphically.

Tab.2.7 – Behaviours over the time of the worldwide annual number of *soft* and *hard target* attacks, period 2000-2019.

Year	Num. of Hard Target Attacks per year	Num. of Soft Target Attacks per year
2000	701	1092
2001	669	1214
2002	499	802
2003	596	646
2004	554	576
2005	1033	945
2006	1119	1579
2007	1452	1717
2008	1548	2986
2009	1391	3140
2010	1740	2885
2011	1990	2832
2012	4456	3466
2013	6116	4994
2014	8110	7396
2015	6442	7112
2016	5543	6974
2017	5058	4948
2018	4623	4380
2019	3876	3945
Total	**57516**	**63629**

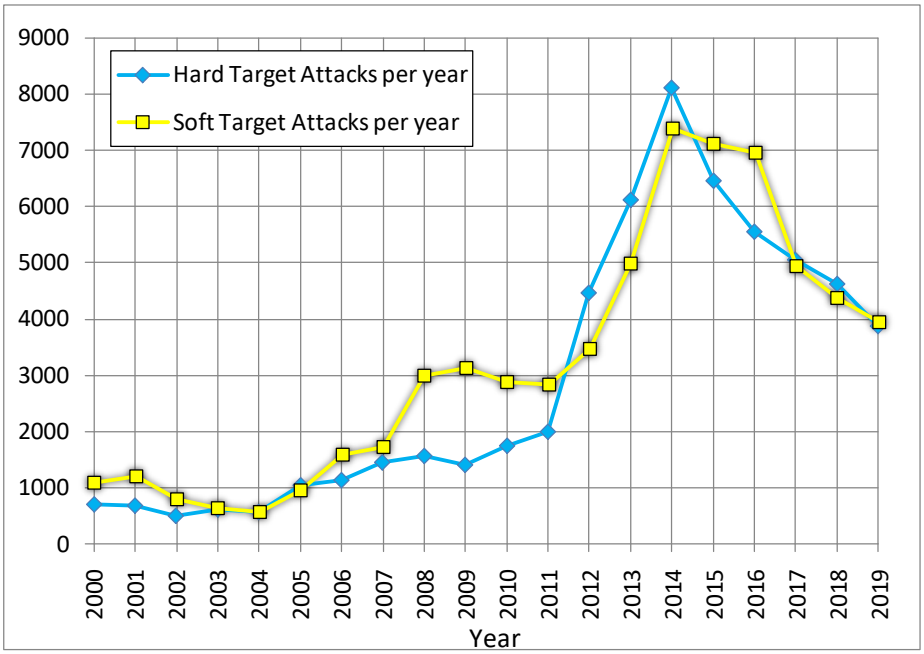

Fig.2.11 – Graphical representation of the annual number of worldwide terrorist events (attacks) for the two categories *soft targets* and *hard targets*, in the period 2000-2019.

Fig.2.11 confirms that in the period considered both *soft* and *hard targets* have considerably increased at worldwide level, with a cumulative prevalence of terrorist events against *soft targets*.

In the following tab.2.8 and fig.2.12, the attention is focused on worldwide terrorist events solely oriented against *soft targets* and the number of fatalities per year in such a case is evaluated.

Tab.2.8 – Behaviours over the time of the worldwide annual number of fatalities for the *soft target* attacks, in the period 2000-2019.

Year	Num. of Soft Target Attacks per year	Num. of Soft Target Fatalities per year
2000	1092	2682
2001	1214	6029
2002	802	3194
2003	646	1865
2004	576	2869
2005	945	3388
2006	1579	6375
2007	1717	7748
2008	2986	5337
2009	3140	6217
2010	2885	4618
2011	2832	4266
2012	3466	5524
2013	4994	9862
2014	7396	21589
2015	7112	17631
2016	6974	16914
2017	4948	10796
2018	4380	8677
2019	3945	7332
Total	63629	152913

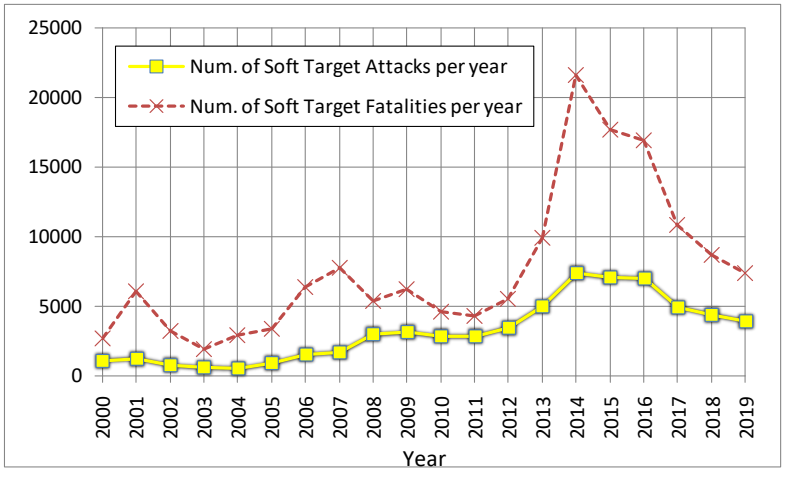

Fig.2.12 – Graphical representation of the worldwide number of annual fatalities and terrorist events (attacks) for the *soft targets*, in the period 2000-2019.

These results confirm the relevance of the number of worldwide fatalities, more than 152,931 in twenty years (48,4% of total deaths in the period) and with an impressive peak of 21,589 deaths in 2014, for the *soft target* case.

To further investigate this *soft target* issue, the 14 sub-categories selected in tab.2.5 for the set of *soft targets* are each individually evaluated in terms of number of annual terrorist events and number of annual fatalities in the 20 years considered, sub-category by sub-category. The obtained results for the worldwide number of attacks are ranked decreasingly and reported in tab.2.9. Furthermore, the attention is focused on the first five sub-categories of the ranking (which represent 89,52% of the occurrences) providing in fig.2.13 a visual representation of the worldwide annual trends of the five sub-categories over the period 2000-2019.

Tab.2.9 – *Soft target* sub-categories worldwide analysis in terms of number of attacks and fatalities per year, in the period 2000-2019.

Soft Target sub-categories (period 2000-2019)	Num. of Attacks	% over total Soft Target Attacks	Num. of Fatalities
Private Citizens & Property	36594	57.51%	108481
Business	10097	15.87%	17243
Religious Figures/Institutions	3563	5.60%	11687
Transportation	3423	5.38%	7070
Educational Institution	3285	5.16%	3088
Utilities	2531	3.98%	1150
Journalists & Media	1673	2.63%	990
NGO	766	1.20%	757
Telecommunication	707	1.11%	91
Airports & Aircraft	407	0.64%	1215
Tourists	194	0.30%	470
Maritime	177	0.28%	473
Food or Water Supply	178	0.28%	194
Abortion Related	34	0.05%	4
Total	**63629**	**100%**	**152913**

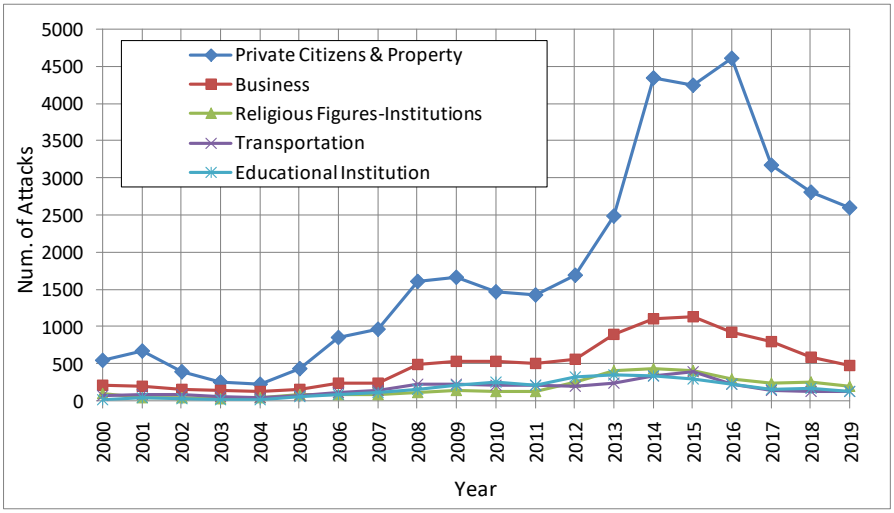

Fig.2.13 – Graphical representation of the worldwide annual number of terrorist events (attacks) for the first five sub-categories in the soft targets ranking, in the period 2000-2019.

Fig.2.13 confirms for the first five sub-categories of the ranking the very significant worldwide increasing trends of the attacks in the time, with a particular emphasis on the first two sub-categories, Private Citizens & Property and Business, that collect more than 73% of the attacks to *soft targets* over the period of 20 years.

To conclude this part of the analysis on *soft targets*, a further study has been carried out on 12 selected *target items* (very specific targets listed in tab.2.10) belonging to three mentioned sub-categories of tab.2.9, precisely: *Private Citizens & Property*, *Business* and *Educational Institution*. These 12 *target items*, belonging to *soft target* sub-categories, were selected considering the most glaring terrorist attacks in Western Countries, only as an example, in order to show the maximum level of detail reachable in the analysis for possible specific targets. The attention has been focused on the *target item*s related to *soft targets* specified in the following tab.2.10.

Tab.2.10 – Selected *target items* of the three sub-categories Private Citizens & Property, Business and Educational Institution for a specific study.

Target items (sorted alphabetically)	Sub-category of Soft Targets
Bank/Commerce	*Business*
Construction	*Business*
Entertainment/Cultural/Stadium/Casino	*Business*
House/Apartment/Residence	*Private Citizens & Property*
Marketplace/Plaza/Square	*Private Citizens & Property*
Medical/Pharmaceutical (Hospital)	*Business*
Memorial/Cemetery/Monument	*Private Citizens & Property*
Museum/Cultural Center/Cultural House	*Private Citizens & Property*
Public Area (garden, parking lot, garage, beach, public building, camp)	*Private Citizens & Property*
Restaurant/Bar/Café	*Business*
Retail/Grocery/Bakery	*Business*
School/University/Educational Building	*Educational Institution*

The complete results for these 12 *target items* are reported in tab.2.11 where, year by year in the period 2000-2019, the number of terrorist worldwide events (attacks) are shown for each *target item*.

Tab.2.11 – Selected *target items* characterization in terms of worldwide annual number of attacks, in the period 2000-2019.

Target Items/Num of annual Events	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	Total
Bank/Commerce	45	27	27	17	10	12	26	10	41	35	39	31	57	79	49	40	29	40	39	22	**675**
Construction	6	10	3	12	12	10	17	12	39	65	65	71	78	94	135	135	84	147	102	84	**1181**
Entertainment/Cultural/Stadium/Casino	26	15	16	5	10	6	3	17	32	14	22	15	19	30	43	30	27	28	13	10	**381**
House/Apartment/Residence	26	28	16	17	10	10	26	16	103	81	98	105	140	183	445	302	454	216	170	174	**2620**
Marketplace/Plaza/Square	39	23	26	18	12	24	50	69	79	99	47	39	85	276	371	376	317	230	109	102	**2391**
Medical/Pharmaceutical	3	5	2	4	4	7	15	13	18	43	37	28	29	76	103	76	55	44	42	53	**657**
Memorial/Cemetery/Monument	2	3	5	4		1	3	2	6	3	4	2	6	12	16	21	9	7	14	3	**123**
Museum/Cultural Center/Cultural House	2	2	1		2		1	1	4	2		4	6	5	14	11	8	1	6	3	**73**
Public Area (garden, parking lot, garage, beach, public building, camp)	11	10	6		2	2	10	5	28	20	9	10	25	64	54	51	25	18	23	36	**409**
Restaurant/Bar/Café	16	21	22	20	14	17	23	28	48	51	53	31	52	157	151	182	136	59	42	35	**1158**
Retail/Grocery/Bakery	22	22	19	20	9	18	35	37	88	110	98	114	128	184	254	384	367	243	114	59	**2325**
School/University/Educational Building	14	34	23	23	19	28	64	82	107	171	213	164	276	244	212	212	153	103	113	81	**2336**
Total	**212**	**200**	**166**	**140**	**104**	**135**	**273**	**292**	**593**	**694**	**685**	**614**	**901**	**1404**	**1847**	**1820**	**1664**	**1136**	**787**	**662**	**14329**

Starting from tab.2.11 it is possible to generate a ranking (see tab.2.12) of the *target items* ordered by the total worldwide number of terrorist events (attacks) in the 20 years considered.

Tab.2.12 – Target item ranking ordered by the total worldwide number of terrorist events (attacks) for each item, in the period 2000-2019.

Target item ranking (period 2000-2019)	Num. of Attacks	%
House/Apartment/Residence	2620	18.3%
Marketplace/Plaza/Square	2391	16.7%
School/University/Educational Building	2336	16.3%
Retail/Grocery/Bakery	2325	16.2%
Construction	1181	8.2%
Restaurant/Bar/Café	1158	8.1%
Bank/Chamber of Commerce	675	4.7%
Medical/Pharmaceutical	657	4.6%
Public Area (garden, parking lot, garage, beach, public building, camp)	409	2.9%
Entertainment/Cultural/Stadium/Casino	381	2.7%
Memorial/Cemetery/Monument	123	0.9%
Museum/Cultural Center/Cultural House	73	0.5%
Total	**14329**	**100%**

Finally, focusing the attention on the first three *target items* in the ranking of tab.2.12, a visual representation of the year-by-year trend, of the annual number of terrorist events is shown, for each item, in fig.2.14.

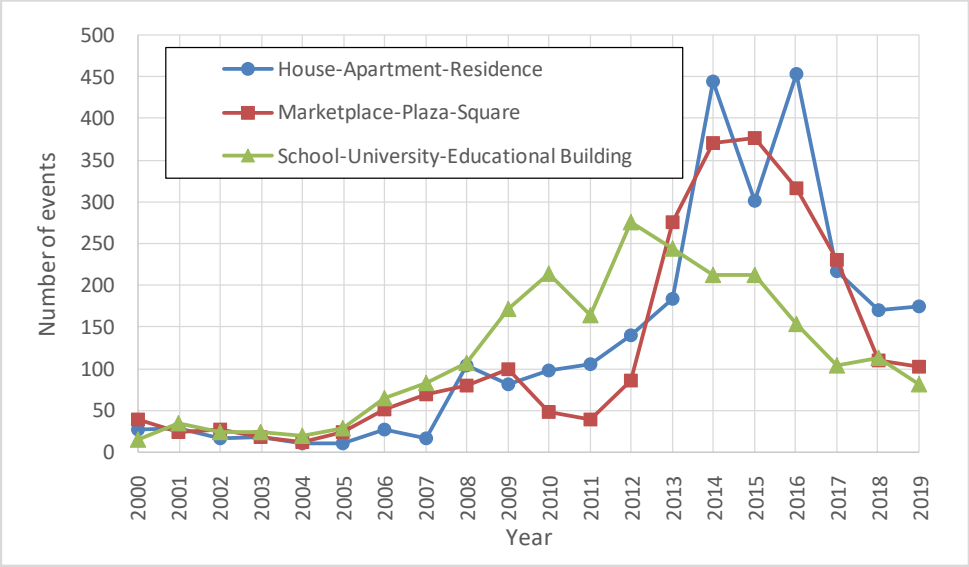

Fig.2.14 – Graphical representation of the worldwide annual number of terrorist events (attacks) for the first three *target items* of the analysed ranking, in the period 2000-2019.

This last fig.2.14 clearly shows the very significant trend increment of the number of attacks for these three specific *target items* in the last 20 years, with some noticeable peaks in the last decade 2010-2019, even 10 times over the first decade 2000-2009 ordinary values.

2.2.3 GTD analysis of building attacks and used weapons

The main goal of this work is to assess risks for buildings due to an explosive and non-conventional terrorist attack. All the previous statistical analysis are necessary to clarify and

characterize the context in the last 20 years for terrorist events. In this final part of the study, we directly face the question of building terrorist attacks and related weapons used over the last 20 years.

For this kind of analysis, it is necessary to consider the GTD *codebook* in different sections: in particular Section V "Weapon Information" and Section VI "Target/Victim Information" are fundamental, the latter of which has already been extensively analysed in the previous Sect.2.2.

As far as Section V "Weapon Information" is concerned, it allows the investigation of the **possible *explosive* and *CBR*** (in the following CBRe) **nature** of the weapon used in the events, finding in the database a detailed and complete taxonomy - listed below- for the types of weapons and **restricting the analysis to the CBRe case only**.

GTD taxonomy of weapons

Chemical - a weapon produced from toxic chemicals that is contained in a delivery system and dispersed as a liquid, vapor, or aerosol. This category includes chemical weapons delivered via explosive device.

Biological - a weapon whose components are produced from pathogenic microorganisms or toxic substances of biological origins.

Radiological - a weapon whose components are produced from radioactive materials that emit ionizing radiation and can take many forms.

Nuclear - a weapon which draws its explosive force from fission, fusion, or a combination of these methods.

Explosives - a weapon composed of energetically unstable material undergoing rapid decomposition and releasing a pressure wave that causes physical damage to the surrounding environment. Note that chemical weapons delivered via explosive are classified as "Chemical".

Firearms - a weapon which is capable of firing a projectile using an explosive charge as a propellant.

Fake Weapons - a weapon that was claimed by the perpetrator at the time of the incident to be real but was discovered after-the-fact to be non-existent or incapable of producing the desired effects.

Incendiary - a weapon that is capable of catching fire, causing fire, or burning readily and produces intensely hot fire when exploded.

Melee - a weapon—targeting people rather than property—that does not involve a projectile in which the user and target are in contact with it simultaneously.

Vehicle - an automobile that is used in an incident that does not incorporate the use of explosives such as a car bomb or truck bomb.

Sabotage Equipment - a weapon that is used in the demolition or destruction of property (e.g., removing bolts from a train tracks.

Other - a weapon that has been identified but does not fit into one of the above categories.

Unknown - The weapon type cannot be determined from the available information.

In the following, when we focus our attention on "buildings", we refer to "all kinds of constructions" independently of the building use. For this reason, the distinction between *soft* or *hard targets* is, from now on, no more of specific interest and a new approach for the identification of building-related *target items* becomes necessary.

On this regard, a punctual verification of GTD proposed *target items* was conducted and on the **113** different definitions available of *target items* (in the codebook [GTD2] the *target items* are denoted within the macro-variable "Target/Victim Subtype" in section VI) only **20** were recognized for buildings as "primary", i.e. directly referring to "building attacks", even taking into account the information field of the database (*summary*) in which a *short description of the event* is provided.

It is to stress out that other potential *target items*, different from the 20 primary *target items* selected, in some rare cases can have a connection with a building attack, but these "secondary"

additional items have been excluded for this analysis on buildings. So, the main focus of this last statistical study is on the 20 primary *target items* directly related to *building attacks*, where with the words "building attacks" we intend *a terrorist event happened inside the structure or, even if external to the structure, very near to its perimeter*.

The 20 selected primary *target items* (*hard* and *soft target*s) for building analysis are listed in tab.2.13.

Tab.2.13 – GTD selected *target items* for building analysis (*hard* and *soft targets*).

Primary target items (sorted alphabetically)	Sub-category of Target
Bank/Commerce	*Business*
Construction	*Business*
Embassy/Consulate	*Government (Diplomatic)*
Entertainment/Cultural/Stadium/Casino	*Business*
Farm/Ranch	*Business*
Government Building/Facility/Office	*Government (General)*
Hotel/Resort	*Business*
House/Apartment/Residence	*Transportation*
Industrial/Textiles/Factory	*Business*
Marketplace/Plaza/Square	*Private Citizens & Property*
Medical/Pharmaceutical (Hospital)	*Business*
Military Barracks-Base-Headquarters-Checkpost	*Military*
Military Recruiting Station/Academy	*Military*
Museum/Cultural Center/Cultural House	*Private Citizens & Property*
Place of Worship	*Religious Figures/Institutions*
Police Building (headquarters, station, school)	*Police*
Prison/Jail	*Police*
Restaurant/Bar/Café	*Business*
Retail/Grocery/Bakery	*Business*
School/University/Educational Building	*Educational Institution*

Starting from these 20 *target items*, a specific analysis on the number of *buildings attacked* using *explosive* and *CBR* (CBRe) weapons has been carried out.

The first obtained results are shown in tab.2.14, characterizing, year by year, the number of worldwide terrorist attacks for, cumulatively, *explosive* or *C* or *B* or *R* events in the period 2000-2019 for any single primary *target item* selected. The list of *target items* represented in the tab.2.14 is sorted from the higher to the lower by number of total events in the 20 years, showing in such a way a ranking of *target items*.

The list of *target items* represented in tab.2.14 is ordered from highest to lowest by total number of events over the 20 years, thus showing a ranking of the *target items*.

From tab.2.14 it is possible to observe that the first 8 items in the ranking represent more than 80% of the CBRe cumulative events (the total number, in fact, is equal to 18,585) related to *buildings* in the period of time considered and reveal a presence of both *soft* and *hard specific targets*.

In fig.2.15, to characterize the trends in the 20 years, the annual number of CBRe attacks have been depicted for the first four items of the ranking presented in tab.2.14.

Tab.2.14 – Results and ranking of *target items* for the worldwide number of building attacks with explosive or CBR (CBRe) weapons, period 2000-2019.

Building target items | Num of CBRe Attacks/year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	Total	%
Military Barracks/Base/Headquarters/Checkpost	33	11	23	25	20	19	20	35	37	9	9	21	171	241	423	319	313	242	182	139	**2292**	12.3
Marketplace/Plaza/Square	32	22	23	18	11	21	47	65	74	97	43	35	78	266	340	360	304	211	97	77	**2221**	12.0
Police Building (headquarters, station, school)	35	22	26	24	32	36	36	70	60	35	54	52	214	346	300	223	167	174	126	146	**2178**	11.7
House/Apartment/Residence	12	16	9	11	8	7	19	11	80	54	85	88	131	144	397	255	397	140	111	105	**2080**	11.2
Retail/Grocery/Bakery	15	14	17	14	7	12	21	33	72	92	80	106	103	136	189	297	273	178	80	37	**1776**	9.6
School/University/Educational Building	12	22	15	10	13	15	43	41	59	142	188	151	204	193	150	164	84	67	49	46	**1668**	9.0
Government Building/Facility/Office	46	29	24	34	31	50	62	38	92	97	97	102	119	118	146	94	106	73	46	70	**1474**	7.9
Place of Worship	61	16	20	13	25	28	42	42	53	71	58	60	99	196	137	152	85	67	51	52	**1328**	7.1
Restaurant/Bar/Café	8	13	17	10	6	15	19	26	41	47	49	24	46	144	134	156	118	49	30	23	**975**	5.2
Bank/Commerce	31	22	15	9	9	6	12	6	23	14	30	28	48	63	26	29	18	11	18	15	**433**	2.3
Medical/Pharmaceutical	1	3	2	3	4	6	11	9	14	34	27	20	24	49	61	52	30	25	18	20	**413**	2.2
Hotel/Resort	7	11	13	16	14	12	4	11	33	17	12	30	39	32	21	30	13	11	10	14	**350**	1.9
Entertainment/Cultural/Stadium/Casino	22	9	13	5	10	5	2	16	26	11	21	11	18	23	33	21	23	19	10	8	**306**	1.6
Construction	2	1	2	4	2	3	4	5	12	28	12	13	15	29	41	25	21	22	17	10	**268**	1.4
Embassy/Consulate	10	8	9	15	12	7	11	7	18	13	28	8	21	23	15	21	15	7	11	7	**266**	1.4
Industrial/Textiles/Factory	4	7	2	2	4	8	2	3	11	7	9	10	11	35	20	20	22	10	10	14	**211**	1.1
Prison/Jail	1	1	1		3		1	2	4	4	6	1	10	14	22	13	15	3	2	3	**106**	0.6
Farm/Ranch	3	2	1	1	1			1	3	5	9	5	8	4	21	8	7	5	10	9	**103**	0.6
Military Recruiting Station/Academy	1		2	1	7	11	6		4	2	2	4	4	3	15	4	14	3	2	6	**91**	0.5
Museum/Cultural Center/Cultural House	2	1	1		2				1	1		3	6	4	9	8	6		1	1	**46**	0.2
Total	**338**	**230**	**235**	**215**	**221**	**261**	**362**	**421**	**717**	**780**	**819**	**772**	**1369**	**2063**	**2500**	**2251**	**2031**	**1317**	**881**	**802**	18585	100

Fig.2.15 confirms the very significant increment in the worldwide trend of the number of building attacks for any specific *target item* considered in the figure for the period 2000-2019, with several noticeable peaks in the last decade 2010-2019, up to 10 times the ordinary characteristic values of the first decade 2000-2009 values.

In a previous analysis for the CBRe weapons [Car1], the author had already shown the general supremacy of the number of *explosive* terrorist attacks with respect to non-conventional *CBR* attacks up to 2017. To gain more insight on the building attacks distribution among CBRe weapons, a new statistical analysis has been carried out and the obtained results are reported in tab.2.15.

This table confirms, with a year-by-year analysis, the supremacy of the explosive weapons in the building attacks with respect to the CBR weapons. In fact, only C weapons result significantly used in building attacks (71 occurrences in 20 years) while B and R weapons are restricted to minimal occurrences (5 and 9 respectively in 20 years). In any case the explosive weapons result used worldwide in 99.54% of the total cases (see tab.2.16), with a number of occurrences in 20 years equal to 18,500.

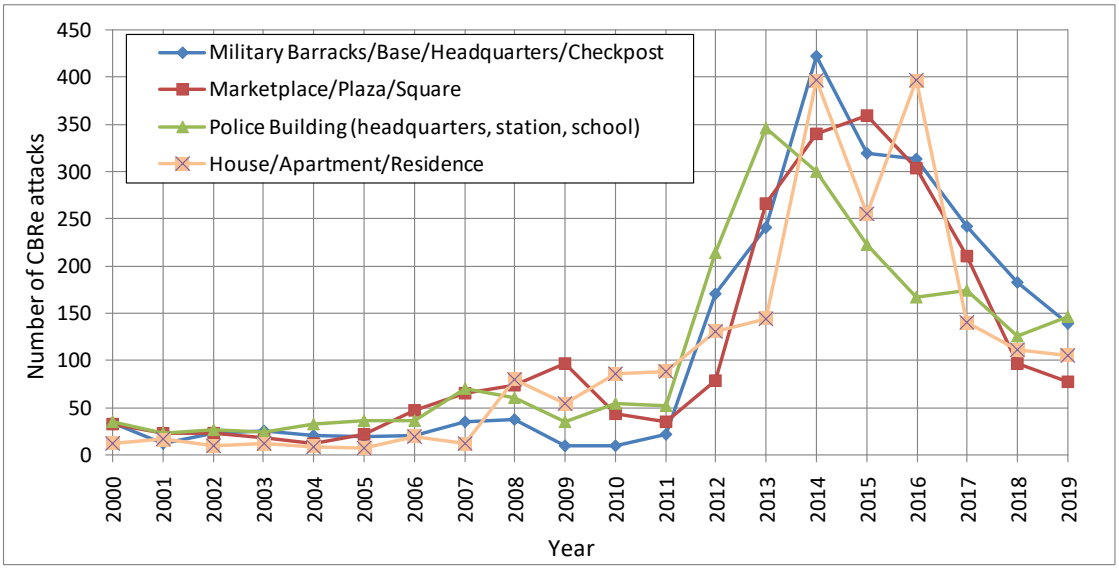

Fig.2.15 – Graphical representation of the worldwide annual number of CBRe terrorist events (attacks) for the first four *target items* of the ranking in tab.2.14, in the period 2000-2019.

Tab.2.15 – Worldwide attacks to buildings per year in the period 2000-2019 with CBRe weapons and for the 20 selected primary *target items*.

Year	*Explosive events*	*C events*	*B events*	*R events*	*Total CBRe* events*
2000	327	2	0	9	**338**
2001	221	6	3	0	**230**
2002	234	1	0	0	**235**
2003	209	5	1	0	**215**
2004	219	1	1	0	**221**
2005	261	0	0	0	**261**
2006	362	0	0	0	**362**
2007	419	2	0	0	**421**
2008	714	3	0	0	**717**
2009	777	3	0	0	**780**
2010	813	6	0	0	**819**
2011	772	0	0	0	**772**
2012	1359	10	0	0	**1369**
2013	2057	6	0	0	**2063**
2014	2496	4	0	0	**2500**
2015	2241	10	0	0	**2251**
2016	2025	6	0	0	**2031**
2017	1316	1	0	0	**1317**
2018	878	3	0	0	**881**
2019	800	2	0	0	**802**
Total	**18500**	**71**	**5**	**9**	**18585**

* CBRe = Chemical, Biological, Radiological and explosive

Tab.2.16 – Worldwide percentage use of CBRe weapons in attacking buildings during the period 2000-2019 for the 20 selected primary *target items*.

Terrorist worldwide events on buildings and type of CBRe Weapon (period 2000-2019)		
Weapon type	**Num. of Attacks**	**%**
Explosive	18500	99.54
C	71	0.38
R	9	0.05
B	5	0.03
Total	**18585**	**100**

These results show that those threats related to the use of explosive weapons are, at least taking into account the last two decades of terrorist attacks, to be considered the most probable and that a serious design of specific countermeasures for the reduction of building vulnerabilities are necessary. At the same time, CBR weapons represent a real possibility for terrorist attacks, especially for C weapons which have been applied in many events to terrorist attacks against buildings, in the last two decades.

The results reported in this part of the work are only a simple example of the important statistical data that could be extracted and processed from the GTD and confirm the interest of a research on *soft targets* and *buildings* specific protection against terrorist events.

2.3 Terrorist attacks in Europe in 2020

In this last section, a specific analysis is provided for terrorist attacks in Europe in the year 2020, taking into account data provided in recent works and reports by the European institutions.

According to the 2021 Europol report [EuU1] on the Terrorism situation in the EU and to the European Parliament document [EuP1], there were 57 terrorist attempts (fig.2.15) in the EU in 2020 (that includes successful, failed and foiled attempts), compared to 55 in 2019.

Additionally, 62 terrorist incidents were reported in 2020 by the UK. Two probable terrorist attacks with a jihadist motive took place in Switzerland.

The number of terrorist attacks in EU Member States in 2020 is comparable to 2019 (119, of which 64 in the UK) but decreased slightly compared to 2018 (129, of which 60 in the UK).

Although they represent only a sixth of all attacks in the EU, jihadi terrorists were responsible for more than half of the deaths (12) and nearly all injuries (47). The total number of fatalities and injuries in the EU doubled from 10 deaths and 27 injuries in 2019 to 21 deaths and 54 injuries in 2020.

The deaths in 2020 were the result of one right-wing terrorist attack (9) and six jihadist terrorist attacks (12). In the UK, three people lost their lives in a jihadist-inspired terrorist attack. One person died in the attacks in Switzerland. With the exception of the targeted assassination of a school teacher on 16 October 2020 in France, the victims in these terrorist attacks appear to have been selected randomly, as perceived representatives of populations that the perpetrators intended to harm on ideological grounds.

A total of 14 ethno-nationalist and separatist terrorist attacks took place in 2020 in France and Spain, while 24 attacks were carried out by left-wing or anarchist terrorist organisations or

individuals, all in Italy. In most cases, these attacks targeted private and public property such as financial institutions and government buildings.

In 2020, three EU countries - Germany, Belgium and France - experienced four terrorist attempts motivated by right-wing extremism. However, only one of them was completed.

In the following fig.2.15 and tabs.2.17-2.18, some here discussed details are reported. The visual information have been extracted by the 2021 Europol report [EuU1].

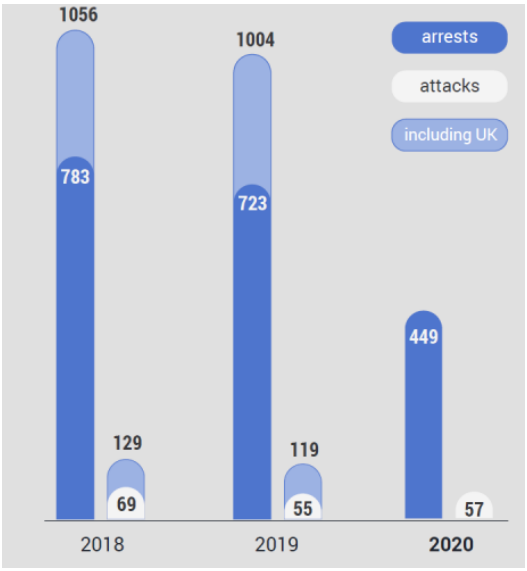

Fig.2.15 – Graphical representation of arrests on suspicion of terrorism and terrorist attacks in the EU in the period 2018-2020 [EuU1].

Tab.2.17 – Details of completed, failed and foiled terrorist attacks in 2020 per EU Member State and per motivational affiliation [EuU1].

Member State	Jihadist terrorism	Right-wing terrorism	Left-wing and anarchist terrorism	Ethno-nationalist and separatist terrorism	Total
Austria	1				1
Belgium	1	1			2
France	8	1	1	5	15
Germany	4	2			6
Italy			24		24
Spain				9	9
TOTAL	14	4	25	14	57

Tab.2.18 – Number of arrests in 2020 per EU Member State and per motivational affiliation [EuU1].

Member State	Jihadist terrorism	Right-wing terrorism	Left-wing and anarchist terrorism	Ethno-nationalist and separatist terrorism	Other types of terrorism	Not specified	TOTAL
Austria	30						30
Belgium	2	1				58	61
Bulgaria	1						1
Czechia					1		1
Cyprus	1						1
Denmark	1			3			4
France	99	5	11	12	-	-	127
Germany	27	14		3			44
Greece	3		14				17
Ireland	18			6			24
Italy	10	1	24	1		9	45
Luxembourg		1					1
Netherlands	15	6		2		1	24
Poland	8	1					9
Portugal			1				1
Romania	2						2
Spain	37	5	2	12		1	57
TOTAL	254	34	52	39	1	69	449

2.4 Conclusion on statistical analysis for terrorist events

All these numbers and figures analysed and discussed in this second section confirm the relevant presence of terrorist events in last decades in the world and, in particular, in Europe up to 2020. The results obtained for the case of building attacks justify the technical interest on the specific research issues faced in this book.

3 Institutional approach on risk assessment for terrorist attacks and natural disasters

Starting from the results discussed in [Car5], in this section an analysis of the different institutional approaches used for the risk definition and evaluation in the field of disaster management is proposed. In particular, the definitions and approaches proposed by the United States of America, by the United Nations and finally by the European Union are considered and compared. The comparison of the three different approaches proposed for the risk evaluation will provide important evidence of different practical applications that make the values of the evaluated level of risk conceptually different in the Institutions considered. These evidences will be useful to define specific models for threat, vulnerability, exposure and risk in the next sections of the book.

3.1 Risk definition introduction

Many different definitions of *risk* are available in the technical literature [Ayy1, Bir1, Bou1, Mod1, Sot1, Car1]. In any of these papers, the concept of *risk* is always associated "*to uncertainties related to future events*". To confirm this approach, in 2009, ISO [ISO1] proposed this very synthetic definition: "*Risk is the effect of uncertainty on objectives*" and in a previous book of the author [Car1] published in 2019 a full section is devoted to analyzing Risk Management fundamental aspects.

In other terms, *Risk* is a characteristic [Ayy1] of an *uncertain future* and is neither a characteristic of the *present* nor of the *past*.

In practice, "*risk* is a *hazard or an exposure to a possibility of loss or damage or ability to suffer a possible loss*" [Bou1] and the estimation of risk [Ayy1] is usually based on the "*expected result of the probability of the event occurring multiplied by the consequence of the event given that it has occurred*". In other words, "*risk will be considered as a combination of the consequences of an event and the associated likelihood/probability of its occurrence*" [Car1, ISO2, EuC1].

We can introduce now a very basic first mathematical relation [Ayy1, Mod1, EuC1] that can represent, under the hypothesis *of independence* between the event occurrence and the impact value, the *Risk R* as the product of the *Probability* (or *Likelihood*) *P* of occurrence of an event and the *Impact I* produced by the same event,

$$Risk = Probability \cdot Impact = P \cdot I \tag{3.1}$$

Focusing the attention on the dimension of these quantities we can observe [Ayy1, Mod1] that:

- ✓ *Risk* is measured as [consequence/time];
- ✓ *Probability* of occurrence is measured as [event/time];
- ✓ *Impact* is measured as [consequence/event];

where the quantities in between the squared brackets are measurement scales.

This basic approach presents *Risk R* as an expected value of loss/damage in a specified period of time due to a potential event.

More in-depth, these first quite simple considerations on the concept of *risk* show that this term implicitly refers to other different underneath quantities.

The first of these quantities we analyze in this work is the term *threat*, and the similar concept of *hazard*, both intended - at this stage of the analysis - as "*a particular event characterized by a given probability of occurrence in a specified time period*".

In the USA institutional technical literature, the concept of *threat* is often defined [FEM1, FEM5, DHS3] as "*any circumstance or event with the potential to cause loss of, or damage to an asset*". Within the military services, the intelligence community, and law enforcement, the term *threat* is typically used to describe the possible context for a *terrorist action* or *manmade disaster*.

In a more extended technical arena [Car1, EuC1, DHS3, ISO3] the term *hazard* is usually used, intending with the meaning of "*natural or man-made source or cause of harm or difficulty*".

It is important to observe that a *hazard* conceptually **differs** [EuC1, DHS3] from a *threat* in the fact that a *threat is intentionally **directed** at an entity, asset, system, network, or geographic area*, while a *hazard is **not directed***.

In some cases, for example in the USA approach, *natural disasters* and *terrorist attacks* are often analyzed with the same *risk* approach. Nevertheless, a technical specification on this regard is necessary: terrorist *threats* are conceptually very different from other types of *hazards*, in particular from a natural one, such as earthquakes, floodings, hurricanes. For these last hazards we can take advantage of many years of historical quantitative data, with the possibility to assess in many cases probabilities and frequencies of occurrence associated with the specific risk, the site, the duration and the magnitude of a potential event. Furthermore, in a *hazard*, the probability of occurrence is generally completely **independent** from both the *asset value*s (people, economic and symbolic values) and the *asset weakness*. On the contrary, the *terrorist threat* depends on human will, historical data are generally not significant for a *direct* prediction and, for their intrinsic intentional nature, the occurrence and possible recurrence of terrorist attacks are very difficult to predict.

The second aspect to observe in this introduction is that the term *impact*, similar in the definition to the terms *consequence*, *loss* and *damage*, relates to a "result" of the event, which our analysis will intend as a negative condition with respect to the starting point before the possible event.

A *consequence/impact*, in its turn, is associated to the implicit presence of *assets* or *exposures* (for example the number of people in specific areas, economical values and activities, symbolic and iconic references, or even political bodies and social values, …) that, in the perspective of "negative consequences", have to be protected.

Another quantity of interest that stems from this first general analysis, is associated to the possible *weaknesses* that characterize the considered *assets*/*exposures* and make them susceptible to the damaging effects of a *hazard* or a *threat*. We will indicate this last quantity as *vulnerability*.

To focus our analysis on the *disaster management* issue, hereafter we consider three different approaches of *national* and *international Institutions* that, with different viewpoints, have faced the Risk Assessment problem.

Firstly, the technical evolution observed in the US DHS (Department of Homeland Security) for the Risk assessment techniques for natural, manmade hazards and terrorist threats adopted starting from 2001 will be presented and analyzed. Secondly, the United Nation (UN) approach will be considered, in particular for natural and manmade hazard. Finally, the European Union (EU)

indications and approaches will be illustrated, also taking into account the research work produced by the JRC (Joint Research Center) of the European Commission. At the end of the analysis the different methods proposed will be compared showing the main differences that arise from these institutional approaches.

3.2 USA DHS approach to the risk assessment for natural disaster and terrorist attacks

With the aim to understand the updated risk assessment definition used by US DHS for natural disaster and terrorist attacks, it is interesting to start this analysis taking into account a USA Congressional Research Service report published in 2007 [CRS1]. This report presented several different risk assessment definitions and related grant program options discussed and adopted by the USA in order to develop, at that time, a comprehensive and long-term strategy for risk management.

The very important aspect to highlight [Car1] in this document is related to a tracking time line representing together **milestone** events and **risk assessment** mathematical *formulas* adopted in US between 2001-2007 after the attacks to the Twin Towers.

In other words, this document describes the US Federal Government's approach to distribute funds to State/Local Governments in order to enhance the institutional and citizen abilities to prepare for and respond to terrorist acts. As discussed in [Car1], this approach largely evolved in the period 2001-2007 during the transformation of the nation's understanding of the "homeland security" concept.

The term "homeland security" borne out of the Twin Towers 2001 attacks and the DHS, which is the US department designated to enhance it, were initially solely **terrorism**-focused. With time, and with other catastrophic incidents, the focus of the department expanded to include a range of potentially destabilizing, non-terrorist threats, such as **natural disasters**. This evolution in mission had a significant impact on the calculation of the threat aspect of the risk formula utilized to allocate some of the homeland security grant funds.

In those years, there were numerous criticisms from various groups over how risk was assessed by the *Department of Justice* (DoJ), before, and the DHS, after, and, as a result, over how federal grants were allocated.

In the US report [CRS1] at least three different *stages* in the evolution of the risk assessment methodology can be recognized.

In **Stage I** (2001-2003), risk was generally assessed and measured according to **population numbers**. In short, *risk R* was equated to *number of people in a certain site* (village, city, state, ...). It is easy to observe that this definition was very distant from the general formula proposed by the technical literature and focused the attention only on the concept of *exposure*, intended as maximum number of people (*population*) potentially impacted by the terrorist attack.

In **Stage II** (2004-2005) the importance of **critical infrastructure, population density and a number of other variables** were considered and new variables were included in the assessment of risk. However, the formula for risk remained *unbelievably additive* and fundamental concepts of the risk basic existing theory were not taken into account in the risk assessment process. Risk was assessed as the **simple sum** of Threat (*T*), Critical Infrastructure (*CI*), and Population Density (*PD*), a formula without any scientific rationale.

In **Stage III** (2006-2007) the **probability of particular events, a threat, was introduced into the formula**. This final approach to allocating the funds required an assessment of *risk R* using a formula that considers the *Threat probability T* to a target/area, multiplied by *Vulnerability V* of the target/area, multiplied by *Consequence C* of an attack on that target/area.

As a result, the basic risk assessment formula adopted by the US Institutions [DHS4] became

$$R = T \cdot V \cdot C \tag{3.2}$$

As we can see, the variables were no longer additive, but were multiplied, implying weighting of variables and some assessment of the likelihood that certain events would occur.

Although DHS continues over the years to discuss its risk definition, it substantially remains for many years, both for *terrorism* and *natural disasters*, in terms of formula (3.2) or, in more generic form, as

$$R = f(T, V, C) \tag{3.3}$$

In particular, formula (3.3) applies when, as for the case of terrorist attacks, it is recognized that a **statistical independence** of the variables is not **directly applicable**.

It is very interesting to observe that, over the period (2004-2007), the FEMA (Federal Emergency Management Agency), an organization within the DHS direct control, used a slightly different formula [FEM2] for the Risk evaluation, adopting the quantity *asset*, when applied in a Guide to Mitigate Potential Terrorist Attacks Against Buildings.

This of FEMA 'How-To Guide' was the first attempt in the institutional literature of defining risk definition [FEM2] of a terrorist attack **against buildings**. The specific definition used is reported here:

"*Risk is the potential for a loss or damage to an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it. Risk is based on the likelihood or probability of the hazard occurring and the consequences of the occurrence*".

The approach proposed by the US [FEM2] was to assemble the values of the *threat* assessment, *asset* value assessment, and *vulnerability* assessment, and determine a numeric value of *risk* in accordance with the following formula

$$Risk = Threat \cdot Vulnerability \cdot Asset$$

Only in the 2008 publication [FEM5] FEMA harmonized its approach for risk definition of a terrorist attacks against buildings with the general DHS risk assessment formula (3.2) introduced above, hence substituting the Asset *A* with the Consequence *C* for the risk assessment methodology.

Finally, it is relevant to stress that in the last version of the National Infrastructure Protection Plan (NIPP) in 2013 [DHS5] it is confirmed that the three quantities Threat, Vulnerability and Consequence must be used for the risk assessment evaluation. More precisely, in a supplement of this

2013 plan [DHS6] addressing the risk management approach to be adopted, it is specified that "*risk assessments can explicitly consider each of these factors* (T, V and C)*, but do not have to do so in a quantifiable manner*".

This means that in conducting assessments, analysts should be particularly careful, when calculating, to check that results are sound and defensible. Furthermore, the same document [DHS6] indicates, as a general rule, that "*simple but defensible methodologies are preferred over more complicated methods*". Risk assessment methodologies based on the quantities Threat, Vulnerability and Consequence, '*serve as a guide but the method adopted must ensure that risk assessments are:*

- *Documented: the methodology and the assessment must clearly document what information is used and how it is synthesized to generate a risk estimate;*
- *Reproducible: the methodology must produce comparable, repeatable results, even though assessments of different critical infrastructure may be performed by different analysts or teams of analysts;*
- *Defensible: the risk methodology must logically integrate its components, making appropriate use of the professional disciplines relevant to the analysis, as well as be free from significant errors or omissions*".

As a last remark, it is important to stress the important difference between the concepts of *Asset* (or *Exposure*, as we will see in next section) and *Consequence* that arises from the aforementioned definitions, and very clearly stated in the DHS Lexicon [DHS3] as well.

This conceptual difference is really relevant from a mathematical viewpoint in the risk evaluation process and, to date, represents a serious distinction between the risk analysis approach proposed by the US and the other international institutions considered in the following sections.

3.3 United Nations approach on disaster risk assessment

In 2016 the United Nations Office for Disaster Risk Reduction (UNDRR) commissioned the development of guidelines [UN4] on National Disaster Risk Assessment (NDRA) as part of a series of thematic guidelines [UN6] under its "Words into Action" initiative to support national implementation of the Sendai Framework.

The Sendai Framework [ONU1, UN2] for Disaster Risk Reduction is a United Nations (UN) program for the time period 2015-2030 that outlines four priorities to prevent new and reduce existing disaster risks:

1. understanding disaster risk;
2. strengthening disaster risk governance to manage it;
3. investing in disaster reduction for resilience;
4. enhancing disaster preparedness for effective response, and to "Build Back Better" in recovery, rehabilitation and reconstruction.

It aims to achieve the substantial reduction of disaster risk and losses in lives, livelihoods and health and in the economic, physical, social, cultural and environmental assets of people, businesses, communities and countries over the next years. It is important to stress the definition of **disaster**

adopted by UN as an event due to a phenomenon or human activity that cause loss of life, injury, property damage, social and economic disruption or environmental degradation. A **disaster** may be natural, anthropogenic or socio-natural in origin but, in the UN approach, this term does **not include** the occurrence of **armed conflicts and terrorist attacks**. Nevertheless, from a technical point of view, it is interesting to detail the UN approach in the risk management international scenario.

The UN Guidelines published in 2017 [UN6], within the Sendai Framework, describe the result of the collaboration between over 100 leading experts from national authorities, international organizations, non-governmental organizations, academia and private-sector entities. All these experts focused the attention on Sendai Framework first Priority for Action: *Understanding Disaster Risk*, which is the basis for all measures on disaster risk reduction.

The Guidelines present a detailed review of the methodologies, approaches and governance mechanisms practised in national disaster risk assessment at worldwide level. The design of the Guidelines permitted the sharing of the findings from studying the most effective existing assessments.

In any case, the UN approach on disaster management takes the clue on the risk concept proposed in ISO 31000 and 31010 [ISO1, ISO2] and, for the risk assessment describes *risk* in terms of likelihood and impact, based on the interaction between four different quantities: *hazard, exposure, vulnerabilities and capacities.* The visual representation of the risk concept for UN is depicted in fig.3.1.

To identify and evaluate the best measures for reducing risk, the risk assessment approach proposed by the UN also analyses the underlying *drivers* of hazard, exposure, vulnerabilities and capacities, as well as the direct and indirect impacts.

The definitions adopted in the last decade by the UN [UN1, UN4, UN5] for these fundamental components are the following:

Disaster risk: *the potential loss of life, injury, or destroyed or damaged assets which could occur to a system, society or a community in a specific period of time, determined probabilistically as a function of hazard, exposure, vulnerability and capacity*.

Disaster risk assessment: *a qualitative or quantitative approach to determine the nature and extent of disaster risk by analysing potential hazards and evaluating existing conditions of exposure and vulnerability that together could harm people, property, services, livelihoods and the environment on which they depend*.

Hazard: *a process, phenomenon or human activity that may cause loss of life, injury or other health impacts, property damage, social and economic disruption or environmental degradation*. Hazards may be natural, anthropogenic or socio-natural in origin. For the UN this term - as discussed above - does **not include** the occurrence or the risk of armed conflicts and other situations of social instability or tension which are subject to international humanitarian law and national legislation. Each hazard is characterized by its location, intensity or magnitude, frequency and probability.

Exposure: *the situation of people, infrastructure, housing, production capacities and other tangible human assets located in hazard-prone areas. Measures of exposure can include the number of people or types of assets in an area. These can be combined with the specific vulnerability and capacity of the exposed elements to any particular hazard to estimate the quantitative risks associated with that hazard in the area of interest*.

Vulnerability: *the conditions determined by physical, social, economic and environmental factors or processes which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards.*

Capacity: *the combination of all the strengths, attributes and resources available within an organization, community or society to manage and reduce disaster risks and strengthen resilience*.

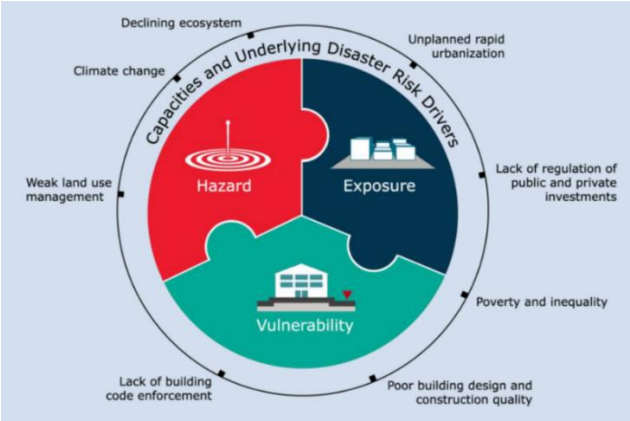

Fig.3.1 - Underlying drivers may influence more than one component of disaster risk [UN6]

Impact (or Consequence): *the total effect, including negative effects (e.g., economic losses) and positive effects (e.g., economic gains), of a hazardous event or a disaster. The term includes economic, human and environmental impacts, and may include death, injuries, disease and other negative effects on human physical, mental and social well-being*.

In general, for the UN [UN5] a single-hazard risk analysis can be carried out by considering the following components:

- **Hazard analysis** - Provides information on where, how big and how frequent the hazard events are, and on how severe their effects can be (e.g. ground shaking for earthquakes, wind speed for cyclones, etc.);
- **Vulnerability analysis** - Provides information on how an identified asset reacts to the effects of the hazard. Identification of vulnerabilities includes the criteria selected for the consequence/impact evaluation, such as people, the economy, the environment and sustainable development gains;
- **Exposure analysis** - Provides information on the presence, attributes and values of assets that may be impacted by a hazard, including criteria selected for evaluating consequences (e.g. impact on people, on the economy, ...).

For all the last three components previously introduced for the risk analysis, it is important to associate a level of uncertainty in the calculations or estimates. This can be done by tracking the uncertainty at every step where an estimate or calculation is made quantitatively or qualitatively.

Once these components have been considered, a specific risk analysis can be carried out for each hazard. It is important to stress that *probability* is an inherent attribute of risk. Probabilistic risk considers a large number of possible scenarios, their likelihood and associated impacts. In this method, a significant amount of scientific information on hazard, exposure and vulnerabilities, as well as insights from historical loss and damage data, is gathered and used to model the phenomenon underneath the disaster risk. In such an approach proposed by the UN, risk *R* is mathematically expressed as a function of Hazard probability *H*, Vulnerability *V* and Exposure *E*, as follows:

$$R = f(H, V, E) \tag{3.4}$$

We can observe that the term *capacity* discussed above, from a mathematical point of view, directly influences mainly Vulnerability, and the term *drivers*, instead, affect all the three variables defining the risk.

3.4 European approach on disaster risk assessment

In 2009 the European Commission [EuC6] adopted a communication on a "community approach" on the prevention of natural and man-made disasters setting out an overall disaster prevention framework. At the end of 2010 the same Commission published a working paper [EuC1] devoted to risk assessment and mapping guidelines for disaster management. In this last document it was recognized that sharing experience characterizing the European countries would have helped to further reduce the impacts of hazards in the most efficient and acceptable ways and would have allowed the joining of forces for the challenges ahead. The working paper stated that, according to the ISO 31010 [ISO2], risks are the *combination of the consequences of an event or hazard and the associated likelihood of its occurrence*.

Furthermore, the European Commission defined *consequences* [EuC6] as *the negative effects of a disaster expressed in terms of human impacts, economic and environmental impacts, and political/social impacts*. As far as the practical risk assessment approach is concerned, in situations where the likelihood of occurrence of a hazard of a certain intensity can be quantified, the document [EuC1] introduces the quantity "probability of occurrence" *P* and when the probability of occurrence of the hazard is independent of the extent of the "impacts" *I* (as in the case for natural hazards, such as earthquakes or storms) risk *R* can be expressed algebraically as:

$$R = P \cdot I \tag{3.5}$$

On the other side, the paper indicates that when the size of the impact *influences* the probability of occurrence (i.e. when two terms are not independent from each other, as in the case of a terrorist attack) the risk cannot be expressed simply as a *product* of two terms but must be expressed as a *functional* relationship.

Furthermore, in the analysis presented in [EuC1] it has been highlighted that:

- in many cases the impacts are dependent on preparedness or preventive behaviour;

- there are advantages in expressing the *impact I* (or similarly the consequence *C*) in a more differentiated manner, that is in terms of *vulnerability* and *exposure*. This leads, in the case of independence of the different variables, to the following basic mathematical relation

(3.6) $$I = C = V \cdot E$$

- Vulnerability *V* is defined as the *characteristics and circumstances of a community, system or asset that make it susceptible to the damaging effects of a hazard*;
- Exposure *E* is the totality of people, properties, systems, or other elements present in hazard zones that are thereby subject to potential losses.

Finally, the paper [EuC1] introduces the general formula for the risk assessment: risk *R* is a function of the probability of occurrence of a hazard *P* (sometimes expressed in the UE documents [EuC3] as *H*, with *P* = *H*), the exposure *E* (total value of all elements at risk), and the vulnerability *V* (specific impact on exposure)

$$R = f(P, V, E)$$

In a particular case in which the three *P*, *V* and *E* variables can be considered for their extent independent of each other, taking into account relations (5) and (6), the *Risk* [EuC3] can be expressed as:

(3.7) $$R = P \cdot I = P \cdot V \cdot E$$

The UE technicians highlight that the introduction of the concept of **vulnerability** makes more explicit that the impacts of a hazard are also a function of the preventive and preparatory measures that are employed to reduce the risk. In other words, as stressed for the UN approach with the quantity *capacity*, effective prevention and preparedness measures can decrease the vulnerability and therefore the risk, and, on the other hand, disaster risk *drivers* can impact the risk management measures, as visually shown in fig.3.2 discussed in [EuC3].

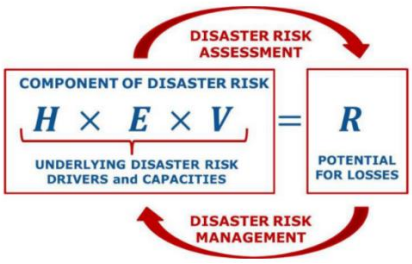

Fig.3.2 - Different perspective in the Disaster Risk Assessment and Disaster Risk Management [EuC3].

It is important to note that the UE Decision No 1313/2013 on a Union Civil Protection Mechanism (UCPM) calls the European States to develop risk assessments periodically [EuC3], by 2015 and every three years afterwards.

Finally, it can be useful to highlight another relevant technical reference for the EU in the technical report "*Science for disaster risk management: knowing better and losing less*" [EuC2], published in 2017 to start the continuous process of summarizing knowledge across the Disaster Risk Management of the European community.

This last work has been proposed for EU countries by the Disaster Risk Management Knowledge Centre (DRMKC), an initiative of the European Commission launched in 2016. The DRMKC provides a networked approach to the science-policy interface in disaster risk management fostering partnership, collective knowledge and innovative solutions.

3.5 Comparison among the different approaches

Comparing the three Institutional approaches above illustrated for describing the US DHS, the UN and the EU Disaster risk assessment methods, we can verify that:

- the UN and EU approaches are quite similar and both describe the concept of risk as a function of probability of a *hazard* occurrence, of the *vulnerability* and of the *exposure* of the *assets*;
- the US DHS approach, instead, introduces the variable *consequence* in substitution of the *asset/exposure* quantity, and, in this way, it defines the risk in a substantial different mathematical form.

Under the very specific hypothesis of *independence of all the variables* used in the *risk* definition, in the EU approach the *risk* R_{EU} is represented by the formula

$$R_{\mathrm{EU}} = P \cdot V \cdot E \tag{8}$$

while the USA approach proposes for the *risk* R_{USA} quantity the formula

$$R_{\mathrm{USA}} = T \cdot V \cdot C \tag{9}$$

where P and T are substantially the same factor, but the consequence C in the R_{USA} formula can be expressed, by formula (3.6), as the product of Vulnerability V and Exposure E, leading to a non-comparable quantity difference in the two definitions of risk.

This last consideration highlights the mathematical different approach between the USA and EU risk definitions: for this last reason the results obtained for the risk values in the two different approaches present a different formal meaning.

4 Building threat assessment and ranking

In this part of the book an original *Building Threat Assessment Method* for the case of terrorist attacks with *explosive* and *CBR agents* will be illustrated. The method was first presented at the 2nd Scientific International Conference on CBRNe - SICC Series Conference in Rome in December 2020 and successively published in the International Journal of Safety and Security Engineering [Car3] in August 2021. Furthermore, the theme of Unmanned Aircraft System (UAS), commonly referred to as "*drone"*, is briefly introduced at the end of the section. In fact, the fast proliferation of UAS has raised security concerns, since they can be used by malicious actors, including terrorists and organized crime. This kind of technology can make possible to arm the UAS with grenades, CBRN agents or Improvised Explosive Devices (IEDs).

4.1 Introduction

Several different possible approaches have been proposed in the last two decades in the technical literature [USA1, DoC1, DoD1, DoJ1, DVA1, FEM1, FEM2, FEM3, FEM5, FEM6, NDP1] to face the problem of the Threat and Risk Assessment for buildings in case of terrorist attacks.

In particular, in the USA the Federal Emergency Management Agency (FEMA) with the "How-to Guide" 452/2005 [FEM2] and the "Reference Manual" 426/BIP06/2011 [FEM3] has provided some technical models applied in the North America professional market.

Nevertheless, many aspects of these US approaches have been changed over the time, starting from the 2003 [FEM1], and even the concepts and the practical evaluations of threats, which are fundamental for the risk management process in case of a terrorist attack, maintain some critical elements.

The objective of this section of the work is to outline the features of an original *Threat Assessment Method* for sites and buildings [Car3] for the case of terrorist attacks with Explosive and CBR agents (in the following CBRe). 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, drawing inspiration from an existing USA primal approach for the selection of threats [FEM2], 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 *Criticality*[1] *Attractiveness* of the site/building. By using all these indexes it is possible to assess the magnitude of the assets present in a site/building, focusing the analysis on a given number of selected parameters as: number of people, direct and indirect economic values, symbolic relevance, type of occupants, government and administrative importance of a possible terroristic target, but even the possible criticalities of the external part, the entry area and the internal weakness of the 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 ranking* for the sites/buildings that shows the attractiveness higher potential for the terrorists. In a similar way, the *Terrorist Capability* index provides a criterion for determining the easily applicable

[1] In this work the term "*criticality*" will indicate a weakness and fragility of a structure/system/person independent by the applied threat. A "*criticality*" becomes a "*vulnerability*" if a specific threat is applied and the weakness reveals to be exploitable by the considered threat. Further considerations on this issue in Sect.5 of the work.

threats in a wide list of proposed attacks based on CBRe weapons. The capability of the terrorist to access weapons and the CBR agents are evaluated, threat by threat, and the analysis in this case focuses the attention on the capability of the considered terrorists to manage arms and not-conventional weapons and to organize an attack exploiting weakness in the service infrastructure and in the target control/security systems. Finally, the method proposes the evaluation of the *threat probability level*, adopting a scale of 7-levels based on logarithm ranges, applying a *tripling* criterion for the quantitative range associated to two different consecutive levels [Car1]. The proposed scale is suitable for being used in a comprehensive Risk Assessment Methodology for sites/buildings, which will be discussed in Sect.7 of this book.

4.2 Building Threats Assessment Method

In the US institutional literature on disaster management, the concept of *threat* is often defined [FEM1, FEM2] 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 [EuC1, Car1] 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 [FEM1, EUC1, Car1, DHS3, ISO3], in addition to the term *threat*, the term *hazard* is often used in several different situations, intending "*natural or man-made source or cause of harm or difficulty*". For example, technicians speak of "natural hazard" typically referring to a natural event such as flooding, a hurricane or a seismic disaster, while "human-caused (manmade or anthropic) hazards" are generally considered *technological hazards* and are different from natural hazards primarily in that they originate from a *direct human activity*. For example, an improperly maintained or protected storage tanks present a potential hazard. It is important to observe that a hazard **differs** [DHS3, EuC1] 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*".

Technological hazards, for example a Hazard-Material (HazMat) leak from a truck, are for this reason generally assumed to be *accidental* and their consequences are unintended. But, from other viewpoints, a *terrorist action* can plan to generate a HazMat leak with an intentional act. In this last case, we highlight the *intentional* aspect of the act denoting the action as a *terrorist threat*, and we consider that a technological hazard can be transformed in a *threat* if it is used as a weapon directed against a target, in an intentional malicious attack.

In this work we focus our attention only on *terrorist threats*, keeping it clear in mind that imagining and identifying a specific threat as *ex-ante* can be a complex task. In fact, terrorist threats are conceptually very different from other kinds of *hazards*, in particular from natural ones, such as earthquakes, floodings, hurricanes. For these last kinds of hazards, we can take advantage of many years of historical quantitative data, with the possibility to assess probabilities and frequencies of occurrence associated with the specific risk, the site, the duration and the magnitude of a potential event. Furthermore, in a hazard, the probability of occurrence is generally completely **independent** by both the asset value (people, economic and symbolic values) and the asset criticalities.

On the contrary, a *terrorist threat* is very difficult to be predicted because it depends on human will, historical data are generally not significant for a *direct* prediction, 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 very difficult topic to deal with. Any building or site in principle can be breached, destroyed or compromised in many different ways. Weapons, explosive devices, CBR agents and tools, and the applicable tactics are numerous and can change faster than a building structure or management can be modified against a specific threat.

In general terms, we can state that terrorists select those targets which 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, economic 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, as discussed in Sect.2 of this work and also illustrated in other references [FEM1, FEM2], shows that over the past decade, terrorists are more rarely attacking *hard targets*, denoting with "hard target" those buildings which are fortified or defended with care, for example, government, military or Intelligence buildings/sites. As described in Sect.2, they often prefer to attack *soft targets*, such as commercial centres, shopping malls, theatres, cinemas, where a terrorist attack can be easily conducted with success and might produce the desired relevant effect. This effect may involve massive casualties and fatalities, physical destruction of the structures, as a symbolic act of strength to induce a psychological shock in the population, demonstrating a community's vulnerability and, last but not least, instilling fear.

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 the acronym *Att* - of the site.

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

- the *value of the assets* characterizing the site, for example, the number of people in the building, the economic and symbolic value of the building. In the following this component will be referred as *Asset Attractiveness* Att_{A} sub-index;
- the potential *criticalities* 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 *Criticality Attractiveness* Att_{C} sub-index.

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

$$Att = Att_{\mathrm{A}} + Att_{\mathrm{C}} \tag{4.1}$$

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 to the institutional/government risk **Assessment Team** when, at federal, national, regional and sub-regional level, it is necessary to conduct a preventive analysis of the potential terrorist targets. Such an activity could be necessary in order to determine on **large territory** (wide area) a *ranking* of sites and buildings on which to implement a risk mitigation policy to reduce the impact of a potential attack. The 'rank' is necessary because, for several reasons and primarily for economic limitations, it is

impossible to apply risk reduction measures everywhere, and so a selection of *potential primary targets* is practically unavoidable.

At the same time, this Attractiveness index can result of interest even for the private **Assessment Teams** that operate in specific fields, for example in 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 be protected against potential terrorist threats.

Taking into account these considerations, the method here illustrated for the **threat assessment** can be considered primarily addressed to these **Teams** of experts.

In general, even the type and size of the weapons to considered in the threat assessment, other than the probability of the threat site by site, is discussed and evaluated in such **Assessment Teams**. These Teams are typically composed by very skilled engineers, architects, CBR and intelligence experts, and experts specialized in the design of structures to mitigate the effects of an attack. As already stressed, the activity of the Assessment Team in the private applications should be carried out in collaboration with the building stakeholders [FEM3].

The threat assessment and analysis for any building can range from a **rapid and generic threat scenario** to a **very detailed examination of many specific different attacks**. Taking into account these categories of approach in the level of the assessment, technical literature proposes different compositions of the **Assessment Team** [FEM3], conducting unavoidably to different durations and costs of the assessment.

Allowing for all these considerations an original *Building Threat Assessment Method* (BTAM) is here proposed to support the **Assessment Teams** to select and identify the sites characterized by a high general *Attractiveness* index, and, for each of these sites, investigate the **primary threats** applicable and a possible ranking of the threats, finally estimating the specific threat probability. In Sect.7 of this book, the analysis here proposed will be enhanced providing a **complete Building Risk Assessment Method**.

The **Building Threat Assessment Method** here discussed aims to provide a simplified approach in **six steps**, where the first five can be carried out by the Assessment Teams, on the bases of skill and experience, even without a direct intelligence information contribution. 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 fig.4.1 and are listed and analyzed in the following.

Fig.4.1 - 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 buildings, e. g. residential, administrative and commercial sites.

Step 3. *Adopt an adequate number of parameters* in order to characterize the *Attractiveness* index (depending on asset values and exploitable criticality in the buildings/sites) and the *Terrorist Capability* index (depending on the terrorist's ease of access to 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. Based on this index, create a *first ranking of sites* showing a 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. Based on 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 estimated 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 the 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 conducted based on the Team experience only.

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

It can be already noted that in Sect.8 of this book the method herein described in detail will be applied to three Case Studies: a *commercial center*, a *government building*, a *little hospital* of an important Italian town. The Case Studies in Sect.8 will be focused on three different specific *threats* selected, as possible examples, in the following.

4.2.1 Step 1 – List of the possible sites/buildings

The first step of the method for the Assessment Team is to establish the perimeter of the area to be analyzed. The considered *area* can vary in dependence of the different cases, target and interested stakeholders. It can be a *wide area* as in the cases of institutional analysis for the case of a district, a town, a region or can be reduced to a single site/building in the case of a specific analysis. The sites/buildings can be useful distinct in categories, following for example, this starting list:

- ✓ government buildings;
- ✓ administrative buildings;
- ✓ diplomatic buildings;
- ✓ police and intelligence centers;
- ✓ healthcare-hospital buildings;
- ✓ university and school buildings;
- ✓ office buildings;
- ✓ commercial centers;
- ✓ financial/bank buildings;
- ✓ symbolic and iconic sites;
- ✓ cultural sites;
- ✓ productive/utility centers and infrastructures;
- ✓ other high asset value infrastructures/sites.

As introduced above, in the following Sect.8 we will focus our attention on real examples of application - Case Studies - of the method on three different types of sites: *a commercial center, a government building, a little hospital*.

4.2.2 Step 2 – List of the possible threats

In the attempt to evaluate **terrorist threats**, it is fundamental to understand 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/classified 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 from the analysis in [FEM2, FEM3], a **basic and flexible list of threats**, including for the purposes of this work at least these different **categories of terrorist events**:

1. **Improvised Explosive Device[2] (IED) 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); explosive, weaponized drones with explosive or IED (see Sect.4.3);
2. **Armed remote attack** – such as attack weapons (rocket propelled grenades, light antitank weapons, ...); ballistic attacks (small weapons handled by one individual);
3. **CBR attack** – such as airborne contamination with Chemical, Biological, Radiological (CBR) agents (used for example to contaminate the air supply of a building), waterborne contamination with CBR agents injected into the water supply, weaponized *drones* with CBR agents (see Sect.4.3), or similar applications with indoor and outdoor CBR attacks.

In tab.4.1 we provide a possible list, stemming from [FEM3], of specific threats that can be considered a **starting point** for the threat assessment process. The list could be integrated and modified taking into account the Assessment Team opinions for the specific situation. For each threat in the table are also shortly provided the application modes, durations and effects of the possible attacks.

[2] In terms of explosives, concern about improvised explosive devices (IEDs) and vehicle-borne improvised explosive devices (VBIEDs) has increased since 9/11 [FEM3, EuC4]. An IED attack is conducted with a homemade bomb and/or destructive device to destroy, incapacitate, harass, or distract. Criminals, vandals, terrorists, suicide bombers, and insurgents use IEDs. Because they are improvised, IEDs can come in many forms, ranging from a small pipe bomb to a sophisticated device capable of causing massive damage and loss of life. IEDs and can be carried or delivered in a vehicle (VBIEDs); carried, placed, or thrown by a person; delivered in a package; or concealed on the roadside. Many commonly available materials, such as fertilizer, gunpowder, and hydrogen peroxide, can be used as explosive materials in IEDs. Explosives must contain a fuel and an oxidant, which provides the oxygen needed to sustain the reaction.

Tab.4.1 - Starting list of possible specific threats for the assessment, specifying application mode, durations and effects of the attack [FEM3].

Threat Category	Application Mode	Duration	Extent of Effects
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)	Detonation of explosive device on or near target; via person, vehicle, or projectile.	Instantaneous; additional secondary devices may be used, lengthening the duration of the threat until the attack site is determined to be clear.	Extent of damage is determined by type and quantity of explosive. Effects generally static other than cascading consequences, incremental structural failure, etc.
Armed Attack - Ballistics (small arms) - Stand-off Weapons (rocket propelled grenades, mortars)	Tactical assault or sniper attacks from a remote location.	Generally minutes to days.	Varies, based upon the perpetrator's intent and capabilities.
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	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/containers; or munitions.	Chemical agents may pose viable threats for hours to weeks, depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water, and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.
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)	Liquid or solid contaminants can be dispersed using sprayers/aerosol generators or by point or line sources such as munitions, covert deposits, and moving sprayers. May be directed at food or water supplies.	Biological agents may pose viable threats for hours to years, depending on the agent and the conditions in which it exists.	Depending on the agent used and the effectiveness with which it is deployed, contamination can be spread via wind and water. Infection can be spread via human or animal vectors.
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	Radioactive contaminants can be dispersed using sprayers/aerosol generators, or by point or line sources such as munitions, covert deposits, and moving sprayers.	Contaminants may remain hazardous for seconds to years, depending on material used.	Initial effects will be localized to site of attack; depending on meteorological conditions, subsequent behavior of radioactive contaminants may be dynamic.

As above introduced, in the Case Studies of Sect.8 we will focus our attention, for the sake of simplicity in showing the application of the method, only on three different specific *threats* extracted from tab.4.1:

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

4.2.3 Step 3 - Parameters for evaluating attractiveness and terrorist capability indexes

The terrorist attack of last decades shows [Car1, FEM1, FEM2] 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 impossible for any stakeholder, from both a technical and benefit/cost point of view, to try **to protect everything from all types of attacks**. 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.

The starting **basic parameters** proposed 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 to quickly evaluate the *Criticalities Attractiveness for a target*, denoted by Att_C, focalized on the general weakness and fragility of the structure and the security organization criticality, 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 takes into account, fundamentally, these three different aspects in determining the site/building target of an attack:

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

Taking into account these analyses, **eleven possible parameters** collected in these **three** above introduced **categories** [Car3] are described in detail.

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 is important to stress that all these parameters are *site-dependent and threat-independent*. The objective of these parameters is to characterize in an adequate 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 statistic of population of the site/building (typical worst case occupancy).

A2. **Surrounding Population Capacity** - The statistic of 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/or 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 strongly influence the choice of the target by the terrorist.

A5. **Economical value of the site** - Intrinsic economic value of the building added to the amount of business and revenue (weekly or monthly evaluated) generated by the activities managed in the site and in the collateral surrounding area (for example within 0.3 km [FEM6] around the main target).

Category B - Parameters to quickly evaluate the Criticality Attractiveness of a target

As far as the *Criticality Attractiveness* is concerned, in this method **three** general different **parameters** are introduced for a quick evaluation. It is important to stress that also these parameters are *site-dependent and threat-independent* at this stage of the analysis. These parameters characterize, independently of the threat, the general criticality 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 defense approach [FEM2]. The proposed parameters are listed in the following.

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

B2. **Entry criticality 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 criticality of the building** (internal security) **-** Take into account and evaluate the internal security 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 equipment) and specific essential functions (day care, administration, engineering, data center, security, food service, …) [FEM2].

It should be noted that in Sect.5 of this book, a much more detailed analysis of the possible criticalities of a building is carried out, with the aim of identifying specific detailed vulnerabilities and introducing risk reduction measures.

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 is important to stress that these 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 with which the source material for the attack can be acquired/make available to carry out the terrorist action. Consideration includes explosive 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 attack, taking into account, where available, how many times a similar agent/weapon was used in the past, in which situation and against what target the attack was oriented.

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 parameter must consider even the implemented past similar terroristic scenario, taking into account, where available, the organization applied.

4.2.3.1 Rating tables for the evaluation of Attractiveness and Terrorist Capability indexes

In this sub-section possible reference Rating Tables are proposed for evaluating all the **eleven parameters** introduced above.

Every parameter is evaluated with a score based on 7-levels, in a semi-quantitative approach [ISO1, ISO2, Car1], 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 Sect.7 and in [Car1]. In the following quantitative Rating Tables a logarithmic scale to base 3 is proposed in order to represent with 7 levels a significant wide quantitative range of values. This choice is also referred in the following as *power of 3 criterion* or *tripling criterion* [Car1]. The list of parameters here proposed and analyzed should be considered "*open and flexible*". This means that is possible for the Assessment Team *select a different base for the logarithm scale, integrate* and *modify* the numbers, the ranges, and the definition of the parameters, avoiding the usage of some of them if considered "not of interest" or "not applicable".

The five proposed example Rating Tables for the *Category A - Parameters for evaluating the Asset Attractiveness of a target*, are the following.

Tab.4.2 - A1: Rating Table for the evaluation of the Site Population Capacity parameter (site dependent-threat independent).

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

Tab.4.3 - A2: Rating Table for the evaluation of Surrounding Population Capacity parameter (site dependent-threat independent).

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

Tab.4.4 - A3: Rating Table for the evaluation of Building Relevance/Symbolic value parameter (site dependent-threat independent).

Rating Value	Building Relevance	Description
7	Very high	The administrative, government, cultural and/or iconic relevance of the building for the Country is *exceptionally elevated*
6	High	The administrative, government, cultural and/or iconic relevance of the building for the Country is *elevated*
5	Medium high	The administrative, government, cultural and/or iconic relevance of the building for the Region/Town is *quite elevated*
4	Medium	The administrative, government, cultural and/or iconic relevance of the building for the Region/Town is *significant*
3	Medium low	The administrative, government, cultural and/or iconic relevance of the building for the Town is *quite significant*
2	Low	The administrative, government, cultural and/or iconic relevance of the building for the Country is *poor*
1	Very low	The administrative, government, cultural and/or iconic relevance of the building for the Country is *quite poor*

Tab.4.5 - A4: Rating Table for the evaluation of the Political/administrative/socio-cultural importance of the occupants of the building (site dependent-threat independent).

Rating Value	Importance of the occupants	Description
7	Very high	The importance of building's occupants and visitors is *exceptionally elevated*
6	High	The importance of building's occupants and visitors is *elevated*
5	Medium high	The importance of building's occupants and visitors is *quite elevated*
4	Medium	The importance of building's occupants and visitors is *significant*
3	Medium low	The importance of building's occupants and visitors is *quite significant*
2	Low	The importance of building's occupants and visitors is *modest*
1	Very low	The importance of building 's occupants and visitors is *quite modest*

Tab.4.6 - A5: Rating Table for the evaluation of the Economical value of the building (site dependent-threat independent).

Rating Value	Range (Euro)	Note
7	>97.2 M	Very high
6	32.4 M to 97.2 M	High
5	10.8 M to 32.4 M	Medium high
4	3.6 M to 10.8 M	Medium
3	1.2 M to 3.6M	Medium low
2	400k to 1.2 M	Low
1	1 to 400k	Very low

The proposed three rating Tables for the *Category B - Parameters to quickly evaluate the Criticality Attractiveness of a target*, are the following.

Tab.4.7 - B1: Rating Table for the quick evaluation of the external criticality of the building.

Rating Value	Criticality	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

Tab.4.8 - B2: Rating Table for the quick evaluation of the entry criticality of the building.

Rating Value	Criticality	Example for application
7	Very high	Open Access to all without identification procedure, no control at the entry for receiving/shipping, no control of entry of utilities, air, HVAC and consumable
6	High	Open access to all, Unprotected Air/Consumable Entry
5	Medium high	Controlled Access of Visitors, Unprotected Air/Consumable Entry
4	Medium	Controlled Access of Visitors and Non-staff Personnel, Unprotected Air/Consumable Entry
3	Medium low	Protected Air/Consumable Entry, Controlled Access of Visitors and Non-Staff Personnel
2	Low	Controlled Access of Visitors and Non-Staff Personnel, simple badge for Personnel access, Controlled shipping area
1	Very low	Controlled Access and identification of Visitors and Non-Staff Personnel, Verification of the necessity to enter with internal offices, Badge and biometric identification for personnel access, very stringent controlled shipping and delivery area

Tab.4.9 - B3: Rating Table for the quick evaluation of the internal criticality of the building.

Rating Value	Criticality	Example for application
7	Very high	No internal security monitoring center operation, absence of specific policies for the protection of critical and essential service (energy, ICT, HVAC services), no business/operation continuity plan applicable
6	High	No internal security monitoring center operation, bland policies for the protection of critical and essential service (energy, ICT, HVAC services), no business/operation continuity plan applicable
5	Medium high	Bland internal security monitoring center operation, bland policies for the protection of critical and essential service (energy, ICT, HVAC services), not-update business/operation continuity plan
4	Medium	Internal security monitoring center operation, minimal policies for the protection of critical and essential service (energy, ICT, HVAC services), generic business/operation continuity plan
3	Medium low	Diurnal operation of the internal security monitoring center, specific policies for the protection of main critical services (energy, ICT), essential business/operation continuity plan applied
2	Low	Full day operation of the internal security monitoring center, specific policies for the protection of critical services (energy, ICT, HVAC services, …), adequate business/operation continuity plan applied
1	Very low	Full day operation of the internal security monitoring center, specific and update policies for the protection of critical and essential services (energy, ICT, HVAC services, day care, administration, engineering, data center …), update and adequate business/operation continuity plan applied

The three proposed Rating Tables for *Category C - Parameters for evaluating the Terrorist Capabilities*, are the following.

Tab.4.10 - C1: Rating Table for the evaluation of Access to Explosive/CBR Agents parameter.

Rating Value	Access capability	Description
7	Very high	Terrorists have a great deal of ease in acquiring or making high-quality weapons necessary for the attack
6	High	Terrorists find it easy to purchase or manufacture the high-quality weapons needed for the attack
5	Medium high	Terrorists have a fair degree of ease in acquiring or making good quality weapons needed for the attack
4	Medium	Terrorists are in a position to purchase or manufacture weapons of sufficient quality necessary for the attack
3	Medium low	Terrorists are in some situations in a position to purchase or realize of just enough quality weapons needed for the attack
2	Low	Terrorists are only rarely able to purchase or make of adequate quality weapons to use in the attack
1	Very low	Terrorists are unable to purchase or make weapons of adequate quality to use in the attack

Tab.4.11 - C2: Rating Table for the evaluation of the Expertise on weapons of the terrorists.

Rating Value	Expertise on weapons	Description
7	Very high	The level of skill and training of the terrorists for handling and crafting a weapon or arming a CBR agent is excellent
6	High	The level of skill and training of the terrorists for handling and crafting a weapon or arming a CBR agent is good
5	Medium high	The level of skill and training of the terrorists for handling and crafting a weapon or arming a CBR agent is quite adequate
4	Medium	The level of skill and training of the terrorists for handling and crafting a weapon or arming a CBR agent is sufficient
3	Medium low	Only in some cases the level of skill and training of the terrorists for handling and crafting a weapon or arming a CBR agent is sufficient
2	Low	The level of skill and training of the terrorists for handling and crafting a weapon or arming a CBR agent is poor
1	Very low	The general level of skill and training of the terrorists for handling and crafting a weapon or arming a CBR agent is very poor

4.2.4 Step 4 – Evaluation and ranking 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 Rating Tables proposed in the previous section for the two components, *Asset* and *Criticality Attractiveness*.

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

- Asset Attractiveness Att_{A};
- Criticality Attractiveness Att_{C}.

As first possible fast approach for the evaluation of these last two sub-indexes, it is proposed to simply **add** the single scores obtained for the parameters of the same category of Step 3. In such way, the two sub-indexes are defined as follows:

$$Att_{\mathrm{A}} = \sum_{i=1}^{5} a_i \tag{4.2}$$

$$Att_{\mathrm{V}} = \sum_{i=1}^{3} b_i \tag{4.3}$$

Tab.4.12 - C3: Rating Table for the evaluation of the Organizational skill and Infrastructure knowledge of the terrorists.

Rating Value	Skill and infrastructure knowledge	Description
7	Very high	The level of organizational skill and technical infrastructure knowledge - in terms of service infrastructures and functions - of the terrorists is excellent
6	High	The level of organizational skill and technical infrastructure knowledge - in terms of service infrastructures and functions - of the terrorists is good
5	Medium high	The level of organizational skill and technical infrastructure knowledge - in terms of service infrastructures and functions - of the terrorists is quite adequate
4	Medium	The level of organizational skill and technical infrastructure knowledge - in terms of service infrastructures and functions - of the terrorists is sufficient
3	Medium low	Only in some cases the level of organizational skill and technical infrastructure knowledge - in terms of service infrastructures and functions - of the terrorists is sufficient
2	Low	The level of organizational skill and technical infrastructure knowledge - in terms of service infrastructures and functions - of the terrorists is scarce
1	Very low	The level of organizational skill and technical infrastructure knowledge - in terms of service infrastructures and functions - of the terrorists is very scarce

where the variables *a* and *b* represent the different parameter scores, obtained applying the Rating Tables in the two different categories (from tab.4.2 to tab.4.6 for Category A and from tab.4.7 to tab.4.9 for Category B).

Recalling relation (4.1) the general attractiveness *Att* value can be evaluated adding the two sub-indexes of the attractiveness for asset and for criticality, calculated by relations (4.2) and (4.3).

It is important to stress that other possible, more sophisticated, mathematical approaches can be proposed for evaluating the sub-indexes here described, for example applying statistical indicators as the arithmetical average, the standard deviation of the values for the dispersion and so on. The analysis of these, and other mathematical and statistical approaches in this part of the method is out of the scope of this analysis.

To understand the application of the method here described and generate a ranking of sites for the attractiveness, in Sect.8 will be shown a specific application to three Case Studies of the procedure described in Step 4. The analysis in Sect.8, as already mentioned, will be focused on the evaluation of three different target-sites, a *commercial center*, a *government building* and *an hospital* for three specific, above indicated, *threats*.

4.2.5 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 Rating Table previously proposed for the evaluation of the terrorist capability parameters, to obtain the final values of the Terrorist Capability index.

As for Step 4, in this work it is proposed, 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 way the Terrorist Capability Ter_C index is defined as follow:

$$Ter_C = \sum_{i=1}^{3} c_i \tag{4.4}$$

where the variable *c* represents the different parameter scores obtained applying the Rating Tables to this category (from tab.4.10 to tab.4.12 for Category C).

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.

In Sect.8.1 the Case Studies considered for the building threat assessment will be applied for the evaluation of three different specific *threats* extracted from tab.4.1: *explosion of a van-bomb*; *explosion of a suicide belt-bomb*; *explosion of a Cesium-137 Dirty Bomb*.

4.2.6 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 ranking generated 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 of **intelligence and law-enforcing institutional experts** and of **intelligence information available**. This means that all the threats considered in the analysis, and in particular the **selected primary threats** in the ranking 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' analysis, the Assessment Team can decide the final **Threat Probability Level**, using a **threat probability scale of 7 levels** proposed in tab.4.13, herein reported.

Tab.4.13 provides, for each level of the scale, 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 [FEM2, FEM3], with some important differences:

Tab.4.13 - Threat Probability Scale.

Threat rating	**Qualitative**	**Quantitative** (probability over a given interval of time)	**Level description**
7	Very High	From 3^{-1} to 3^{0} (from 1/3 to 1)	The probability level of a threat, weapon, and tactic being used against the *site or building* is *imminent*. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is *credible*.
6	High	from 3^{-2} to 3^{-1} (from 1/9 to 1/3)	The probability level of a threat, weapon, and tactic being used against the *site or building* is *expected*. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is *credible*.
5	Medium High	from 3^{-3} to 3^{-2} (from 1/27 to 1/9)	The probability level of a threat, weapon, and tactic being used against the *site or building* is *probable*. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is *credible*.
4	Medium	from 3^{-4} to 3^{-3} (from 1/81 to 1/27)	The probability level of a threat, weapon, and tactic being used against the *site or building* is *possible*. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is *not verified*.
3	Medium Low	from 3^{-5} to 3^{-4} (from 1/243 to 1/81)	The probability level of a threat, weapon, and tactic being used in the *region* is *probable*. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is *not likely*.
2	Low	from 3^{-6} to 3^{-5} (from 1/729 to 1/243)	The probability level of a threat, weapon, and tactic being used in the *region* is *possible*. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is *not likely*.
1	Very Low	< 3^{-6} (< 1/729)	The probability level of a threat, weapon, and tactic being used in the *region* or against the *site or building* is *very negligible*. Internal decision-makers and/ or external law enforcement. Law enforcement and intelligence agencies determine the threat is *non-existent or extremely unlikely*.

- following the six steps method here discussed, the Assessment Team has, at this point, a *clear picture of the scenario* regarding the sites and the threats. Only under this condition it is possible to provide a reliable evaluation of the specific threat probability in a specific site;

- a *quantitative* reference value for any level of the scale is proposed. This information is very important to try to assess the range of probability that characterizes the level to be selected, corresponding to a measurable information not only described in a qualitatively way. The most suitable interval of time for quantitative probability evaluation is discussed in Sect.7;
- the proposed scale adopts a *logarithm approach* for the range definition of the levels. This kind of approach, as discussed in [Car1, Car3], presents many advantages and will be illustrated in detail in Sect.7 devoted to the description of the complete Risk Assessment Method proposed for sites and buildings in a terrorist scenario;
- the Assessment Team can flexibly associate at the beginning of the Step 6 analysis, the probability interval value of a level to a specified *period of time* (for example, over 1 month or 3 months or 6 months or 1 year). This choice strongly depends on the precision and reliability of intelligence information available, at the time of the Team decision, for possible terrorist attacks.

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 ranking (Step 4) and applying to this target all the selected primary threats beginning from the threat in first position in the ranking (Step 5), up to the last selected threat in the rank.

It is important to stress that in absence of institutional intelligence experts and of direct intelligence information for this Step 6 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 presented in tab.4.13. In this last case the evaluation will be conducted based on the *Team experience only*.

4.3 Unmanned Aircraft System as a new vector for CBRe threats

An Unmanned Aircraft System (UAS), commonly referred to as "*drone*", consists of [EuC4]:

- an *Unmanned Aerial Vehicle* (UAV);
- the *remotely located operator*;
- a *ground control system*, the component through which the communication between UAV and operator is achieved.

Initially, since the first human flights, they were constructed and operated within a military context, but their technological advancement, cost reduction and diverse capabilities have led to their extensive use in the civilian domain, as they can satisfy the needs of the industry, business and consumer sectors.

The UAS have been employed for conducting various activities, such as inspections, surveillance, agriculture-related activities, courier services, topographical mapping, marketing, catering and emergency response. In recent years, the public has been extensively using UAS for recreational purposes as a result of the increased accessibility to a great number of affordable solutions. Beyond visual line of sight flights that allow a drone to fly beyond visual range and the expansion of 5G networks - that support faster data speeds and lower latency - are expected to further boost the use of drones, while increasing worries regarding security [EuC4].

In fact, this fast proliferation of “drones” affordable solutions has raised security concerns, since they can be used by malicious actors, including terrorists, for criminal acts. Their accessibility, difficult detection, simple and remote piloting, make them a valuable and powerful tool, a new possible very “flexible weapons” vector in the hands of aggressors who can use them to conduct attacks by weaponizing UAS with grenades, CBRN agents or Improvised Explosive Devices.

Recent examples from around the world [Kob1, Kob2] demonstrated that UAS are becoming a significant security issue for both public spaces and critical infrastructures, as even off-the-shelf units can be easily transformed into effective weapons and used intentionally for malicious purposes.

As a result of this possible malicious applications, there are a number of available countermeasure systems that incorporate technologies that are able [EuC4] to detect, identify, track and/or intercept a single UAS or a potential “swarm” attack which exploits multiple drones to accomplish a common objective. A new possible resource for the terrorists that has to be taken into account by the Assessment Team when carrying out the threat analysis and establishing the list of threats with the possible applicable vectors.

5 Building vulnerability assessment: criticality analysis and vulnerability evaluation

Assessing the *vulnerabilities* of the building/site for a specific *threat* is one of the key issues in the *risk* assessment process, as introduced in Sect.3 and discussed in detail in Sect.7.

In the literature we can find, especially at institutional level, many attempts to characterize different aspects of the building: relevant references can be found in the USA technical literature [FEM2-FEM6, DHS1] and, recently, in the European Commission research published by JRC [EuC4, EuC5].

In the following, after a short introduction, an original Building Vulnerability Assessment Method is proposed.

5.1 Introduction

As a general statement, *vulnerabilities* are the characteristics of an asset, system, location, process, or operation that render it susceptible to destruction, incapacitation, or exploitation by mechanical failures, natural hazards, terrorist attacks, or other malicious acts.

A vulnerability is defined as any weakness that can be exploited by an aggressor to make an asset susceptible to damage. The purpose of the vulnerability assessment process is to identify all the physical and organizational vulnerabilities of an asset that increase the exposure of that asset to risks from a specific threat. Vulnerability assessments are designed to provide an in-depth analysis of the characteristics of the facility or associated elements to identify weaknesses and lack of redundancy, as well as to determine protective or corrective actions that can be designed or implemented to reduce the vulnerabilities.

An evaluation of site and building vulnerabilities involves meeting with building owners and operation personnel; reviewing background information, such as construction documents and prior threats to the facility; conducting site and building inspections; and reviewing emergency and operational procedures.

5.2 Building Vulnerability Assessment Method

A *Building Vulnerability Assessment Method* (BVAM) is here proposed taking the clue on the checklist developed by the USA Department of Veterans Affairs [FEM3] and on the risk analysis model presented in [Car1].

The method is structured in three different Steps, as is represented in fig.5.1.

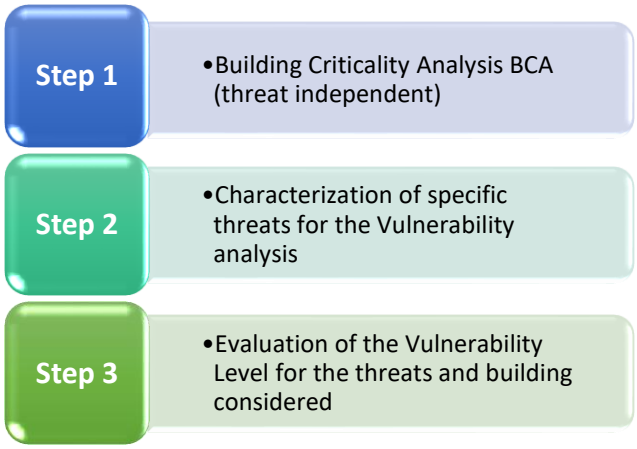

Fig.5.1 – Building Vulnerability Assessment Method in 3 Steps.

Step 1 of the method proposes to verify with the *Building Criticality Analysis* (BCA) the criticality of several tens of items extracted by the best practices on the analysis of building structure and functions (aspects to consider during the design of a new building or renovation of an existing building).

Step 2 of the method aims to characterize a given number of specific threats to apply to the building.

Step 3 focuses on a final assessment of the *level of vulnerability* associated with the different specific considered threats, for the specific building and the specific asset to be protected, using a proposed Vulnerability Scale at 7-levels.

The result of the evaluation for the *level of vulnerability* will be used for final Risk Assessment phase (Sect.7).

5.2.1 Step 1: Building Criticality Analysis

The Building Criticality Analysis (BCA) approach proposed for Step 1 can be imaged as a powerful and general screening tool for a preliminary assessment of weaknesses for different aspects of the building structural, site and functions. In addition, this analysis makes it possible to examine design issues that could potentially reveal exploitable vulnerabilities.

The proposed BCA includes many *items* to analyse and to evaluate. The results of the evaluation substantially determines if critical components/systems continue to properly work in order to enhance deterrence, detection, denial, and damage limitation, and to ensure the emergency system correct operation during a real crisis situation.

The Building Criticality Analysis here proposed is structured into *nine* different sections, indicated as '*topics'*, listed in the following tab.5.1.

Tab.5.1 – Criticality topics and number of items per topic (Step 1).

Topic Num.	Criticality Topics	Number of Items
1	Site characteristics	12
2	Architecture	10
3	Structural systems	7
4	Building envelope	5
5	Utility systems	8
6	Mechanical systems and HVAC	10
7	Infrastructure and systems of internal essential services (plumbing, gas systems, electrical power, fire alarms, telephone and ICT services)	11
8	Security systems	8
9	Emergency, security and operation continuity plans	5
Total	*9 Topics*	*76 Items*

To conduct a complete Building Vulnerability Assessment, each *topic* of the Criticality Analysis should be assigned to the identified Assessment Team. Such a Team should be composed by engineers, architects, or subject matter experts who are knowledgeable and qualified to perform a precise analysis of the assigned area. Each Assessor should consider the *questions* and *guidance* provided in this section and in Appendix A to identify possible *criticalities* and, at the end of the Steps, the most adequate *level of vulnerability* for *any specific* considered threat.

In the tab.5.1 we can find the list of the different *topics* (from the *site* characterization to the *emergency, security and operation continuity plans* evaluation) that have to be carefully analysed in order to highlight possible criticalities and, related, potential vulnerabilities.

A *criticality* corresponds to a *general weakness* which could be potentially exploit for a building attack.

A *criticality* becomes, in the here proposed approach, a *vulnerability* when a detailed and specific *threat* is considered and applied to a specific building and asset.

It is important to observe that not all the criticalities generate a correspondent vulnerability, this correlation depends on the specific threat, asset and building considered, as will be discussed in the following.

The nine different *topics* proposed in the approach reflect different aspects and functions typical of a building: the objective of this analysis is to characterize all the fundamental existing building characteristics for determining an accurate criticality analysis result.

For any different *topic,* a list of *items* – each associated with one or more *questions* - is proposed and, for each *item*, a *criticality assessment* of the specific considered aspect is fixed by the Assessors using a proposed Criticality Scale.

With this BCA, at least *76 different items* proposed here, described in detail in Appendix A, can be carefully considered and evaluated in *Step 1* of the method for the building under evaluation, independent of a specific threat.

The **criticality evaluation** of single item is carried out adopting a *4-levels scale* based on a quantitative weight score. Also, for this scale the *tripling criteria* is applied, as illustrated in tab.5.2.

The rationales for adopting a quantitative scale based on the *tripling criteria* is widely discussed in Sect.7 of this book and in [Car1].

Each criticality scale proposed for the items defines four *criticality levels* in a specific manner, depending on the item considered. The 76 different criticality scales are detailed in Appendix A.

Tab.5.2 – Criticality Scale for item analysis on 4 levels
(criticality weights based on the *tripling criteria*).

Criticality Scale (for items)	**Criticality Weight**
Extreme	27
Elevated	9
Marginal	3
Negligible	1
Not Applicable	-

Using this scale, the Assessment Team will provide for each item a relevant weight to highlight the criticality conditions for the final vulnerability assessment.

For each *topic*, at the end of the weighted analysis applied to any different *item*, a cumulative *topic criticality* evaluation is provided, applying to all the obtained weights (population data set) the *average* (arithmetical mean)[3], denoted by *m*, and the *standard*[4] *deviation*, denoted by *s*, indexes [Rou1]. Starting to these indexes a third index can be introduced, the *modified average*, denoted by m_{mod} , defined as

$$m_{mod} = m + s$$

Such three quantities - *m*, *s* and m_{mod} - can summarize the criticality of the considered topic, providing a *fast* indication of the *average*, the *dispersion* and a *reference maximum value* of the evaluated criticality weights in a topic, as will be shown in practice in Sect.8.

As introduced above in tab.5.1, the nine proposed topics are described through several items specifically detailed in Appendix A. In the following the nine Topic Tables used in the BCA here proposed are reported. Every line of the tables represents a specific item and the *questions* that the Assessment Team have to face for evaluating the criticality, taking into account the criticality scale proposed for that item in Appendix A.

[3] The **average** value, as known, is a single number taken as representative of a list of numbers and is defined for our purpose as the sum of the numbers divided by how many numbers are in the list (arithmetic mean).

[4] For a finite set of numbers, the population **standard deviation** is found by taking the square root of the average of the squared deviations of the values subtracted from their average value. The population standard deviation is a measure of the amount of variation or dispersion of a set of values. Low standard deviation indicates that the values tend to be close to the mean of the set of values, while a high standard deviation indicates that the values are spread out over a wider range.

As discussed above, every table presents, in any line, a space for a single evaluation expressed by a criticality weight. Furthermore, for each one of the tables is proposed to add, in the last two lines, the evaluation of the *average* and *standard deviation* of the criticality weight assigned by the Assessment Team, this for providing a fast indication of the general criticality of the topic. In many situations, the mitigation of the risk will correspond (see Sect.7) to mitigate the vulnerability associated with the criticality identify in this analysis. The practical application of this analysis will be illustrated in a case study proposed in Sect.8 where also the above introduced *modified average* will be evaluated, providing a further Criticality Scale based on *modified average* index (tab.8.17).

Tab.5.3 – Topic 1, table of items.

Topic 1 - Site characteristics			
Item num.	***Item***	***Questions***	***Criticality weight***
1.1	*Surrounding structures/facilities*	Are there any major/critical infrastructures surrounding the building?	
1.2	*Terrain characteristics*	Does the terrain place the building in a depression or low area?	
1.3	*Curb Lane Parking characteristics*	Is curb lane parking place for uncontrolled parked vehicles unacceptably close to the building?	
1.4	*Perimeter barriers for pedestrian access*	Is a perimeter fence or other types of barrier controls in place for the pedestrian access?	
1.5	*Vehicles access points*	Are the vehicles access points to the site or building well designed?	
1.6	*Pedestrian Access Control*	Is there pedestrian access control at the perimeter of the site or of the building?	
1.7	*Private Vehicle Access Control*	Is there private vehicle access control at the perimeter of the site or of the building?	
1.8	*Shipping/Delivery Vehicle Access Control*	Is there access control of shipping and delivery vehicles at the building entrance?	
1.9	*Alternative Potential Access*	Is there any exploitable potential access to the building through utility paths or water runoff?	
1.10	*Anti-ram devices*	What are the existing types of vehicle anti-ram devices for the building?	
1.11	*Site lighting in the external area*	Is the site lighting adequate from a security perspective in roadway access and parking areas?	
1.12	*External connection to the building*	Is any of the nearby in-ground and out-ground infrastructures directly connected to the building?	
		Topic 1	
		Average of Criticality weights	
		Standard Deviation of Criticality weights	

Tab.5.4 – Topic 2, table of items.

Topic 2 - Architecture			
Item num.	***Item***	***Questions***	***Criticality weight***
2.1	*Mixed tenant building*	Is it a mixed-tenant building?	
2.2	*Receptacles to hide explosive devices*	Are there trash receptacles and mailboxes in close proximity to the building that can be used to hide explosive devices?	
2.3	*Public and critical points in the building*	Are public toilets, service spaces, or access to stairs or elevators located in any non-secure areas, including the queuing area before screening at the public entrance?	
2.4	*Equipment for access control and screening*	Do public and employee entrances include equipment for access control-screening and, in perspective, adequate space for possible future installation?	
2.5	*Reinforced walls and doors*	Are doors and walls along the line of security screening adequately reinforced?	
2.6	*Roof access control*	Is roof access controlled and limited to authorized personnel by means of adequate mechanisms?	
2.7	*Building critical assets*	Are critical assets (people, activities, building systems and components) well separated from main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking? Are the critical building systems and components adequately hardened and controlled?	
2.8	*Separation of critical assets and loading docs/shipping areas*	Are loading docks, receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.?	
2.9	*Mailroom space and equipment*	Have the mailroom adequate equipment and space available to examine incoming packages and for an explosive disposal container?	
2.10	*Debris generation limitation*	Are ceiling, internal walls, overhead utilities and lighting systems designed to remain in place without generate danger debris during hazard events?	
		Topic 2	
		Average of Criticality weights	
		Standard Deviation of Criticality weights	

Tab.5.5 – Topic 3, table of items.

Topic 3 - Structural Systems			
Item num.	***Item***	***Questions***	***Criticality weight***
3.1	*Construction characteristics*	What type of construction? What type of concrete and reinforcing steel? What type of steel? What type of foundation?	
3.2	*Structural and Non-Structural Components*	Are any of structural/non-structural components vulnerable either directly or indirectly to explosive blast?	
3.3	*Progressive collapse*	Is the building capable of sustaining the removal of a column for one floor above grade at the building perimeter without progressive collapse?	
3.4	*Floor of loading dock*	Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?	
3.5	*Mailroom explosion mitigation*	Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?	
3.6	*In-ground structural systems*	Would failure of part of the in-ground infrastructure affect the structural system of the building?	
3.7	*Underground water presence*	Does the presence of underground water under the building generate instability and unacceptable flooding?	
		Topic 3	
		Average of Criticality weights	
		Standard Deviation of Criticality weights	

Tab.5.6 – Topic 4, table of items.

Topic 4 - Building Envelope			
Item num.	***Item***	***Questions***	***Criticality weight***
4.1	*Envelope protection level*	What is the designed or estimated protection level of the building envelope against a possible high magnitude explosive threat?	
4.2	*Envelope fenestration balance*	Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.)	
4.3	*Glazing characteristics*	Are the glazing of the building secure in case of blast?	
4.4	*High external pressure resistence*	Is the building designed to correctly resist to high external pressure (as for the case of blast)?	
4.5	*Envelope and window glazing external condition*	What are the current condition of windows and of the rest of the envelope (cladding, curtain walls, veneer, ...)?	
		Topic 4	
		Average of Criticality weights	
		Standard Deviation of Criticality weights	

Tab.5.7 – Topic 5, table of items.

Topic 5 - Utility systems and internal distribution infrastructures			
Item num.	***Item***	***Questions***	***Criticality weight***
5.1	*Domestic water service*	What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank)? Is the domestic water service reliable and certified for the water quality? Is there a secure and sufficient alternate drinking water supply?	
5.2	*Security of water entry points*	Are the entry points for the water supply in a secure location and managed in a secure manner?	
5.3	*Water for the fire suppression system*	Is the source and the distribution system of water for the fire suppression service adequate to manage incendiary events?	
5.4	*Sewer System*	Are sewer systems well designed, implemented and protected?	
5.5	*Fuel storage for continuity operations*	Is an adequate quantity of fuel stored at the building? How is it stored? How is it secured?	
5.6	*Electrical service redundancy*	Is there a redundant and reliable electrical service source?	
5.7	*Security of electrical entry points*	Is the incoming electric service to the building well designed and secure?	
5.8	*ICT services*	By what means does the main telephone and data communications interface the building? Are there multiple or redundant locations for the telephone and digital communication services? Are these locations secure and not accessible by unauthorized people? Is the provided data service secure?	
		Topic 5	
		Average of Criticality weights	
		Standard Deviation of Criticality weights	

Tab.5.8 – Topic 6, table of items.

Topic 6 - Mechanical systems – HVAC			
Item num.	***Item***	***Questions***	***Criticality weight***
6.1	*Air intakes and exhaust louvers*	Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure) Are the intakes and exhausts accessible to the public?	
6.2	*Roof access*	Is roof access limited to authorized personnel by means of adequate mechanisms?	
6.3	*Air filtration*	What are the types of air filtration adopted for the building? Is there any collective or specific protection for chemical, biological, and radiological contamination designed into the building?	
6.4	*Air CBR sensors*	Are there provisions for air monitors or sensors for CBR agents?	
6.5	*Air intakes and exhaust closure*	Does it exist a method for fast air intakes and exhausts closure when necessary?	
6.6	*Air-handling systems zoning*	Are there large central air handling units or are there multiple units serving separate zones? Can critical areas be served from other units if a major system is disabled?	
6.7	*Air intakes and exhaust system security*	Are supply, return, and exhaust air systems for critical areas secure?	
6.8	*Air pressurization*	Is air pressurization well designed and monitored regularly?	
6.9	*Smoke evacuation systems*	Are there any smoke evacuation systems installed?	
6.10	*HVAC maintenance*	Does the HVAC maintenance staff have the proper training, procedures, and preventive maintenance schedule to ensure system functionality?	
		Topic 6	
		Average of Criticality weights	
		Standard Deviation of Criticality weights	

Tab.5.9 – Topic 7, table of items.

Topic 7 - Infrastructure and systems of internal essential services			
Item num.	***Item***	***Questions***	***Criticality weight***
7.1	*Domestic water distribution*	For the water distribution, are looping of piping architecture and section valves for redundancy tasks adopted?	
7.2	*Hot water management*	Is the method of heating domestic water resilient to fault at the heat source?	
7.3	*Gas distribution*	For the gas distribution, are looping of piping architecture and section valves for redundancy tasks adopted?	
7.4	*Gas storages*	Where are gas storage tanks located? (heating, cooking, medical, process) How are they piped to the distribution system? (above or below ground)	
7.5	*Electrical rooms and panels*	How are the electrical rooms located relative to other higher risk areas, starting with the main electrical distribution room at the service entrance? Are electrical rooms and distribution panels serving branch circuits secured?	
7.6	*Security system wiring*	Is security system wiring located separately from electrical and other service systems?	
7.7	*Emergency power distribution*	How is the emergency power distributed? Is the emergency power system independent from the normal electrical service, particularly in critical areas?	
7.8	*Fire alarm system*	Is fire alarm system well designed, implemented and correctly maintained?	
7.9	*Communication system rooms*	Where are communication systems wiring closets located? (voice, data, signal, alarm) Are they collocated with other utilities? Are they in secure areas? Does the fundamental communication system have an UPS (uninterruptible power supply) or an alternative supply system?	
7.10	*ICT disaster recovery*	Is there an alternative site with suitable ICT equipment and network which allows continuation of operations in case of attacks?	
7.11	*Mass notification system*	Is there a mass notification system that reaches all building occupants?	
		Topic 7	
		Average of Criticality weights	
		Standard Deviation of Criticality weights	

Tab.5.10 – Topic 8, table of items.

Topic 8 - Security Systems			
Item num.	***Item***	***Questions***	***Criticality weight***
8.1	*Perimeter and internal security*	Are CCTV (Closed Circuit Television) cameras used, 24 hours/7 days a week recorded and monitored at the perimeter and in the critical areas of the building?	
8.2	*Video signal quality*	Is the quality of video images adequate both during the day and hours of darkness?	
8.3	*Video recording continuity*	Are the recording systems and cameras supported by an uninterruptible power supply, battery, or building emergency power?	
8.4	*Intrusion detection system and alarms*	Is the physical IDS well designed, adequately spread in the building and well monitored?	
8.5	*Emergency call buttons and boxes*	Are call-button or intercom call-boxes or a building intercom system used throughout the building?	
8.6	*Security control equipment and scanners*	Are security scanners (X-ray, magnetometer, magnetic imaging, ...) used for security purposes in some areas of the building?	
8.7	*Safe mail handling*	Are the security controls in place to handle the processing of mail and protect against potential CBRe exposures adequate?	
8.8	*Security Control Room*	Is there a designated security control room and console in place to monitor security, alarm, and other building systems?	
8.9	*Communication system rooms*	Where are communication systems wiring closets located? (voice, data, signal, alarm) Are they collocated with other utilities? Are they in secure areas? Does the fundamental communication system have an UPS (uninterruptible power supply) or an alternative supply system?	
		Topic 8	
		Average of Criticality weights	
		Standard Deviation of Criticality weights	

Tab.5.11 – Topic 9, table of items.

Topic 9 - Emergency, security and operation continuity plans			
Item num.	***Item***	***Questions***	***Criticality weight***
9.1	*Security plan*	Do updated and written security and emergency plans exist for the building?	
9.2	*Security plan testing*	Is the security plan periodically tested and update?	
9.3	*Risk analysis activity*	Does the security plan include risk analysis and the countermeasure actions?	
9.4	*Emergency plan*	Is an emergency plan up-date and well-designed available to implement in the case of natural and anthropic disasters?	
9.5	*Operational continuity plan*	Is it available an up-date and well-designed operational continuity plan to apply?	
		Topic 9	
		Average of Criticality weights	
		Standard Deviation of Criticality weights	

5.2.2 Step 2: Characterization of specific threats for the vulnerability analysis

Once the general criticalities of the building have been analysed, to assess the vulnerability it is necessary to introduce and characterize the specific threats that the Assessment Team deems to be more probably applied to the building under assessment. In the Step 2 of the here proposed BVAM method, starting from the results obtained in Sect.4 for the primary threats, a specific vulnerability analysis is carried out considering the selected threats.

As anticipated, in Sect.8 we will provide an example of application to a Case Study of the proposed approach on three different *threats* extracted from tab.4.1, namely: the explosion of a van-bomb, the explosion of a suicide belt-bomb and, finally, the explosion of a Cesium-137 Dirty Bomb.

In this *Step 2* the Assessment Team conducts the following activities:

- ✓ for each selected threat, it is analysed in detail: the agent/explosive and vector types, the possible maximum size/quantity of the agent/material used in the possible attack and the possible specific location with respect to the building where the threat might be applied;
- ✓ the results obtained for the BCA in the different analysed topics of Step 1 provide immediate indications of the weaknesses that can be exploited, becoming effective *vulnerabilities*. In fact, when the selected threats are applied to the building attack scenario, these indications provide the fundamental elements to, on the one hand propose a mitigation of the vulnerability by reducing the associated criticality, and on the other hand assess the specific vulnerability of the building (Step 3) closely related to the analysed threats.

An example of this Step 2 analysis is shown in Sect.8.

5.2.3 Step 3: Evaluation of the Vulnerability Level for the building

At the end of *Step 2* the Assessment Team has a clear representation of the exploitable criticalities of the building with respect to the threats and the assets considered. As for the case of the threat probability evaluation, it will be necessary to assess a level of Vulnerability in this *Step*.

For each different threat analysed, the Assessment Team will evaluate a specific Building Vulnerability level, using a **Vulnerability Scale of 7 levels** proposed in tab.5.12 below.

Tab.5.12 - Vulnerability Scale.

Vulnerability rating	**Qualitative**	**Quantitative** (num. of successes out of the total num. of attempts)	**Level description**
7	Very High	From 3^{-1} to 3^{0} (from 1/3 to 1)	One or more major vulnerabilities have been identified that make the asset extremely susceptible to an aggressor and for the specific threat considered. The building lacks redundancies/physical protection/ resilience and the entire building would only be functional again a very long period of time after an event.
6	High	from 3^{-2} to 3^{-1} (from 1/9 to 1/3)	One or more major vulnerabilities have been identified that make the asset highly susceptible to an aggressor and for the specific threat considered. The building has poor redundancies/physical protection/resilience and most parts of the building would only be functional again a long period of time after an event.
5	Medium High	from 3^{-3} to 3^{-2} (from 1/27 to 1/9)	An important vulnerability has been identified that makes the asset very susceptible to an aggressor and for the specific threat considered. The building has inadequate redundancies/physical protection/ resilience and most critical functions would only be operational again a long period of time after an event.
4	Medium	from 3^{-4} to 3^{-3} (from 1/81 to 1/27)	A vulnerability has been identified that makes the asset fairly susceptible to an aggressor and for the specific threat considered. The building has insufficient redundancies/physical protection/resilience and most parts of the building would only be functional again a considerable period of time after an event.
3	Medium Low	from 3^{-5} to 3^{-4} (from 1/243 to 1/81)	A vulnerability has been identified that makes the asset somewhat susceptible to an aggressor and for the specific threat considered. The building has incorporated a fair level of redundancies/physical protection/resilience and most critical functions would only be operational again a considerable period of time after an event.
2	Low	from 3^{-6} to 3^{-5} (from 1/729 to 1/243)	A minor vulnerability has been identified that slightly increases the susceptibility of the asset to an aggressor and for the specific threat considered. The building has incorporated a good level of redundancies/physical protection/resilience and the building would be operational within a short period of time after an event.
1	Very Low	< 3^{-6} (< 1/729)	No relevant vulnerability appears after the analysis. The building has incorporated excellent redundancies/ physical protection/resilience and the building would be operational immediately after an event.

Tab.5.12 provides, for each level of the scale, a 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 [FEM2, FEM3], with some important differences:

- following the method in three steps for vulnerability assessment here proposed, the Assessment Team has, at this point, a *clear picture of the scenario* regarding the building criticalities and the threats to be applied. Only under this condition is possible to provide a reliable evaluation of the specific level of vulnerability;
- a *quantitative* reference value for any level of the scale is proposed. This information is very important to attempt of assessing the range that characterize the vulnerability level to be selected, corresponding to a measurable information not only described in a qualitatively way;
- the proposed scale adopts, even in this case, a *logarithm approach* for the range definition of the levels. This type of approach, as discussed in [Car1], has many advantages and will be detailed in Sect.7 devoted to describing the proposed comprehensive risk assessment method for sites and buildings in a terrorist scenario.

In practice, by applying these steps the Assessment Team also proceeds with the vulnerability analysis in an orderly fashion, starting with the criticality of the building, applying all selected primary threats starting with the top ranked threat presented in BTAM in Sect.4, Step 5, to the last selected threat in the ranking.

6 Building Exposure Assessment

The concept of Exposure has been introduced in Sect.3 and is one of the three fundamental quantities to be evaluated in the model for the risk assessment presented in Sect.7 and published in the references [Car1, Car4].

As anticipated in Sect.3, we define [EuC1] the Exposure *E* as the "*totality of people, property, systems, or other elements present in hazard zones that are thereby subject to potential losses*". In simple words, Exposure *E*, sometimes referred to in the literature as *asset*, can be considered the total value of all elements at risk. Practical assessment of Exposure can include the number of people or other types of assets in an area [UN1].

Clarified this definition, we can observe that Exposure analysis provides information on the presence, attributes and values of assets that may be impacted by a threat, including criteria or categories selected for evaluating consequences (impact on people, on the economy, on public confidence, etc.) [UN5, Car1].

This section will describe how to perform a *Building Exposure Assessment* (BEA), in practice to evaluate the values of the assets. To facilitate the identification of these building assets, it could be very useful for the Assessment Team interview people who are most familiar with them. Inputs from building owners, facility staff, and tenants, as well as any others who can help identify the most valuable assets, should be sought by the Team.

In this analysis, an asset is a resource of value requiring protection. An asset can be:

- *tangible*, as for people, tenants, structures, facilities, equipment, activities, information, etc;
- *intangible*, as for reputation of an institution or company, a work process organization, a building symbolic/historical value, etc.

The identification of the more relevant assets and, consequently, the assessment of the Exposure value, is conducted with the aim to well-evaluate the possible consequence (or impact) in the case of a terrorist event. Consequences are here intended as the adverse effects of a terrorist attack and reflect the nature and severity of losses sustained as a result of such an event [FEM3]. Consequences are typically expressed in terms of *direct* effects as fatalities, injuries, property damage, economic losses, or other types of adverse effects, such as psychological or social impacts on the victims. In the wake of some incidents, the immediate losses reverberate through the society, triggering *indirect* or *secondary* losses, which can be far-reaching and sometimes even more devastating than the *direct* losses. This is particularly true in cases where large areas, or sites/facilities with critical functions or significance, are affected. Terrorist attacks, such as 9/11 Twin Towers attack, affect society as a whole and require a much more comprehensive analysis of potential assets characterizing the building.

In any case, the approach here proposed for the BEA is focused on *direct* and *tangible* effects and the characterization of the Exposure quantity of a building will be divided into the following two categories:

- **Population capacity** in the building or in the surrounding area, for protecting public health and safety avoiding effects on human life and physical wellbeing (e.g., deaths, injuries).
- **Economic values** of the building and of the business related to the building and surrounding area. This category implies the possible direct effects on the economy with respect to the

building and its functions (e.g., cost to rebuild asset, cost to respond to and recover from the attack, downstream costs resulting from the disruption of operations or service, economical effect on surrounding infrastructures and facilities).

We observe that further studies are needed to gain more insight into the *intangible* category defined by the **Symbolic and institutional relevance values** expressed in terms of effect on public morale and trust in the government. This encompasses those changes in perceptions emerging after a significant terrorist event that affect the public's sense of safety and wellbeing, and the effect on the local government's ability to maintain order, deliver minimum essential public services, ensure public health and safety.

The scales provided in the following will adopt a similar type of numerical values and approach discussed in Sect.4 for the Building Threat Assessment Method, but with a fundamental **difference**: in the scales proposed for BEA we consider **only the part of the asset** subjected by **potential loss** in dependence of the **specific considered threat**. On the contrary, in Sect.4 the proposed tables are applied **independently by the threats**, considering the entire potential value associated with the considered asset for the specific building. This is a **very relevant difference** that must always be taken into account in the analysis activities conducted by the Assessment Team.

The following described specific Exposure scales will be applied in the risk assessment method (Sect.7) separately from the other and the different results obtained for every different asset will not be integrate in a **single risk value**, but remain separately evaluated. In fact, as a general concern, we can state that comparing **different types** of assets requires value judgments that can be **highly subjective**. Different stakeholders and decision makers will have different perspectives and value standards comparing for example a given number of fatalities with some economic damages. In any case, the losses associated to the human beings - fatalities and casualties - would be the **primary criterion for assigning the risk rating**, and, eventually, other types of potential asset losses should only very partially raise or lower that obtained primary rating.

With reference of such above analysis, **three** specific Exposure scales for the assessment of the assets subjected to potential losses will be provided in this section:

- *Scale for Site Population Specific Capacity*, characterizing the statistical population of the specific point of the site/building attacked with a specific threat.
- *Scale for Surrounding Population Specific Capacity*, characterizing the statistical population of the specific surrounding area (for example within 0.3 km), considering the specific point of the building attacked with a specific threat.
- *Scale for the Economical Specific Value of the Site*, characterizing the intrinsic economic value of the building added to the amount of business and revenue weekly generated by the activities managed in the specific point of the attack and in its collateral surrounding area (for example within 0.3 km [FEM3] around the main target).

An example of these three scales is provided in the following. The Assessment Team 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 as a function of the specific context to be analyzed. The ranges here proposed have been designed for a general application in an Italian building located in an important city.

Tab.6.1 - Site Population Specific Capacity Exposure Scale
(representing only people subjected to potential losses).

Exposure rating (Site Population Capacity)	**Qualitative**	**Quantitative** (number of people)
7	Very High	>2430
6	High	811 to 2430
5	Medium High	271 to 810
4	Medium	91 to 270
3	Medium Low	31 to 90
2	Low	11 to 30
1	Very Low	0 to 10

Tab.6.2 - Surrounding Population Specific Capacity Exposure Scale
(representing only people subjected to potential losses).

Exposure rating (Surrounding Population Capacity)	**Qualitative**	**Quantitative** (number of people)
7	Very High	>24300
6	High	8101 to 24300
5	Medium High	2701 to 8100
4	Medium	901 to 2700
3	Medium Low	301 to 900
2	Low	101 to 300
1	Very Low	0 to 100

Tab.6.3 - Exposure Scale of the Economical Specific Value of the building
(representing only specific economical assets subjected to potential losses).

Exposure rating (Economical value)	**Qualitative**	**Quantitative Range (Euro)** Revenue per week
7	Very High	>97.2 M
6	High	32.4 M to 97.2 M
5	Medium High	10.8 M to 32.4 M
4	Medium	3.6 M to 10.8 M
3	Medium Low	1.2 M to 3.6M
2	Low	400k to 1.2 M
1	Very Low	1 to 400k

7 Risk assessment for buildings

In this section a method suitable for assess the risk value of a terrorist attack in a given site/building is described. The essential elements of this method were already illustrated in 2019 on a previous book published by the author of this work devoted to "Terrorist attacks and natural/anthropic disasters" [Car1]. In 2021, on the International Journal of Safety and Security Engineering [Car4], the same author published a paper on a "Multi-Risk Assessment Method for Natural Disasters and CBRNe Attacks". Starting from these two references, in the following a specific and original *Building Risk Assessment Method* (BRAM) is presented and discussed, taking into account the considerations, approaches and results obtained in the previous sections of this book.

General speaking, risk assessment is a forecasting activity that has been challenging the modern societies since a long time. The more our societies get complex and interconnected, the more they are exposed to several, different - and possibly new - risks. The pandemic that is spreading worldwide since the beginning of 2020 is a dramatic example of this trend.

Although we are generally aware that there are risks, very often the evaluation *ex-ante* of these risks appears so complex and overwhelming that we give up, restricting ourselves to occasional strengthening of the security measures in place, without actually knowing who and why is more exposed to risks.

In the last two decades, several national and international institutions have deployed approaches, standards and strategies [DHS4, DHS5, DHS6, ISO1, ISO2, UN6, EuC1, EuC2] to face risk assessment in different contexts: some of these approaches were illustrated and discussed in Sect.3 of this book. At the same time, many companies have developed accurate, but very 'narrowband' risk assessment tools, based on the specific aspect of risk they face.

The effort presented in this section is to deploy a *risk and impact assessment technique* for buildings that can be adopted in whatever operating scenario, and in presence of whatever threat described in tab.4.1, but that can provide a sufficiently accurate estimate of the risk in a simple fashion. The method allows to manage the different kinds of risk related to the threats analyzed and results 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.

7.1 Multi-Risk Assessment Method characteristics

Some years ago, the author of this book proposed in the Italian academic arena a first very *essential* approach for risk assessment to be used for the Italian Civil Protection and Civil Defence applications [Car1]. The method, completed and published on a paper in 2021, has been indicated in as *Multi-Risk Assessment Method (MRAM)* [Car4]. This general method results flexible, scalable and suitable to estimate both *impact* and *risk* in qualitative, semi-quantitative, and, in some case, quantitative fashion for catastrophic or calamitous events, including terrorist non-conventional CBRNe attacks.

The MRAM described in [Car4] drawing part of the inspiration from some approaches proposed in the USA for Critical Infrastructures protection and for the management of natural/terrorist disasters [FEM2, RAM1, RAM2]. The general MRAM presents the following characteristics [Car4]:

- it applies both natural/anthropic disaster and terroristic attacks (CBRNe) to estimate the risk of an event;
- it allows to build risk rankings useful for prioritization activities of risk mitigation;
- it allows to manage and to analyse different kinds of risk (all-hazards/threats approach) being useful for addressing investments in preparedness, protection and resilience of critical areas and critical infrastructures;
- the risk is evaluated by using three mathematical quantities: Threat, Vulnerability and Exposure, where any quantity is evaluated selecting a "level" on a predefined scale;
- it is scalable and modular based on the application context;
- the method is focused on the safety of the population (fatalities and casualties), although a similar approach can be adopted to estimate the economic risk also;
- it allows to perform the impact analysis for an event by estimating the order of magnitude for the number of dead/injured;
- logarithm scales are adopted for defining the "levels" of the scales to make easier the interpretation of the results and the management of the method;
- it needs more detailed data for quantitative analysis, but less stringent precision is due for qualitative analysis that is oriented to the 'order of magnitude' approach in the results;
- risk formula is oriented to a very fast-run application of the method both for political decisions and technical one, in general used for Decision Support System applications.

It is important to highlight this method applies *logarithmic scales* for the following reasons:

- a logarithmic scale is a non-linear scale often used when there is a large range of amplitude in the analysed quantities. In particular, a logarithmic scale to base 2 or to base 3 it is proposed in the MRAM in consideration of the range of value and the number of levels that is needed to manage in the analysis;
- logarithmic scales make it possible to manage easily "orders of magnitude", rather than a standard linear scale, so the value represented by each equidistant mark on the scales is the value at the previous mark multiplied by a constant, the logarithm base value;
- for the semi-quantitative case, as a function of the base b of the logarithm, a power of b criterion holds. For example:
    - ✓ an increment of 1 in the value of the risk level corresponds to multiply by b the original previous risk value (in the case b=3 that will be, as we see in the following, of interest in our analysis for building, this represents a *tripling criterion* or *power of 3 criterion*);
    - ✓ an increment of 2 in the value of the risk corresponds to multiply by b^2 (in the case b=3 this increment corresponds to a factor equal to 3^2=9 with respect to the original previous risk value);
    - ✓ an increment of 3 in the value of the risk corresponds to multiply by b^3 (in the case b=3 this increment corresponds to a factor equal to 3^3=27 with respect to the original previous risk value);
    - ✓ and so on …

For the application of this kind of method, the following definitions of fundamental quantities, introduced in Sect.3, are adopted:

- ✓ *Threat T* represents the number of occurrences of an event over a given *interval of time* selected by the Assessment Team (for example, one of the intervals among 1 or 3 or 6 or 12 months can be chosen for the interval of time at the beginning of the analysis). The dimension of *T* is [event/time]. Threat *T* is expressed in terms of probability on a discrete scale, through a finite and scalable number of levels represented by a threat probability scale or array. For terrorist attacks it is dependent on, as discussed in Sect.4 of this book, the *asset attractiveness* of the target, *criticality attractiveness* of the target and on the *terrorist capabilities*.
- ✓ *Vulnerability V* represents a possible weakness of people, of a system, of a structure or a territory through which a threat can carry damage. Vulnerability *V* is a dimensionless quantity and can be expressed with a number between 0 and 1 (with the meaning similar to the probability); its value depends on the considered threat and on the analyzed kind of damage;
- ✓ *Exposure E* represents the maximum potential target/asset that can be affected by the threat. The dimension of *E* is [total asset/event]. Exposure *E* must be evaluated based on objective parameters (for example, the number of people present in the considered scenario interested by the event).

In the following the general MRAM will be **specialized** for the application to **building** and will be indicated as *Building Risk Assessment Method*. In the analysis, it will be shown how to estimate, in specific cases related to buildings, the three previous defined quantities *T*, *V* and *E* and, finally, how to assess the *Impact I* (dimension [consequence/event]) and *Risk R* (dimension [consequence/time]).

7.2 Building Risk Assessment Method

In order to evaluate and compare in a rank, for the case of terrorist attacks of buildings, different risk scenarios in a multi-threat approach a *Building Risk Assessment Method* (BRAM) is herein described.

The BRAM here proposed is characterized by the following design choices:

- ✓ application of scales of 7-rating values for all the fundamental Threat, Vulnerability and Exposure quantities (represented with logarithm scales);
- ✓ adoption of logarithm to base 3 in the ‘level’ definitions of the scales,
- ✓ choice of the *time interval of observation* for the Threat definition proposed equal to one of these possible values: 1 or 3 or 6 or 12 *months*, depending on information available and on the Assessment Team indications;
- ✓ application of the *tripling criterion* for the quantitative increment of values and ranges, moving from one level to the successive in a scale. This is a consequence of the logarithm to base 3 adoptions.

It is to note that the first two choices related to the number of levels (7) in the scales and to the logarithm base (3), provide the capability to design in an efficient and compact manner the scales for the building risk analysis, as will be evident below.

Furthermore, all the results obtained up to now in this book, in particular in Sect.4 for the threat assessment, in Sect.5 for the Vulnerability Assessment and, finally, Sect.6 for Exposure Assessment, will be applied in this risk assessment method for buildings.

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

1. the value of the Threat *T* is related to, as discussed in previous Sect.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), as reported in the relation

   $$T=f(Att_A, Att_C, Ter_C, Int_I)$$

   The BTAM described in Sect.4 provided a possible approach for the estimation of the quantity *T* and tab.4.13 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 previous Sect.5, to the Criticalities of the building (Cri_B) but even to the Threat Type (Thr_T) selected by the terrorist for the attack and to the Exposure Specific (Exp_S) characteristics (in term of the asset considered: people, economy, and so on), as reported in the relation

   $$V=f(Cri_B, Thr_T, Exp_S)$$

   The BVAM described in Sect.5 provided a possible approach for the estimation of the quantity *V* and tab.5.12 represents a useful tool for the final assessment of vulnerability rating values;
3. the value of the Exposure *E* is related, as discussed in previous Sect.6, to different 'assets' to be protected. The different assets are typically independent one from the other and for each asset type a different risk analysis is in principle needed. In the following, the analysis will be focused on the asset indicated as **Site Population Specific Capacity** for the building, introduced in Sect.6 tab.6.1, and the risk will be assessed in terms of deaths and injuries after the possible terrorist event. It is important to note that with the information and the method provided in this section, in a similar manner the risk assessment could be separately evaluated for the *Surrounding Population Specific Capacity* (tab.6.2) and *Economical Specific Value* (tab.6.3) assets, as discussed in Sect.6.

Under the hypothesis summarized above for the three variables *T*, *V* and *E*, taking into account the results in the institutional literature presented in Sect.3, the following risk and impact formulas will be applied in the BRAM approach:

(7.1) $R = T \cdot V \cdot E$

(7.2) $I = V \cdot E$

where R stands for the *risk* associated value, T stands for the *threat* associated probability, V stands for the *vulnerability* associated value, E stands for the *exposure* associate value and I stands for the *impact* associate value

The five variables above can be translated in the $\log_3(x)$ domain, with the base 3 previous proposed for the building analysis, introducing the concept of *levels*:

$L_R = log_3(R)$ = *Risk level*

$L_T = log_3(T)$ = *Threat level*

$L_V = log_3(V)$ = *Vulnerability level*

$L_E = log_3(E)$ = *Exposure level*

$L_I = log_3(I)$ = *Impact level*

Then, due to logarithm properties, the risk and impact formulas (7.1) and (7.2) can be re-written as *risk* and *impact level* formulas, i.e.:

(7.3) $L_R = L_T + L_V + L_E$

(7.4) $L_I = L_V + L_E$

and using (7.3) and (7.4) we can write

(7.5) $L_R = L_T + L_I$.

In such a way, in the new logarithm-based domain we can add the value instead of multiplying it as in (7.1) and (7.2).

The next step is to design proper scales for all the fundamental quantities here discussed.

As a general rule, the range of the first level in the scale will be typically settled on the base of the minimal desired granularity for the analysis. The choice to fix at 7 the number of rating values (levels) of the scale combined with the logarithm to base 3 choice guarantees to reach for the fundamental quantities an adequate amplitude over the entire analysis interval of interest, as will be evident in the following proposed scales.

The Threat probability scale is suitably tuned according to the minimum probability scenario. BRAM method proposes a semi-quantitative threat scale shown in tab.7.1 with 7 rating values

(levels), reasonably assuming a minimum probability for the threat *T* around 1 over 1000 intervals of time of observation. As already discussed, the interval of time must be fixed by the Assessment Team choosing among 1 or 3, or 6 or 12 *months*. For the analysis carried out in Sect.4, this tab.7.1 is equivalent to tab.4.13 in which the 7 rating values of threat are described for the specific case of a building terrorist attack.

Tab.7.1 – BRAM semi-quantitative threat scale (over a given interval of time).

Threat rating	Qualitative scale	from >	to <=	Threat probab. Min	Threat probab. Max
7	Very High	0.33	1	1/3	1
6	High	0.11	0.33	1/9	1/3
5	Medium High	0.037	0.11	1/27	1/9
4	Medium	0.012	0.037	1/81	1/27
3	Medium Low	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	

The Vulnerability scale has to be suitably tuned according to the minimum vulnerability scenario. BRAM method proposes a semi-quantitative vulnerability scale shown in tab.7.2 with 7 rating values, reasonably assuming a minimum value for the vulnerability *V* around 1 over 1000 attempts. For the analysis carried out in Sect.5, this tab.7.2 is equivalent to tab.5.12 in which the 7 rating values of the vulnerability are described for the specific case of a building terrorist attack.

Tab.7.2 - BRAM semi-quantitative and qualitative vulnerability scale.

Vulnerability rating	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 High	0.037	0.11	1/27	1/9
4	Medium	0.012	0.037	1/81	1/27
3	Medium Low	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	

The Exposure scale, as discussed in Sect. 6, can focus on different assets to represent: number of people in the building, number of people in the near external part of the building, economic amount of business per week due to the building activities and intrinsic value of the building.

To evaluate all these three different types of risk a specific analysis should to be carried out separately for each asset. As discussed above, for introducing the use of the semi-quantitative Exposure scale in the general BRAM, we will consider in this section only the first fundamental asset, the *number of people in the building*, as shown in tab.7.3. Even in this case, the scale is constituted

by 7 rating values, reasonably assuming a maximum number of people in the building around 3000. For the analysis carried out in Sect.6, this tab.7.3 is similar to tab.6.1 in which the 7 rating values of the exposure are described by several different ranges, representing the number of persons subject to potential harm.

Tab.7.3 - BRAM semi-quantitative and qualitative exposure scale for the Site Population Specific Capacity asset.

Exposure rating	Qualitative scale	Number of people
7	Very High	>2430
6	High	811 to 2430
5	Medium High	271 to 810
4	Medium	91 to 270
3	Medium Low	31 to 90
2	Low	11 to 30
1	Very Low	0 to 10

Starting from the previous described rating tables, we observe to have a 7-levels *vulnerability* scale (tab.7.2) and 7-levels *exposure* scale (tab.7.3) at our disposal. Using these last two tables, a *semi-quantitative* **Impact matrix** can be created, as shown in tab.7.4. For the considerations discussed before, in this matrix the *tripling criterion* (or power of 3 criterion) applies for each increment of 1 in the rating value and the matrix elements representing the impact rating values are calculated simply by adding the row and column indices, as suggested by formula (7.4).

Tab.7.4 - Example of BRAM semi-quantitative impact *I* matrix (where *E* stands for Exposure, *V* stands for Vulnerability).

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

The use of colors and the definition of an appropriate scale allows us to pass from a semi-quantitative scale with 13 rating values to a qualitative 7-levels scale shown in tab.7.5.

Tab.7.5 - BRAM qualitative impact scale.

Impact rating	Qualitative Impact
from 13 to 14	Very high
from 11 to 12	High
from 9 to 10	Medium high
from 7 to 8	Medium
from 5 to 6	Medium low
from 3 to 4	Low
2	Very low

The following meaning is associated to the qualitative impact colors:

- *Very high impact*, exceptionally grave effect on public health and safety (thousands of deaths and serious injuries possible);
- *High impact*, grave effect on public health and safety (hundreds of dead and serious injured possible);
- *Medium high impact*, serious effect on public health and safety (some tens of cases of deaths and serious injuries possible);
- *Medium impact*, moderate to serious effect on public health and safety (some cases of death and serious injury possible);
- *Medium low impact*, moderate effect on public health and safety (some case of non-serious consequences for human health possible);
- *Low impact*, minor effect on public health and safety (no deaths or serious injuries, unlikely non-serious injuries);
- *Very Low impact*, negligible effect on public health and safety (any significant consequence on human health).

These definitions can be verified evaluating for each level even the quantitative impact value applying (7.2) and the corresponding V and E numerical values available for each element of the matrix.

For a qualitative and semi-quantitative estimation of risk, remember the 7-levels *threat* scale (tab.7.1), the results obtained in tab.7.4 for the Impact rating at 13 distinct semi-quantitative values and formula (7.5), it is possible to create a *semi-quantitative* risk matrix at 19 elements. Similarly, to the impact case, in this new matrix the *tripling criterion* (or power of 3 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 (7.5).

Tab7.6 - BRAM semi-quantitative risk *R* matrix
(where *I* stands for Impact, *T* stands for Threat).

T \ I	2	3	4	5	6	7	8	9	10	11	12	13	14
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
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

Again, the use of colors and the definition of an appropriate scale allows us to pass from a semi-quantitative scale of 19 levels to a qualitative scale of 7-levels of risk, as shown in the following tab.7.7.

Tab.7.7 - BRAM qualitative risk scale.

Risk rating values	Qualitative Risk
from 20 to 21	Very high
from 18 to 19	High
from 16 to 17	Medium high
from 13 to 15	Medium
from 10 to 12	Medium low
from 7 to 9	Low
from 3 to 6	Very low

The following meaning is associated to the qualitative risk levels and colors:

- *Very high risk*, in the short term an exceptionally grave disaster with exceptionally grave effect on public health and safety is very likely;
- *High risk*, in the short-medium term a grave disaster with grave effect on public health and safety is likely;
- *Medium high risk*, in the short-medium term a serious disaster with serious effect on public health and safety is probable;
- *Medium risk*, in the medium term a moderate to serious event with moderate to serious effect on public health and safety is possible;
- *Medium low risk*, in the medium-long term an event with a low effect on public health and safety is possible;

- *Low risk*, even in the medium long term, an event with effect on public health and safety is unlikely;
- *Very low risk*, even in the long term, an event with consequence on human health is very unlikely.

The BRAM here described for the case of *Site Population Specific Capacity* asset shows the fundamental characteristics of the method and provides a guideline for the application for other specific assets, different by the number of people in the building, discussed in Sect.6 and characterized by tab.6.2 and tab.6.3 for *Surrounding Population Specific Capacity* asset and *Economical Specific Value assets*, respectively.

7.3 BRAM, Internal-External Vulnerability and Vulnerability Reduction Factor

The application of the BRAM is strictly conditioned in the obtained results by the capability of selected *Risk Assessment Team* in charge of the analysis to interpret the considered scenario and to select the appropriate levels of the risk parameters. For these reasons, the method can be applied only under the strict control of experts in the field of interest for the risk evaluation. Some decisions have to be taken based on experience, with a holistic vision of the scenario, in particular, as we will discuss in the following, for the Vulnerability quantity.

In order to provide a further useful tool to the Assessment Team, as in the case of the MRAM application [Car1, Car4], the BRAM proposes, only for the asset in the Exposure that are related to the health condition of the population, to distinguish between two different types of Vulnerability: *Internal Vulnerability* and *External Vulnerability*.

Internal Vulnerability (V_i) represents the statistical weakness of a human being (in case of damage to population) with respect to a given threat. Internal Vulnerability values are expressed in the range $0 \leq V_i \leq 1$, as in the case of a probability. Example: humans are defenseless against lethal viruses (i.e. Ebola) as their immune system is inadequate to face them. This is a case of internal vulnerability and, for example, $V_i = 0.65$ is the statistical possibility to die after the Ebola infection.

External Vulnerability (V_e) represents (in case of damage to population) the weakness of structures/systems with respect to a given threat (for example, in case of an explosion) or the effectiveness of the attack (for example, in case of a non-conventional attack the damage strongly depends on the CBR vector used). External Vulnerability values are also expressed in the range $0 \leq V_i \leq 1$, as in the case of a probability. Example: a lethal virus can be spread by aerosol or spread in the water pipes or in an air conditioning system. The three vectors assumed imply different infection probabilities and number of people in contact with the agent, and therefore different external vulnerabilities.

Overall (or *Total*) *Vulnerability* (V_t) is computed as a function of V_i and V_e . Assuming that V_i and V_e are independent variables (that is almost always true), then

$$V_t = V_i \cdot V_e$$

If a dependence exists between V_i and V_e , the conditional probability can be calculated through Bayes theorem.

Setting a value for the measure of the Vulnerability is one of the most delicate phases of the proposed method. The same criticality is true, in general, for every risk assessment method as discussed in ISO 31010 [ISO2] and highlight in [Car1].

As for the MRAM, also BRAM proposes the use of a numerical factor, so called *Vulnerability Reduction Factor* (VRF) to evaluate the amount of reduction of the vulnerability obtained by means of the *countermeasures* introduced to mitigate the risk.

The scale of this factor is expressed as a set of classes. In tab.7.8 an example of 3-factor based scale is here proposed: stepping from a class to the successive one, the VRF increases by a factor equal to 3, maintaining the tripling criterion assumed in all the previous risk analysis proposed scales.

Tab.7.8 -Vulnerability reduction factor (base 3).

Vulnerability reduction scale	Value of the Vulnerability Reduction Factor (VRF)
Class 9	$3^{-9}=1/19683$
Class 8	$3^{-8}=1/6561$
Class 7	$3^{-7}=1/2187$
Class 6	$3^{-6}=1/729$
Class 5	$3^{-5}=1/243$
Class 4	$3^{-4}=1/81$
Class 3	$3^{-3}=1/27$
Class 2	$3^{-2}=1/9$
Class 1	$3^{-1}=1/3$
Class 0	$3^{0}=1$

With reference to tab.7.8, a Class 2 countermeasure allows a vulnerability reduction equivalent to dividing by 9 (i.e. multiplied by 3^{-2}) the vulnerability original value, while a Class 0 countermeasure is completely ineffective, as it corresponds to a division by 1 (i.e. 3^0) of the original vulnerability value.

The same applies, with the power of 2 instead of 3, in tab.7.9.

Tab.7.9 - Vulnerability reduction factor (base 2).

Vulnerability reduction scale	Value of the Vulnerability Reduction Factor (VRF)
Class 10	$2^{-10} = 1/1024$
Class 9	$2^{-9} = 1/512$
Class 8	$2^{-8} = 1/256$
Class 7	$2^{-7} = 1/128$
Class 6	$2^{-6} = 1/64$
Class 5	$2^{-5} = 1/32$
Class 4	$2^{-4} = 1/16$
Class 3	$2^{-3} = 1/8$
Class 2	$2^{-2} = 1/4$
Class 1	$2^{-1} = 1/2$
Class 0	$2^{0} = 1$

When multiple countermeasures are applied to face the same vulnerability *Total Vulnerability Reduction Factor* (VRF_{tot}) can be determined:

- if the countermeasures are independent - as it generally occurs - VRF_{tot} is the product of VRF_x associated to the single countermeasures;
- if there is a dependence among countermeasures, VRF_{tot} must be computed as a combined or conditioned probability.

Once evaluated VRF_{tot} starting from the *Original Vulnerability* V_o (with no countermeasures applied that is often set to 1) we can calculate the *Residual Vulnerability* V_r as

$$V_r = V_o \cdot VRF_{tot} .$$

Starting from the *Residual Vulnerability* we can re-apply the BRAM and evaluate the ***Residual Risk*** that remains after the *risk treatment* (i.e. after the introduction of countermeasures for the vulnerability reduction).

As last practical notice, the BRAM method can be integrating with the creation of a *Catalogue of countermeasures* in which at any *countermeasures* is associated, by experts, a possible set of values of Vulnerability Reduction Factors, in order to make the risk management treatment phase faster, reliable and, possibly, easier.

8 Case studies and discussion of obtained results

In this part of the work the attention is focused on some Case Studies and the application of BTAM and BVAM, two methods introduced in previous sections.

In particular, BTAM is the method discussed in Sect.4 for the *threat assessment*. For this case three different existing buildings will be taken into account and, as anticipated in the Sect.4, three specific threats will be applied to the different building in the analysis.

BVAM is the method discussed in Sect.5 for the *vulnerability assessment*. The method will be applied to a single case study, a *commercial center*, in order to show the different aspect to consider in the assessment when three different *threats* are applied to the building.

Finally, at the end of the section the results obtained applying the two original methods proposed in this work are discussed providing considerations about the usefulness of these approaches.

8.1 BTAM application to three different Case Studies

To make the description of the different part of the method presented in Sect.4 more tangible and to show a practical application, we will focus our attention on some examples. Starting from Sect.4 indications, only *three threats* of the many proposed in Tab.4.1 as potential possible threats will be selected and three *specific* and *real sites/buildings* will be taken into account for the analysis. Under these first hypotheses, three Case Studies will be analyzed: *a commercial center*, *a government building*, *a little hospital* of an Italian important town.

The essential characteristics of the three Case Studies selected are herein described.

Commercial Center

The small Commercial Center is located in the outskirts of an important town, with an average number of 500 people in the Center during the day, considering both customers and workers of the Shopping Center. The Center is surrounded by a park and many residential buildings, for an average of 3000 inhabitants within 0.3 km around the Center. The building was built in at the end of 80’s and is not particularly relevant from a symbolic viewpoint. The Center is used by residents in the neighborhood. The building value is, today, 5 million euro and the amount of weekly business is of about 0.4 million euro. 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 services energy, ICT, HVAC, no specific business/operation continuity plan applied for the majority of the shops in the Center.

Summary of the essential data for evaluating asset attractiveness in the following table.

Commercial Centre	Data
Site population	500
Surrounding population (0.3 km)	3000
Building relevance	low
Importance of the occupants	medium low
Economic value	5.4Meuro

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 some 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 around the building. The building was built between the 15th and 16th century and is one of the icons of the town. The building value is, today, about 50 million euro and the amount of weekly business around the building is more of 3 million euro. 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. Badges 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.

Summary of the essential data for evaluating asset attractiveness in the following table.

Government Building	Data
Site population	2000
Surrounding population (0.3 km)	1500 (0.3)
Building relevance	very high
Importance of the occupants	very high
Economic value	53 M euro

Hospital

Situated in the same region of the other two buildings, with an average number of 150 people in the little public Hospital estimated during the day, 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 60’s and is one of the three hospitals in the health district. The building updated value, considering devices and facilities, is roughly 30 million euro and the amount of weekly business within 0.3 km around 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 and emergencies

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 services. Operation continuity plan existing.

Summary of the essential data for evaluating asset attractiveness in the following table.

Hospital	Data
Site population	150
Surrounding population (0.3 km)	500 (0.3)
Building relevance	medium
Importance of the occupants	medium low
Economic value	30 M euro

Selected Threats

As discussed in Sect.4, for the Case Studies we will focus our attention only on three different specific *threats* extracted from tab.4.1. The threats considered in the following analysis will be:

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

8.1.1 BTAM practical application

To understand the application of the threat assessment method previously described and generate a *ranking of sites* for the attractiveness, in tab.8.2 and tab.8.3 are shown an example of use of the procedure described in Step 4 to evaluate relations (4.2) and (4.3) for the indexes Asset Attractiveness and Criticality Attractiveness. The analysis is focused on the evaluation of the three different *Case Studies* above characterized in a certain detail, *a commercial center*, *a government building* and *an hospital*. The analysis, as already specified in Sect.4 for Step 3 and Step 4 of the BTAM, is at this stage of the method *threat-independent*.

Tab.8.2 - Example of application of Step 4 for evaluating the Category A parameters (Sect.4.2.3-4.2.4) for Asset Attractiveness.

Asset Attractiveness		**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	3	7	3
A5-Economic value	a_5	4	6	5
Total Score (Att_A sub-index)		**19**	**30**	**19**

Tab.8.3 - Example of application of Step 4 for evaluating the Category B parameters (Sect.4.2.3-4.2.4) for Criticality Attractiveness.

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

Starting from the Asset and Criticality Attractiveness sub-indexes evaluated, applying relation (4.1) for the general Attractiveness *Att* index, we obtain for these three *Case Studies* the results reported in tab.8.4.

Tab.8.4 - Evaluation of general Attractiveness *Att* index for the example.

Attractiveness indexes	**Commercial Center**	**Government building**	**Hospital**
Asset Attractiveness (Att_A)	19	30	19
Criticality Attractiveness (Att_C)	19	4	14
General Attractiveness (*Att* index)	**38**	**34**	**33**

From the tab.8.4 numerical results it is possible to generate a ranking for the sites, as shows in tab.8.5.

Tab.8.5 - Example of ranking for the site general Attractiveness.

Rank	Sites	*Att* index
1	**Commercial Center**	38
2	**Government building**	34
3	**Hospital**	33

The ranking of tab.8.5 shows 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* could be assessed, from a terrorist viewpoint, as the potential more attractive target among the analyzed sites. This final result here discussed is coherent with the statistical analyses of last decades for terrorist attacks presented in Sect.2, where the last statistical results confirm the evidence that '*soft targets*' are in practical cases often preferred by the terrorists, typically for the reduced measures implemented in the structure to mitigate the risk of an attack.

As discussed above, the analysis is focused in this section on the evaluation of only three different specific *threats* extracted from tab.4.1. The selected threats, already indicated, are: the *explosion of a van-bomb*; the e*xplosion of a suicide belt-bomb*; the *explosion of a Cesium-137 Dirty Bomb*.

As analyzed in Sect.4.2.3 for Category C of Step 3 in the model, these terrorist capability parameters are *threat dependent*, are evaluated *independently of the site/building* characteristics at this stage of the method, and describe the general skill and capability supposed for the terrorists. To evaluate these parameters the Assessment Team must assume knowledge of the capabilities of the terrorist groups under consideration.

In tab.8.6 is reported an example of application of the method proposed for evaluating the Terrorist Capability.

Tab.8.6 - Example of application of the method proposed for evaluating the terrorist capability.

Terrorist capability (*Ter*$_C$)		***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**

From the tab.8.6 numerical results it is possible to generate a ranking for the threats (*primary threat selection*), as shows in tab.8.7.

Tab.8.7 – Example of ranking for the analyzed threats.

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

The results of tab.8.7 show as, considering the main characteristics of terrorists and of the selected threats, the *Suicide belt bomb* appears, in this illustrative example, the general threat easily applicable for the aggressors, followed by the *van-bomb* and, last in the rank, the *dirty bomb*.

The Step 6 of the method proposed in Sect.4 consists in the evaluation, for *each site/building ordered in the ranking* generate in the tab.8.5, of the level of the *probability of any specific threat* of interest, specified in tab.8.7. 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 *intelligence information available*.

This means that all the threats considered in the analysis, and in particular the selected primary threats in the ranking of tab.8.7, 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 tab.4.13.

This table 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.

In practice, applying BTAM the Assessment Team approaches the analysis in an ordered mode, starting from the site/building at the *top of the ranking* (tab.8.5) and applying to this target all the *selected primary threats* beginning from the *threat* in *first position* in the ranking (tab.8.7), up to the *last selected threat* in the rank.

As an example of Step 6 application, we consider only the results obtained for the *Commercial Centre* before discussed and, throughout the joint analysis of the above results and of the information available by the *intelligence* and law *enforcing experts*, the **Threat Probability Level** is assessed applying tab.4.13.

The results obtained for the **Threat Probability Level**, assuming an *interval of time* for the observation **equal to 6 months**, is reported in tab.8.7a for the three threats here considered.

Tab.8.7a – Example of Threat Probability Level estimated by the Assessment Team in Step 6 of BTAM.

Threats (Commercial Center)	***Threat Probability Level*** (over 6 months)
Suicide belt bomb	**5**
Van Bomb	**4**
Cesium 137 Dirty Bomb	**2**

8.2 BVAM application to a Case Study

To make the description of the different part of the *vulnerability assessment method* for building (BVAM) described in Sect.5 more tangible and to show a practical application, we will focus in this part of the work our attention on a specific Case Study, the *Commercial Center* presented in Sect.8.1. In the analysis we will take into account the three possible terrorist attacks indicated in tab.8.7 and herein reported:

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

8.2.1 Building Criticality Analysis (BVAM Step 1)

To understand the application of the BVAM in three *steps* described in Sect.5 an example of application for the Commercial Center considered in the previous section is provided. Step 1 of the BVAM indicates the necessity of a wide *Building Criticality Analysis*. The information herein reported were evaluated by an inspection of the Commercial Center, after a permission of the property. The results are processed using a **prototype BCA software tool** developed on a *spreadsheet application*. The results obtained for this specific Case Study using the **BCA software tool** are reported in the following ten tables where the cells with a *white* background correspond to the *data entry area* of the spreadsheet available for the Assessment Team. The numbers show in *red* in the tables correspond, instead, to the *automatic data processing* of the software tool.

Tab.8.8 – Case study results for Topic 1 of BCA.

Topic 1 - Site characteristics				Automatic
Item num.	***Item***	***Questions***	***Criticality weight***	***Quantitative weight***
1.1	*Surrounding structures/facilities*	Are there any major/critical infrastructures surrounding the building?	Negligible	**1**
1.2	*Terrain characteristics*	Does the terrain place the building in a depression or low area?	Negligible	**1**
1.3	*Curb Lane Parking characteristics*	Is curb lane parking place for uncontrolled parked vehicles unacceptably close to the building?	Elevated	**9**
1.4	*Perimeter barriers for pedestrian access*	Is a perimeter fence or other types of barrier controls in place for the pedestrian access?	Marginal	**3**
1.5	*Vehicles access points*	Are the vehicles access points to the site or building well designed?	Marginal	**3**
1.6	*Pedestrian Access Control*	Is there pedestrian access control at the perimeter of the site or of the building?	Elevated	**9**
1.7	*Private Vehicle Access Control*	Is there private vehicle access control at the perimeter of the site or of the building	Elevated	**9**
1.8	*Shipping/Delivery Vehicle Access Control*	Is there access control of shipping and delivery vehicles at the building entrance?	Elevated	**9**
1.9	*Alternative Potential Access*	Is there any exploitable potential access to the building through utility paths or water runoff?	Elevated	**9**
1.10	*Anti-ram devices*	What are the existing types of vehicle anti-ram devices for the building?	Extreme	**27**
1.11	*Site lighting in the external area*	Is the site lighting adequate from a security perspective in roadway access and parking areas?	Marginal	**3**
1.12	*External connection to the building*	Is any of the nearby in-ground and out-ground infrastructures directly connected to the building?	Negligible	**1**
		Topic 1		
		Average of Criticality weights	**7.00**	
		Standard Deviation of Criticality weights	**6.93**	

Tab.8.9 – Case study results for Topic 2 of BCA.

Topic 2 - Architecture				Automatic
Item num.	***Item***	***Questions***	***Criticality weight***	***Quantitative weight***
2.1	*Mixed tenant building*	Is it a mixed-tenant building?	Marginal	**3**
2.2	*Receptacles to hide explosive devices*	Are there trash receptacles and mailboxes in close proximity to the building that can be used to hide explosive devices?	Elevated	**9**
2.3	*Public and critical points in the building*	Are public toilets, service spaces, or access to stairs or elevators located in any non-secure areas, including the queuing area before screening at the public entrance?	Marginal	**3**
2.4	*Equipments for access control and screening*	Do public and employee entrances include equipments for access control-screening and, in perspective, adequate space for possible future installation?	Extreme	**27**
2.5	*Reinforced walls and doors*	Are doors and walls along the line of security screening adequately reinforced?	Elevated	**9**
2.6	*Roof access control*	Is roof access controlled and limited to authorized personnel by means of adequate mechanisms?	Elevated	**9**
2.7	*Building critical assets*	Are critical assets (people, activities, building systems and components) well separated from main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking? Are the critical building systems and components adequately hardened and controlled?	Elevated	**9**
2.8	*Separation of critical assets and loading docs/shipping areas*	Are loading docks, receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.?	Extreme	**27**
2.9	*Mailroom space and equipments*	Have the mailroom adequate equipment and space available to examine incoming packages and for an explosive disposal container?	NA	**-**
2.10	*Debris generation limitation*	Are ceiling, internal walls, overhead utilities and lighting systems designed to remain in place without generate danger debris during hazard events?	Extreme	**27**
		Topic 2		
		Average of Criticality weights	**13.67**	
		Standard Deviation of Criticality weights	**9.71**	

Tab.8.10 – Case study results for Topic 3 of BCA.

Topic 3 - Structural Systems				Automatic
Item num.	***Item***	***Questions***	***Criticality weight***	***Quantitative weight***
3.1	*Construction characteristics*	What type of construction? What type of concrete and reinforcing steel? What type of steel? What type of foundation?	Marginal	**3**
3.2	*Structural and Non-Structural Components*	Are any of structural/non-structural components vulnerable either directly or indirectly to explosive blast?	Elevated	**9**
3.3	*Progressive collapse*	Is the building capable of sustaining the removal of a column for one floor above grade at the building perimeter without progressive collapse?	Marginal	**3**
3.4	*Floor of loading dock*	Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?	Extreme	**27**
3.5	*Mailroom explosion mitigation*	Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?	Elevated	**9**
3.6	*In-ground structural systems*	Would failure of part of the in-ground infrastructure affect the structural system of the building?	Elevated	**9**
3.7	*Underground water presence*	Does the presence of underground water under the building generate instability and unacceptable flooding?	Elevated	**9**
		Topic 3		
		Average of Criticality weights	**9.86**	
		Standard Deviation of Criticality weights	**7.47**	

Tab.8.11 – Case study results for Topic 4 of BCA.

Topic 4 - Building Envelope				Automatic
Item num.	***Item***	***Questions***	***Criticality weight***	***Quantitative weight***
4.1	*Envelope protection level*	What is the designed or estimated protection level of the building envelope against a possible high magnitude explosive threat?	Extreme	**27**
4.2	*Envelope fenestration balance*	Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.)	Elevated	**9**
4.3	*Glazing characteristics*	Are the glazing of the building secure in case of blast?	Elevated	**9**
4.4	*High external pressure resistence*	Is the building designed to correctly resist to high external pressure (as for the case of blast)?	Elevated	**9**
4.5	*Envelope and window glazing external condition*	What are the current condition of windows and of the rest of the envelope (cladding, curtain walls, veneer, ...)?	Marginal	**3**
		Topic 4		
		Average of Criticality weights	**11.40**	
		Standard Deviation of Criticality weights	**8.14**	

Tab.8.12 – Case study results for Topic 5 of BCA.

Topic 5 - Utility systems and internal distribution infrastructures				Automatic
Item num.	***Item***	***Questions***	***Criticality weight***	***Quantitative weight***
5.1	*Domestic water service*	What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank)? Is the domestic water service reliable and certified for the water quality? Is there a secure and sufficient alternate drinking water supply?	Marginal	**3**
5.2	*Security of water entry points*	Are the entry points for the water supply in a secure location and managed in a secure manner?	Marginal	**3**
5.3	*Water for the fire suppression system*	Is the source and the distribution system of water for the fire suppression service adequate to manage incendiary events?	Marginal	**3**
5.4	*Sewer System*	Are sewer systems well designed, implemented and protected?	Marginal	**3**
5.5	*Fuel storage for continuity operations*	Is an adequate quantity of fuel stored at the building? How is it stored? How is it secured?	Marginal	**3**
5.6	*Electrical service redundancy*	Is there a redundant and reliable electrical service source?	Extreme	**27**
5.7	*Security of electrical entry points*	Is the incoming electric service to the building well designed and secure?	Marginal	**3**
5.8	*ICT services*	By what means does the main telephone and data communications interface the building? Are there multiple or redundant locations for the telephone and digital communication services? Are these locations secure and not accessible by unauthorized people? Is the provided data service secure?	Elevated	**9**
		Topic 5		
		Average of Criticality weights	**6.75**	
		Standard Deviation of Criticality weights	**7.90**	

Tab.8.13 – Case study results for Topic 6 of BCA.

Topic 6 - Mechanical systems – HVAC				Automatic
Item num.	***Item***	***Questions***	***Criticality weight***	***Quantitative weight***
6.1	*Air intakes and exhaust louvers*	Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure) Are the intakes and exhausts accessible to the public?	Marginal	**3**
6.2	*Roof access*	Is roof access limited to authorized personnel by means of adequate mechanisms?	Elevated	**9**
6.3	*Air filtration*	What are the types of air filtration adopted for the building? Is there any collective or specific protection for chemical, biological, and radiological contamination designed into the building?	Extreme	**27**
6.4	*Air CBR sensors*	Are there provisions for air monitors or sensors for CBR agents?	Extreme	**27**
6.5	*Air intakes and exhaust closure*	Does it exist a method for fast air intakes and exhausts closure when necessary?	Elevated	**9**
6.6	*Air-handling systems zoning*	Are there large central air handling units or are there multiple units serving separate zones? Can critical areas be served from other units if a major system is disabled?	Elevated	**9**
6.7	*Air intakes and exhaust system security*	Are supply, return, and exhaust air systems for critical areas secure?	Elevated	**9**
6.8	*Air pressurization*	Is air pressurization well designed and monitored regularly?	Extreme	**27**
6.9	*Smoke evacuation systems*	Are there any smoke evacuation systems installed?	Extreme	**27**
6.10	*HVAC maintenance*	Does the HVAC maintenance staff have the proper training, procedures, and preventive maintenance schedule to ensure system functionality?	Marginal	**3**
		Topic 6		
		Average of Criticality weights	**15.00**	
		Standard Deviation of Criticality weights	**10.04**	

Tab.8.14 – Case study results for Topic 7 of BCA.

Topic 7 - Infrastructure and systems of internal essential services				Automatic
Item num.	***Item***	***Questions***	***Criticality weight***	***Quantitative weight***
7.1	*Domestic water distribution*	For the water distribution, are looping of piping architecture and section valves for redundancy tasks adopted?	Marginal	**3**
7.2	*Hot water management*	Is the method of heating domestic water resilient to fault at the heat source?	Marginal	**3**
7.3	*Gas distribution*	For the gas distribution, are looping of piping architecture and section valves for redundancy tasks adopted?	Marginal	**3**
7.4	*Gas storages*	Where are gas storage tanks located? (heating, cooking, medical, process)	Marginal	**3**
7.5	*Electrical rooms and panels*	How are the electrical rooms located relative to other higher risk areas, starting with the main electrical distribution room at the service entrance? Are electrical rooms and distribution panels serving branch circuits secured?	Marginal	**3**
7.6	*Security system wiring*	Is security system wiring located separately from electrical and other service systems?	Elevated	**9**
7.7	*Emergency power distribution*	How is the emergency power distributed? Is the emergency power system independent from the normal electrical service, particularly in critical areas?	Marginal	**3**
7.8	*Fire alarm system*	Is fire alarm system well designed, implemented and correctly maintained?	Marginal	**3**
7.9	*Communication system rooms*	Where are communication systems wiring closets located? (voice, data, signal, alarm) Are they collocated with other utilities? Are they in secure areas? Does the fundamental communication system have an UPS (uninterruptible power supply) or an alternative supply system?	Marginal	**3**
7.10	*ICT disaster recovery*	Is there an alternative site with suitable ICT equipment and network which allows continuation of operations in case of attacks?	Marginal	**3**
7.11	*Mass notification system*	Is there a mass notification system that reaches all building occupants?	Elevated	**9**
		Topic 7		
		Average of Criticality weights	**4.09**	
		Standard Deviation of Criticality weights	**2.31**	

Tab.8.15 – Case study results for Topic 8 of BCA.

Topic 8 - Security Systems				Automatic
Item num.	***Item***	***Questions***	***Criticality weight***	***Quantitative weight***
8.1	*Perimeter and internal security*	Are CCTV (Closed Circuit Television) cameras used, 24 hours/7 days a week recorded and monitored at the perimeter and in the critical areas of the building?	Elevated	**9**
8.2	*Video signal quality*	Is the quality of video images adequate both during the day and hours of darkness?	Elevated	**9**
8.3	*Video recording continuity*	Are the recording systems and cameras supported by an uninterruptible power supply, battery, or building emergency power?	Marginal	**3**
8.4	*Intrusion detection system and alarms*	Is the physical IDS well designed, adequately spread in the building and well monitored?	Elevated	**9**
8.5	*Emergency call buttons and boxes*	Are call-button or intercom call-boxes or a building intercom system used throughout the building?	Elevated	**9**
8.6	*Security control equipments and scanners*	Are security scanners (X-ray, magnetomer, magnetic imaging, ...) used for security purposes in some areas of the building?	Extreme	**27**
8.7	*Safe mail handling*	Are the security controls in place to handle the processing of mail and protect against potential CBRe exposures adequate?	Elevated	**9**
8.8	*Security Control Room*	Is there a designated security control room and console in place to monitor security, alarm, and other building systems?	Elevated	**9**
8.9	*Communication system rooms*	Where are communication systems wiring closets located? (voice, data, signal, alarm) Are they collocated with other utilities? Are they in secure areas? Does the fundamental communication system have an UPS (uninterruptible power supply) or an alternative supply system?	Elevated	**9**
		Topic 8		
		Average of Criticality weights	**10.33**	
		Standard Deviation of Criticality weights	**6.18**	

Tab.8.16 – Case study results for Topic 9 of BCA.

Topic 9 - Emergency, security and operation continuity plans				Automatic
Item num.	***Item***	***Questions***	***Criticality weight***	***Quantitative weight***
9.1	*Security plan*	Do updated and written security and emergency plans exist for the building?	Marginal	**3**
9.2	*Security plan testing*	Is the security plan periodically tested and update?	Elevated	**9**
9.3	*Risk analysis activity*	Does the security plan include risk analysis and the countermeasure actions?	Elevated	**9**
9.4	*Emergency plan*	Is an emergency plan up-date and well designed available to implement in the case of natural and anthropic disasters?	Elevated	**9**
9.5	*Operational continuity plan*	Is it available an up-date and well designed operational continuity plan to apply?	Elevated	**9**
		Topic 9		
		Average of Criticality weights	**7.80**	
		Standard Deviation of Criticality weights	**2.40**	

Finally, a results summary table is provided by the BCA software tool at the end of Step 1 in the criticality evaluation, showing the *average*, the *standard deviation* and the *modified average* (a third index obtained by adding *average* and *standard deviation*) introduced in Sect.5. This last modified index can be used to characterize, with a single value, a reference maximum value useful to evaluate the *cumulative criticality* of the considered topic.

The following tab.8.17 shows the summary results obtained for the Case Study.

Tab.8.17 – Summary of the results obtained for the Case Study (Commercial Center).

Topic Criticality Analysis				
Topic Num.	***Topic***	***Average***	***Standard Deviation***	***Modified Average***
Topic1	Site characteristics	**7.00**	**6.93**	**13.93**
Topic2	Architecture	**13.67**	**9.71**	**23.37**
Topic3	Structural Systems	**9.86**	**7.47**	**17.33**
Topic4	Building Envelope	**11.40**	**8.14**	**19.54**
Topic5	Utility systems and internal distribution infrastructures	**6.75**	**7.90**	**14.65**
Topic6	Mechanical systems – HVAC	**15.00**	**10.04**	**25.04**
Topic7	Infrastructure and systems of internal essential services	**4.09**	**2.31**	**6.41**
Topic8	Security Systems	**10.33**	**6.18**	**16.52**
Topic9	Emergency, security and operation continuity plans	**7.80**	**2.40**	**10.20**

The *modified average* index can be interpreted using a final Criticality Scale based on modified average, herein reported.

Tab.8.18 – Criticality Scale based on Modified Average.

Criticality Modified Average Scale	Range
Extreme	>15
Elevated	7-15
Marginal	3-6
Negligible	1-2
NA	-

Taking into account this last scale, the analysis of tab.8.17 results highlight that:

- Topic #2, 3, 4, 6, 8 show an *extreme* criticality;
- Topic #1, 5, 9 show an *elevated* criticality;
- Topic #7 shows a *marginal* criticality.

These results show a high level of criticality of the building and the weaknesses are specifically identified by the 76 items analyzed.

8.2.2 Characterization of specific threats (BVAM Step 2)

As anticipated in Sect.5.2, in this Case Study we focus our attention only on **three** different *threats* extracted from Tab.4.1. The threats considered are:

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

For each selected threat, as discussed in Sect.5.2, the Assessment Team has to specify in detail:

- ✓ the type of agent/explosive,
- ✓ the type of vector for the agent/explosive,
- ✓ the possible maximum size/quantity of the agent/material,
- ✓ the possible specific location, with respect to the building, where the threat might be applied.

Specific and detailed information on different type of explosion and blast characteristics [Dus1] can be found also in a recent European Commission JRC technical report [EuC4] and in USA FEMA Reference manual to mitigate attacks against buildings [FEM3].

The typical reference for the vectors and the possible maximum mass charges are reported in the following fig.8.1 [EuC4] and in fig.8.2 a chart representation of the effects on glass, walls concrete and people as a general function of TNT mass charge and the explosion stand-off are depicted.

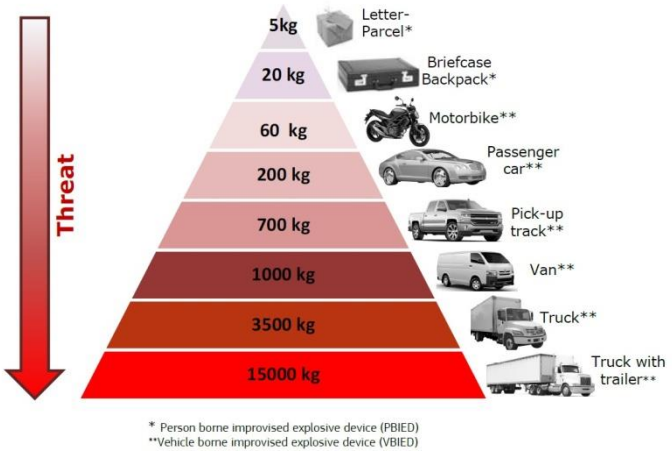

Fig.8.1 - Upper charge mass limit per mean of transportation [EuC4].

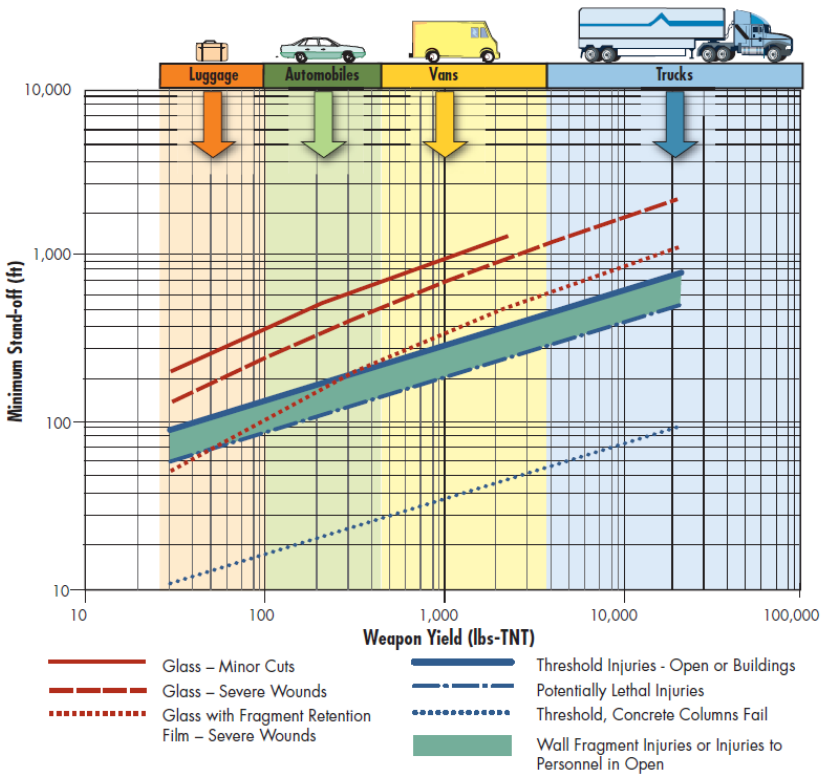

Fig.8.2 - Generic range-to-effects chart for explosive weapons [FEM3].

The following six tables summarize, for the three threats considered, all these information assumed by the Assessment Team.

Tab.8.19 – Characterization of the threats for the explosion of a van-bomb.

Case: Explosion of a van-bomb	**Specific data**
Type of agent/explosive	TNT
Type of vector	Van
Maximum size/quantity of the agent/material	800 kg
Specific location, with respect to the building, where the threat might be applied	Area of access for shipping/delivery vehicles

Tab.8.20 – Characterization of the threats for the explosion of a suicide belt-bomb.

Case: Explosion of a suicide belt-bomb	**Specific data**
Type of agent/explosive	TNT
Type of vector	Belt-bomb
Maximum size/quantity of the agent/material	5 kg
Specific location, with respect to the building, where the threat might be applied	Internal part of the building, in front to the mall access

Tab.8.21 – Characterization of the threats for the explosion of Cesium-137 Dirty Bomb.

Case: Explosion of a Cesium-137 Dirty Bomb	**Specific data**
Type of agent/explosive	TNT and $Cesium^{137}$
Type of vector	Pick-up truck
Maximum size/quantity of the agent/material	400 kg TNT and 90 g $Cesium^{137}$
Specific location, with respect to the building, where the threat might be applied	In the external parking area of the building

Finally, for each specific threat considered, a further evaluation of the criticality items of Step 1 is carried out with the aim of highlighting both the ***primary*** weaknesses that can be *directly* exploited as actual vulnerabilities for the practical realization of the threat under analysis, and the ***secondary*** weaknesses that, in an *indirect* manner, contribute to making the consequences of the attack more severe. This or these items should have been recorded in Step 1 with level of criticality 'elevated' or 'extreme' to be exploitable.

If a mitigation action of the vulnerabilities has to be performed by the Assessment Team, it is fundamental to reduce first the *primary* vulnerabilities and, only successively and in presence of adequately resources, to face the *secondary*.

Tab.8.22 – Main exploitable vulnerabilities of the building in case of an *explosion of a van-bomb*.

Criticality item- Exploitable vulnerability (explosion of a van-bomb)	**Level of criticality**	**Vulnerability type**
1.8 – There is not vehicle access control at the shipping/delivery entry	Elevated	Primary
2.5 - Doors and walls along the line of security screening are not adequately reinforced	Elevated	Secondary
2.7 - Critical assets (people, activities, building systems and components) are not well separated from main entrance, vehicle circulation, parking	Elevated	Secondary
2.10 - Ceiling, internal walls, overhead utilities and lighting systems are not designed to remain in place without generate danger debris during hazard events	Extreme	Secondary
4.1 - The designed or estimated protection level of the building envelope against a possible high magnitude explosive threat is low	Extreme	Secondary
4.3 - Glazing of the building are not secure in case of blast	Elevated	Secondary
4.4 - The building is not designed to resist to high external pressure (as for the case of blast)	Elevated	Secondary
5.6 - There is not a redundant and reliable electrical service source	Extreme	Secondary
7.11 – There is not a mass notification system that reaches all building occupants	Elevated	Secondary
8.1 - CCTV (Closed Circuit Television) cameras used, 24 hours/7 days a week recorded and monitored at the perimeter and in the critical areas of the building are insufficient	Elevated	Secondary
8.2 - The quality of video images is not adequate both during the day and hours of darkness	Elevated	Secondary
9.4 - The emergency plan is not up-date and well designed	Elevated	Secondary
9.5 - It is not available an up-date and well-designed operational continuity plan to apply	Elevated	Secondary

Tab.8.23 – Main exploitable vulnerabilities of the building in case of *a suicide belt-bomb* attack.

Criticality item- Exploitable vulnerability (explosion of a suicide belt-bomb)	**Level of criticality**	**Vulnerability type**
1.6 - There is not pedestrian access control at the perimeter of the site or of the building	Elevated	Primary
2.4 - Public and employee entrances do not include equipment for access control-screening	Extreme	Primary
2.7 - Critical assets (people, activities, building systems and components) are not well separated from main entrance, vehicle circulation, parking	Elevated	Secondary
2.10 - Ceiling, internal walls, overhead utilities and lighting systems are not designed to remain in place without generate danger debris during hazard events	Extreme	Secondary
4.3 - Glazing of the building are not secure in case of blast	Elevated	Secondary
5.6 - There is not a redundant and reliable electrical service source	Extreme	Secondary
7.11 – There is not a mass notification system that reaches all building occupants	Elevated	Secondary
8.1 - CCTV (Closed Circuit Television) cameras used, 24 hours/7 days a week recorded and monitored at the perimeter and in the critical areas of the building are insufficient	Elevated	Secondary
8.2 - The quality of video images is not adequate both during the day and hours of darkness	Elevated	Secondary
8.6 - Security scanners (X-ray, magnetometry, magnetic imaging, ...) are not used for security purposes in some areas of the building	Extreme	Primary
9.4 - The emergency plan is not up-date and well designed	Elevated	Secondary
9.5 - It is not available an up-date and well-designed operational continuity plan to apply	Elevated	Secondary

Tab.8.24 – Main exploitable vulnerabilities of the building in case of *a Cesium 137 Dirty Bomb* attack.

Criticality item- Exploitable vulnerability (explosion of a Cesium 137 Dirty Bomb)	**Level of criticality**	**Vulnerability type**
1.3 - Curb lane parking is place for uncontrolled parked vehicles unacceptably close to the building	Elevated	Primary
1.7 – There is not private vehicle access control at the perimeter of the site or of the building	Elevated	Primary
2.5 - Doors and walls along the line of security screening are not adequately reinforced	Elevated	Secondary
2.7 - Critical assets (people, activities, building systems and components) are not well separated from main entrance, vehicle circulation, parking	Elevated	Secondary
2.10 - Ceiling, internal walls, overhead utilities and lighting systems are not designed to remain in place without generate danger debris during hazard events	Extreme	Secondary
4.1 - The designed or estimated protection level of the building envelope against a possible high magnitude explosive threat is low	Extreme	Secondary
4.3 - Glazing of the building are not secure in case of blast	Elevated	Secondary
4.4 - The building is not designed to resist to high external pressure (as for the case of blast)	Elevated	Secondary
5.6 - There is not a redundant and reliable electrical service source	Extreme	Secondary
6.4 - There are not provisions for air monitors or sensors for CBR agents	Extreme	Secondary
6.5 – It does not exist a method for fast air intakes and exhausts closure when necessary	Elevated	Secondary
7.11 – There is not a mass notification system that reaches all building occupants	Elevated	Secondary
8.1 - CCTV (Closed Circuit Television) cameras used, 24 hours/7 days a week recorded and monitored at the perimeter and in the critical areas of the building are insufficient	Elevated	Secondary
8.2 - The quality of video images is not adequate both during the day and hours of darkness	Elevated	Secondary
9.4 - The emergency plan is not up-date and well designed	Elevated	Secondary
9.5 - It is not available an up-date and well-designed operational continuity plan to apply	Elevated	Secondary

8.2.3 Evaluation of vulnerability level (BVAM Step 3)

Taking into account the results obtained in the two previous BVAM steps, it is now possible for the Assessment Team to assess the specific vulnerability of the building (Step 3 of the method) closely related to the analyzed threats.

All the three analyzed threats show the possibility to exploit relevant vulnerabilities characterized by *elevated* or *extreme* level of criticality. In this situation the vulnerability can be associated with both the economical values related to the area and to the people that are engaged, for any reason, in or near the building perimeter. In particular, the building areas interested for human health impacts are the internal area for the case of suicide belt and also the external area for the other two cases, with maximum consequence in term of area impacted in the case of Dirty Bomb explosion.

Using the tab.5.12 the Assessment Team can decide the vulnerability rating for the three threats, for example assigning for the *Site Population Capacity asset* (Sect.5) the **Vulnerability Level** equal to **7** to the three considered cases.

8.3 Discussion of results

The Case Studies analysed show some interesting properties of the proposed methods.

In particular, starting from the BTAM results we can observe that:

- the method can be applied to *any type of building*, regardless of whether they are *soft or hard targets*;
- the *asset* and *criticality attractiveness parameters* are adequate for a rapid evaluation, characterizing elements that can be easily assessed, in most cases, in a quantitative manner through the rating tables provided in Sect. 4.;
- the parameters for estimating *terrorist capability* can be applied repeatedly as many times as there are different types of terrorist groups considered in the analysis. This also makes it possible to select the most prepared and evolved terrorist groups and to limit the scope of investigation for the attacks based on explosive/CBR agents;
- the Assessment Team can apply the *method with flexibility*, modifying the tables if deemed necessary to better describe the characteristics of the parameters, and also can decide to limit the evaluations to a subset of the proposed set of parameters, for example in order to be faster in the analysis;
- the Assessment Team approach the analysis of the Step 6 in a *ordered mode*, starting from the *site/building at the top of the ranking* (Step 4 results) and applying to this target all the selected primary threats beginning from the threat in first position in the ranking (Step 5 results), up to the last selected threat in the rank;
- at the end of the application of the above adopted method in six steps, the Assessment Team has a *clear and comprehensive picture of the scenario* regarding the sites and the threats. Only under this pre-condition is possible to attempt a reliable evaluation of the specific threat probability in a specific building;

- in the last step of the method, the *information that comes from the Intelligence or law-enforcement experts* finds its necessary place alongside the evaluations of the previous parameters that are more objective in their nature. Since the method was imagined to be applied above all by the Institutions as, for example, the *secret services* and *civil defence services*, this solution makes it possible to optimize the analyses of an *informative* nature typical of intelligence with a precise knowledge of the main characteristics of the buildings and of the threats under evaluation;
- a *quantitative* range for any level of the threat probability scale is a useful parameter. This information is very important to attempt of assessing the range of probability that characterize the level to be selected, corresponding to a measurable information not only described in a qualitatively way;
- the Assessment Team can *flexibly associate* at the beginning of the Step 6 analysis, the probability interval value of a level to a specified *interval of time* (for example, over 1 month or 3 months or 6 months or 1 year). This choice is strictly related to the precision and reliability of intelligence information available for possible terrorist attacks and results very important for prevention actions.

As far as the BVAM results is concerned, we can observe that:

- the adoption, for Step 1, of the prototype BCA software tool developed for the analysis of the criticality of the building greatly simplifies the activity of the Assessment Team. Furthermore, the last summary sheet of the criticality topic results provides, in a single screen (tab.8.17), a very effective description of the general criticality of the building and, at the same time, gives a direct indication of the most serious areas in which to introduce possible countermeasures for the mitigation of the vulnerability;
- the detailed description of the threats carried out in Step 2 allows to evaluate with punctuality which of the criticalities emerged during Step 1 of the method are really exploitable, providing a very precise information for the design of countermeasures for risk reduction purposes;
- the Step 3 of the method allows, finally, to select a level of vulnerability among the 7-levels proposed in the scale having clear in mind what specific criticalities have actually emerged as a result of Step 2.

As a final consideration of this discussion, we can highlight that the Case Studies analyzed show consistent and easily interpretable results and, for most of the analysis steps, objective assessments. This makes it possible to carry out a coherent analysis and to obtain reliable results in an extremely complex context such as that related to risk assessment for terrorist attacks on a building.

9 Conclusions and future developments

Risk assessment is a forecasting activity that has been challenging the modern societies since a long time. The more our societies get complex and interconnected, the more we are exposed to several, different - and possibly new - risks. The pandemic that is spreading since the beginning of 2020 is a dramatic example of this trend.

Although we are generally aware that there are risks, very often the evaluation ex-ante of these risks appears so complex and overwhelming that we give up, restricting ourselves to occasional strengthening of the security measures in place, without actually knowing who and why is more exposed to risks.

In the last 20 years, several national and international institutions have deployed standards and strategies to face risk assessment in different contexts.

The effort presented in this book was to deploy a *building risk assessment technique* that could be adopted in whatever operating scenario, and in presence of almost whatever threat or hazard, but that can provide a sufficiently accurate estimate of the risk in a simple manner. The methods presented allow to manage different kinds of risk for buildings and provide results useful for prioritizing actions and investments in preparedness, protection and resilience of buildings.

As shown in the book, the recent terrorist activities are no longer focused exclusively on institutional sites or high-value targets, but there has been an increase in the number of attacks against *easy-to-hit* targets.

In this scenario the *protection of buildings* from terrorist attacks has become one of the most important components of the defence strategy adopted firstly by USA after the 9/11 event and, in recent years, by European Countries. This is because *buildings* can represent one of the preferred targets of terrorists, being the central venue of a country's economic life and the embodiment of its wealth and culture.

Specifically, the focus of activities in this issue is on introducing technical methods and approaches that are applicable to building protection design, aiming to protect people and property by enforcing the security of the external part of the site, of the building perimeter and of its internal functions. This is of particular interest on a limited number of probable and destructive attack types, mainly those using various *explosive* devices or *CBR* agents.

Taking into account all these elements, the *objective of this book* was to outline methods and approaches for:

- identifying the principal components of building *risk*;
- characterizing the building *threats* for the case of *explosive* or *CBR* weapons;
- highlighting the building *criticalities* that can be exploited as *vulnerabilities* for a terrorist attack with the selected weapons;
- assessing the building *risk* level for different considered cases in a wide geographical area, ranking, at the end of the analysis, the risks according to their relevance;
- reducing building risk levels by introducing *countermeasures* and manipulating the three risk components, in particular the *vulnerabilities*.

The fundamental hypothesis underlying this work was that an *Assessment Team* - a group of professionals including engineers, architects, risk managers, CBR advisers and other technical experts - is involved in this *risk assessment process* to ensure that the obtained results are met with *sound* protective measures that will increase the capability of the building to resist potential terrorist attacks.

In *Section* 2 of this book, with the aim to introduce a robust statistical characterization for terrorist attacks to buildings as the base of this study, a wide analysis on 20 years of terrorist attacks was carried out starting from the information made available by Global Terrorism Database. As a fundamental result of the analysis, it was confirmed that a greater number of attacks were, in the last years, oriented against *simple* public and private buildings, facilities and areas to target and kill individuals, typically civilians. In recent years, such kind of *simple* targets has been denoted in the literature as *soft targets*, in opposition of the term *hard targets* related to government, military, police and intelligence sites. In the work a specific definition of *soft target* and *hard target* was proposed with reference to Global Terrorism Database fields of information and a statistical comparison between the two attack categories, *soft targets* and *hard targets*, in the period 2000-2019 was described in depth. Furthermore, an analysis on the detailed target items, such as *houses, apartments, marketplace, schools, universities, restaurant, theatres* and other *specific items* was considered and statistically analysed. Furthermore, the issue of *building terrorist attacks* was faced, characterizing 20 years of building attacks in term of weapon used, focusing in particular the investigation on *explosive* an *CBR agent* weapons.

In *Section 3*, an analysis of the different institutional approaches used for the risk definition and evaluation in the field of disaster management was illustrated. In particular, the approaches proposed for the risk definitions by United States of America, by United Nations and finally by European Union were considered. The comparison of the three different proposed approaches provided important evidence of different practical application that makes the values of the *evaluated level of risk* conceptually different in the Institutions considered. These evidences were used to define the specific models for *threat, vulnerability, exposure* and *risk* proposed in the book.

In *Section 4*, the essential features of an original *Threat Assessment Method* for sites and buildings for the case of terrorist attacks with *explosive/CBR* agents was detailed described. The proposed method, based on an approach in *six steps*, provides a structured guide useful to the Assessment Team. 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 ranking 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. Furthermore, a **Threat Probability Scale of 7 levels** was discussed for the Assessment Team support and the theme of Unmanned Aircraft System, commonly referred to as '*drone*', was briefly introduced because their security concerns, since they could be used as a powerful *weapon vector* by terrorists.

In *Section 5* an original *Building Vulnerability Assessment Method* was illustrated in detail. The method proposed for the vulnerability assessment provides an analytical procedure based on *76 different items* organized in *9 topics* for identifying the building *criticalities*. These criticalities were detailed in **Appendix A** of the book and a **software prototype was developed** to support the

Assessment Team in the *criticality analysis*. Finally, the described method provides to the Assessment Team a **Vulnerability Scale of 7 levels** to specify, for the building and the threats analyzed, the different levels of *vulnerability*.

In *Section 6* the issue of *Building Exposure Assessment* was faced: the assessment proposed for the building *exposure* was focused on *direct* and *tangible* effects on *assets* and the characterization of the exposure of a building was divided into two asset categories: *population capacity* and *economic values*. Three different **Exposure Scales of 7 levels** were introduced and discussed to provide a further practical tools for the risk assessment stage.

In *Section 7* an original *Risk Assessment Method* for buildings was described: the proposed method can be adopted in whatever operating scenario, and in presence of whatever threat discussed in this book, and can provide a sufficiently accurate estimate of the risk in a simple fashion based on **Scale of 7 levels** for *threat*, *vulnerability* and *exposure* introduced in the previous sections. The method described allows to manage the different kinds of risk related to the threats analyzed and the results useful for identifying a **ranking of risks** for different buildings, and for prioritizing actions and investments in preparedness, protection and resilience of the buildings.

In *Section 8* a detailed analysis and several results of different *Case Studies* were provided, applying the fundamental *methods* proposed in the work. In particular, the attention was focused on the application of the *threat* assessment method and the *vulnerability* assessment method discussed in Section 4 and 5, respectively. For the *threat assessment* three different existing buildings were taken into account and three different threats were applied to the buildings in the analysis. For the *vulnerability assessment* the method was applied to a single case study, a *commercial center*, in order to show the different aspect to consider in the assessment when different *threats* are applied. The results of considered Case Studies show the practical application of the original methods described in the book, providing real example of threat and vulnerability assessments.

As far as possible future developments on the issue are concerned, several aspects can be listed for further studies:

- ✓ to make the activities of the risk Assessment Team more efficient, the software prototype proposed in Section 5 for the Building Criticality Analysis could be extended to all the methods described in the book, in particular for BTAM, BVAM and BRAM. This type of activity could be carried out by software developers in cooperation with risk assessment experts;
- ✓ the application of the introduced methods could be presented to the institutional intelligence and law enforcing authorities for an experimental application campaign on domestic buildings, with the aim to refine on the field the parameters of the methods and the software prototype;
- ✓ in the application of BTAM parameters of Section 4, more sophisticated mathematical approaches could be studied and proposed for evaluating the sub-indexes for Attractiveness and Terrorist Capabilities, for example applying more sophisticated statistical indexes;
- ✓ in the methods discussed in this book, it could be explicitly introduced and analyzed the UAS based threats, collecting the wide technical literature already available on weaponized *drones* and characterizing the main types of UAS attack with explosive/CBR agents against building. On this issue related to unmanned vehicles, it could be useful to analyze in depth also the

application of UAS for CBRN *reconnaissance* and, furthermore, the issue of the *countermeasure* systems able to detect, identify, track and/or intercept a single UAS or a potential 'swarm' attack that exploits multiple drones to accomplish a common objective;

- ✓ finally, an action at European Union level, in particular towards JRC researchers, could be started in order to present the results of the work on building risk assessment and provide, if applicable, a cooperation to the European researchers engaged in this field.

10 Appendix A: Building Criticality Analysis

In this Appendix the detailed description of the 9 *topics* and the 76 *items* introduced in Sect.5 and summarized in tab.5.12 is provided. In particular, for each item a specific *Criticality Scale* is presented for the evaluation of weaknesses, deficiencies and fragilities in the building. The Assessment Team, with the skill and adequate knowledge of the main security issues discussed in depth in USA and EU reference documents [FEM3, EuC4], should adopt this approach as a reference tool to highlight the criticalities of the building under evaluation. The results of this characterization constitute a fundamental input for the Step 2 of the method provided in Sect.5 for the Building Vulnerability Assessment.

10.1 Site characteristics

The intent for this first topic is evaluate in depth the *site characteristics* around the building finding possible criticalities.

10.1.1 Surrounding structures/facilities

Analyse the adjacent land used immediately outside the perimeter (for example 0,3 km of ray) of the building/site taking into account the note reported below for Critical Infrastructures.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.1 - *Are there any major/critical infrastructures surrounding the building?*

1.1 - Criticality Scale (Surrounding structures/facilities)		Weight
Extreme	Many significant critical infrastructures are adjacent to the main building considered	27
Elevated	Some significant critical infrastructures are adjacent to the main building considered	9
Marginal	No major critical infrastructure and only infrastructures of secondary importance are adjacent to the main building considered	3
Negligible	None significant infrastructure is adjacent to the main building considered	1
NA	Not Applicable: it is not possible give a relevant answer to the question	-

Examples of Critical Infrastructures [FEM3] that can be considered by the Assessment Team includes:

- *Telecommunications and ICT infrastructures*
- *Electric power systems*
- *Gas and oil facilities*
- *Banking and finance institutions*
- *Transportation networks*
- *Water supply systems*
- *Government services*
- *Emergency services*

The following facilities are not critical infrastructures, but have collateral damage potential to carefully consider in the analysis:

Agricultural facilities: chemical distribution, storage, and application sites; crop spraying services; farms and ranches; food processing, storage, and distribution facilities.

Commercial manufacturing/industrial facilities: apartment buildings; business/corporate centres; chemical plants; factories; fuel production, distribution, and storage facilities; hotels and convention centres; industrial plants; raw material production, distribution, and storage facilities; research facilities and laboratories; shipping, warehousing, transfer, and logistical centres.

Events and attractions: festivals and celebrations; open-air markets; parades; rallies, demonstrations, and marches; religious services; scenic tours; theme parks.

Health care system components: family planning clinics; health department offices; hospitals; radiological material and medical waste transportation, storage, and disposal; research facilities and laboratories, walk-in clinics.

Political or symbolically significant sites: embassies, consulates, landmarks, monuments, political party and special interest groups offices, religious sites.

Public/private institutions: academic institutions, cultural centres, libraries, museums, research facilities and laboratories, schools.

Recreation facilities: auditoriums, casinos, concert halls and pavilions, parks, restaurants and clubs (frequented by potential target populations), sports arenas, stadiums, theatres, malls, and special interest group facilities; note congestion date and times for shopping centres.

10.1.2 Terrain characteristics

Analyse the terrain place that characterizes the building is fundamental: depressions or low areas can trap heavy vapours, inhibit natural decontamination by prevailing winds, and reduce the effectiveness of in-place sheltering.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.2 - *Does the terrain place the building in a depression or low area?*

1.2 - Criticality Scale (Terrain characteristics)		Weight
Extreme	A very deep depression characterizes the terrain where the structure is built	27
Elevated	A significant depression characterizes the terrain where the structure is built	9
Marginal	A moderate depression characterizes the terrain where the structure is built	3
Negligible	None significant depression characterizes the terrain where the structure is built	1
NA	Not Applicable: it is not possible give a relevant answer to the question	-

10.1.3 Curb Lane Parking characteristics

The distance from the building to the nearest curb lane parking could be another criticality. Where distance from the building to the nearest curb provides insufficient setback, it could be useful to restrict parking in the curb lane. Setback is common terminology for the distance between a building and its associated roadway or parking. It is analogous to stand-off between a vehicle bomb and the building. The benefit per meter of increased stand-off between a potential vehicle bomb and a building is very high when close to a building.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.3 - *Is curb lane parking place for uncontrolled parked vehicles unacceptably close to the building?*

1.3 - Criticality Scale (Curb Lane Parking characteristics)		Weight
Extreme	A too short distance characterizes the curb lane parking place close to the building	27
Elevated	A relatively short distance characterizes the curb lane parking place close to the building	9
Marginal	A significant distance characterizes the curb place parking lane close to the building	3
Negligible	An adequate distance characterizes the curb place parking lane close to the building	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.1.4 Perimeter barriers for pedestrian access

The intent of the analysis of this item is to guarantee a perimeter defence and to channel pedestrian traffic onto a site through known access control points and paths. The intent is to have a well-protected single visitor entrance.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.4 - *Is a perimeter fence or other types of barrier controls in place for the pedestrian access?*

1.4 - Criticality Scale (Perimeter fence and barriers for pedestrian)		Weight
Extreme	None perimeter fence or barrier is implemented for the building	27
Elevated	Insufficient perimeter fences or barriers are implemented for the building	9
Marginal	Significant perimeter fences or barriers are implemented for the building	3
Negligible	Well-designed perimeter fences or barriers are implemented for the building	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.1.5 Vehicles access points

The goal for the vehicles access is to have at least two access points, one for passenger vehicles and one for delivery trucks due to the different procedures needed for each. Having two access points also helps if one of the access points becomes unusable, then traffic can be routed through the other access point.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.5 - *Are the vehicles access points to the site or building well designed?*

1.5 - Criticality Scale (Vehicles access points)		Weight
Extreme	Exist only a single and narrow vehicle access point for passengers and delivery trunk	27
Elevated	Only a single, very wide, vehicle access point for passengers and delivery trunk	9
Marginal	Two different vehicle access points, for passengers and for delivery trunk, respectively	3
Negligible	More than two vehicle access points	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.1.6 Pedestrian Access Control

Another fundamental item is related to the possible pedestrian access control. Such kind of inspection should occur preferably at the site perimeter with the ability to regulate the flow of people. Control can be applied on-site parking with identification checks, security personnel, and access control systems.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.6 - *Is there pedestrian access control at the perimeter of the site or of the building?*

1.6 - Criticality Scale (Pedestrian Access Control)		Weight
Extreme	It does not exist any kind of pedestrian access control both at the external border and at the building perimeter	27
Elevated	Only a infrequent sample check access control on pedestrian is applied by security at the perimeter	9
Marginal	A pedestrian access control at the site perimeter is frequently applied by security	3
Negligible	A pedestrian access control at the site perimeter is carefully applied by security	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.1.7 Private Vehicle Access Control

Another fundamental item is related to the possible private vehicle access control. Such kind of inspection should occur preferably at the site perimeter with the ability to regulate the flow of vehicles

one at a time. Control can be applied on-site parking with identification checks, security personnel, and access control systems.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.7 - *Is there private vehicle access control at the perimeter of the site or of the building?*

1.7 - Criticality Scale (Private Vehicle Access Control)		Weight
Extreme	It does not exist any kind of vehicle access control both at the external border and at the building perimeter	27
Elevated	Only a infrequent sample check access control on private vehicles is applied by security at the site perimeter	9
Marginal	A private vehicle access control is frequently applied at the site perimeter by security	3
Negligible	A private vehicle access control is carefully applied at the site perimeter by security	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.1.8 Shipping/Delivery Vehicle Access Control

Another fundamental item is related to the possible shipping/delivery vehicle access control at the building entry. Such kind of control should occur preferably at the external site perimeter with the ability to regulate the flow of vehicles one at a time. Control can be applied before entering in the building area, on external parking for example, distant from the perimeter, with identification checks, security personnel, and access control systems.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.8 - *Is there access control of shipping and delivery vehicles at the building entrance?*

1.8 - Criticality Scale (Shipping/Delivery Vehicle Access Control)		Weight
Extreme	It does not exist any kind of shipping/delivery vehicle access control both at the external border and at the building perimeter	27
Elevated	Access control on shipping and delivery vehicles is rarely applied to the perimeter of the site	9
Marginal	A control of access to the site perimeter of shipping and delivery vehicles is applied frequently	3
Negligible	Access control of shipping/delivery vehicles at the site external perimeter is carefully applied	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.1.9 Alternative Potential Access

The analysis must evaluate the alternative potential site access, for example through utility tunnels, corridors, manholes, storm water runoff culverts, etc. In general, must be ensured the security even for these alternative access points.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.9 - *Is there any exploitable potential access to the building through utility paths or water runoff?*

1.9 - Criticality Scale (Alternative Potential Access)		Weight
Extreme	Many alternative accesses to the building are accessible without any security measure	27
Elevated	Only one alternative access to the building is accessible without any security measure	9
Marginal	The alternative accesses to the building are not easily accessible and periodically verified	3
Negligible	All the alternative accesses to the building are secured with specific measures	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.1.10 Anti-ram devices

Anti-ram barriers are protection measures against attack of criminals with the typical use of vehicle driving high speed into the direction of the building. Anti-ram protection may be provided by adequately designed: bollards, street furniture, sculpture, landscaping, walls, and fences. The anti-ram protection must be able to stop the threat vehicle size (weight) at the speed attainable by that vehicle at impact.

Passive anti-ram and barriers include bollards, walls, hardened fences (steel cable interlaced), trenches, ponds/basins, concrete planters, street furniture, plantings, trees, sculptures, and fountains. Active barriers include popup bollards, swing arm gates, and rotating plates and drums, etc.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.10 - *What are the existing types of vehicle anti-ram devices for the building?*

1.10 - Criticality Scale (Anti-ram devices)		Weight
Extreme	All the paths for accessing the building with a vehicle are without anti-ram devices	27
Elevated	The paths for accessing the building with a vehicle are with not sufficient anti-ram devices	9
Marginal	Some anti-ram devices are on the paths for accessing to the building	3
Negligible	Anti-ram devices well protect the paths for accessing the building with a vehicle	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.1.11 Site lighting in the external area

Security protection can be better successfully addressed through adequate lighting. The type and design of lighting, including illumination levels, could be a critical item. It is fundamental that the site lighting is well coordinated with the CCTV system.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.11 - *Is the site lighting adequate from a security perspective in roadway access and parking areas?*

1.11 - Criticality Scale (Site lighting in the external area)		Weight
Extreme	The external site lighting is completely inadequate	27
Elevated	The external site lighting is incomplete and not sufficient for some areas	9
Marginal	The external site lighting is existing and periodically maintained	3
Negligible	The external site lighting is adequate, well designed and punctually maintained	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.1.12 External connection to the building

On the site, the building and in-ground infrastructure can be physically connected by passageways, subways, tunnels, connectors stairways, entrance/exit portals, ventilation shafts, and by direct utility connections from utility lifelines.

These physical connections can have unwarranted security impacts from events in the in-ground infrastructure that then affect the building, such as explosive blast, CBR release and access control that then enter the building being assessed. An event in the in-ground or out-ground infrastructure can interact with the building through the soil and water table, in addition to the physical connections. The physical connections could be structurally connected, seismically isolated, or some other method to tie the external infrastructure to the building.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 1.12 - *Is any of the nearby in-ground and out-ground infrastructures directly connected to the building?*

1.12 - Criticality Scale (External connection to the building)		Weight
Extreme	Many external in-ground and out-ground infrastructures are directly connected to the building and unprotected	27
Elevated	Some external in-ground and out-ground infrastructures are directly connected to the building and poorly protected	9
Marginal	The in-ground and out-ground infrastructures directly connected to the building are sufficiently protected	3
Negligible	The in-ground and out-ground infrastructures directly connected to the building are well designed and adequately protected or they do not exist at all	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.2 Architecture

The intent for this second *topic* is to carefully evaluate the *architecture* of the building, finding possible criticalities.

10.2.1 Mixed tenant building

It should be assured to separate high-risk tenants from low-risk tenants and from publicly accessible areas. Mixed uses may be accommodated through such means as separating entryways, controlling access, and hardening shared partitions, as well as through special security operational countermeasures.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 2.1 - *Is it a mixed-tenant building?*

2.1 - Criticality Scale (Mixed tenant building)		Weight
Extreme	High-risk tenants are not separated from low-risk tenants and from publicly accessible areas	27
Elevated	High-risk tenants have been in only few components separated from low-risk tenants and from publicly accessible areas	9
Marginal	High-risk tenants have been in many components separated from low-risk tenants and from publicly accessible areas	3
Negligible	High-risk tenants have been completely separated from low-risk tenants and from publicly accessible areas	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.2.2 Receptacles to hide explosive devices

The size of the trash receptacles and mailbox openings in the building and in the immediately external area should be restricted to prohibit insertion of packages. Street furniture, such as newspaper vending machines, should be kept sufficient distance (e.g. 10 meters) from the building, or brought inside to a secure area.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 2.2 - *Are there trash receptacles and mailboxes in close proximity to the building that can be used to hide explosive devices?*

2.2 - Criticality Scale (Receptacles to hide explosive devices)		Weight
Extreme	The number and the size of possible receptacles in the building and in the immediately external area is elevated and wide, respectively	27
Elevated	The size of various receptacles in the building and in the immediately external area is significant	9
Marginal	The size of possible receptacles in the building and in the immediately external area is very small	3
Negligible	The possible receptacles in the building and in the immediately external area have been substantially eliminated	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.2.3 Public and critical points in the building

In general, public points (i.e. public toilets, service spaces, access to stairs or elevators, queuing area before screening, etc.) into the building should be well separated from critical or non secure areas. Retail activities should be prohibited in non-secured areas. To mitigate the risk consider to verify the presence of separating entryways, controlling access, hardening shared partitions, and special security operational countermeasures.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 2.3 - *Are public toilets, service spaces, or access to stairs or elevators located in any non-secure areas, including the queuing area before screening at the public entrance?*

2.3 - Criticality Scale (Public and critical points in the building)		Weight
Extreme	Public and service spaces, or access to stairs or elevators located in the building are in most of the cases near to non-secure and critical areas	27
Elevated	Public and service spaces, or access to stairs or elevators located in the building are in some cases near to non-secure areas	9
Marginal	Public and service spaces, or access to stairs or elevators located in the building are moderately distant from any non-secure areas	3
Negligible	Public and service spaces, or access to stairs or elevators located in the building are very distant from any non-secure areas	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.2.4 Equipment for access control and screening

These include walk-through metal detectors, magnetic imaging equipment and x-ray devices, identification check, electronic access card and turnstiles.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 2.4 - *Do public and employee entrances include equipment for access control-screening and, in perspective, adequate space for possible future installation?*

2.4 - Criticality Scale (Equipment for access control and screening)		Weight
Extreme	Public and employee entrances does not include adequate access control-screening equipment and, in perspective, it's not available space for possible installation	27
Elevated	Public and employee entrances include a insufficient number of access control-screening equipment and, in perspective, it's available an insufficient space for possible new installation	9
Marginal	Public and employee entrances include a sufficient number of access control-screening equipment and, in perspective, it's available a sufficient space for possible future installation	3
Negligible	Public and employee entrances include an adequate number of access control-screening equipment and, in perspective, it's available an adequate space for possible new installation	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.2.5 Reinforced walls and doors

The important item of reinforced walls and doors has to be considered in particular for exterior entrances to the building or to access critical areas within the building, especially if blast hazard must be mitigated.

Typically, the postulated threat in designing entrance access control includes rifles, pistols, or shotguns: in this case the screening area should have bullet-resistance to protect security personnel and uninvolved bystanders. Glass, if present, should also be bullet-resistant.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 2.5 - *Are doors and walls along the line of security screening adequately reinforced?*

2.5 - Criticality Scale (Reinforced walls and doors)		Weight
Extreme	Doors and walls along the line of security screening result all non-reinforced	27
Elevated	Some doors and walls along the line of security screening result non-reinforced	9
Marginal	The majority of doors and walls along the line of security screening result adequately reinforced	3
Negligible	All the doors and walls along the line of security screening result adequately reinforced	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.2.6 Roof access control

Roof both for the strategic position and for many equipment there located represents, for many types of attacks, necessary preferred point. In particular, the air intakes, the HVAC equipment and the related filters could be a natural point of insertion for CBR agents into the building.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 2.6 - *Is roof access controlled and limited to authorized personnel by means of adequate mechanisms?*

2.6 - Criticality Scale (Roof access control)		Weight
Extreme	Roof access is not controlled and adequately limited to authorized personnel	27
Elevated	Roof access is poorly controlled and limited to authorized personnel by means of adequate mechanisms	9
Marginal	Roof access is sufficiently controlled and limited to authorized personnel by means of adequate mechanisms	3
Negligible	Roof access is strictly controlled and limited to authorized personnel by means of adequate mechanisms	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.2.7 Building critical assets

This item focuses on critical building components that include:

- Emergency generator including fuel systems, day tank, fire sprinkler, and water supply;
- Normal fuel storage;
- Main switchgear;
- Telephone distribution and main switchgear;
- Fire pumps;
- Building control centres;
- Uninterruptible Power Supply (UPS) systems controlling critical functions;
- Main refrigeration and ventilation systems if critical to building operation;
- Elevator machinery and controls;
- Shafts for stairs, elevators, and utilities;

- Critical distribution feeders for emergency power.

Evacuation and rescue actions require emergency systems to remain operational during a disaster and they should be located away from attack locations. Primary and backup systems should be physically separated to reduce the risk of both being impacted by a single incident.

Utility systems should be located at least 20 meters from front entrances and parking areas. One way to harden critical building systems and components is to enclose them within hardened walls, floors, and ceilings. Do not place them near high-risk areas where they can receive collateral damage.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 2.7 - *Are critical assets (people, activities, building systems and components) well separated from main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking? Are the critical building systems and components adequately hardened and controlled?*

2.7 - Criticality Scale (Building critical assets)		Weight
Extreme	Critical assets do not result well separated by high-risk area and the critical building systems and components are not adequately hardened and controlled	27
Elevated	Critical assets result only in a few cases separated by high-risk area and the critical building systems and components are poorly hardened and controlled	9
Marginal	Critical assets result sufficiently separated by high-risk areas and the critical building systems and components are sufficiently hardened and controlled	3
Negligible	Critical assets result well separated by high-risk areas and the critical building systems and components are adequately hardened and controlled	1
NA	Not Applicable: it is not possible give a relevant answer to the question	-

10.2.8 Separation of critical assets and loading docs/shipping areas

Loading docks should be designed to keep vehicles from driving into or parking under the building. If loading docks are in close proximity to critical equipment, consider hardening the equipment and service against blast. Consider a 20 meters separation distance in all directions.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 2.8 - *Are loading docks, receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances including electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.?*

2.8 - Criticality Scale (Separation of critical assets and loading docs/shipping areas)		Weight
Extreme	Loading docs/shipping areas do not result separated by critical assets	27
Elevated	Loading docs/shipping areas result in some cases near Critical assets	9
Marginal	Loading docs/shipping areas result sufficiently separated by critical assets	3
Negligible	Loading docs/shipping areas result well separated by critical assets	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.2.9 Mailroom space and equipment

Mailroom can be critical for a possible attack: for this reason, a screening activity in this space should be necessary. Screening of all deliveries to the building includes ordinary mail, commercial package delivery services, delivery of office supplies, etc.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 2.9 - *Have the mailroom adequate equipment and space available to examine incoming packages and for an explosive disposal container?*

2.9 - Criticality Scale (Mailroom space and equipment)		Weight
Extreme	The mailroom has not adequate equipment and space available to examine incoming packages	27
Elevated	The mailroom has old and malfunctioning equipment and few space available to examine incoming packages	9
Marginal	The mailroom has sufficient equipment and space available to examine incoming packages	3
Negligible	The mailroom has adequate equipment and space available to examine incoming packages	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.2.10 Debris generation limitation

When an explosive blast shatters a window, the blast wave enters the interior space, putting structural and non-structural building components under loads not considered in standard building design.

Mount all overhead utilities and other fixtures to minimize the likelihood that they will fall and injure building occupants.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 2.10 - *Are ceiling, internal walls, overhead utilities and lighting systems designed to remain in place without generate danger debris during hazard events?*

2.10 - Criticality Scale (Debris generation limitation)		Weight
Extreme	Ceiling, internal walls, overhead utilities and lighting systems are very poorly designed and they generate very danger debris	27
Elevated	Ceiling, internal walls, overhead utilities and lighting systems are not adequately designed and they can generate danger debris	9
Marginal	Ceiling, internal walls, overhead utilities and lighting systems are sufficiently robust to remain in place without generate danger debris	3
Negligible	Ceiling, internal walls, overhead utilities and lighting systems are well designed to remain in place without generate danger debris	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.3 Structural Systems

The intent for this third *topic* is to carefully evaluate the *type of construction, the structural components and systems* of the building, finding possible criticalities.

10.3.1 Construction characteristics

The analysis of the type of construction provides an indication of the robustness to abnormal loading and load reversals [FEM3]. A reinforced concrete moment-resisting frame provides greater ductility and redundancy than a flat-slab or flat-plate construction. The ductility of steel frame with metal deck depends on the connection details and pre-tensioned or post-tensioned construction provides little capacity for abnormal loading patterns and load reversals. The resistance of load-bearing wall structures varies to a great extent, depending on whether the walls are reinforced or un-reinforced.

As a rule, if the building is designed for ductile behaviour, such as seismic, blast or progressive collapse, it is expected to behave better than non-ductile design.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 3.1 - *What type of construction? What type of concrete and reinforcing steel? What type of steel? What type of foundation?*

3.1 - Criticality Scale (Construction characteristics)		Weight
Extreme	The type of construction, concrete and reinforcing steel quality eventually adopted are very poorly designed and not implemented for resisting to explosive blast attacks	27
Elevated	The type of construction, concrete and reinforcing steel quality eventually adopted are not adequately designed and not implemented for resisting significant explosive blast attacks	9
Marginal	The type of construction, concrete and reinforcing steel quality eventually adopted are sufficiently well designed and implemented for resisting significant explosive blast attacks	3
Negligible	The type of construction, concrete and reinforcing steel quality eventually adopted are very well designed and implemented for resisting big explosive blast attacks	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.3.2 Structural and Non-Structural Components

Adequate building structural and non-structural components are essential to mitigating injury and damage in case of attacks.

Primary Structural Elements provide the essential parts of the building's resistance to catastrophic blast loads and progressive collapse. These include columns, girders, roof beams, load-bearing walls, and the main lateral resistance system.

Secondary Structural Elements consist of all other load-bearing members, such as floor beams, slabs, etc.

Primary Non-Structural Elements consist of elements (including their attachments) that are essential for life safety systems or elements that can cause substantial injury if failure occurs, including ceilings or heavy suspended mechanical units.

Secondary Non-Structural Elements consist of all elements not covered in primary non-structural elements, such as partitions, furniture, and light fixtures.

There are two types of structural/architectural components that are of particular concern:

- a separate structural component that is very dominant within the building (e.g., long span auditorium covers, water tanks, transmission towers, etc.). Most of such massive components will exceed a fraction of the weight of floor immediately attached to them. Auditoriums-within a building need special attention, especially if they include a usable floor space on top of them;
- structural/architectural components that are not part of the main structural system (e.g., massive awnings, massive signs or flagpoles). When these are damaged the failure mechanism can impact the structural system.

An explosive blast that affects these components can cause a disproportionate failure in the building. For this reason, ductile connections are preferred to limit failure.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 3.2 - *Are any of structural/non-structural components vulnerable either directly or indirectly to explosive blast?*

3.2 - Criticality Scale (Structural and Non-Structural Components)		Weight
Extreme	Structural and non-structural components are very poorly designed and implemented for resisting to explosive blast attacks	27
Elevated	Structural and non-structural components are not in many cases adequately designed and implemented for resisting to explosive blast attacks	9
Marginal	Structural and non-structural components are sufficiently well designed and implemented for resisting to explosive blast attacks	3
Negligible	Structural and non-structural components are very well designed and implemented for resisting to explosive blast attacks	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.3.3 Progressive collapse

Design the building to mitigate progressive collapse is a very relevant independent analysis necessary to determine a system's ability to resist structural collapse upon the loss of a major structural element or the system's ability to resist the loss of a major structural element.

Designers that face this issue may apply static and/or dynamic methods of analysis to meet this requirement and ultimate load capacities may be assumed in the analyses.

Combine structural upgrades for retrofits to existing buildings, such as seismic and progressive collapse, into a single project due to the economic synergies and other cross benefits. Existing facilities may be retrofitted to withstand the design level threat or to accept the loss of a column for one floor above grade at the building perimeter without progressive collapse. Note that collapse of floors or roof must not be permitted.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 3.3 - *Is the building capable of sustaining the removal of a column for one floor above grade at the building perimeter without progressive collapse?*

3.3 - Criticality Scale (Progressive collapse)		Weight
Extreme	The building is not designed for resist to removal of columns without progressive collapse	27
Elevated	The building is poorly designed for adequately resist to removal of columns without progressive collapse	9
Marginal	The building is designed for sufficiently resist to removal of columns without progressive collapse	3
Negligible	The building is designed for very well resist to removal of columns without progressive collapse	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.3.4 Floor of loading dock

It is fundamental to design the floor of the loading dock for blast resistance especially if the area below is occupied or contains critical areas/utilities.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 3.4 - *Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?*

3.4 - Criticality Scale (Floor of loading dock)		Weight
Extreme	The loading dock are very poorly designed and implemented to limit damage to adjacent areas in case of attacks	27
Elevated	The loading dock are in many cases inadequately designed and implemented to limit damage to adjacent areas in case of attacks	9
Marginal	The loading dock are sufficiently well designed and implemented to limit damage to adjacent areas in case of attacks	3
Negligible	The loading dock are very well designed and implemented to limit damage to adjacent areas in case of attacks	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.3.5 Mailroom explosion mitigation

Where mailrooms and unscreened retail spaces are located in occupied areas or adjacent to critical utilities, walls, ceilings, and floors, they should be blast- and fragment- resistant.

Methods to facilitate the venting of explosive forces and gases from the interior spaces to the outside of the structure may include blow-out panels and window system designs that provide protection from blast pressure applied to the outside, but that readily fail and vent if exposed to blast pressure on the inside.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 3.5 - *Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?*

3.5 - Criticality Scale (Mailroom explosion mitigation)		Weight
Extreme	Mailrooms and unscreened retail spaces are not designed to mitigate the effects of an explosive blast event	27
Elevated	Mailrooms and unscreened retail spaces are poorly designed to mitigate the effects of an explosive blast event	9
Marginal	Mailrooms and unscreened retail spaces are sufficiently well designed to mitigate the effects of an explosive blast event	3
Negligible	Mailrooms and unscreened retail spaces are well designed to mitigate the effects of an explosive blast event	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.3.6 In-ground structural systems

Structural systems of underground infrastructures include reinforced concrete tunnels, steel tunnels, and steel or reinforced concrete frames. Some modern construction includes pre-stressed or post-tensioned constructions.

Some older underground infrastructures were built using masonry, brick or limestone walls or abutments. Older masonry brick construction can be less ductile than modern reinforced concrete or steel construction.

When the infrastructure and the building are in close proximity, or when they are rigidly linked, the failure of one system might initiate the failure of the other system.

Similarly, a failure in the physical connection between the in-ground infrastructure and the building might cause failure in both the building and in-ground infrastructures

The part of the structure closest to the in-ground infrastructure is the most vulnerable. It should be hardened so that any local failure would not initiate progressive collapse in the rest of the building. Aside from hardening, other measures available are increased ductility, increased setback, or better access control.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 3.6 - *Would failure of part of the in-ground infrastructure affect the structural system of the building?*

3.6 - Criticality Scale (In-ground structural systems)		Weight
Extreme	In-ground infrastructure is poorly designed and implemented to resist to structural failure	27
Elevated	In-ground infrastructure is not in some aspects sufficiently well designed and implemented to resist to structural failure	9
Marginal	In-ground infrastructure is sufficiently well designed and implemented to resist to structural failure	3
Negligible	In-ground infrastructure is well designed and implemented to resist to structural failure	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.3.7 Underground water presence

Presence of underground water can have negative and unexpected effects on underground infrastructure and nearby buildings. Attenuation of blast pressures in wet soil is much lower than that in dry soil. Also, blast pressures can reflect from the surface of the underground water table, creating an undesirable vertically propagating blast wave that will hit the building from the bottom, causing uplift of part or the whole building (an unexpected loading direction).

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 3.7 – *Does the presence of underground water under the building generate instability and unacceptable flooding?*

3.7 - Criticality Scale (Underground water presence)		Weight
Extreme	The presence of underground water under the building has been very poorly managed and it is very likely the occurrence of instability phenomena and of unacceptable flooding	27
Elevated	The presence of underground water under the building has been insufficiently managed and it is not to be excluded the presence of instability phenomena and of flooding	9
Marginal	The presence of underground water under the building has been sufficiently well managed and it's very unlikely the presence of instability phenomena and of flooding	3
Negligible	The presence of underground water under the building has been correctly managed and does not generate instability and flooding	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.4 Building Envelope

The intent for this fourth *topic* is to carefully evaluate the *building envelope,* finding possible criticalities.

10.4.1 Envelope protection level

The performance of the building envelope varies to a great extent on the materials. Different construction includes brick or stone with block back-up, steel stud walls, pre-cast panels, curtain wall with glass, stone, or metal panel elements.

Shear walls that are essential to the lateral and vertical load bearing system and that also function as exterior walls should be considered primary structures and should resist the actual blast loads predicted from the threats specified. Where exterior walls are not designed for the full design loads, special consideration shall be given to construction types that reduce the potential for injury.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 4.1 - *What is the designed or estimated protection level of the building envelope against a possible high magnitude explosive threat?*

4.1 - Criticality Scale (Envelope protection level)		Weight
Extreme	The building envelope has not been well designed and implemented against a possible high magnitude blast	27
Elevated	The building envelope has not been in some part well designed and implemented against a possible high magnitude blast	9
Marginal	The building envelope has been sufficiently well designed and implemented against a possible high magnitude blast	3
Negligible	The building envelope has been well designed and implemented against a possible high magnitude blast	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.4.2 Envelope fenestration balance

The envelope fenestration is another important aspect to be considered. The envelope percent fenestration is typically a balance between protection level, cost, the architectural look of the building within its surroundings, and building codes. One goal could be to keep fenestration to below, for example, 40% of the building envelope vertical surface area, but the process must balance differing requirements. A blast engineer may prefer no windows, an architect may favour window curtain walls. Building codes can require specific fenestration percentage of floor area, fire codes can require a prescribed window opening area if the window is a designated escape route, and so on for other application.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 4.2 - *Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.)*

4.2 - Criticality Scale (Envelope fenestration balance)		Weight
Extreme	The window system is not adequately designed and balanced in all the building envelope to mitigate the hazardous effects of flying glazing following an explosive event	27
Elevated	The window system is, in some parts, insufficiently well designed to mitigate the hazardous effects of flying glazing following an explosive event	9
Marginal	The window system is sufficiently well designed to mitigate the hazardous effects of flying glazing following an explosive event	3
Negligible	The window system is very well designed to mitigate the hazardous effects of flying glazing following an explosive event	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.4.3 Glazing characteristics

The blast effects on glass and glazing have to be carefully considered. The performance of the window glass will depend on the used materials. Glazing may be single pane or double pane, monolithic or laminated, annealed, heat strengthened or fully tempered.

Glass-clad polycarbonate or laminated polycarbonate are two types of usable glazing material. If windows are upgraded to bullet-resistant, burglar-resistant, or forced entry- resistant, then ensure that doors, ceilings, and floors, as applicable, can resist the same for the areas of concern.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 4.3 – *Are the glazing of the building secure in case of blast?*

4.3 - Criticality Scale (Glazing characteristics)		Weight
Extreme	The glazing of the buildings are poorly designed and completely inadequate implemented to be secure in case of blast	27
Elevated	The glazing of the buildings are in many cases insufficiently implemented to be secure in case of blast	9
Marginal	The glazing of the buildings are sufficiently well designed and implemented to be secure in case of blast	3
Negligible	The glazing of the buildings are well designed and implemented to be secure in case of blast	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.4.4 High external pressure resistance

As general requirement, a building has to resist at a certain level of external pressure. The pressure could be produced, for example, by a very high wind or a blast situation.

At the same time, seismic gaps in the building permit independent lateral movement between the wall and the structure. This gap might not be adequate for high pressures, such as very high winds or

blast situations. In fact, seismic gaps need careful detailing so as to not cause loss of wall support during dynamic blast situations that stress the flexibility of the wall system.

The wind speed/wind pressure used to design a building could be used to indicate the adequacy of the components of the building envelope during a blast event.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 4.4 – *Is the building designed to correctly resist to high external pressure (as for the case of blast)?*

4.4 - Criticality Scale (High external pressure resistance)		Weight
Extreme	The building is not designed and implemented to adequately resist to high external pressure	27
Elevated	The building is in many aspects insufficiently implemented to correctly resist to high external pressure	9
Marginal	The building is sufficiently well designed and implemented to correctly resist to high external pressure	3
Negligible	The building is well designed and implemented to correctly resist to high external pressure	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.4.5 Envelope and window glazing external condition

Window, glazing, and building envelope design information is sometimes not well coordinated between architects and structural engineers for assessment of explosive blast response. During the interview process, a review of problems (leaks, glass falling out, loss of seal between double pane glass, window operating difficulties, etc.) and retrofits undertaken to overcome these problems can provide valuable assessment information.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 4.5 - *What are the current conditions of windows and of the rest of the envelope (cladding, curtain walls, veneer, ...)?*

4.5 - Criticality Scale (Envelope and window glazing external condition)		Weight
Extreme	Current conditions of the windows and of the rest of the envelope (cladding, curtain walls, veneer) are completely inadequate and it does not exist an adequate maintenance activity	27
Elevated	Current conditions of the windows and of the rest of the envelope (cladding, curtain walls, veneer) are, in many cases, inadequate and it does not exist a periodic maintenance activity	9
Marginal	Current conditions of the windows and of the rest of the envelope (cladding, curtain walls, veneer) are sufficiently adequate and it exist a periodic maintenance activity	3
Negligible	Current conditions of the windows and of the rest of the envelope (cladding, curtain walls, veneer) are adequate and it exist a punctual maintenance activity	1
NA	Not Applicable: it is not possible give a relevant answer to the question	-

10.5 Utility systems and internal distribution infrastructures

The intent for this fifth *topic* is to evaluate the *essential services provided by the utility operators/systems* for the building and the *internal infrastructures and systems distributing the services*, finding possible criticalities.

10.5.1 Domestic water service

Domestic water service is fundamental for any type of building. Furthermore, domestic water results critical for continued building operation during an emergency. While bottled water can satisfy requirements for drinking water and minimal sanitation, domestic water meets many other needs – flushing toilets, building heating and cooling system operation, cooling of emergency generators, humidification, etc.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 5.1 - *What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank)? Is the domestic water service reliable and certified for the water quality? Is there a secure and sufficient alternate drinking water supply?*

5.1 - Criticality Scale (Domestic water service)		Weight
Extreme	The source of domestic water is not sufficiently reliable and quality certified, there is an insufficient source of alternate drinking water for emergency	27
Elevated	The source of domestic water is not in some cases sufficiently reliable and quality certified, there is a often insufficient source of alternate drinking water for emergency	9
Marginal	The source of domestic water is sufficiently reliable and quality certified, there is a sufficient and secure source of alternate drinking water for emergency	3
Negligible	The source of domestic water is reliable and quality certified, there is a secure and sufficiently adequate alternate drinking water supply for emergency	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.5.2 Security of water entry points

In general, it is fundamental that the water entering points at the building are secure.

Verify the security of the entry points and that only authorized personnel have access to the water supply and its components.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 5.2 - *Are the entry points for the water supply in a secure location and managed in a secure manner?*

5.2 - Criticality Scale (Security of water entry points)		Weight
Extreme	Entry points for the water supply are not in a secure location and the management of the water systems is completely inadequate	27
Elevated	Entry points for the water supply are not in a sufficiently secure location and managed in a sufficiently secure manner	9
Marginal	Entry points for the water supply are located in a sufficiently secure location and managed in a sufficiently secure manner	3
Negligible	Entry points for the water supply are located in a secure location and managed in a secure manner	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.5.3 Water for the fire suppression system

The fire suppression system water may be supplied from the domestic water or it may have a separate source, separate storage, or non-potable alternate sources.

For a site with multiple buildings, the concern is that the supply should be adequate to fight the worst-case situation that can occur. Standpipes, water supply control valves, and other system components should be secure or supervised. The incoming fire protection water line should be encased, buried, or located at least 20 meters from high-risk areas. The interior mains should be looped and sectionalized. Collocating fire water pumps puts them at risk for a single incident to disable the fire suppression system.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 5.3 - *Is the source and the distribution system of water for the fire suppression service adequate to manage incendiary events?*

5.3 - Criticality Scale (Water for the fire suppression system)		Weight
Extreme	The source and the distribution system of water for the fire suppression is completely insufficient to manage incendiary events	27
Elevated	The source and the distribution system of water for the fire suppression is insufficiently to manage very wide incendiary events	9
Marginal	The source and the distribution system of water for the fire suppression is sufficiently adequate to manage incendiary events	3
Negligible	The source and the distribution system of water for the fire suppression is well adequate to manage very wide incendiary events	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.5.4 Sewer System

Sanitary and storm water sewers should be protected from unauthorized access. The main concerns are backup or flooding into the building, causing a health risk, shorting out electrical equipment, and loss of building use.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 5.4 - *Are sewer systems well designed, implemented and protected?*

5.4 - Criticality Scale (Sewer System)		Weight
Extreme	The sewer systems do not result well designed, implemented and protected	27
Elevated	The sewer systems do not result in some components well designed, implemented and protected	9
Marginal	The sewer systems result sufficiently well designed, implemented and protected	3
Negligible	The sewer systems result well designed, implemented and protected	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.5.5 Fuel storage for continuity operations

Fuel supplies make the building resilient for critical operation. Typically, natural gas, propane, or fuel oil is required for continued operation.

Fuel storage protection is essential for continued operation. Main fuel storage should be located away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals).

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 5.5 – *Is an adequate quantity of fuel stored at the building? How is it stored? How is it secured?*

5.5 - Criticality Scale (Fuel storage for continuity operations)		Weight
Extreme	No fuel is stored at the building for continuity operations	27
Elevated	An insufficient quantity of fuel is stored at the building, not sufficiently distant from risk areas and in an insufficient secure manner	9
Marginal	A sufficient quantity of fuel is stored at the building, sufficiently distant from risk areas and in a relatively secure manner	3
Negligible	An adequate quantity of fuel is stored at the building, away from risk areas and in a secure manner	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.5.6 Electrical service redundancy

Utilities are the general source unless co-generation or a private energy provider is available.

The utility may have only one source of power from a single substation. There may be only single feeders from the main substation.

Besides installed generators to supply emergency power, portable generators or rental generators available under emergency contract can be quickly connected to a building with an exterior quick disconnect already installed.

Testing under actual loading and operational conditions ensures the critical systems requiring emergency power receive it with a high assurance of reliability.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 5.6 - *Is there a redundant and reliable electrical service source?*

5.6 - Criticality Scale (Electrical service redundancy)		Weight
Extreme	It is not available a redundant electrical service source in the building	27
Elevated	A redundant but insufficient electrical service source is available. The service is not adequately maintained	9
Marginal	A redundant and sufficiently reliable electrical service source is available and periodically maintained	3
Negligible	A redundant and reliable electrical service source is available and maintained in the building	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.5.7 Security of electrical entry points

Electrical supply at one location creates a vulnerable situation unless an alternate source is available. Typically, the service entrance is a locked room, inaccessible to the public.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 5.7 - *Is the incoming electric service to the building well designed and secure?*

5.7 - Criticality Scale (Security of electrical entry points)		Weight
Extreme	The incoming electric service to the building is not well designed and is insecure	27
Elevated	The incoming electric service to the building is not adequately well designed and is easily accessible even by unauthorized people	9
Marginal	The incoming electric service to the building is sufficiently well designed, is secure and accessible only by authorized operators	3
Negligible	The incoming electric service to the building is well designed, is secure and accessible only by authorized operators	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.5.8 ICT services

ICT services, internet access, telephony systems, video conference services, data transfer and storage are nowadays essential for any activity. It is fundamental to evaluate possible criticalities at macro-level for the ICT services and internal networks. Typically, in a building the communication ducts or other conduits are widely available and spread.

Secure locations of communications wiring entry to the site or building are required. At the same time, secure location for internal Servers/Firewalls/Data Storage facilities are fundamental. The security must be applied both to physical and logical form to avoid unauthorized access to the network and to the equipment.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 5.8 - *By what means does the main telephone and data communications interface the building? Are there multiple or redundant locations for the telephone and digital communication services? Are these locations secure and not accessible by unauthorized people? Is the provided data service secure?*

5.8 - Criticality Scale (ICT services)		Weight
Extreme	The ICT equipment locations an digital services are not secure and well managed	27
Elevated	The ICT equipment locations are not sufficiently secure and well managed. These locations could be easily accessed by unauthorized people. Not in all cases the digital services are sufficiently secure and reliable	9
Marginal	The ICT equipment locations are sufficiently secure and well managed. These locations are not accessible by unauthorized people. All the digital services are provided in a sufficiently secure and reliable way	3
Negligible	The ICT equipment locations are secure, well managed and are not accessible by unauthorized people. All the digital services are provided in a secure and reliable way	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.6 Mechanical systems - HVAC

The intent for this sixth *topic* is to carefully evaluate the *mechanical systems and Heating Ventilation Air Conditioning (HVAC) equipment*, finding possible criticalities, especially for the possible CBR attack cases.

10.6.1 Air intakes and exhaust louvers

Air intakes should be located preferably on the roof or as high as possible. The fencing or enclosure should have a sloped roof to prevent throwing anything into the enclosure near the intakes.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 6.1 - *Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure) Are the intakes and exhausts accessible to the public?*

6.1 - Criticality Scale (Air intakes and exhaust louvers)		Weight
Extreme	The air intakes and exhaust louvers of the building are easily accessible in the low part of the building	27
Elevated	The air intakes and exhaust louvers of the building are in some cases easily accessible and not as high as practical	9
Marginal	The air intakes and exhaust louvers of the building are sufficiently as high as practical and inaccessible to the public	3
Negligible	The air intakes and exhaust louvers of the building are as high as practical and are not accessible to the public	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.6.2 Roof access

Roofs are in general very exposed and critical areas. From the roof is possible to easy conduct several type of malicious attacks. Roofs are critical like entrances to the building and are like

mechanical rooms when HVAC is installed. Adjacent structures or landscaping should not allow access to the roof.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 6.2 - *Is roof access limited to authorized personnel by means of adequate mechanisms?*

6.2 - Criticality Scale (Roof access)		Weight
Extreme	The roof access is not limited and controlled	27
Elevated	The roof access is not sufficiently strictly limited to authorized personnel by means of adequate mechanisms	9
Marginal	The roof access is sufficiently strictly limited to authorized personnel by means of sufficiently adequate mechanisms	3
Negligible	The roof access is strictly limited to authorized personnel by means of well adequate mechanisms	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.6.3 Air filtration

Air filtration constitutes a critical issue. Typically, it is possible to apply different filter kinds to the air before blowing it into the building. In general, we can speak of [CDC1, CDC2]:

- Minimum Efficiency Reporting Values, or MERVs, report a filter's ability to capture larger particles between 0.3 and 10 microns (µm);
- HEPA is a type of pleated mechanical air filter. It is an acronym for 'High Efficiency Particulate Air (filter)'. This type of air filter can theoretically remove at least 99.97% of dust, pollen, mould, bacteria, and any airborne particles with a size of 0.3 microns (µm). The diameter specification of 0.3 microns responds to the worst case; the most penetrating particle size. Particles that are larger or smaller are trapped with even higher efficiency. Using the worst-case particle size results in the worst-case efficiency rating (i.e. 99.97% or better for all particle sizes). HEPA can adopt: Activated charcoal for gases - Ultraviolet C for biological. Consider mix of approaches for optimum protection and cost effectiveness.

All air cleaners require periodic cleaning and filter replacement to function properly.

Air handling units serving critical functions during continued operation may be retrofitted to provide enhanced protection during emergencies. However, upgraded filtration may have negative effects upon the overall air handling system operation, such as increased pressure drop.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 6.3 - *What are the types of air filtration adopted for the building? Is there any collective or specific protection for chemical, biological, and radiological contamination designed into the building?*

6.3 - Criticality Scale (Air filtration)		Weight
Extreme	Air filtration systems are not implemented in the building for protection against chemical, biological and radiological contamination	27
Elevated	Air filtration systems are implemented only partially in the building for protection against chemical, biological and radiological contamination	9
Marginal	Air filtration systems are sufficiently well implemented in the building for protection against chemical, biological and radiological contamination	3
Negligible	Air filtration systems are well implemented in the building for protection against chemical, biological and radiological contamination	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.6.4 Air CBR sensors

The possibilities to use sophisticated air monitors and sensors for high spectrum CBR agent's detection is today a concrete opportunity. In practice, duct mounted sensors are found in limited cases, generally in laboratory areas. Modern CBR sensors generally have a good spectrum of high reliability but they are costly.

Many different technologies are, nowadays, undergoing research to provide higher capability.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 6.4 - *Are there provisions for air monitors or sensors for CBR agents?*

6.4 - Criticality Scale (Air CBR sensors)		Weight
Extreme	The building is not equipped with air monitors and sensors for CBR agent's detection	27
Elevated	The building is insufficiently equipped with air monitors and sensors for CBR agent's detection	9
Marginal	The building is sufficiently equipped with air monitors and sensors for CBR agent's detection	3
Negligible	The building is adequately equipped with air monitors and sensors for high spectrum CBR agent's detection	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.6.5 Air intakes and exhaust closure

In crisis situation or during not operational period could be particularly useful to very fast close the air intakes and exhaust. Motorized (low-leakage, fast-acting) dampers are the preferred method for closure with fail-safe to the closed position so as to support in-place sheltering.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 6.5 – *Does it exist a method for fast air intakes and exhausts closure when necessary?*

6.5 - Criticality Scale (Air intakes and exhaust closure)		Weight
Extreme	No method is adopted for fast air intakes and exhausts closure when necessary	27
Elevated	Not in all cases motorized dumpers or other methods are provided for fast air intakes and exhausts closure when necessary	9
Marginal	Motorized dumpers are provided for fast air intakes and exhausts closure when necessary	3
Negligible	Efficient motorized dumpers are provided for fast air intakes and exhausts closure when necessary	1
NA	Not Applicable: it is not possible give a relevant answer to the question	-

10.6.6 Air-handling systems zoning

Understanding the critical areas of the building that must continue functioning is a very important task and focuses security and hazard mitigation measures.

It is possible to apply HVAC zones that isolate lobbies, mailrooms, loading docks, and other entry and storage areas from the rest of the building HVAC zones and maintaining negative pressure within these areas. In such a way you will contain CBR releases. It is important to identify common return systems that service more than one zone, effectively making a large single zone.

Conversely, emergency egress routes should receive positive pressurization to ensure contamination does not hinder egress.

Independent units can continue to operate if damage occurs to limited areas of the building.

During chemical, biological, and radiological situations the intent is to either keep the contamination localized in the critical area or prevent its entry into other critical, non-critical, or public areas. Systems can be cross-connected through building openings (doorways, ceilings, partial wall), ductwork leakage, or pressure differences in air handling system. In standard practice, there is almost always some air carried between ventilation zones by pressure imbalances, due to elevator piston action, chimney effect, and wind effects. Smoke testing of the air supply to critical areas may be necessary.

To support in-place sheltering, the air handling systems require the ability for authorized personnel to rapidly turn off all systems. However, if the system is properly filtered, then keeping the system operating will provide protection as long as the air handling system does not distribute an internal release to other portions of the building.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 6.6 - *Are there large central air handling units or are there multiple units serving separate zones? Can critical areas be served from other units if a major system is disabled?*

6.6- Criticality Scale (Air-handling systems zoning)		Weight
Extreme	The building HVAC system does not provide support for fast in-place sheltering between different critical and non-critical areas	27
Elevated	The building HVAC system does not provide in some cases support for fast in-place sheltering between different critical and non-critical areas	9
Marginal	The building HVAC system provide sufficiently support for fast in-place sheltering between different critical and non-critical areas	3
Negligible	The building HVAC system provide adequately support for fast in-place sheltering between different critical and non-critical areas	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.6.7 Air intakes and exhaust system security

The air systems to critical areas, intended as supply, return, and exhaust paths, should be inaccessible to the public.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 6.7 - *Are supply, return, and exhaust air systems for critical areas secure?*

6.7- Criticality Scale (Air intakes and exhaust system security)		Weight
Extreme	The equipment, supply, return, and exhaust air paths of the HVAC system for all critical areas are not secure	27
Elevated	The equipment, supply, return, and exhaust air paths of the HVAC system for all critical areas are not - in some cases - secure	9
Marginal	The equipment, supply, return, and exhaust air paths of the HVAC system for all critical areas are sufficiently secure	3
Negligible	The equipment, supply, return, and exhaust air paths of the HVAC system for all critical areas are secure	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.6.8 Air pressurization

Some areas required positive or negative pressure to function properly. Pressurization is critical in a hazardous environment or emergency situation.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 6.8 - *Is air pressurization well designed and monitored regularly?*

6.8- Criticality Scale (Air pressurization)		Weight
Extreme	Air pressurization does not result well designed and is not monitored regularly	27
Elevated	Air pressurization does not result in all cases sufficiently well designed and monitored regularly	9
Marginal	Air pressurization results sufficiently well designed and monitored regularly	3
Negligible	Air pressurization results well designed and monitored regularly	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.6.9 Smoke evacuation systems

For an internal blast, a smoke removal system may be essential, particularly in large, open spaces. The equipment should be located away from high-risk areas, the system controls and wiring should be protected, and it should be connected to emergency power. This exhaust capability can be built into areas with significant risk on internal events, such as lobbies, loading docks, and mailrooms. Consider filtering of the exhaust to capture CBR contaminants.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 6.9 - *Are there any smoke evacuation systems installed?*

6.9- Criticality Scale (Smoke evacuation systems)		Weight
Extreme	In the building is not installed any smoke evacuation system	27
Elevated	In the building are installed an insufficient number of smoke evacuation systems	9
Marginal	In the building are installed a sufficient number of smoke evacuation systems	3
Negligible	In the building are installed an adequate number of smoke evacuation systems	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.6.10 HVAC maintenance

Functional equipment must interface with operational procedures in an emergency plan to ensure the equipment is properly operated to provide the protection desired.

The HVAC system can be operated in different ways depending upon an external or internal release and where in the building an internal release occurs. Thus, maintenance and security staff must have the training to properly operate the HVAC system under different circumstances, even if the procedure is to turn off all air movement equipment.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 6.10 - *Does the HVAC maintenance staff have the proper training, procedures, and preventive maintenance schedule to ensure system functionality?*

6.10- Criticality Scale (HVAC maintenance)		Weight
Extreme	HVAC maintenance staff have a poor sufficient training, procedures, and preventive maintenance schedule to ensure even the minimal system functionality	27
Elevated	HVAC maintenance staff have not the sufficient training, procedures, and preventive maintenance schedule to ensure complete system functionality	9
Marginal	HVAC maintenance staff have the sufficient training, procedures, and preventive maintenance schedule to ensure system functionality	3
Negligible	HVAC maintenance staff have the proper training, procedures, and preventive maintenance schedule to ensure complete system functionality	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7 Infrastructure and systems of internal essential services

The intent for this *topic* is to carefully evaluate the *infrastructure and systems of internal essential services (plumbing, gas systems, electrical power, fire alarms, telephone and ICT services*) finding possible criticalities.

10.7.1 Domestic water distribution

Looping of piping architecture and use of section valves provide redundancies in the event sections of the system if damaged. Central shaft locations for piping are more vulnerable than multiple riser locations.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.1 – *For the water distribution, are looping of piping architecture and section valves for redundancy tasks adopted?*

7.1 - Criticality Scale (Domestic water distribution)		Weight
Extreme	Looping of piping architecture and section valves for redundancy tasks are not adopted	27
Elevated	Looping of piping architecture and section valves for redundancy tasks are not sufficiently adopted	9
Marginal	Looping of piping architecture and section valves for redundancy tasks are adopted in many situations	3
Negligible	Looping of piping architecture and section valves for redundancy tasks are adopted in any possible situation	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7.2 Hot water management

In general, single source of hot water with one fuel source is more vulnerable than multiple sources and multiple fuel types.

Domestic hot water availability is a very important operational concern for many building occupancies.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.2 – *Is the method of heating domestic water resilient to fault at the heat source?*

7.2 - Criticality Scale (Hot water management)		Weight
Extreme	The method of heating domestic water is not resilient to a single fault at the heat source	27
Elevated	The method of heating domestic water is only in a few cases resilient to a single fault at the heat source	9
Marginal	The method of heating domestic water is in the most of the cases resilient to a single fault at the heat source	3
Negligible	The method of heating domestic water is resilient to a single fault at the heat source	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7.3 Gas distribution

Looping of piping architecture and use of section valves provide redundancies in the event sections of the system if damaged. The pipes can be above or below ground.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.3 - *For the gas distribution, are looping of piping architecture and section valves for redundancy tasks adopted?*

7.3 - Criticality Scale (Gas distribution)		Weight
Extreme	Looping of piping architecture and section valves for redundancy tasks are not adopted	27
Elevated	Looping of piping architecture and section valves for redundancy tasks are not sufficiently adopted	9
Marginal	Looping of piping architecture and section valves for redundancy tasks are adopted in many situations	3
Negligible	Looping of piping architecture and section valves for redundancy tasks are adopted in any possible situation	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7.4 Gas storages

Gas storage near or in the building could be a possible target attack. The concern is that the tanks and piping could be vulnerable, for example, to a moving vehicle or a bomb blast either directly or by collateral damage due to proximity to a higher-risk area. Localized gas cylinders could be available in the event of damage to the central tank system. It is important to verify how the storages are piped to the distribution system, above or below ground.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.4 - *Where are gas storage tanks located? (heating, cooking, medical, process) How are they piped to the distribution system? (above or below ground)*

7.4 - Criticality Scale (Gas storages)		Weight
Extreme	The gas storage tanks are not located in a secure mode and are piped to the distribution system above the ground	27
Elevated	Not all the gas storage tanks are located in a sufficient secure mode and are piped to the distribution system below the ground	9
Marginal	The gas storage tanks are located in a sufficient secure mode and are piped to the distribution system below the ground	3
Negligible	The gas storage tanks are located in an adequate secure mode and are piped to the distribution system below the ground	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7.5 Electrical rooms and panels

Critical electrical systems are typically collocated in secured rooms. They can be collocated with other building systems. Verify that critical electrical systems are not located in place outside of secured electrical areas.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.5 - *How are the electrical rooms located relative to other higher risk areas, starting with the main electrical distribution room at the service entrance? Are electrical rooms and distribution panels serving branch circuits secured?*

7.5 - Criticality Scale (Electrical rooms and panels)		Weight
Extreme	Electrical rooms and distribution panels serving branch circuits are not secured	27
Elevated	Electrical rooms and distribution panels serving branch circuits are not in some cases sufficiently secured	9
Marginal	Electrical rooms and distribution panels serving branch circuits are sufficiently secured	3
Negligible	Electrical rooms and distribution panels serving branch circuits are adequately secured	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7.6 Security system wiring

Security system refers to all the measures, equipment and alarms that are taken to exclusively protect a place and to ensure that only people with permission enter or leave the protected areas.

The security system should be able to operate even if the main electrical power and ICT network are in fault. The wiring of the Security System should be completely separated by other signal distribution network.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.6 - *Is security system wiring located separately from electrical and other service systems?*

7.6 - Criticality Scale (Security system wiring)		Weight
Extreme	Security system wiring is not located separate from electrical and other service systems	27
Elevated	Security system wiring is not located, in many cases, sufficiently separate from electrical and other service systems	9
Marginal	Security system wiring is located sufficiently separate from electrical and other service systems	3
Negligible	Security system wiring is located adequately separate from electrical and other service systems	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7.7 Emergency power distribution

There should be no single critical node that allows both the normal electrical service and the emergency backup power to be affected by a single incident. Automatic transfer switches and interconnecting switchgear could be a pint of weakness. Emergency and normal electrical equipment should be installed separately, at different locations, and as far apart as possible.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.7 - *How is the emergency power distributed? Is the emergency power system independent from the normal electrical service, particularly in critical areas?*

7.7 - Criticality Scale (Security system wiring)		Weight
Extreme	Emergency power system does not result independent from the normal electrical service, in any area of the building	27
Elevated	Emergency power system does not result, in all the cases, sufficiently independent from the normal electrical service, even in the critical areas	9
Marginal	Emergency power system results sufficiently independent from the normal electrical service, particularly in critical areas	3
Negligible	Emergency power system results completely independent from the normal electrical service in all the areas	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7.8 Fire alarm system

Fire alarm systems is fundamental and its correct operation vital. As essential task, it must warn building occupants to evacuate for life safety. Then they must inform, directly or indirectly, the responding agency to dispatch fire equipment and personnel.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.8 - *Is fire alarm system well designed, implemented and correctly maintained?*

7.8 - Criticality Scale (Fire alarm system)		Weight
Extreme	Fire alarm system does not result well designed, implemented and correctly maintained	27
Elevated	Fire alarm system does not result, in some aspects, well designed, implemented and correctly maintained	9
Marginal	Fire alarm system results sufficiently well designed, implemented and correctly maintained	3
Negligible	Fire alarm system results well designed, implemented and correctly maintained	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7.9 Communication system rooms

We intend in this item general internal management of digital voice, telephone service, data, digital signal, alarm, denoted as communication systems.

It is important to verify to have separation distance from other utilities and higher risk areas to avoid collateral damage. Security approaches on the closets include door alarms, closed circuit television, swipe cards, or other logging notifications to ensure only authorized personnel have access to these closets. One of the intents is to prevent tampering with the systems.

ICT main distribution facility, data centres, routers, firewalls, and servers can be typically located in different areas and must be properly protected to unauthorized access. The physical topology of a network is the way in which the cables and computers are connected to each other. The configuration and the availability of surplus cable or spare capacity on individual cables can reduce vulnerability to hazard incidents. Ensure access to terminals and equipment for authorized personnel only and a correct information security management for confidentiality, integrity and availability.

Another critical point is to make available redundant communications systems and to verify they work properly.

The redundancy for electrical power for digital ICT fundamental equipment is represented by the UPS (uninterruptible power supply). Such an equipment ensures reliability during electrical power fluctuations or fault. The UPS is also needed to await any emergency power coming on line or to allow orderly shutdown.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.9 - *Where are communication systems wiring closets located? (voice, data, signal, alarm) Are they collocated with other utilities? Are they in secure areas? Does the fundamental communication system have an UPS (uninterruptible power supply) or an alternative supply system?*

7.9 - Criticality Scale (Communication system rooms)		Weight
Extreme	The communication system rooms and networks are not well protected, well design and the redundant supply electrical system does not work	27
Elevated	The communication system rooms and networks are not sufficiently well protected, well design and the redundant supply electrical system is insufficiently maintained	9
Marginal	The communication system rooms and networks are sufficiently well protected, well design and a redundant supply electrical system is operative and maintained	3
Negligible	The communication system rooms and networks are well protected, well design and a redundant supply electrical system is operative and maintained	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7.10 ICT disaster recovery

An alternative site with suitable ICT equipment and network which allows continuation of operations or that mirrors - operates in parallel to - the existing operation is beneficial if equipment is lost during a natural or manmade disaster. The need is based upon the criticality of the operation and how quickly replacement equipment can be put in place and operated.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.10 - *Is there an alternative site with suitable ICT equipment and network which allows continuation of operations in case of attacks?*

7.10 - Criticality Scale (ICT disaster recovery)		Weight
Extreme	An alternative site with suitable ICT equipment and network which allows continuation of operations in case of attacks does not exist	27
Elevated	An alternative site with suitable ICT equipment and network which allows continuation of operations in case of attacks is only partially implemented and maintained	9
Marginal	An alternative site with essential ICT equipment and network which allows continuation of operations in case of attacks is implemented and periodically maintained	3
Negligible	An alternative site with suitable ICT equipment and network which allows continuation of operations in case of attacks is properly implemented and maintained	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.7.11 Mass notification system

Depending upon building size, a mass notification system will provide warning and alert information, along with actions to take before and after an incident.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 7.11 - *Is there a mass notification system that reaches all building occupants?*

7.11 - Criticality Scale (Mass notification system)		Weight
Extreme	A mass notification system is not working	27
Elevated	A mass notification system is poorly implemented and it reaches a minimal part of the building occupants	9
Marginal	A mass notification system is sufficiently working and it reaches the majority of all building occupants	3
Negligible	A mass notification system is correctly working and it reaches all building occupants	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.8 Security Systems

The intent for this eighth *topic* is to carefully evaluate the *Security Systems* applied to the building, finding possible criticalities.

10.8.1 Perimeter and internal security

Security technology is frequently considered to compliment or supplement security personnel forces and to provide a wider area of coverage. Typically, these physical security elements provide the first line of defence in deterring, detecting, and responding to threats and reducing vulnerabilities. They must be viewed as an integral component of the overall security program. Their design, engineering, installation, operation, and management must be able to meet daily security challenges from a cost effective and efficiency perspective. During and after an incident, the system, or its backups, should be functional for the planned design.

Consider CCTV cameras to view and record activity at the perimeter and in the critical areas of the building. Particular attention must be paid at primary entrances and exits.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 8.1 - *Are CCTV (Closed Circuit Television) cameras used, 24 hours/7 days a week recorded and monitored at the perimeter and in the critical areas of the building?*

8.1 - Criticality Scale (Perimeter and internal security)		Weight
Extreme	CCTV cameras are not used at the perimeter and in the critical areas of the building	27
Elevated	CCTV cameras are in some cases properly used and periodically monitored at the perimeter and in the critical areas of the building	9
Marginal	CCTV cameras are sufficiently used, 24 hours/7 days a week recorded and periodically monitored at the perimeter and in the critical areas of the building	3
Negligible	CCTV cameras are properly used, 24 hours/7 days a week recorded and well monitored at the perimeter and in the critical areas of the building	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.8.2 Video signal quality

It is important an adequate CCTV video signal quality, both during the day and hours of darkness. For the night period it is important the infrared camera use.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 8.2 - *Is the quality of video images adequate both during the day and hours of darkness?*

8.2 - Criticality Scale (Video signal quality)		Weight
Extreme	The quality of video images results insufficient in all hours of the day	27
Elevated	The quality of video images results insufficient in some hours of the day	9
Marginal	The quality of video images results sufficiently adequate both during the day and hours of darkness	3
Negligible	The quality of video images results adequate both during the day and hours of darkness	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.8.3 Video recording continuity

It is important to assure the continuity of the video signal acquisition and recording, even during the absence of main electrical power provisioning.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 8.3 - *Are the recording systems and cameras supported by an uninterruptible power supply, battery, or building emergency power?*

8.3 - Criticality Scale (Video recording continuity)		Weight
Extreme	The video recording systems and cameras are not supported by an uninterruptible power supply, battery, or building emergency power	27
Elevated	The video recording systems and cameras are only partially supported by an uninterruptible power supply, battery, or building emergency power	9
Marginal	The video recording systems and cameras are sufficiently supported by an uninterruptible power supply, battery, or building emergency power	3
Negligible	The video recording systems and cameras are well supported by an uninterruptible power supply, battery, or building emergency power	1
NA	Not Applicable: it is not possible give a relevant answer to the question	-

10.8.4 Intrusion detection system and alarms

Intrusion Detection System detects unwanted elements (person or object) entering into a controlled area/zone.

Verify the presence of balanced magnetic contact switch sets for all exterior doors, including overhead/roll-up doors and review roof intrusion detection. Verify the presence of glass break sensors for windows up to scalable heights.

More generally, physical Intrusion Detection System (IDS) sensors are: electromagnetic, fiber optic, active infrared, bi-static microwave, seismic, photoelectric, ground, fence, glass break (vibration/shock), single, double and roll-up door magnetic contacts or switches.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 8.4 – *Is the physical IDS well designed, adequately spread in the building and well monitored?*

8.4 - Criticality Scale (Intrusion detection system and alarms)		Weight
Extreme	The physical IDS results completely inadequate	27
Elevated	The physical IDS results in many parts insufficiently well designed, spread in the building and monitored	9
Marginal	The physical IDS results sufficiently well designed, spread in the building and monitored	3
Negligible	The physical IDS results well designed, adequately spread in the building and well monitored	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.8.5 Emergency call buttons and boxes

Call buttons or intercom call-boxes should be provided at key public contact areas and as needed in offices of managers and directors, in garages and parking lots, and in the other high-risk zones of the building.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 8.5 – *Are call-button or intercom call-boxes or building intercom systems used throughout the building?*

8.5 - Criticality Scale (Emergency call buttons and boxes)		Weight
Extreme	No intercom call system is in the building	27
Elevated	An intercom call system is spread, used and maintained n only a few parts of the building	9
Marginal	An intercom call system is sufficiently spread, used and maintained throughout the building	3
Negligible	A well design intercom call system is properly used and maintained throughout the building	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.8.6 Security control equipment and scanners

The scanner of security being considered excellent today relies upon Magnetic imaging, technique based on passive millimetre wave detection to create full body images of controlled people. These scanners can see through clothing to reveal metallic and non-metallic objects or other suspicious things on a person's body, but they cannot identify explosives by their chemical signatures.

X-ray imaging, based on low-level X-rays to create a two-dimensional image of the body, is also used.

The metal detector – or magnetometers - is another frequently used form of control. A magnetometer uses an electromagnetic field to detect metal objects, such as concealed handguns. This security devices can't detect ceramic or plastic weapons, however.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 8.6 – *Are security scanners (X-ray, magnetomer, magnetic imaging, ...) used for security purposes in some areas of the building?*

8.6 - Criticality Scale (Security control equipment and scanners)		Weight
Extreme	Security scanners are not used for security purposes in the building	27
Elevated	Security scanners are used for security purposes only in a few critical areas of the building	9
Marginal	Security scanners are used for security purposes in the majority critical areas of the building	3
Negligible	Security scanners are widely used for security purposes in all critical areas of the building	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.8.7 Safe mail handling

It is important to put into action the screening and handling [DHS7] of all incoming packages and letters, commercial common couriers, or special messengers. In the majority of the business, commercial and administrative buildings, the "mailroom" is the central receiving and distribution function for all incoming and outgoing mail and packages.

This kind of threats can involve CBRe substances that are both dangerous and disruptive.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 8.7 – *Are the security controls in place to handle the processing of mail and protect against potential CBRe exposures adequate?*

8.7 - Criticality Scale (Safe mail handling)		Weight
Extreme	No security controls are in place to handle the processing of mail and protect against potential CBRe exposures	27
Elevated	Some, but not efficient, security controls are in place to handle the processing of mail and protect against potential CBRe exposures	9
Marginal	Sufficient security controls are in place to handle the processing of mail and protect against potential CBRe exposures	3
Negligible	Efficient and reliable security controls are in place to handle the processing of mail and protect against potential CBRe exposures	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.8.8 Security Control Room

Monitoring can be done at an off-site facility, at an on-site monitoring center during normal duty hours, or at a 24- hour on-site monitoring centre. These kinds of Security control room are fundamental for the building security management.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 8.8 – *Is there a designated security control room and console in place to monitor security, alarm, and other building systems?*

8.8 - Criticality Scale (Security Control Room)		Weight
Extreme	No security control room is located in the building	27
Elevated	A provisional security control room with a console to monitor some alarms, and some other systems is located in the building	9
Marginal	A sufficiently efficient security control room with a console in place to monitor security, alarm, and other systems is located in the building	3
Negligible	An efficient security control room with a modern console in place to monitor security, alarm, and other systems is located in the building	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.9 Emergency, security and operation continuity plans

The intent for this ninth *topic* is to carefully evaluate the *presence of emergency, security and operation continuity plans* applied to the building, finding possible criticalities.

10.9.1 Security plan

The development and implementation of a security plan - even devoted to antiterrorism security - provides a roadmap that outlines the strategic direction and vision, operational, managerial, and technological mission, goals, and objectives of the organization's security program. The security plan has to be communicated and disseminated to key management personnel and departments in the building. At the same time, the security plan has to be benchmarked or compared against related organizations and operational entities that can cooperate during potentially attacks.

In the plan, threats/hazards, vulnerabilities, risks and security countermeasures have to be addressed and prioritized relevant to their criticality and probability of occurrence. The security plan has to be addressed the protection of people, property, assets, and information, specifying these components: access control, surveillance, response, building hardening and protection against CBR and cyber-network attacks.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 9.1 - *Do updated and written security and emergency plans exist for the building?*

9.1 - Criticality Scale (Security plan)		Weight
Extreme	Security and emergency plans do not exist for the building at all	27
Elevated	Security and emergency plans exist for the building but are not written	9
Marginal	Security and emergency plans exist for the building but are not updated	3
Negligible	An update, complete and written security and emergency plans exist for the building	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.9.2 Security plan testing

It's important to test the activations and procedures specified in the security plan. The security plan has to be communicated and practical applied by key management, operative e security personnel in the building.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 9.2 - *Is the security plan periodically tested and updated?*

9.2 - Criticality Scale (Security plan testing)		Weight
Extreme	The security plan is not tested and updated	27
Elevated	The security plan is tested very rarely and in very few parts	9
Marginal	The security plan is tested and updated only for the most relevant parts	3
Negligible	The security plan is periodically tested and updated	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.9.3 Risk analysis activity

The Risk analysis activity is the input to the building design and to possible mitigation measures should be included in the facility project to reduce risk and increase safety of the building and people.

The risk analysis activity is part of the security plan and address the findings from the asset, threat/hazard, and vulnerability analyses to develop, recommend, and consider implementation of appropriate security countermeasures.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 9.3 – *Does the security plan include risk analysis and the countermeasure actions?*

9.3 - Criticality Scale (Risk analysis activity)		Weight
Extreme	The security plan does not include a risk analysis and a list of countermeasures	27
Elevated	The security plan includes a partial risk analysis and a limited list of countermeasures	9
Marginal	The security plan includes a sufficient risk analysis and a list of countermeasures	3
Negligible	The security plan includes a well-structured risk analysis and an in-depth list of countermeasures	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.9.4 Emergency plan

An emergency plan contains all the procedure for managing in an ordered way crisis situation. It is an operative tool necessary to mitigate the damage in the case of natural and anthropic disasters, assuming in a fast way decisions and applying consequence reduction actions.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 9.4 – *Is an emergency plan up-date and well designed available to implement in the case of natural and anthropic disasters?*

9.4 - Criticality Scale (Emergency plan)		Weight
Extreme	No emergency plan is available to implement in the case of natural and anthropic disasters	27
Elevated	An incomplete and non-updated emergency plan is available to implement in the case of natural and anthropic disasters	9
Marginal	A sufficiently updated emergency plan is available to implement in the case of natural and anthropic disasters	3
Negligible	An updated and well-designed emergency plan is available to implement in the case of natural and anthropic disasters	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

10.9.5 Operational continuity plan

In order to mitigate the effects of an emergency and the damage, an operational continuity (or business continuity) plan should be produced following international standard approach [ISO4, ISO5].

This kind of plan increment the resilience of the building, providing measure that assure possible continuity in the main operations managed in the area.

Answer to the question proposed and evaluate on the below reported Criticality Scale the critical weight for this item.

Question 9.5 – *Is it available an updated and well designed operational continuity plan to apply?*

9.5 - Criticality Scale (Operational continuity)		Weight
Extreme	No operational continuity plan is available to implement in the case of serious incidents	27
Elevated	An incomplete and non-updated operational continuity plan is available to implement in the case of serious incidents	9
Marginal	A sufficiently updated operational continuity plan is available to implement in the case of serious incidents	3
Negligible	An updated and well-designed operational continuity plan is available to implement in the case of serious incidents	1
NA	Not Applicable: it is not possible to give a relevant answer to the question	-

11 Glossary

BCA = Building Criticality Analysis

BEA = Building Exposure Assessment

BRAM = Building Risk Assessment Method

BTAM = Building Threat Assessment Method

BVAM = Building Vulnerability Assessment Method

CBR = Chemical, Biological, Radiological

CBRe = Chemical, Biological, Radiological and explosive

CBRN = Chemical, Biological, Radiological and Radiological

CBRNe = Chemical, Biological, Radiological, Radiological and explosive

CCT = Closed Circuit Television

DHS = Department of Homeland Security

DoJ = Department of Justice

DRM = Disaster Risk Management

EU = European Union

FEMA= Federal Emergency Agency

HVAC = Heating, Ventilation, and Air Conditioning

HazMat = Hazard Material

ICT = Information and Communication Technology

IDS = Intrusion Detection System

IED = Improvised Explosive Device

ISO=International Standard Organization

JRC = Joint Research Centre (European Commission)

MRAM=Multi-Risk Assessment Method

NDRA = National Disaster Risk Assessment

NIPP = National Infrastructure Protection Plan

RAMCAP = Risk Analysis and Management for Critical Asset Protection

SICC = Scientific International Conference on CBRNe

UAS = Unmanned Aircraft System

UAV = Unmanned Aerial Vehicle

UN = United Nations

UNDRR = United Nations Office for Disaster Risk Reduction

USA = United States of America

VBIED = Vehicle-Borne Improvised Explosive Device

VRF=Vulnerability Reduction Factor

12 References and Publications

[Ayy1] B. M. Ayyub, Risk Analysis in Engineering and Economics. University of Maryland, Chapman & Hall/CRC, New York, p.35-38, 2003

[Bir1] 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., 2007

[Bou1] S. Bouchon, The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State of-the-Art, 2006

[Car1] M. Carbonelli, Terrorist attacks and natural/anthropic disasters: risk analysis methodologies for supporting security decision making actors, Aracne CBRN Series, Rome 2019

[Car2] M. Carbonelli, A. Iannotti, A. Malizia, Disaster Management of a Major CBRN Accident, A. J. Masys (ed.), Handbook of Security Science, 6 February 2021, Springer Nature Switzerland AG 2020, https://link.springer.com/referenceworkentry/10.1007%2F978-3-319-51761-2_36-1

[Car3] M. Carbonelli, M. Carestia, R. Quaranta, Threat Assessment Method for Buildings in Case of Terrorist Attacks, International Journal of Safety and Security Engineering, Vol. 11, No. 4, August 2021, pp. 285-294, https://doi.org/10.18280/ijsse.110401

[Car4] M. Carbonelli, L. Gratta, A General Multi-Risk Assessment Method for Natural Disasters and CBRNe Attacks, International Journal of Safety and Security Engineering, Vol. 11, No. 4, August 2021, pp. 345-352, https://doi.org/10.18280/ijsse.110407

[Car5] 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, 12 December 2020, Rome, https://www.sicc-series.com/book-of-abstract/

[Car6] 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, ISSN 1743-3509 (on-line), 13 December 2022

[Car7] M. Carbonelli, Eventi terroristici mondiali e aree geografiche interessate da attacchi nel periodo 2000-2019, Safety & Security Magazine, Tecna Editrice S.r.l., 29 September 2022, https://www.safetysecuritymagazine.com/articoli/eventi-terroristici-mondiali-e-aree-geografiche-interessate-da-attacchi-nel-periodo-2000-2019

[Car8] M. Carbonelli, Soft target, hard target e attacchi terroristici: analisi del Global Terrorism Database, Safety & Security Magazine, Tecna Editrice S.r.l., 04 November 2022, https://www.safetysecuritymagazine.com/articoli/soft-target-hard-target-e-attacchi-terroristici-analisi-del-global-terrorism-database/

[Car9] M. Carbonelli, Attacchi terroristici agli edifici: analisi a livello mondiale per gli ultimi venti anni, Safety & Security Magazine, Tecna Editrice S.r.l., 6 December 2022, https://www.safetysecuritymagazine.com/articoli/attacchi-terroristici-agli-edifici-analisi-a-livello-mondiale-per-gli-ultimi-venti-anni/

[CDC1] Center for Desease Control and Prevention CDC, Guidance for Filtration and Air-Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attacks, April 2003, DHHS (NIOSH - National Institute for Occupational Safety and Health) Publication Number 2003-136, https://www.cdc.gov/niosh/docs/2003-136/

[CDC2] Center for Desease Control and Prevention CDC, Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attack, May 2002,

DHHS (NIOSH- National Institute for Occupational Safety and Health) Publication Number 2002-139, https://www.cdc.gov/niosh/docs/2002-139/

[CRS1] CRS - Congressional Research Service USA, The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress, February 2, 2007, https://www.hsdl.org/?abstract&did=470027

[DHS1] USA Department of Homeland Security, Integrated Rapid Visual Screening of Buildings, DHS BIPS04 September 2011, https://www.dhs.gov/xlibrary/assets/st/st-bips-04-irvs.pdf

[DHS2] USA Department of Homeland Security, Soft Targets and Crowded Places Security Plan Overview, May 2018, https://www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf

[DHS3] DHS. Risk Steering Committee: DHS Risk Lexicon, Edition September 2010, https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

[DHS4] DHS "National Infrastructure Protection Plan", Homeland Security Dept 2006. https://www.hsdl.org/?abstract&did=464612

[DHS5] DHS, NIPP 2013 Partnering for Critical Infrastructure Security and Resilience, 2013, https://www.cisa.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience OPPURE https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf TBF

[DHS6] DHS, NIPP2013 Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach, 2013, https://www.cisa.gov/publication/nipp-2013-ci-risk-management-approach

[DHS7] DHS, Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors, 2012, https://www.cisa.gov/sites/default/files/publications/isc-mail-handling-screening-nonfouo-sept-2012-508.pdf

[DoC1] U.S. Department of Commerce, Critical Infrastructure Assurance Office (DOC CIAO) Vulnerability Assessment Framework 1.1, October 1998

[DoD1] U.S. Department of Defense (DoD)Unified Facilities Criteria (UFC), UFC 4-010-01, DoD Minimum Antiterrorism Standards for Buildings, July 31, 2002

[DoJ1] U.S. Department of Justice - National Criminal Justice (NCJ) NCJ181200, Fiscal Year 1999 State Domestic Preparedness Equipment Program, Assessment and Strategy Development Tool Kit, May 15, 1999

[Dus1] D. O. Dusenberry, Handbook for Blast Resistant Design of Buildings, John Wiley & Son Inc., 2010

[DVA1] USA Department of Veterans Affairs - Physical Security Assessment for the Department of Veterans Affairs Facilities, Recommendations of the National Institute of Building Sciences Task Group to the Department of Veterans Affairs, 6 September 2002

[End1] W. Enders e T. Sandler, «After 9/11: Is it All Different Now? https://www.jstor.org/stable/30045111?seq=1,» The Journal of Conflict Resolution, vol. 49, n. 2, pp. 259-277, 2005.

[Ers1] N. K. Ersun, «The "New Terrorism" and its Critics» Studies in Conflict & Terrorism DOI: 10.1080/1057610X.2011.571194, vol. 34, n. 6, pp. 476-500, 2011.

[EuC1] 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

[EuC2] European Commission, Poljanšek et al., Science for disaster management, DRMKC Disaster Risk Management Knowledge Centre, Joint Research Center (JRC), Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-60679-3, JRC102482.

https://ec.europa.eu/jrc/en/publication/science-disaster-risk-management-2017-knowing-better-and-losing-less

[EuC3] European Commission, Poljanšek, K., et al., Recommendations for National Risk Assessment for Disaster Risk Management in EU, Publications Office of the European Union, Luxembourg 2019, ISBN 978-92-79-98366-5, JRC114650. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC114650/jrc114650_nrarecommendations_updatedfinal_online1.pdf

[EuC4] European Commission, Guideline on Building perimeter protection: Design recommendations or enhanced security against terrorist attacks, Joint Research Center (JRC), Luxembourg 2020, ISBN 978-92-76-21443-4 ISSN 1831-9424, https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en

[EuC5] European Commission, Review on Soft target/Public space protection guidance, Joint Research Center (JRC), 2° Edition, Luxembourg 2018, ISBN 978-92-79-79907-5 ISSN 1831-9424. https://publications.jrc.ec.europa.eu/repository/handle/JRC110885

[EuC6] European commission, The Communication on the Internal security strategy addressed the need for an integrated approach between security and other policies. COM(2009) 82 final, 2009

[EuP1] European Parliament, Terrorism in the EU: terror attacks, deaths and arrests in 2020, August 2021, https://www.europarl.europa.eu/news/en/headlines/society/20210628STO07262/terrorism-in-the-eu-terror-attacks-deaths-and-arrests-in-2020

[EuU1] Europol (2021), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, | ISBN 978-92-95220-26-3 | ISSN 2363-0876, Luxembourg, https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf

[FEM1] USA Federal Emergency Management Agency, Reference Manual to Mitigate Potential Terrorist Attacks against Buildings, Risk Management Series, FEMA 426 December 2003, https://www.fema.gov/pdf/plan/prevent/rms/426/fema426.pdf

[FEM2] 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

[FEM3] 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

[FEM4] USA Federal Emergency Management Agency, Rapid Visual Screening of Buildings for Seismic Hazards: A Handbook, FEMA 154 January 2015, Edition3, https://www.fema.gov/sites/default/files/2020-07/fema_earthquakes_rapid-visual-screening-of-buildings-for-potential-seismic-hazards-supporting-documentation-third-edition-fema-p-155.pdf

[FEM5] USA Federal Emergency Management Agency, Incremental Protection for Existing Commercial Buildings from Terrorist Attack, FEMA 459 April 2008, https://www.fema.gov/sites/default/files/2020-08/fema459_complete.pdf

[FEM6] 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

[Gau1] F. Gaub, Trends in terrorism, European Union Institute for Security Studies (EUISS), 2017, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_Terrorism_in_Europe_0.pdf.

[GTD1] Global Terrorism Database (GTD), START (National Consortium for the Study of Terrorism and Responses to Terrorism), (2021), University of Maryland. https://www.start.umd.edu/gtd

[GTD2] Global Terrorism Database codebook: Methodology, inclusion criteria, and variables, START (National Consortium for the Study of Terrorism and Responses to Terrorism), (2021, August). University of Maryland. https://www.start.umd.edu/gtd/downloads/Codebook.pdf

[Hes1] J. Hesterman, Soft target hardening, CRC Press, December 2014

[Hes2] J. Hesterman, M. J. Fagel, Soft Targets and Crisis Management. What Emergency Planners and Security Professionals Need to Know, CRC Press, 2016

[ISO1] ISO 31000, Risk management -- Principles and guidelines, International Organization for Standardization, last edition 2018.

[ISO2] ISO 31010, Risk management -- Risk assessment techniques. International Organization for Standardization, 2009.

[ISO3] ISO Guide 73, Risk management - Vocabulary, International Organization for Standardization, 2009.

[ISO4] ISO 22301, Security and resilience - Business continuity management systems - Requirements, last edition 2019.

[ISO5] ISO 22313, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301, last edition 2020

[Kob1] G. D. Koblentz, Emerging technologies and the future of CBRN terrorism, The Washington Quarterly, 42:2, 2020 (summer edition), https://doi.org/10.1080/0163660X.2020.1770969

[Kob2] G. D. Koblentz, Drones and the future of CBRN, G. Mason University, Centre for Security Policy Studies, Conference on *Drones and CBRN threats*, 24 March 2021, https://www.youtube.com/watch?v=UnI8JMRogtE

[Mod1] M. Modarres, Risk Analysis in Engineering: techniques, tools and trends, Taylor & Francis Group, Boca Raton (FL) USA, 2006

[NDP1] National Domestic Preparedness Coalition, State of Florida HLS-CAM vulnerability and criticality matrix, http://www.ndpci.us/hls_cam/

[ONU1] United Nations, Sendai Framework for Disaster Risk Reduction 2015 – 2030, UN World Conference in Sendai, Japan, on March 18, 2015, https://www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf

[RAM1] ASME, Risk Analysis and Management for Critical Asset Protection: the framework, ASME Innovative Technologies Institute, Washington (US) 2005

[RAM2] ASME, Prioritizing Critical Infrastructures Using the RAMCAP Plus Approach, ASME Innovative Technologies Institute, Washington (US) 2009

[Rou1] M. Rouad, Probability, Statistics and Estimation, Creative Commons Attribution-NonCommercial 4.0, first edition 2013, English version 2017, http://www.incertitudes.fr/book.pdf

[Sot1] 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

[UN1] 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

[UN2] United Nations – General Assembly, Sendai Framework for Disaster Risk Reduction 2015–2030, Resolution adopted by the General Assembly on 3 June 2015, https://www.preventionweb.net/files/resolutions/N1516716.pdf

[UN3] United Nations, Office of Counter-Terrorism, Open Briefing of the Counter-Terrorism Committee on 'Building partnerships in protecting soft targets from terrorist attacks', Statement of Mr. Vladimir Voronkov, June 2019 https://www.un.org/sites/www.un.org.counterterrorism/files/190625_Statement_USG_CTC_Briefing_Soft_Targets.pdf

[UN4] United Nations Office for Disaster Risk Reduction Words into Action guidelines: National disaster risk assessment, 2016, https://www.undrr.org/publication/words-action-guidelines-national-disaster-risk-assessment

[UN5] UNISDR (2016), 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. https://www.preventionweb.net/files/50683_oiewgreportenglish.pdf

[UN6] United Nation Office for Disaster Risk reduction, National Disaster Risk Assessment: Governance System, Methodologies, and Use of Results, 2017, Consultative Version. https://www.unisdr.org/files/globalplatform/591f213cf2fbe52828_wordsintoactionguidelin e.nationaldi.pdf

The events that in the last decades marked a real fracture in the global comprehension of terrorism are, without any doubt, the attacks to the New York World Trade Center and to the Pentagon orchestrated by religiously-inspired al Qaeda on September 11, 2001, which are popularly referred to as 9/11 attack. It is essential to point out that recent terrorist activities have been no longer focused exclusively on institutional buildings or high-value targets, but there has been an increase in the number of attacks against easy-to-hit targets. In this scenario the protection of buildings from terrorist attacks has become one of the most important components of the defence strategy adopted firstly by USA after the 9/11 event and, in recent years, by European Countries. This is because buildings can represent one of the preferred targets of terrorists, being the central venue of a country's economic life and the embodiment of its wealth and culture. For the reasons described above, a comprehensive approach to assessing the risk of buildings against terrorist attacks has become a key issue in last years at both institutional and academic levels. – FROM THE INTRODUCTION

Marco Carbonelli, Electronic Engineer, holds a PhD in Industrial Engineering and an International Master's level II degree in "Protection against CBRNe events" from the University of Rome Tor Vergata. He is a qualified NBC expert at the Interforce NBC Defence School in Rieti (Italy), an expert in Risk Management, ICT security, critical infrastructure protection, civil protection - civil defence crisis and emergency management, GDPR application in the field of personal data protection. He has worked as a researcher in the field of TLC and then ICT for twenty years, since 2006 in the Italian Central Public Administration. He has published about 180 technical papers nationally and internationally, author of several technical-scientific books, and lecturer at the University of Rome of Tor Vergata Industrial Engineering and Economics & Finance Departments. He is member of O.S.S.I.S.Na. - Osservatorio per la Sicurezza del Sistema Industriale Strategico Nazionale, within the non-profit association CISINT – Centro Italiano di Strategia e Intelligence.

CISINT
OSSISNa
www.cisint.org

ISBN 979-12-210-4808-7