International Journal of Safety and Security Engineering
Vol. 14, No. 3, June, 2024, pp. 671-678
Journal homepage: http://iieta.org/journals/ijsse

Parametric Assessment of Strategic Buildings for CBRNe and Hybrid Threat Resilience

Vincenzo Puccia[1*], Daniele Di Giovanni[2]

[1] Corpo Nazionale Vigili del Fuoco, Comando VVF Padova, Via San Fidenzio 3- 35128 Padova, Italy
[2] University Roma Tor Vergata, Via Cracovia, 50, 00133 Rome, Italy

Corresponding Author Email: vincenzo.puccia@vigilfuoco.it

(This article is part of the Special Issue **SICC Series CBRNe Conference**)

https://doi.org/10.18280/ijsse.140301

Received: 22 February 2024
Revised: 21 April 2024
Accepted: 8 May 2024
Available online: 24 June 2024

Keywords:
building vulnerability, strategic building, threat analysis, CBRNe, building security

ABSTRACT

This paper presents an innovative method for rapidly assessing building vulnerability, with a focus on potential threats. The approach begins with a historical analysis and a review of state-of-the-art literature obtained from open sources. Subsequently, a tool is introduced, incorporating weighted parameters related to threat typology and available mitigation elements. Critical issues in the overall building vulnerability analysis are pinpointed through a scenario-based approach. While primary literature references are based on explosive attacks (such as Beirut in the '80 s, Nairobi in the '90 s, Oklahoma City in the '90s, etc.), the method also considers non- conventional weapons such as Chemical, Biological, Radiological, and Nuclear (CBRN) threats, along with emerging threats involving direct energy targeting (e.g., Havana Syndrome). The analysis covers six domains: Layout, Structure & Boundary, Technological Plants, In & Out Ways, Cyber, and Building Security Management. Each domain undergoes a comprehensive analysis, identifying threats and developing scenarios and sub-scenarios associated with presumed risks affecting the building. Specific characteristics for each action are identified, with parametric weights assigned to reflect their significance in the overall vulnerability assessment.

1. INTRODUCTION

The last twenty-five years have shaped the idea of an asymmetric war, with a high technology power fighting in total air and sea control groups of resistant or terroristic organizations very far from its military capabilities, on the other hand the latest geopolitical events drive again to a potential comparison between peers, or close to peers, in technological/military terms. Thus, a new kind of challenge rose in terms of building vulnerability, especially if the desire to interrupt functionality is focused, rather than the search for media visibility by hitting a symbolic building and killing lots of people randomly. With those premises, a vulnerability assessment for strategic buildings for a wide range of threats, including CBRN scenarios, could be of great interest. Particularly the CBRN threats with a relatively little mass of unconventional agent or radioactive substance could impact on the functionality of the structure also with the simple suspect of a contamination inside the working/operative areas, requiring long verification and eventually decontamination procedures and impacting on the health of occupants from key operators topolicy makers. The study delves into the analysis of vulnerability to threats, particularly explosive and CBR threats, when applied to buildings. Pursuing a thorough examination of available open-source literature [1-11], the question arose regarding how to structure the threat analysis. The initial consideration highlighted the potential significance of historical research in threat analysis, with the expectation that insights could be gleaned from case studies. The second consideration revolved around the interruption of building function as the ultimate goal of potential attacks. If this was the focal point, the analysis of potential scenarios needed to extend beyond explosive incidents to encompass sabotage attempts, which were not necessarily violent. As the wheels of history began to turn again, and considering the hybrid scenarios now significant, a broader perspective was deemed a valuable choice. This study aims to develop a parametric tool for conducting a rapid vulnerability assessment of a site. The tool is designed to be applied in the risk analysis of strategic or critical buildings.

It is crucial to note that the tool is designed to evaluate vulnerability to threats individually. Therefore, a cross-scenario involving a primary event that compromises the building's capacity, followed by a second event or a sequence of events, is not considered. The initial phase of this project involved a literature review to establish the open-source state of the art. Notably, most of these papers and booklets were from the first decade of the 21st century, reflecting the post-9/11 counter-terrorist efforts.

Following the literature review, a historical analysis was conducted, tracing various attacks and bombings from the 20th and 21st centuries. While there was a lack of explicit CBRN

references related to buildings, the Clark and Guarrieri paper [12] introduced a stochastic approach and a Monte Carlo method to simulate a CBRN attack. Afterwards, an innovative approach for rapid vulnerability assessment was developed, adopting a modular framework that initiates by defining domains to classify threats. The concept of domains, borrowed from Civil Defence, was employed to categorize threats based on the historical analysis of various case studies.

This study expanded its scope to encompass a broad range of threats to buildings, not limited solely to terrorist acts. It considered asymmetric attacks by terrorist groups and explored hybrid scenarios. These hybrid events involve tactics to disable strategic buildings, disrupting essential services during a major crisis. Such events could concern disrupting power supply, blocking transportation systems, and more, without the need for detonating IEDs or firing a single bullet.

2. THE STRUCTURE OF THE PARAMETRIC ASSESSMENT TOOL

In this work, a scenario approach was employed to develop a tool for vulnerability assessment. But what exactly is a scenario? The term, now common in Major Hazard Safety Studies, emerged with the rise of Quantitative Risk Analysis in the 1960s and 1970s as an independent multidisciplinary field. A scenario analysis serves as a tool to identify and mitigate risks that may not exist at present. Several threats were identified, stemming from historical analysis and the presumed use of weapons or disruptive agents.

3. HISTORICAL RESEARCH AND ANALYSIS

The historical analysis of building attacks [13-22] primarily focuses on explosive or improvised explosive device events. Notably, these events involve explosive charges either inside the buildings or in close proximity, often with varying levels of external protection. It is essential to recognize that the events used for insights into building vulnerabilities pertain to diverse tactical contexts. The author emphasizes that a comparison between two events is logical only when the boundary conditions are somewhat comparable.

The outlined case studies include:

1. King David Hotel Bombing (1946) – A Hidden explosive charge inside the building.
2. Tehran U.S. Embassy Crisis (1979) – A Building taken under control.
3. Bologna Railway Station Bombing (1980) – A Soft target with difficulty implementing full protection.
4. London Iranian Embassy Siege (1980) - Building taken control by a terrorist group.
5. Spanish Coup d'état Attempt (1981) – An Attempt to take control of a strategic building.
6. U.S. Marines Barracks Bombing (1983) – A Perimeter violation with a large explosive charge.
7. French Barracks Beirut Bombing (1983) - Another perimeter violation.
8. U.S. Embassy in Beirut Bombing (1983) – A car Park too close.
9. U.S. Embassy in Soviet Union (Mid '80s) – Consideration on vulnerability during construction (Figure 1).
10. Brighton Hotel Bombing (1984) – A Sleeping hidden explosive charge (Figure 2).
11. World Trade Center Car Bombing (1993) - (Suspected) A CBRN attack attempt coupled with a bombing on a soft target.
12. Parliament of Brittany (Bretagne) Fire (1994) – An Unwanted result of a strike, vulnerability of a heritage building.
13. Oklahoma City Bombing (1995) – A Too close parking area near a symbolic target.
14. Khobar Towers Bombing (1996) – An Underestimated security distance.
15. U.S. Embassies Bombing (1998) – A Car bombing with limited security distances.
16. American Airlines Flight 77 The Crash on the Pentagon (2001) – the Scale factor consideration.
17. Jordan Embassy Bombing, Baghdad (2003) – An Underestimated security distances and unattended car wreck projection. Canal Hotel Bombing (UN Assistance Mission Headquarters) – A Thoughtless approach on security measures.
18. Nassiriya Italian Carabinieri MSU Site Bombing (2003) – A Perimeter violation with a large explosive charge.
19. Havana Syndrome Disease (2016). A discussed episode with a potential new threat debut.
20. Capitol Hill Assault (6 January 2021) - A Public order problem as a threat for a strategic building.

Figure 1. The US embassy in Moscow still under construction

Figure 2. Brighton hotel bombing 1984

4. STATE OF THE ART AND LITERATURE REVIEW

The search for building vulnerabilities concerning both conventional and unconventional attacks, focusing CBRN scenarios, yields a plethora of official publications, research papers, and websites from think-tanks, public authorities, and private companies addressing this issue. Among these sources, the Royal United Services Institute think tank (www.rusi.org)

[9, 10] provides a direct reference on the question of protecting a building from an expanding array of potential threats. The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank, as per its website, offering direct access to various open-source Whitehall papers. Various documents and publications from Federal Emergency Management Agency (FEMA) address the vulnerability of buildings to bombing, and a specific publication from The Council of Research relates to CBRN protection of buildings.

After an analysis on the available open-source literature [1-11], the question was how to structure the threat analysis in a new and original way.

The first consideration was that for a first threat analysis array identification an historical research, see the previous paragraph 3, could probably result of interest. Some common characteristics could be found in those case studies. The second consideration was related to the building function interruption as a scope of the hostile action. Focusing the building function interruption as the real goal for the potential attacks, the analysis of potential scenarios must be enlarged to malicious attempts not only with explosives but also by sabotage attempts in various ways, not necessarily resulting in bloody events. On the other hand, a scenario-based approach, in analogy to the Risk Analysis for Oil & Gas industry, on new potential source of threat was an original contribution, regarding the available literature, mainly focused on terroristic threats.

5. THE PROPOSAL OF A QUICK TOOL

This work presents an innovative approach—a quick tool concept—for the vulnerability assessment of significant buildings, with a focus on strategic structures. The objective is to encompass all types of threats that may be initiated by 'opponent forces.' The aim is to complement the existing state of the art on this subject by extending the focus to a broader range of potential actions. While the primary reference is undoubtedly to terrorist organizations, this study deliberately incorporates aspects of hybrid confrontation, including considerations of cyber-attacks or CBRN attacks—potentially surpassing the capabilities of typical terrorist groups. Among the selected events used as sources of insight into potential threats, especially regarding the specific aspects of a particular menace or attack, a scale factor parameter has been identified. This parameter acts as a distorting lens in terms of scenario effects, mitigating the menace in some cases and exacerbating it in others. The historical analysis, while primarily focusing on bombings, also considers events without a final attack (such as the US Embassy in Moscow confrontation) and recent events still under discussion, such as the 'Havana Syndrome disease.'. Furthermore, the concept of introducing a 'sleepy threat' into a building that could remain dormant for weeks, months, or even years before revealing its malicious intent is explored. This concept was exemplified in the Brighton Hotel Bombing of 1984. Conversely, the consideration of a threat working undetected by emitting gamma rays or other less detectable forms of direct energy poses a chronic risk to the health of individuals working inside, accompanied by a significant psychological impact. Thus, the primary focus lies on the functional capability and its maintenance, going beyond the evaluation of a direct attack, be it explosive or CBRN, on the building. From this perspective, it is crucial to consider the impact of temporarily rendering an entire strategic structure out of service, especially when coinciding with another significant event that could have a broad impact on the entire nation. The goal was to develop an original tool and an original work with reference to those available on the open literature [3, 5-7, 23-26].

The quantitative structure and the mathematical formulas used for the parametric tool were deducted adapting the well knows Quantitative Risk Analysis formulation.

The parameters were so built-in form of Products for each of the six domains, using a final summation for the overall result.

5.1 Threat analysis

The threat analysis begins by identifying areas of interest in terms of direct malicious and voluntary threats posed to a building. The historical search for the most compelling case studies related to direct threats and the bibliographic search on CBRN threats led to the identification of domains for the threats, employing a scenario-based approach. While defining threats [3] can offer a well-posed theoretical definition, FEMA documents [6, 23-26] present various approaches, all similarly based on an index system. But what is a threat? FEMA defines a threat as: *'Natural, technological, or human-caused occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.'* Consequently, a multitude of scenarios could arise from a single threat. In this way a Threat acts here as the Hazard acts in the risk analysis in chemical industry and nuclear power plants, with the Hazard Identification (HazId) process corresponding to a Threat Identification process.

5.2 The domains

The threats are categorized into six main domains of scenarios (Table 1). For each domain, a set of threats was identified. Subsequently, specific elements influencing the scenario's magnitude were considered for each threat. This involved highlighting particular parameters such as Vulnerability Weakness, Detection measures, and Mitigation measures, along with a potential Scale Effect. Vulnerability weakness exacerbates the vulnerability produced by a threat, while detection and mitigation measures, obviously, reduce the vulnerability.

Table 1. The classifications of threats is in six domains

1-Layout based
2-Structure & boundary based
3-Technological plant based
4-In/Out ways based
5-Cyber based
6-Management based

The first domain is, unsurprisingly, the layout, as indicated by the historical analysis of bombing attacks. This type of event is not only the most common but also the easiest way for asymmetric and insurgent forces to challenge a state-structured organization or a heavily fortified military presence. To understand the variables involved in such events, a review was conducted, spanning from the Lebanon attacks to the Oklahoma City bombing. Particularly interesting cases include the Brighton Hotel Bombing and the first World Trade

Center bombing attempt, where a suspected CBRN threat was embedded in the Improvised Explosive Device (IED), fortunately without the intended effect.

Table 2. The scenario cluster embedded in the layout domain

1-External explosion
2-Terroristic/military assault
3-External weapon

The three scenarios clusters reflect the building layout vulnerabilities with regard to various events as: Parked car bomb, IED/bomb in Trash container, Suicide car/truck bomb, Terroristic assault, Military assault, Traditional light weapons (e.g. Sniper Rifle), Rocket/anti-tank weapons, Drones, Direct Energy Weapons (Table 2).

The Structure & Boundary Domain encompasses scenario clusters related to the stability of the structure and the boundaries of the building (Table 3). Three groups of scenarios are identified concerning Structure & Boundary.

Table 3. The scenario cluster embedded in the structure & boundary domain

1- External impact
2- External CBRN act
3- Underground action

These scenario clusters were identified by considering the behaviour of the structure and the enclosure boundaries concerning mechanical impacts, including fragments or vehicles, the impact of shockwaves and fire, and the sealing of boundaries in relation to CBRN agents. Various references are available addressing these issues [9, 27-29].

They reflect the building Structure & Boundary vulnerabilities with regard to various events as: external body mechanical impact, shock wave impact, fragments impact, external fire impact, external air weapon impact, Arson Attempt, external toxic gas release, external biologic agent release, external radiological material dispersion, external nuclear weapon explosion, High Atmosphere nuclear weapon explosion (electronic pulse blast), sewers as way of threat, underground tunnels/cavities (Explosive or CBRN underground attacks).

The Technological Plants Domain encompasses scenario clusters related to the technological plants that enable the functioning of the building for its intended purpose. Indeed, this thesis work aims not only to address the physical vulnerability to a potentially deadly threat but also to consider the interruption of functions, especially during the initial hours of a hybrid attack. And this result could potential be obtained without any bloodshed. Just blocking the functionality of the building regarding the following macro scenarios:

Table 4. The scenario cluster embedded in the technological plants domain

1-Water supply
2-Sewers
3-Air treatment
4-Power supply
5-natural gas sabotage
6-Heating supply
7-Data/internet supply

Those scenarios reflect the building Technological plant vulnerabilities with regard to various events as (Table 4):

- Water supply external contaminating agent;
- Supply Interruption;
- Sewers external contaminating agent;
- Sewers function Interruption;
- external penetration;
- Air treatment external contaminating agent;
- Air treatment Service interruption;
- Power Service interruption;
- Natural gas internal explosion;
- Heating supply service interruption;
- Data/internet Supply Jamming or service interruption.

The In/Out Ways-Based Domain addresses gate management and, more broadly, scenario clusters related to perimeter violation, forced entry, takeover attempts, suicide bombing by explosive belts, and similar incidents (Table 5). In essence, this domain encompasses scenarios related to the violation of the building's internal volume, whether through normal doors or access points (e.g., the helicopter deck at the top of the building) or through other specifically opened means by hostile teams.

Table 5. The scenario cluster embedded in the in/out ways-based domain

1-External openings violation
2-External façade intrusion
3-External roof intrusion
4-External helicopter deck threats
5-External underground tunnels threats

For the external pedestrian openings, the scenarios are:

- military hostile attack;
- terrorist act by people on feet;
- introduction of explosive letters or bomb parcel;
- introduction of person with explosive belt;
- introduction of a CBR Agent by letter/parcel;
- introduction of a CBR Agent hidden in person, riots, long term siege from hostiles groups.

For the external car exits the scenarios are:

- military hostile attack by vehicle;
- terrorist act by vehicle;
- placement of sleeping bomb/IED (e.g. to park a sleeping time controlled bomb/IED).

For the external façade intrusion, the scenarios are related to hostile special forces intrusion, while for the External roof intrusion, the scenario is hostile parachute OpSF intrusion.

For the external helicopter deck threats the scenarios are:

- terroristic act by helicopter;
- military attack by helicopter.

For the external underground tunnels threats the scenarios are:

- military hostile attack;
- terrorist act by people on feet;
- external penetration.

On Cyber-Based Domain, it is essential to emphasize that the cyber risk, tragically prevalent at the date falls outside the direct scope of this work. Nevertheless, the scenario-based approach includes events that could potentially impact the functioning of the building negatively (Table 6). This domain encompasses scenarios that are inherently cyber, typically involving malicious software causing a prolonged (hours to days) outage of the building's services.

Table 6. The scenario cluster embedded in the cyber-domain

1-Denial of service
2-Data subtraction
3-Hacking of internal plants
4-Hacking of the building service
5-Loss of control on specific service

The scenarios considered are:
- block of the function of the service;
- data loss and block of the function;
- block of the function of internal plants;
- hazards after hacking natural gas/block of the function/loss of control.

The Management-Based Domain encompasses scenarios related to internal management, ranging from typical espionage operations involving data subtraction or secret data theft to the contamination of basic functional elements such as water, air, or food (Table 7). The foundational concept for this domain is that internal security management and internal security measures are crucial for preventing disruptions to document security and maintaining the uninterrupted function of strategic building services; e.g., deliberate food poisoning, could significantly impact the structure's function, finding substitutes for the affected operators could be a challenging and slow process, and this task is even more daunting for cadres and upper officers.

Table 7. The scenario cluster embedded in the management based domain

1-Security violations
2-Theft of reserved data
3-Theft of precious values
4-Food contamination
5-Water reserve contamination
6-Air contamination

The scenarios related to those threats are:
- security control violation;
- internal restaurant intoxication;
- internal water reserve contamination;
- air treatment contamination.

5.3 The tool parameters

After identifying these scenarios, four main parameters were established for each type of threat to characterize the overall vulnerability of the building to specific threats (Table 8).

Table 8. The tool parameters

1-Vulnerability weakness
2- Detection measure
3- Mitigation measure
4- Scale size effect

These elements form the basis of a checklist, and associated coefficients are applied in the algorithm to produce an overall domain value estimation for the building's vulnerability.

5.4 Detection and mitigation measures

Detection measures are essential elements operating to provide early alarms about specific aspects within each domain. A comprehensive set of detection measures significantly decreases overall building vulnerability (Table 9). Particularly crucial for threats not easily detectable, like CBRN or emerging technologies such as drones and direct energy weapons, detection sensors linked to alarm systems play a critical role in countering penetration attempts by human teams.

Mitigation measures encompass devices, trained personnel, technological systems, and construction details designed to reduce threat vulnerabilities. They may require direct human action or work passively. Examples include bulletproof glass at windows for rifle fire threats. Coefficients are assigned based on effectiveness, with simpler measures having lower coefficients. Passive forms of mitigation, like shielding windows with microwave shielding film, are considered.

That effort conducted to the identification of:

Table 9. The tool parameters

Vulnerability Weakness	n.94
Detection measures	n.42
Mitigation measures	n.56
Scale Size Effect	n.3
alternatives (scale working: *against, neutral, in favour* to service function)	

5.5 The magnitude weighted approach

Following the effort to characterize the variables to be included in the checklist, additional considerations emerged regarding assigning weight to the target of the attack in terms of temporary or permanent strategic damage after the building attack. The literature review on the state of the art, along with an evaluation of how to implement the "strategic value" of the building, led to a parametric choice, like the approach adopted by FEMA documents [6, 23-26].

Beyond traditional deadly attempts, the complexity of modern geopolitical threats necessitates a broader approach to building vulnerabilities, including hybrid threats. A strategic building's significance could be compromised not only by physical attacks but also by cyber threats or those disrupting key functions temporarily. To address these concerns, additional fields have been introduced, focusing on (Table 10).

Table 10. Magnitude weighted parameters

I. Target value
II. Biotargets strategic function
III. Target scale of continuity service needs

Each field includes checkboxes tailored to its parameters, and a coefficient is assigned with only one selection allowed for each field.

6. THE ALGORITHM CHOICE – THE DOMAIN THREAT RISK INDEX

For the algorithm choice, a straightforward formula based on the product of coefficients was adopted. The idea of a product of coefficients is drawn from risk analysis and parametric tools used in risk evaluation for industrial plants, such as the OSHA method, ICI Index method, or Control of Major Hazard UE Seveso Directive parametric tool. This

concept, resembling a Threat Risk Index, accounts for the impact of various parameters on Threat magnitude and impact.

Vulnerability Weakness (Vi): This acts as a magnifier lens on the single threat, increasing its potential effectiveness or likelihood of occurrence. A coefficient greater than unity is associated, with weights evaluated by the author.

Detection Measure (Di): This reduces the single threat magnitude. A coefficient smaller than unity is associated, with weights evaluated by the author.

Mitigation Measure (Mi): This mitigates the single threat magnitude. A coefficient smaller than unity is associated, with weights evaluated by the author.

Scale Size (Si): This is a coefficient sometimes useful to evaluate the effect of the real dimension of the building concerning a single threat. A coefficient normally equal to unity is associated. In specific cases, the coefficient could be elevated or reduced, considering the scale factor for a specific threat.

After specifying parameters for the Threat Domains, a trinomial form is established to assess the building's value in terms of Intrinsic Value, Strategic Function, and Scale of Continuity.

Target Value (Tvi): This parameter has six different values depending on the value of the target. For symbolic targets (e.g., national landmarks), a value of 1 was selected initially, given the challenge of assigning a quantitative value without political or sociological support. Other coefficients have values greater than unity, contributing to the total value of the product.

Target Strategic Function (SFi): This parameter, with eleven different values, considers the specific function of the building. It complements the target value by accounting for the building's strategic function, such as a Ministry for Health or an Air Traffic Control building. The coefficients' values are greater than unity.

Target Scale of Continuity Service Needs (SCi): With seven different values, this parameter considers continuity aspects for the strategic building and the availability of backup systems in case of unavailability after an attack in the broader sense of hybrid confrontation. Coefficient values are greater than unity, with a site featuring real-time backup evaluated more favourably than a site without any backup available. For example, a civil aviation control room can transfer control to another flight control centre in case of a fatal emergency. In this approach, the value of a single threat is represented as the product of several coefficients:

$$\mathbf{(Threat)_i = \Pi V_i \times \Pi D_i \times \Pi M_i \times Tv_i \times SF_i \times SC_i}$$

Mathematical Formula I, the single domain Threat Index Value

However, it can be beneficial to have an index for each domain to highlight strengths or weaknesses in a confrontation with other structures. A simple generalization involves summing the individual threats within a domain:

$$\mathbf{(Threat\ Domain)_J} = \sum_i (Vi \times Di \times Mi \times Tvi \times Sfi \times Sci) = \sum_i \prod Xi$$

Mathematical Formula II, the Overall Threats Index Value

In the precedent mathematical compact formulas, the vulnerability coefficients are connected in a product with the detection coefficients, the mitigation coefficients and the three target characterization coefficients.

At last, the algorithm is represented in a compact mathematical formulation, where *Xi* indicates the generic coefficient.

The final result is a table of six values, one for each domain. It is important to note that, like all indexed systems, the proposed algorithm is unavoidably subject to arbitrariness in both its formulation and the values assigned to coefficients. The theoretical justification of the algorithm's form is based on representing a single threat as a mathematical product, borrowing this mathematical formulation from the risk analysis approach. However, are finement of their values could be achieved through a supplementary application of Bayes 'Theorem on subjective probability, as potential future development of this work. Specifically, the "weight" associated with the coefficients of Vulnerability Weakness, Detection Measures, and Mitigation Measures could be more precisely defined with the input of a diverse pool of experts in building security, CBRN consequence modelling, and Cyber Security. This collective expertise would contribute to a more robust and nuanced evaluation of the "weight" for each specific coefficient.

7. A TEST: THE NATIONAL CONTROL BUILDING OF A MAIN NATURAL GAS GRID OPERATOR

A test was conducted using a developed checklist, focusing on the control centre for the natural gas transport network of a main national gas grid operator in Italy (Figure 3). The new dispatching control room utilizes Supervisory Control and Data Acquisition (SCADA)software to manage real-time variations in parameters for thousands of remotely controlled systems.

Figure 3. The control building for a main natural gas grid operator

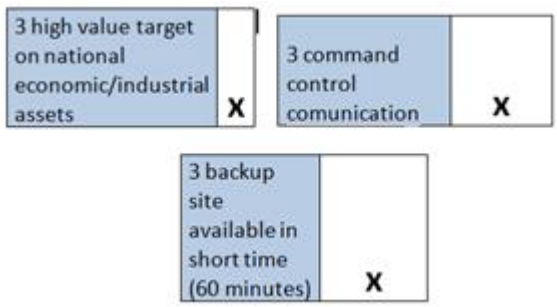

Figure 4. Magnitude weighted parameters for the target value assessment

The design of the block is evidently influenced by security considerations. The block is surrounded by an external wall.

No external windows are apparent, and only within the internal closed courtyard is the structure visible as a regular reinforced concrete block. Identifiable air inlets are not evident, but the main air treatment plants are situated on the top of the roof without visible openings. The strategic importance of the target is evident (Figure 4), as it represents one of the most valuable assets for ensuring the continuity of national services. The risk index was computed across all six domains (Figure 5).

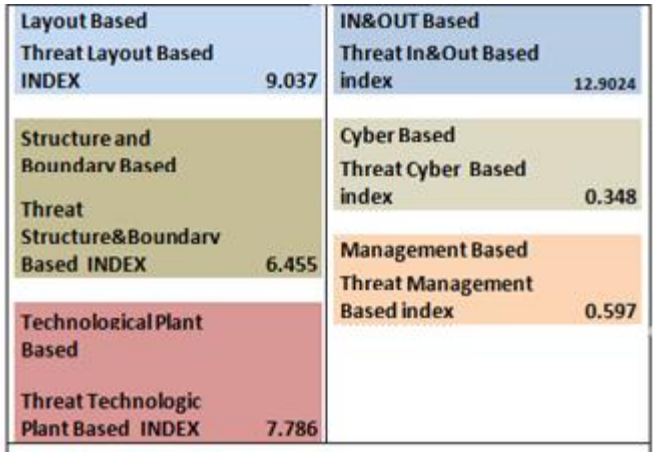

Figure 5. The final threat parameters for each of the six domains

To give an explanation to the weights of various evaluation indicators, it must be considered that they are an index of vulnerability to the threats in each domain previously described.

8. LIMITATIONS AND FUTURE DEVELOPMENTS

The previous results are obviously affected by an intrinsic arbitrariness linked to the weights attributed to the parameters previously described. These parameters can however be refined with specific research, with the collaboration of security officers. The methodological approach is anyway valid.

9. CONCLUSIONS

This work delves in to a specific aspect of building vulnerability analysis within the broader scope, and it could be used as a rapid tool to shortly classify a group of strategic buildings or a single building in terms of Vulnerability to External Malicious Threats, with a focus on CBRN Threats. Originally intended to focus solely on threat analysis, it expanded to encompass detection measures, mitigation measures, and target value characterization. The role of Threat parallels Hazard in risk analysis within chemical and nuclear industries. The historical analysis of building attacks serves as a basis for identifying and classifying scenarios. The scenario-based approach extends the analysis to hybrid scenarios, inspired by FEMA documents. Six domains, associated threats, and specific detection and mitigation measures were identified.

A unique parameter, the scale factor, adjusts the final evaluation based on the threat's scale relative to the building. The Risk Index algorithm, borrowing from the theoretical formulation of Risk Analysis, combines coefficients of vulnerability weakness, detection, mitigation, the scale factor, and the target value trinomial factor. Its efficacy relies on methodological correctness to provide a relative value among different evaluated buildings.

ACKNOWLEDGMENT

Heartfelt thanks are extended to the Italian National Fire brigade for facilitating my attendance in the CBRN Master Level II. Gratitude is also expressed to the teaching staff of Tor Vergata University for their invaluable advice.

REFERENCES

[1] Eskew, E.L., Jang, S. (2014). Damage assessment of a building subjected to a terrorist attack. Advances in Structural Engineering, 17(11): 1693-1704. https://doi.org/10.1260/1369-4332.17.11.1693

[2] National Research Council, Division on Engineering. (2007). Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities: Abbreviated Version. National Academies Press.

[3] Engels, J.I. (Ed.). (2018). Key Concepts for Critical Infrastructure Research. Springer.

[4] Thatcher, T.L., Wood, E.E., Edelson, E.C., Sextro, R.G. (2008). Simplifying the assessment of building vulnerability to chemical, biological and radiological releases. https://eta.lbl.gov/publications/simplifying-assessment-building.

[5] National Research Council, Division on Earth, Life Studies, Board on Life Sciences, Board on Chemical Sciences, Committee on Protecting Occupants of DOD Buildings from Chemical, & Biological Release. (2007). Protecting Building Occupants and Operations from Biological and Chemical Airborne Threats: A Framework for Decision Making. National Academies Press.

[6] Chipley, M. (2003). Reference manual to mitigate potential terrorist attacks against buildings: Providing protection to people and building. Federal Emergency Management Agency.

[7] Various Authors, Physical Security Assessment for Department of Veterans Affairs Facilities, Recommendations of the National Institute of Building Sciences Task Group to the Department of Veterans Affairs, September 2002.

[8] Grier, P. (2012). Cleaning the bug house air force magazine 102. https://www.airandspaceforces.com/article/0912embassy/.

[9] Royal United Service Institute open-source data. https://rusi.org/publication/protecting-buildings-attack.

[10] Royal United Service Institute open-source data. https://rusi.org/publication/preventing-terrorist-attacks-buildings.

[11] CDC NIOSH Guidance for protecting buildings environment from airborne Chemical, Biological or Radiological attacks, 2002. https://www.cdc.gov/niosh/docs/2002-139/pdfs/2002-139.pdf?id=10.26616/NIOSHPUB2002139.

[12] Clark, T.A., Guarrieri, T.R. (2021). Modeling terrorist attack cycles as a stochastic process: Analyzing chemical,

biological, radiological, and nuclear (CBRN) incidents. Journal of Applied Security Research, 16(3): 281-306. https://doi.org/10.1080/19361610.2020.1761743
[13] Wikipedia Open Source on US Marines Barracks Bombings in Beirut 1983 and others bombing attacks reported in this study. https://en.wikipedia.org/wiki/1983_Beirut_barracks_bombings.
[14] Open Source Gospanews. https://www.gospanews.net/en/2020/11/12/nassiriya-alarms-ignored-before-carabinieri-massacre-veteran-hero-tells-tragedy-video-and-calvary-without-military-honors/.
[15] F.B.I: Website. https://www.fbi.gov/history/famous-cases/oklahoma-city-bombing.
[16] U.S. Office of Justice web resource on WTC 1993 Bombing Attack. https://www.ojp.gov/ncjrs/virtual-library/abstracts/world-trade-center-bombers-1993.
[17] Canal Hotel Bombing, Wikipedia Free source. https://en.wikipedia.org/wiki/Canal_Hotel_bombing.
[18] Global Security UN HQ Compound. https://www.globalsecurity.org/military/world/iraq/un-hq-baghdad-bombing.htm.
[19] Centre for Protection of National Infrastructures (U.K.) Protection against Ballistic Attacks. https://www.cpni.gov.uk/protection-ballistic-attack.
[20] FBI web page on US embassies bombing in east Africa in 1998. https://www.fbi.gov/history/famous-cases/east-african-embassy-bombings.
[21] Wikipedia free source on US Embassy bombing east Africa 1998. https://en.wikipedia.org/wiki/1998_United_States_embassy_bombings#Attacks_and_casualties.
[22] Wikipedia free source on Havana Syndrome. https://en.wikipedia.org/wiki/Havana_syndrome.
[23] University of Maryland Factsheet on Terrorist Attacks Involving Package Bombs, 1970 -2017. https://www.start.umd.edu/pubs/START_PackageBombs_FactSheet_Oct2018.pdf.
[24] Center for Strategic and international Studies. List of significant cyber accidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
[25] Risk Assessment a How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings FEMA 452 / January 2005.
[26] Risk Assessment Primer to protect commercial buildings against terrorist attacks FEMA 427/December 2003.
[27] Various Authors Site and Urban Design for Security Guidance Against Potential Terrorist Attacks -FEMA 430 December 2007. https://www.fema.gov/sites/default/files/2020-08/fema430.pdf.
[28] Pfeifer, J.W. (2013). Fire as a weapon in terrorist attacks. Combating Terrorism Center, 6(7). https://ctc.usma.edu/fire-as-a-weapon-in-terrorist-attacks/.
[29] John Hopkins University Protecting Building Occupants from Exposure to Biological Threats. https://www.centerforhealthsecurity.org/our-work/Center-projects/completed-projects/protecting_building_occupants/faq.html.