WP1–BE and SUOD: State of the Art (SoA), risks and human behavior

T1.3 Terroristic acts (SUOD) in BE: SoA with identification of conditions/factors (in outdoor BE) influencing the risk. Current mitigation strategies analysis. Definition of human behavior including crowding conditions by combining SoA data and real-world events analysis

DELIVERABLE ID	D1.3.2
Deliverable Title	Current BE terrorism risk management and reduction strategies
Delivery date	M6
Revision	1.0
Main partner	UNIVPM
Additional partners	
Authors of the contribution	Gabriele Bernardini (UNIVPM); Enrico Quagliarini (UNIVPM); Michele Lucesoli (UNIVPM)
Deliverable type	report
Number of pages	44

Abstract

A resilient and sustainable Built Environment should ensure an adequate level of safety in case of unintentional as well as of intentional disasters. The most significant intentional disasters in today's BE is related terrorist attacks, which can involve strategical elements of the BE as well as elements with a symbolic value, like those subject to crowding. Risk-mitigation and reduction strategies (RMRSs) to face terrorist threat should be selected according to the specific features of the BE where to intervene. Meanwhile, these strategies can have a specific impact on the terrorist menace which varies over time and over space, as well as by considering the necessity to preserve the security or the safety of the BE and of its users. This deliverable provides an analysis of the current RMRSs starting from the different classification provided by literature works. Then, regulations and guidelines from different Countries all over the Word are analyzed by organizing the RMRSs according to four key factors in the BE: the physical elements in the BE, the BE layout, the access and surveillance system of the BE and the management issues before and during an attack. The discussion of results evidences how the selection of specific RMRSs should depend on the possibility to apply it to the BE according to sustainability and redundancy criteria. Furthermore, human-centered aspects should be also included for the RMRSs selection, by moving towards holistic methodologies that include the simulation of the emergency conditions. On these terms, this deliverable creates the bases for following activities while be combined to the risk matrix definition in D1.3.1.

Keywords

Terrorist attack; risk mitigation; risk reduction; classification; Built Environment; emergency response

Approvals

Role	Name	Partner
Coordinator / Task leader	Enrico Quagliarini	UNIVPM

Revision versions

Revision	Date	Short summary of modifications	Name	Partner
0.1	20.03.2020	Comments on section 3 and reorganization of the Annexes according to D1.3.1	Fabio Fatiguso, Elena Cantatore	POLIBA
0.2	05.04.2020	Solving comments and integrating section 3 and the Annexes	Michele Lucesoli	UNIVPM
0.3	05.06.2020	Abstract and graphical abstract revision	Gabriele Bernardini, Michele Lucesoli	UNIVPM
1.0	16.07.2020	final proofreading and editing	Enrico Quagliarini	UNIVPM

Summary

1. Introduction

Terrorist acts are performed in the Built Environment (BE) by people "who aim to hurt innocent people, kill or injure them, or inflict significant damage on essential infrastructure at a single instant or over time, or plan to do so, in order to bring about political, religious or ideological aims" (Gordon et al. 2017). In this sense, although they are characterized by the "will" of the attackers, they are generally triggered by a hazardous event that emerges quickly as well as (generally) unexpectedly (UNDRR; National Consortium for the Study of Terrorism and Responses to Terrorism (START) 2019). Hence, according to the disaster classification of D.1.1.1 (see i.e. Section 2.1), they can be characterized as a human-made and SUdden Onset Disaster (SUOD), and, in particular, as destructive actions due to human-made causes and showing sudden onset occurrences (Cozzolino 2012; Jore 2019).

Terrorist acts are generally performed in the BEs placed in urban areas, due to the significant features of such targets in terms of *quality* (e.g.: strategic buildings and symbolic targets[1], such as cultural, religious and institutional places; critical infrastructures allowing the operational, societal and economic functioning of communities, which can be generally defined as "hard targets"; presence of sensitive people in the BE, such as those politically or religiously exposed) and *quantity* (in terms of e.g.: number and typologies of BE users, including tourists; economic values of the BE and of the hosted activities) of the exposed elements (National Research Council 1987; Karlos et al. 2018; Zoli et al. 2018)[2]. In this sense, BEs placed in largest cities seems to be more potentially affected by terrorist acts in respect to small villages, due to the possibility to maximize the effects in term of fatalities, material, economic and symbolic (including psychological or political effects) damages (Coaffee et al. 2009; Woo 2015; Beňová et al. 2019).

According to the international classifications of terrorist targets, by including the ones of the European Commission definitions (Bennett 2017; Karlos et al. 2018; Lapkova et al. 2018; Beňová et al. 2019), BEs and their composing elements can be divided into "hard" and "soft" targets depending on the principal risk management and protection strategies that are applied to them. In general terms, "hard targets" are characterized by codified and significant control (including restrict access levels to the public) and protection (including armed guards) measures (e.g. government buildings, military institutions; additional strategic buildings according to National regulation[1]) (Bennett 2017; Marchment and Gill 2019).

Meanwhile, all those vulnerable civilian sites hosting a large numbers of people (usually, unarmed and without/with limited access restrictions) can be considered as "soft targets", and they "may be selected by terrorists in their effort to maximize casualties, thus inflicting fear to the population and attaining media coverage" (Karlos et al. 2018). In relation to the *characteristics of use* of the BE and the related elements categorization offered by D1.1.1-Section 3 and by the survey form defined in D.1.1.2-Section 2.5, sights and sensitive targets generally own "high concentration of people, low or no security against violent attacks and attraction for the attacker" due to the exposure contents (Lapkova et al. 2018), thus being ideal "soft targets" for terrorist acts. *Slights* (e.g. including pedestrian areas) and specific *sensitive targets* composing the BEs (e.g. cultural or religious ones) are all the elements in the urban BEs that generate tourism, independently or not to the construction or symbolic features, thus additionally generating a critical crowding level in relatively small areas (for outdoor public spaces, squares, avenue and so on) (Woo 2015; Karlos et al. 2018; Lapkova et al. 2018; Kılıçlar et al. 2018). In fact, such BEs can also temporarily host mass gathering events, such as

[1] Concerning strategic buildings for the Italian context, please also compare D.G.R. n. 1384/2003 and *Decreto del Capo del Dipartimento di Protezione Civile* n. 3685 of 21/10/2003

[2] See also D.1.1.2-Section 2.5 for BE elements definition and related characterization data collection.

concerts, festivals, etc., being very attractive for terrorists "for their insufficient or minimal security measures" (Beňová et al. 2019). Finally, some other strategic buildings[1] devoted to educational and health purposes can both host high people concentration and have a symbolic value due to their intended use (Karlos et al. 2018; Beňová et al. 2019), while being affected by potential additional crowd conditions in presence of specific events.

Different risk management and reduction strategies to face terrorism threats in BEs are essentially aimed at deterring, detecting, delaying and managing the effects of a terrorist attack and depend on the BE ("target") in which they are applied (Home Office in partnership with the Department for Communities and Local Government 2012a; ANZCTC 2017; Bennett 2017; Karlos et al. 2018). According to what reported in D1.3.1, Section 2 about general issues concerning safety of BE against terrorist acts, "Hard targets" generally adopt codified standards for counter-terrorism actions due to their internal organization as well as to their scarce relationship with other surrounding BEs (e.g. military areas are surrounded by protection barriers). On the contrary, strategies involving "soft targets" (including open public spaces in the BE) should be specifically defined according to specific aspects, e.g. (Coaffee et al. 2009; Home Office in partnership with the Department for Communities and Local Government 2012b; Mistretta et al. 2014; Marchment and Gill 2019; Cuesta et al. 2019; Laufs et al. 2020): spatial and functional interactions between the target itself, the possible composing elements (e.g. buildings facing Linear or Areal BEs, areas inside an open space in the BE) and the bordering BEs; possibility to contemporarily host different activities and spaces uses; dependencies with "hard targets" placed nearby; individuals' perception issues; aesthetic features of the BE, especially in relation to historical scenarios. Such strategies could be also used in a combined manner, so as to be as effective as possible (Coaffee et al. 2009; Li et al. 2017; Karlos et al. 2018; Kılıçlar et al. 2018; Beňová et al. 2019; Cuesta et al. 2019):

1. *before the terrorist act*, to deter, detect and delay the emergency conditions thanking to, i.e., preventive risk-mitigation solutions based on system implementation in the BE or BE management procedures by stakeholders and Law Enforcement Agencies-LEAs);
2. *in attack-affected conditions*, to manage them, i.e., by using LEAs support and by organizing the BE and its elements to also actively promote safe behaviors in the exposed individuals.

In this sense, the risk-mitigation and management solutions should be hence oriented towards the following main sustainability criteria (John Garrick et al. 2004; Coaffee et al. 2009; Bernardini et al. 2017; Gayathri et al. 2017; Li et al. 2017; Festag 2017; Ahmed and Memish 2019; Beňová et al. 2019; Ghazi and Abaas 2019; Laufs et al. 2020; Zhu et al. 2020):

- moving towards redundancy criteria of the resilient BE by combing different strategies to ensure that each of them could support the risk-reduction process (according to different operational procedures) in all the phases of the disaster;
- selecting solutions to be effective for more than one terroristic threat/attack typology;
- adopting a human-centered approach to include the behavioral reaction of the exposed individuals (especially in crowds) and of the terrorists, also in respect to the human-BE interactions (i.e. for the promotion of correct emergency behaviors);
- including mass gatherings conditions while the strategies planning, so as to ensure safety and security aspects in relation to different BE use situations;

- considering the possibilities of connecting different BEs (at local scale, e.g. indoor-outdoor; at a global/urban scale) to face the disaster (e.g. compare to "invacuation" strategies, in which the traditional approach to safety is inverted)[3];
- promoting a psychological function of the strategies, so as to ensure being perceived as reliable by the citizen, to deter the terrorists but also to guarantee the livability of the BE under normal use conditions.

For instance, a sustainable and integrated solution can be related to the implementation in the BE of video surveillance systems, which could be used before the event to detect "anomalous" behaviors related to possible terrorists and during the event to coordinate the security forces actions and the evacuation process (Laufs et al. 2020). Connecting the risk-management and reduction strategies from these "sustainability perspective" will lead to move towards a holistic protection perspective, although specific strategies can exist depending on the considered terrorist attack (e.g. armed assault, bombing, vehicle attack and so on).

In view of the above, this report is aimed at tracing a review of the current strategies for risk-management and risk-reduction adopted in a consolidated manner in the BE and in its composing elements, by mainly focusing on the "soft targets" characterization because of the aforementioned criticalities in applying such solution an because of the complexity in relation to the BE S²ECURe application field. To this scope, while a complete overview of risk assessment towards a risk matrix for terrorist act is performed by D1.3.1, the activities of this research are based on the analysis of existing counter-terrorism measures codified by national and international regulations and guidelines.

In particular, they are discussed according to the main common classification criteria proposed in Section 2, then focusing on a BE-composing elements perspective, in view of the aforementioned categories and key challenges for sustainable risk-mitigation and reduction solutions. In particular, results offered by Section **Errore. L'origine riferimento non è stata trovata.** are organized also in relation to timing issues (effectiveness of the solutions before/during the attack), dependency on the attack typology, relation with crowded places and mass gathering events. Additional relations with the criteria of sustainability (including redundancy, correlation with BE livability, application to the BE typologies) are additionally discussed in Section **Errore. L'origine riferimento non è stata trovata.**.

2. Classifications of risk management and reduction strategies in relation to the BE prone to terrorist acts

This section outlines the bases of the classification of Risk Management and Reduction Strategies (in the following, RMRSs) to be adopted in the BE by dealing with the fundamental issues previously pointed out by literature works, as specifically pointed out below, and international review guidelines (i.e. EU-related ones due to the overall BE S²ECURe project application context (Karlos et al. 2018)). Hence, the first part of the section involves the considerable existing classification approaches to RMRSS (Section **Errore. L'origine riferimento non è stata trovata.**), and such classification can be also used as bases for general risk assessment and risk matrix development according to D1.3.1 outcomes (i.e. compare to Section 5 in D1.3.1) (Federal Emergency Management Agency 2009; Matsika et al. 2016). Then, the second part concerns the

[3] According to *PD 25111:2010 – "Guidance on Human Aspects of Business Continuity"* and similarly to "shelter-in-place" strategies, the "invacuation" proposes "the movement of people to pre-identified areas inside the building/site in order to protect them from external dangers during an incident", without leaving the disaster-affected BE. In many terrorist acts (e.g. armed assault in pedestrian areas or cehicle attack), it concerns the possibility to remain inside the building or reaching the nearest one, and to wait inside for the security forces arrival.

criteria to organize and discuss the RMRSs adopted by this work, by additionally listing the analyzed documents (Section **Errore. L'origine riferimento non è stata trovata.**).

2.1. Overview of considerable existing classifications

According to the literature overview offered by Section 1, RMRSs can be classified according to the main criteria summarized by Table 1. Target-oriented classifications are based on the specific features of the BE prone to the terrorist act, mainly in terms of hosted activities (see Section 2.1.1). The attack-oriented classification evidences that RMRSs should face specific threat conditions (see Section 2.1.2). Time-dependent and space-dependent strategies underlines how RMRSs have different goals depending on their relationship with the terrorist attack timing (see Section 2.1.3). Space-dependent oriented classifications are based on the localization of the strategies into the BE itself (see Section **Errore. L'origine riferimento non è stata trovata.**), thus sharing implementation criteria with architectural and management issues in RMRSs application in the BE (see Section 2.1.5).

Table 1. Summary of classification of RMRSs in the terrorism-prone BEs, by outlining main classification options, differences to classify the RMRSs depending on their purpose or implementation-related features, the main references and the interactions among the classification criteria.

General classification criteria (Section S number)	Main classification options	Differences in RMRSs (main references)	Main References
Target-oriented (S 2.1.1)	Hard/soft target	based or not on restricted access control, invasive surveillance and strongly-protected BE border limits	(Bennett 2017; Zoli et al. 2018; Beňová et al. 2019)
	Level of (in)visibility	perception by the BE users due to the level of implementation in the BE	(Coaffee et al. 2009)
	BE main intended use	differences of operational procedures in BE use and in BE configuration due to the normal use by occupants and stakeholders	(Federal Emergency Management Agency 2009; NaCTSO - National Counter Terrorism Security Office 2017; Karlos et al. 2018)
	Safety/security	limiting failures and protecting the public versus limiting intentional damages and protecting the public order	(Bernardini et al. 2017; Jore 2019)
Attack-oriented (S 2.1.2)	Threat type	where/from where the attack is performed by the terrorists	(Federal Emergency Management Agency 2009)
	Typology of attack	facing the effects of weapons used by the assaulters	(Kalvach and et al. 2016; NaCTSO - National Counter Terrorism Security Office 2017; Lapkova et al. 2018; Beňová et al. 2019)
Time-dependent (S 2.1.3)	Before/during	effectiveness before the attack (e.g. to deter it) or during it (e.g. to manage the consequences)	(Kalvach and et al. 2016)
Space-dependent (S 2.1.4)	Different zones (layer of defense) of the BE	area/line of application of the strategy in the BE layout in respect to the surrounding and internal elements	(GSA 2007; Federal Emergency Management Agency 2011; Bernardini et al. 2017)
Physical versus Management (S 2.1.5)	physical/management	implemented into physical elements of the BE or by using operational procedures (based on staff actions)	(NaCTSO - National Counter Terrorism Security Office 2017; Joint Counterterrorism Assessment Team (JCAT) 2018; Karlos et al. 2018)

2.1.1. Target-oriented classifications

A basic classification of RMRSs can be related to the *target definition* on which they are applied (Bennett 2017; Zoli et al. 2018; Beňová et al. 2019). Contrary to RMRSs for "soft targets", the classification of general RMRSs for "hard target" mainly involves the restriction of the area access to the public and the existence of invasive surveillance solutions by Security Forces. From this point of view, RMRSs can be generally divided into *active and passive strategies* (Coaffee et al. 2009). "Hard" strategies include "electronic surveillance, private security guards, and the laws and rules of conduct that can restrict actions, influence behaviors or impede interaction", while "soft" strategies "are rather more subtle and include aesthetic and 'streetscape' features" (Coaffee et al. 2009). Active and passive RMRSs could be classified according to their *level of (in)visibility in the BE*, thus influencing different perception levels on the hosted users as well as on the terrorists (Coaffee et al. 2009). In particular, *invasive RMRSs* are generally characterized by a high impact on the BE in terms of application since they include a widespread implementation of the measures (active strategies like video surveillance systems or Security Forces control) and a significant aesthetic impact (passive strategies like heavy barriers), thus being more oriented towards the context of the hard targets. Hence, they generally have a low level of sustainability for the BE especially in relation to normal use conditions, being oriented to overt security purposes. On the contrary, *visible RMRSs* are integrated in the BE by maintaining a reduced aesthetic impact since they can be used also for normal use conditions according to a 'camouflaged' approach (passive strategies like urban furniture that can be used as barriers in case of terrorist attack). Finally, *invisible RMRSs* are not perceived by the public since they are "covertly embedded within the urban landscape" (Coaffee et al. 2009) or they are applied to specific elements in the BE which are not generally acknowledge as security-oriented by the public (e.g. façades). In this sense, visible and invisible RMRSs are more oriented towards the soft-targets application, by leading to a "security by design" approach for a sustainable BE (Karlos et al. 2018).

In the general context of the risk matrix for terrorist acts defined by D1.3.1 (i.e. Section 2.1), according to the aforementioned target-oriented classification and focusing on "soft target"-related issues, other approaches can distinguish the RMRSs depending on the *BE main intended use* (Federal Emergency Management Agency 2009; NaCTSO - National Counter Terrorism Security Office 2017; Karlos et al. 2018), basing on the national regulations concerning them. In particular, RMRSs can be divided according to the following classification, which is based on the combination between intended use of BE and crowd conditions (e.g. occupants' loads, typology of hosted individuals in terms of familiarity with the BE and so on):

- *public spaces*, such as commercial ones (mainly, great shopping centers), sporting (stadia, arenas and playgrounds in general, both in indoors and outdoors) and entertainment (e.g. theaters, cinemas) BEs, accommodation facilities (e.g. hotels), restaurant and bars/pubs, BEs hosting mass gathering events or possible crowd conditions (both indoor and outdoor, e.g. pedestrian areas). It is important to evidence how such solutions can be closely combined to those related to additional safety fields, i.e. fire safety and workers' safety and health, especially for those hosted by buildings in the BE;
- *BEs for education, religion and health*, since they can be grouped in with similar crowd conditions, partially controlled access systems (e.g. depending on the different areas of the BE, like for schools or hospitals) and symbolic features as a terrorist target;
- *BEs for transportation*¸ which are characterized by the possibility of areas with restricted access and also need to coordinate the RMRSs by contemporarily involving the BE occupants' and passengers'

(on board the means of transport) safety, the modelling of specific damage and injuries due to the transportation hub typology, and the business continuity elements.

BE as working places[4] *and residential buildings* could be involved by less complex strategies essentially due to the possibility to control the access to the areas, thus intervening on specific elements of the BE or on management issues (also compare to classification shown by Section **Errore. L'origine riferimento non è stata trovata.**) (Federal Emergency Management Agency 2006, 2009; Government 2015).

In such a context, RMRSs connected to significant crowd levels in these BEs assume a transversal rule due to the risk-increasing factors induced in the management of terrorist acts (NaCTSO - National Counter Terrorism Security Office 2017; Australian Institute for Disaster Resilience (AIDR) 2018). Nevertheless, regulations and guidelines evidence the dependency between such scenarios and specific RMRSs in outdoor BE (e.g. open spaces in the BE) in respect to, i.e. the hosted event (in terms of crowd typology and quantity), the event layout in the BE, the definition of different zones open to public, the access system, the emergency management system and facilities (Joint Counterterrorism Assessment Team (JCAT) 2018; Ministero dell'interno 2018).

Another target-oriented classification could involve the differences between *safety* and *security* goals for RMRSs to be implemented in the BE (Bernardini et al. 2017; NaCTSO - National Counter Terrorism Security Office 2017; Joint Counterterrorism Assessment Team (JCAT) 2018; Jore 2019). Although additional differences and similarities between the two goals exist, it can be evidenced how (Bernardini et al. 2017; Jore 2019):

- *safety* strategies are essentially oriented towards the protection of the hosted users from all the failures that can appear in the BE (thus limiting the fatalities due to the BE use in some risk-increasing conditions, e.g. those of mass gathering events, as well as due to the consequences of the terrorist acts, e.g. injuries and deaths due to the attack-related emergency);
- *security* strategies are essentially oriented towards the contrast of intentional actions due to the terrorist act so as to preserve the public order (thus including, e.g., all the measure performed by the Security Forces before and during the attack).

Such differences have been also clearly codified in some national regulations[5] to provide a specific support to designers while deploying strategies in specific context, i.e. those connected to mass gathering events, which can be used as RMRSs (e.g. also compare the concept of safety personnel and security personnel in the BE (Joint Counterterrorism Assessment Team (JCAT) 2018)).

Finally, another target-oriented classification can focus on the whole actions identified according to the users' participation, by outlining (Federal Emergency Management Agency 2007; (NaCTSO) et al. 2012; Coaffee and Fussey 2015; Karlos et al. 2017; Peleson 2019):

- *Active actions*, when a bi-univocal relation between overarching governances and urban users is activated, by including prevention (I.e. active military intelligence), mitigation (I.e. Active Education of BE users) and Security/safety (active surveillance solutions);
- *Passive actions*, in which any feedback is established by users and overarching rules/guidelines/indication are simply applied, by including prevention (I.e. passive normative

[4] in this case, please also compare strategies related to safety and health of workers from a national point of view.
[5] I.e., in Italy, compare to: circolare 7/6/17 Min. Interni n. 555/OP/0001991/2017/1; direttiva del Capo Dipartimento VVF, Soccorso Pubblico e Difesa Civile, prot. 11464 del 19/6/17; circolare 28/7/17 N. 11001/110(10) Min. Interni

regulations) mitigation (I.e. passive information of the BE users) and Security/safety (i.e. soft strategies for urban spaces design and security)

In this sense, such strategies can have a relation of impact with respect to the implementation through the aforementioned "hard" and "soft" strategies, as well as with respect to the relation and interaction levels with the users (compare to D1.3.1, Section 2.3 and Section 2.4).

2.1.2. Attack-oriented classification

The RMRSs can vary depending since they should response to the features of the terrorist acts. Main classifications can refer to the following issues.

Firstly, RMRSs can be organized according to the *threats types* (Federal Emergency Management Agency 2009) to be faced. Internal threats, which essentially involves the "intrusion into the building[6] by a person or persons with the intent of executing an attack", could be mainly faced by access control strategies (compare to hard/soft target classifications) inside the BE, contrarily to external threats, which imply the attack from the outside of the BE.

Secondly, some RMRSs can be effective in a limited number of *typologies of attack* (Kalvach and et al. 2016; NaCTSO - National Counter Terrorism Security Office 2017; Lapkova et al. 2018; Beňová et al. 2019). Concerning different attack typologies, please also compare D1.3.1, Section 3.2 (National Consortium for the Study of Terrorism and Responses to Terrorism (START)). Although the "modus operandi" of the terrorists can vary over time and space, main recurring typologies can be classified as follows (in squared brackets are reported the analogous attack-types of the Global Terrorism Database GTD classification according to D1.3.1 Section 4.1.1):

1. *bombing attack* by different strategies, and mainly: explosive devices (including Improvised Explosive Devices-IDEs), directly placed in the BE; car bomb (parked); suicide bombing attack and car bomb driven by a suicide attacker running into the target, based on the terrorist's actions in the BE; bomb delivered by mail [Bombing/Explosion];
2. *armed assault* (pistol, machine gun and so) which implies one or more active shooters (including sniper's assault), and which lead to assassination [Armed Assault];
3. *attack with a cold weapon* (e.g. knife), by one or more active terrorists [Armed Assault];
4. *hostage taking* and *barricade situations* (in transportation BEs, also hijacking) [Barricade Incident; Kidnapping; Hijacking];
5. *crowd attack to a soft target*, such as in case of insurrections [Unarmed Assault];
6. *vehicle running into the target*, which could be performed in open spaces in the BE or towards the BE elements perimeter [Armed Assault];
7. *arson*, which can be essentially fight by combining RMRSs to fire safety strategies [Armed Assault];
8. *unmanned Aircraft systems*, which can be used to perform direct attack as well as to support the use of other weapons or to collect information before an attack [Armed Assault].
9. *Chemical, Biological and Radiological (CBR) attacks*, which can be performed in different ways, as for bombing attack-related ones [Armed Assault];
10. *facility attacks*, which can compromise the functionality of a BE by limiting/affecting the state of their infrastructural elements (e.g. water or electrical supply, cyberterrorism towards the BE

[6] In general terms, into the BE.

facilities), thus provoking not only physical damages but also economic and social ones [Facility/Infrastructure Attack];

Most of the aforementioned "modus operandi" involve short-terms effects on the BE and its users (e.g. points 1 to 8), while some kinds of attack could produce long-terms risk conditions in the BE (i.e. point 9) or disruption (e.g. point 10).

Finally, terrorist attacks are evolving in a dynamic manner, "shifting from symbolic, highly planned attacks to attacks that could occur anywhere, at any time, with the potential for mass casualties and infrastructure damage" (US department of Homeland Security 2018). RMRSs could have the necessity to face localized attacks as well as Complex Coordinated Terrorist Attacks (CCTAs), such as multiple attackers' teams, attack locations, and attacks types. RMRSs to face CCTAs require a more complex cooperation system between the solutions implemented within the BE, the First Responders, the Security Forces, and the community (Ruiz Estrada and Koutronas 2016; US department of Homeland Security 2018).

2.1.3. Time-dependent classifications

RMRSs to be implemented in the BE could be also distinguished *depending on time*, thus being correlated to the kind of threat and attack as discussed in Section 2.1.2. Preventive (effective *before*, i.e. to deter, detect and delay) and emergency management (effective *during*) strategies can be mainly identified since they respond to different counter-terrorism goals (Federal Emergency Management Agency 2009; Home Office in partnership with the Department for Communities and Local Government 2012a; Kalvach and et al. 2016; Bernardini et al. 2017; Li et al. 2017; Gordon et al. 2017). Furthermore, emergency management strategies to be applied during and after the incident have different priorities depending on the operational timeline, thus limiting the effectiveness of some of them to specific time spans (Kalvach and et al. 2016). This kind of classification can be also related to the timing of behavioral issues in case of a terrorist act, thus relating the RMRSs to the contrast of risky behaviors or the promotion of correct responses by the users of the BE (Bernardini et al. 2017; Li et al. 2017; Gordon et al. 2017; Lin et al. 2020; Zhu et al. 2020). In this view, RMRSs could be related to the different phases characterizing a terrorist act, which show different behaviors depending on the man-man, man-BE and man-threat sources interactions (Bernardini et al. 2017; Zhu et al. 2020)[7].

2.1.4. Space-dependent classifications

Regardless of the BE target-related features and main intended use and of the BE specific layout (e.g. in relation to the configuration of open spaces in the BE, as suggested by D1.1.1-Section 3), RMRSs to be implemented in the BE could be distinguished *depending on space*, thus being correlated to the kind of threat and attack as discussed in Section 2.1.2 as for time-depending classification.

From a general point of view, since terrorist acts are generally focused on specific elements in the BE, RMRSs should be differently organized according to the considered distance from the target, by creating different zones (Federal Emergency Management Agency 2006, 2011; Australian Institute for Disaster Resilience (AIDR) 2018; Consiglio Nazionale delle Ricerche - COMMISSIONE DI STUDIO PER LA PREDISPOSIZIONE E L'ANALISI DI NORME TECNICHE RELATIVE ALLE COSTRUZIONI 2018; Li Piani 2018). This concept is mainly associated to bombing or armed assaults (compare the stand-off distances and the related zones), but it could be also applied for other kind of attack, e.g. vehicle attacks (i.e. relation between areas that can be accessible or not by the vehicles). Hence, such a classification evidences how the strategies should be

[7] Such aspects will be analyzed by D1.3.3 according to the BE S²ECURe tasks goals.

deployed by considering the effective BE features and the relation between each part of it and the surrounding BEs (GSA 2007; Federal Emergency Management Agency 2011; Li Piani 2018).

On these bases, "zone" or "layer of defense" design approaches to the BE has been organized by previous guidelines, thus focusing on the BE site definition (GSA 2007; Federal Emergency Management Agency 2011). Figure 1 schematize the main elements of the "zone" and the "layer of defense" design approaches for general BEs (e.g. the simplest configuration given by an isolated building site – see Figure 1-A), linear BEs (see Figure 1-B) and areal BEs (see Figure 1-C).

In particular, the main and essential RMRSs-related scheme can be based on existing regulations based on the following 3 "layers of defense" (Federal Emergency Management Agency 2011):

- the *First (or Outer) Layer* (in the following, *L1*) is composed by all the barriers placed at the borders of the considered BE (e.g. for isolated buildings, the property line; for complex linear or areal BEs in urban scenarios, the limit of the area considered to be protected by RMRSs). The urban areas and the BEs placed beyond *L1* are not controlled by the BE stakeholders and users. *L1*-related RMRSs are essentially based on the possibility to create a limit for the BE-related RMRSs as well as to provide a first limit of the standoff distance around the considered BE in respect to the surrounding BEs. In such context, all the RMRSs related to urban resilience could be included (e.g. involvement of the population, security and safety strategies for urban areas, security forces operation and counterterrorism actions) (Gordon et al. 2017; Karlos et al. 2018; Laufs et al. 2020);
- the *Second (or Middle) Layer* (in the following, *L2*) is associated to the BE part deployed from the BE internal border to the exterior limit of the core elements in the BE (i.e. the building envelope, or, in more general terms, the physical envelope of subparts of the BE also in outdoors, such as specific barriers enclosing areas in the BE[8]). Hence, *L2*-related RMRSs provide a standoff around each elements of the BE to be protected, being under the direct control of the BE stakeholders. The BE site hence includes all the areas in the considered BE, by referring to both those which can host the core elements into the BE (compare to the following Third Layer) and to the distribution spaces (e.g. access roads, evacuation paths, ancillary spaces);
- the *Third (or Inner) Layer* (in the following, *L3*) usually refers to the envelope and/or to the inside of the core elements in the BE, which can be majorly identified as attack goals. It can mainly involve buildings, according to the original regulation approach (Federal Emergency Management Agency 2011), but also outdoor areas, such as band stages, art stands, observation areas open to the audience (Bernardini et al. 2017; US department of Homeland Security 2018). This layer separates "unsecured from secured areas". Hence, *L3*-related RMRSs are effective to limit the possibility that a terrorist act could happen or affect the core of the BE.
-

[8] e.g. courtyards, gardens, restricted access areas in public open spaces in the BE (including those related to temporary BE use conditions, such as for mass gathering events).

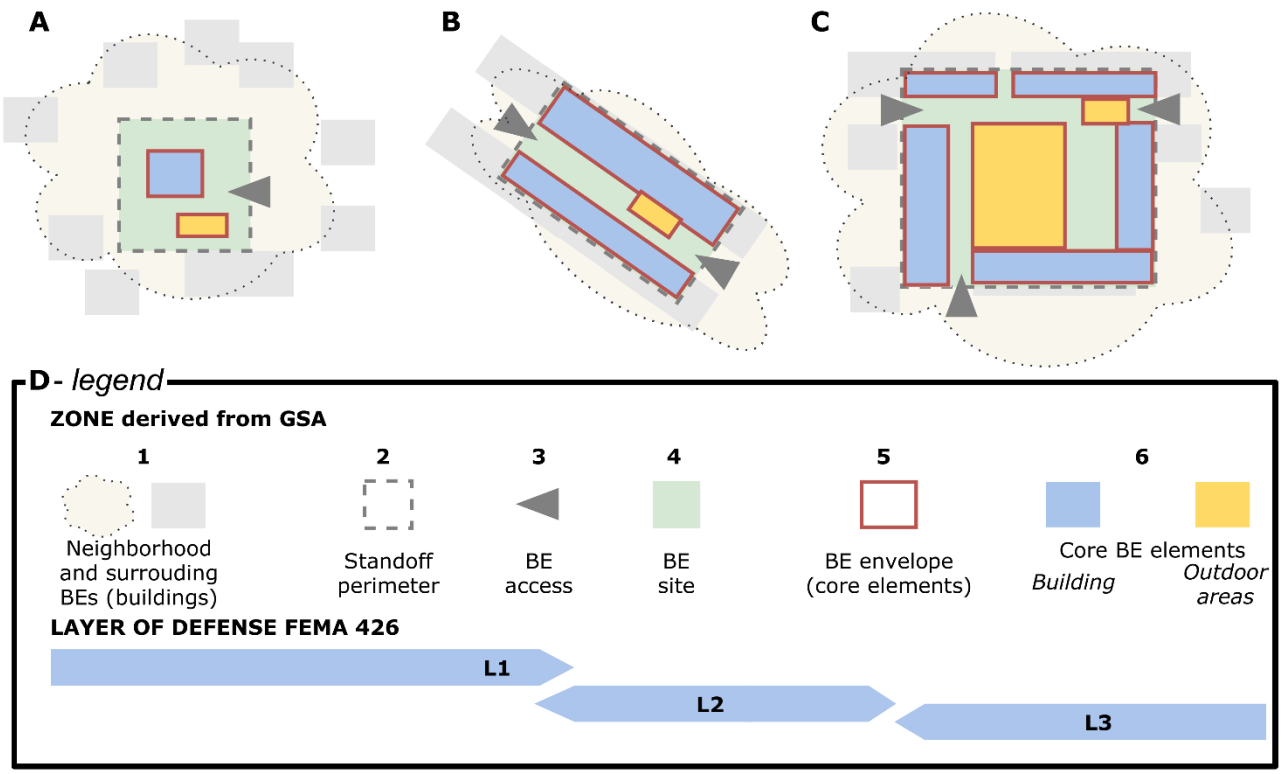


Figure 1. Scheme of the "zones" and "layer of defense" approaches to RMRSs in BE for: A-general BE (e.g. isolated or single buildings); B-linear BE; C-areal BE. On the bottom (D), the zoning scheme derived from (GSA 2007) *is compared to the layer of defense given by FEMA 426* (Federal Emergency Management Agency 2011)*, by evidencing the legend for the upper part of the figure.*

2.1.5. Physical versus management-oriented classifications

Previous works categorize the RMRSs depending on *physical and management-related elements* composing the BE on which designers should act to reduce or to respond to the terrorist risk (Federal Emergency Management Agency 2009, 2011; NaCTSO - National Counter Terrorism Security Office 2017; Joint Counterterrorism Assessment Team (JCAT) 2018; Karlos et al. 2018).

The main *physical* elements composing the BE are essentially the buildings and the open spaces in the BE (by including all their furniture), according to D1.1.1 results (i.e. compare D1.1.1-Section 3), thus following the general "layer of defense" scheme discussed by Section 2.1.4 (Federal Emergency Management Agency 2011). In particular, if considering the furniture in the BE (mainly, for open spaces in the BE), we could considered permanent and temporary application of the RMRSs-related elements (Coaffee et al. 2009; Joint Counterterrorism Assessment Team (JCAT) 2018; Ghazi and Abaas 2019), thus dealing with livability and (in)visibility concepts (also compare to Section 2.1.1 discussion).

The physical measures adopted in three layers should be additionally supported by *management* strategies, essentially based on the operational aspects in the BE, and, mainly on (Federal Emergency Management Agency 2011; NaCTSO - National Counter Terrorism Security Office 2017; Karlos et al. 2018; Kılıçlar et al. 2018): security and safety planning strategies to be applied before and after the attack, based on risk assessment methodologies which can better identify the BE vulnerabilities; people involvement, so as to

improve risk-awareness, preparedness and response of the users towards an attack; policies, regulation and finance (including insurance-oriented) support to the activities hosted in the BE (mainly, economic ones and those with social impact). Finally, some RMRSs can involve different physical and management issues, regardless of the BE to protect: main examples are represented by drone-based and video surveillance-based RMRSs, which should adopt specific management actions by being supported by the implementation of physical measures in the BE (Karlos et al. 2018; Laufs et al. 2020).

2.2. Adopted organization criteria for RMRSs and bases of their evaluation

Main regulations and guidelines from all over the World to define general RMRSs to be applied in the BE prone to terrorist acts are analyzed according to a *BE-key factors oriented approach* which takes advantages of the classification criteria defined in the previous sections, as well as of those related to other SUODs (i.e. fire safety).

Firstly, the documents have been selected by starting from existing international reports (i.e. (Karlos et al. 2018)) and by considering if they are publicly available in EU working languages (i.e. French, English), while Italian documents have been included so as to focus on the BE S²ECURe national application context. In particular, recent documents are considered by focusing on updated versions, but those including essential definitions on RMRSs, BE-related strategies and design guidelines for the following regulation and guidelines are also included. Table 2 summarizes the list of documents selected by the current work. Furthermore, a series of common keywords has been defined by collecting similar approach for each selected strategy, as proposed by national regulations and guidelines.

Then, RMRSs are discussed according to the following key factors:

- *design of the physical elements in the BE*, by focusing on those used as perimeters (e.g. buildings façade, barriers in outdoor areas) and those placed inside the BE (e.g. areas and building components with a specific function);
- *BE layout*, by involving RMRSs dealing with the organization of different spaces (indoor, outdoor) composing the BE, distance-related issues (i.e. standoff), emergency facilities;
- *access control and surveillance in the BE*, dealing with the strategies to implement towards such goals on the border of/inside the BE;
- *safety and security management of the BE*, evidencing how safety and security staff actions could reduce the BE risk before/during the threat.

Then, each of the RMRSs is assessed according to the main aforementioned classification criteria: soft/hard target application; level of (in)visibility in the BE; BE main intended use; significant effects of the RMRSs on crowded places; main attacks typologies faced (excluding CCTAs) by stressing the modalities; the effectiveness before or during the attack; the Layer of Defense applicability; applicability to the main elements composing the BE (i.e. buildings versus open spaces in the BE or part of them). Furthermore, the main reference documents are pointed out according to Table 2. Finally, dependencies between the RMRSs are discussed with the aim to evidence how they could be jointly implemented for the improvement of safety and security in the terrorism-prone BE.

Table 2. Documents selected in this work for the risk-mitigation and reduction strategies analysis, by organizing them by Country and identifying each document according to a specific identification code (ID code) used in the following results and discussion sections.

Country	Number of documents	ID code	Document: institutions and/or authors (year) title [language], other identification data including website
Australia	3	AU1	Live Performance Australia (2019) *Audience and Crowd Management Hazard Guide* [English]
		AU2	Commonwealth of Australia (2017) *Australia's Strategy for Protecting Crowded Places from Terrorism* [English] ISBN: 978-1-925593-95-2
		AU3	Australian Institute for Disaster Resilience (2018) *Safe and Healthy Crowded Places* [English] Handbook 15
Czech Rep.	1	CR1	Soft Targets Protection Institute/Kalvach, Z., et al., 2016. *Basics of soft targets protection - guidelines (2nd version)*, https://www.mvcr.cz/cthh/soubor/basics-of-soft-target-protection-guidelines.aspx
France	3	FR1	Ministère de la Culture et de la Communication (2016) *Vigilance attentat: les bons réflexes-Guide à destination des organisateurs de rassemblements et festivals culturels* [French] https://www.culture.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels
		FR2	Ministèere de la Culture et de la Communication (2016) Vigilance attentat: les bons réflexes-Guide à destination des dirigeants d'établissements culturels patrimoniaux [French] https://www.culture.gouv.fr/Actions-de-renforcement-et-de-surveillance-des-lieux-culturels
		FR3	Ministère de l'Intérieur, de la Culture et de la Communication, Secrétariat général de la Défense et de la Sécurité National (2017) *Gérer la Sûreté et la Sécurité des événements et Sites Culturales* [French]
India	1	IN1	National Disaster Management Authority (2014*) Managing Crowd at Event and Venues of Mass Gathering* [English]
Italy	3	IT1	Ministero degli interi (2017) *Circolare 7/6/17 n.555/OP/0001991/2017/1* [Italian]
		IT2	Ministero degli interi (2017) *Direttiva 28/07/2017 n. 11001/110(10)* [Italian]
		IT3	Ministero degli interi (2018) Direttiva 18/07/2018 n. 11001/1/110/(10) [Italian]
UK	3	UK1	Home Office in partnership with the Department for Communities and Local Government (2012) *Crowded Places: The Planning System and Counter-Terrorism* [English] ISBN: 978-1-84987-392-5
		UK2	Pool Re/Julian Enoizi (2017) *Terrorism Threat & Mitigation Report* [English]
		UK3	Home Office in partnership with the Centre for the Protection of National Infrastructure and the National Counter-Terrorism Security Office (2012) *Protecting Crowded Places: Design and Technical Issues* [English] ISBN: 978-1-84987-393-2
United States	5	US1	Joint Counterterrorism Assessment Team (JCAT) (2018) *Planning and Preparedness Can Promote an Effective Response to a Terrorist Attack at Open-Access Events* [English]
		US2	Homeland Security Science and Technology (2018) *Planning Considerations: Complex Coordinated Terrorist Attacks* [English]
		US3	Homeland Security Science and Technology (2009) *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks* [English] FEMA 455
		US4	Homeland Security Science and Technology (2011) *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* [English] FEMA-426/BIPS-06/ Edition 2
		US5	U.S. Department of Homeland Security (2006) *Safe Rooms and Shelters Protecting People Against Terrorist Attacks* [English] FEMA 453

3. Resulting organization of considerable RMRSs in the BE

The section is organized according to the key factors in the BE defined by Section 2.2, while interdependencies among the RMRSs are also evidenced.

3.1. RMRSs by design of the physical elements in the BE

Table 3 groups the main RMMs concerning the *"design of the physical elements in the BE"* by dividing them according to the BE application elements. Each RMRS is also discussed according to the classification criteria of Section 2.2.

The "*safe perimeter*" strategy can be performed by implementing specific obstacles in the BE, placing them at the standoff perimeter or also at the BE envelope, with the paramount aim to avoid the vehicles access into the target. Such solutions can have an invasive impact on the site, especially in case of heavy barriers (e.g. reinforced concrete barriers), which are more suitable for hard targets. In soft targets, visible/invisible solutions should be preferred by using (Coaffee et al. 2009; Federal Emergency Management Agency 2011):

- permanent (e.g. benches, bollards including retractable bollards, planters, also with an artistic value) or temporary street furniture (heavy elements, such as Jersey barriers; fasten-to-floor barriers);
- trees and green areas;
- raised areas in the BE where to host the target core (e.g. raised sidewalks);
- (low-)walls and ha-ha walls which can induce BE altimetric variation;
- water obstacles;
- fences;
- active systems such as drop-arm crash beams;
- temporary barriers with vehicles;
- planimetric configuration of the open spaces in the BE, especially those related to vehicle-accessible areas, by means of e.g. chicanes (creating a curved path on a straight way), speed bumps, pavement treatments.

In this sense, the application of barriers inside existing BE should be faced also from an aesthetic and functional point of view, by considering if the BE can host The distance among the elements (mainly, in case of punctual elements such as bollards) and the resistance to impacts of the barriers are selected by designers mainly depending on the vehicle typology and speed (Federal Emergency Management Agency 2011). It is important to underline how such strategy can limit the access from the BE surroundings, but should guarantee the possibility of moving out of the BE site in emergencies (e.g. correct dimensioning of passages, barriers that can be knocked out by evacuees). In this sense, the selection of the specific solution should be properly merged into the BE layout-related RMRS and combined to effective access control strategies (to ensure the barriers operation during the time and the correct access by those who are allowed to enter the BE) as well as to safety management procedures, especially those related to emergency response (Federal Emergency Management Agency 2011; Bernardini et al. 2017; Joint Counterterrorism Assessment Team (JCAT) 2018).RMRSs focusing on "*Building shape*" should be provided in relation to the BE areas placed within it and in the surrounding. They are mainly applied to buildings, and should be related to *safe perimeter* and *standoff* measures (compare to Section 3.2), while being combined to management strategies (see Section 3.4) to be effective (Federal Emergency Management Agency 2011). In fact, to reduce the risk of building occupants, designers may place unoccupied or low occupancy areas in proximity of the entrances and of the perimeter (e.g. buildings envelope), especially in case of scarce *safe perimeter* strategy or in case of insufficient *standoff* measures. Consequently, the placement of secured and unsecured areas within a building should be planned by separating them with buffer zones. The most significant purposes of such RMRS in relation to the surrounding BE are:

- facing blast loads effects. In this sense, building characteristics to be considered concern mainly the overall building size and its geometric configuration. Restrained buildings extending following

horizontal configurations are preferred instead of high-rise ones more exposed to blast waves. The aspects of building geometry that have particular importance for the protection from blast include also the presence of reentrant corners, circular and concave forms, and the overall irregularity of the building form. The immediate building surroundings could additionally ensure a positive effects, by using safe perimeter-based solutions (e.g. barriers against bombings, outdoor spaces plano-altimetric configuration and so on);

- preventing possible assaults of terrorists inside the buildings (e.g. intrusion and armed assaults or following bombing as internal threats) or in the immediate surroundings, by ensuring the possibility to block views of the inside assets to potential attackers, or to improve the control by the building itself (see Section 3.3). The aforementioned buffer zones could support such strategies while being combined to building orientation, vegetation use, building components and external areas planning elements (e.g. obstruction screen and man-made hillsides), which may obscure views from the outside, impeding the finding of information facilitating planned attacks.

Such characteristics evidence how they can be limitedly sustainable in case of application to existing BE, unless the interventions are applied to the elements in the open spaces in the BE. Finally, the coordination between *building shape* and *emergency layout*-oriented (see Section 3.2) strategies will can increase the evacuation motion towards the shelters or the building exits, as for general fire safety solutions.

The "*Façade protection*" can guarantee the limitations of threat and damages propagation from the outside into the buildings, thus being related, as for RMRSs related to the design of the "*structure*", to bombing attacks (Federal Emergency Management Agency 2009, 2011; NaCTSO - National Counter Terrorism Security Office 2017). In particular, the protection of façade (and, mainly of windows and doors, which are the most vulnerable elements) should be guarantee by additionally considering the "*building shape*" as well as the BE layout-related RMRSs (Federal Emergency Management Agency 2011). In detail, adequate measures should be adopted in relation to each situation inside buildings where explosions could lead to falling glass from above over passing areas (including immediate open spaces in the BE), so as to protect the external target areas from internal threats. From a technical point of view, façades and windows might include the use of laminated glass with an inner layer of polyvinyl butyral well secured into the frames is auspicated. Glazing frames must be well secured to the building's structural frame. For what concerns their positions, the more the windows are placed low down, the more the distance that flying glass will travel into the room is reduced. Security doors provide enhanced protection against forced entry and an overall resilience of the outer shield of the building. Security doors can be bomb-resistant, bullet-resistant and extreme-intrusion-attempts resistant (Kalvach 2016). Such characteristics evidence how they can be limitedly sustainable in case of application to existing BE, unless the interventions are applied to the simple retrofit of the existing building components.

*Table 3. RMRSs concerning "**design of the physical elements in the BE**" according to the considered documents and to the organization criteria given by Section 2.2. The main references according to Table 2 ID codes. "-" refers to no specific associable data.*

RMRS identification	Safe perimeter	Building shape	Façade protection
BE application elements	building, outdoor areas and open spaces	buildings	buildings
Specific components	Perimeter	Envelope	Envelope
RMRSs strategy definition	Perimeter security of the BE (or of a part of the BE) by using bollards, barriers, walls, and other obstacles to prevent external threats	Designing buildings BE with certain shapes and heights make difficult the intrusions, while facilitate sheltering/in-place protection s for trapped people and reduce blast waves effects	Protection of windows and faca contrast explosive blast (reinfor façades) and to limit the visibili the outside (i.e. tinted or reflec glasses for windows)
Main attacks typologies faced (qualitatively ordered)	Bombing attack by vehicle; vehicle running into the target, provoking mortal collisions with pedestrians;	All the attack related to internal threats in the BE, i.e. bombing, armed assault, attack with a cold weapon; for hostage taking, limited effects in facilitating sheltering/in-place protection	Armed assault, protecting build occupants from bullets (limiting attackers' view and blocking bu Reinforced facades allows to so explosion waves effects
Soft/hard targets application	Both soft and hard targets can consider more than one perimeter line (external border of the BE; limit of specific areas in the BE)	For both soft (including residential buildings) and hard targets	Protect buildings envelope shou mandatory for hard targets and recommended for soft targets
Visibility classification	Invasive/visible/ invisible	invisible	Visible/invisible
Applicability to BE main intended use	Public spaces, BEs for education, religion and health, BEs for transportation, BE as working places	All BE use (residential BE mainly oriented towards intrusion-aware solutions)	Public spaces, BEs for transport as working places
Significant effects on crowded places	Useful in mass gathering event to protect crowd from vehicle-borne attack	Specific buildings shape could facilitate the crowd motion towards shelters (for buildings, please compare to general fire safety strategies)	-
Effectiveness before/during the attack	Some vehicle barrier and bollards can be permanent, others are removable and employable only in case of necessity to better face the attack-damaged conditions (e.g. supporting evacuation process in the BE)	Effectiveness can be reached in phases of attack preparations, and during the event.	Effectiveness are evidenced onl of attack with explosive or arm incursion
Layer of defense	L1+L3	L3	L3
Permanent/temporary solution	Permanent for hard targets and for all the BE with codified use during the time; temporary for mass gathering events in outdoor BE	Permanent; temporary for mass gathering events in outdoor BE	Permanent; temporary for mas gathering events in outdoor BE
Main interactions with other key factors: *related RMRSs*	BE layout: *Standoff, Emergency layout* Access control and surveillance in the BE: *Access control* Safety and security management of the BE: *Emergency plan*	BE layout: *Sheltering, Areas division, Emergency layout*; Access control and surveillance in the BE: *Illumination* Safety and security management of the BE: *Emergency plan*	-
Refs – ID codes	US1 US4 UK3	US4	CR1 US4 UK3

3.2. RMRSs by BE layout

Table 4 groups the main RMMs concerning the *"BE layout"* by dividing them according to the BE application elements. Each RMRS is also discussed according to the classification criteria of Section 2.2.

The "*standoff*"-oriented RMRSs can be implemented in relation to the *safe perimeter* and related BE site layout (compare to Section 3.1), where minimum distances can be respected in combination with the disposition of barriers and other expedients to maintain away vehicles from the entrance of buildings or from their more vulnerable parts (Federal Emergency Management Agency 2011). Standoff-oriented RMRSs are specifically adaptable to avoid bombing attacks not only using parked vehicles but also from the possibility of hiding the explosive devices within urban elements and furniture (e.g.: trash receptacles, manhole covers) that should be placed at certain distance from possible targets.

"*Sheltering*" RMRSs are a user-centered solution aimed at protecting the BE occupants in safe areas placed as close as possible to their position before the attack. Such strategies are widely adopted inside buildings, especially in those with should face other kind of emergencies, such as climate-related events (e.g. floods: sheltering in the upper floors; tornadoes: sheltering in part of the building characterized by high structural resistance) (Lin et al. 2020). Their efficiency depends on the implementation of proper "*emergency layout*" and "*emergency plan*" measures as well as on "*structure*"-oriented measures to contrast the attack-related damages (Federal Emergency Management Agency 2006). Besides the possibility to face internal and building-centered threats, "sheltering" inside buildings can be a valid approach for outdoor areas in the BE in case of attacks due to external threats in respect to the buildings themselves, such as vehicle running into outdoor areas in the BE (e.g. pedestrian areas) or armed assault (guns or knives), or even CBR (in cases of lower level of risks and small attacks) (Federal Emergency Management Agency 2006; NaCTSO - National Counter Terrorism Security Office 2017; Australian Institute for Disaster Resilience (AIDR) 2018). In these contexts, "invacuation" ("inward evacuation") procedure**Errore. Il segnalibro non è definito.** can be performed so as to move the exposed individuals from damaged open spaces in the BE to indoor protected places, additionally "moving people away from external windows/walls" to protect the individuals from the effects of attacks in the surroundings. According to national regulations (e.g. (NaCTSO - National Counter Terrorism Security Office 2017)), if these conditions occur or "if the threat is outside your venue or the location is unknown", people may be exposed to greater danger if the evacuation route takes them past the threat (such as a suspect device, contaminated environment or attackers)". The effectiveness of such RMRS can be guaranteed when combined to: (1) "design of physical elements in the BE" (compare Section **Errore. L'origine riferimento non è stata trovata.**) by mainly adopting "*Façade protection"* measures to contrast the attack itself; (2) the aforementioned "emergency layout" strategies by integrating them with the support of management solutions (i.e. signaling the sheltering areas in a correct way by means of signs or by using "emergency plan"-related actions by safety and security staff members; promoting "users' involvement" also before the event – compare Section **Errore. L'origine riferimento non è stata trovata.**); (3) additional "access control and surveillance" solutions to impede that attackers could arrive to the shelters (compare Section**Errore. L'origine riferimento non è stata trovata.**).

"*Areas division*" and "*emergency layout*" related measures can be guaranteed by correctly applying the RMRSs relative to safe perimeter with the employment, for instance, of mobile barriers and similar BE furniture (see Section 3.1 on *safe perimeter* related solutions). Through their implementation, open spaces in the BE should be divided into sectors able to host a definite number of occupants in mass gathering events. Specific areas in the BE should be so circumscribed where locating emergency facilities, at the same time

access and exit points should be identified with well-delineated borders by controlling the crowd flows (Bernardini et al. 2017; Joint Counterterrorism Assessment Team (JCAT) 2018).

*Table 4. RMRSs concerning "**BE layout**" according to the considered documents and to the organization criteria given by Section 2.2. The main references according to Table 2 ID codes.. "-" refers to no specific associable data.*

RMRS identification	Standoff	Sheltering	Areas division	Emergency layout
BE application elements	open spaces	buildings, open spaces	buildings, open spaces	open spaces
Specific components	open spaces (depending on their use), BE furniture	paths and waiting areas in the BE (mainly, inside the buildings)	spaces depending on their use, BE furniture	paths in the BE
RMRSs strategy definition	Keeping the stand-off distances referred to the BE furniture placement (e.g.: locating BE core elements away from parking areas, trash receptacles, vantage points, site boundary and perpendicular lines of approach)	Predisposition of Shelters area inside the BE (mainly, into buildings) by promoting a protective approach to the internal layout (in correlation to RMRSs involving evacuation paths and emergency facilities)	Open spaces layout division and organization for mass gathering events, sectors division, management of evacuation paths, areas access positioning	Emergency facilities and related areas positioning, emergency devices distributions, wayfinding and gathering areas and emergency exits
Main attacks typologies faced (qualitatively ordered)	Bombing; Armed assault	Building occupant can use internal building shelters to face each type of attack. Shelters in open spaces can be effective for attack with a cold weapon and when the attacker has been stopped by Security Forces	Bombing; armed assault; attack with a cold weapon; further effects of vehicle running into the target; crowd attack	Bombing; armed assault; attack with a cold weapon; further effects of vehicle running into the target; crowd attack
Soft/hard targets application	Mainly adoptable by hard targets, but the same solutions can be adopted where possible in soft targets as well	For the cost and complexity of the realizations of such protective measures, hard targets are considered as main application context	Soft target, by mainly focusing on BE hosting relevant and mass gathering events.	Permanently implemented in hard targets; for soft targets, different implementation levels can be applied, especially in case of high-risk conditions (e.g. crowding)
Visibility classification	Visible/invisible	Invasive	Visible	Visible
Applicability to BE main intended use	Public spaces, BEs for education, religion and health, BEs for transportation, BE as working places	Public spaces, BE as working places	Public spaces	Public spaces, BEs for transportation
Significant effects on crowded places	No specific effects	In case of a mass gathering event close to buildings, people in risky open spaces can reach the internal shelters.	These typologies of solutions are specifically aimed to increase pedestrian safety in overcrowding conditions by clearly defining the perimeter of areas with different uses in normal and emergency conditions	Supporting emergency facilities is mandatory in mass gathering events in each National regulation

Effectiveness before/during the attack	Their adoption can be aimed to reduce the damage level during possible explosions and to impede the approach of terrorists close to the BE core elements	Specific internal partitions offer to buildings occupants a refuge during the attack; these predisposed areas are studied in their location, structure and ventilation systems	Measures show their effectiveness during the attack managing the crowd dynamics and their evacuation	Emergency facilities are employed by evacuees and personnel during the attack and in the subsequent phases to give a first assistance in case of necessity
Layer of defense	L1+L2	L3	L1+L2	L1+L2+L3
Permanent/temporary solution	Permanent for building-related applications; permanent or temporary for open spaces	Permanent for building-related applications; permanent or temporary for open spaces	Permanent or temporary solutions by means of BE furniture	Permanent or temporary solutions involving related management strategies
Main interactions with other key factors and related RMRSs	Design in the BE: *Safe perimeter, Façade protection* Access control and surveillance in the BE: *Access control, Security services, Illumination*	Design in the BE: *Structure, Building Shape, Façade protection* (partially, due to invacuation strategies) Access control and surveillance in the BE: *Access control* Safety and security management of the BE: *Emergency plan*	Design in the BE: *Building Shape* Safety and security management of the BE: *Emergency plan*	Design in the BE: *Safe perimeter, Building Shape* Safety and security management of the BE: *Emergency plan, Security personnel, Users' involvement, First aid*
Refs – ID codes	UK3 US4	US5 UK3	IT1 IT2 IT3 AU3 US1	IT1 IT2 IT3 CZ1 AU3 US1 US5

3.3. RMRSs by access control and surveillance in the BE

Table 5 groups the main RMMs concerning the *"access control and surveillance in the BE"* by dividing them according to the BE application elements. Each RMRS is also discussed according to the classification criteria of Section 2.2.

The "*access control*" is a paramount strategy for hard targets or in case of a mass gathering events (Federal Emergency Management Agency 2011; Joint Counterterrorism Assessment Team (JCAT) 2018; Cuesta et al. 2019; Laufs et al. 2020). According to the safe perimeter RMRSs in Section 3.1, "safety borders" have to be established in order to guarantee that occupants inside the barriers-enclosed BE are controlled from the detention not only of weapons but also from other banned items (e.g.: glass bottles) dangerous in crowded places[5]. Safety personnel is often employed to manage such controls, by following specific management procedures (see Section 3.4). The combination between such actions and the safe perimeter solutions (i.e. heavy barrier) could be considered as heavily invasive, but this RMRS is one of the strongly deterrent for terrorist attacks (Coaffee et al. 2009), although they can move the possibility to have an attack outside the shielded (controlled) area. However, novel technologies could be employed to speed up the access controls and to make them less invasive (e.g. body scanners, metal detectors and optical devices for people counter). The "*security services*" could be adopted in this sense (Australian Institute for Disaster Resilience (AIDR) 2018), although they should be extended at a wider scale to better improve the overall resilience of the BE systems placed in a urban area (Gordon et al. 2017; Karlos et al. 2018; Cuesta et al. 2019; Laufs et al. 2020). One of the most significant solutions can involve video surveillance systems (CCTV) distributed on the overall BE, which can support the investigations of intelligence authorities to: (1) prevent possible terrorist attacks by comprehending suspected behaviors before the attack; (2) detect the attackers after the event. Recent technologies have also permitted the development and installation of "mass" facial recognition control systems in surveillance devices particularly employed to strengthen the security measures in public infrastructures such as airports and train stations (Bálint 2018). In addition, such tools can also support the disaster-reaction phase by supporting the First Responders in rescuing the damaged population in the BE. In this sense, this solution and other similar measures (e.g.: unmanned aerial vehicles) are currently involved and experimented to improve the urban resilience, they are commonly defined as smart city strategies and in relation to their employed technology can be invisibly merged in the BE. Anyway, the effectiveness of these two RMRSs are strictly influenced by the application of reliable *coordination* actions (see Section 3.4) as well as by the robustness of the infrastructure which collect and disseminate the information between the First Responders and the LEAs (Zoli et al. 2018; Laufs et al. 2020).

Besides these two main control and surveillance RMRSs classes, the "*illumination*" may provide a great support, being a real and a psychological deterrent for continuous or periodic observations by an aggressor (Federal Emergency Management Agency 2011). The strengthening of nightly lighting is a low-cost solution to discourage unwanted/undesirable activities on sites (and within buildings). In addition, different illuminance conditions can be designed to be increased over the time, and site lighting can be helpful as a response to different levels of alert, or to support users in attack-affected conditions (e.g. proper illuminance of the *emergency layout*) [5]. Finally, the security illumination tools should be combined to CCTV systems, since the cameras may need high intensity, low intensity, or infrared light for proper operation.

*Table 5. RMRSs concerning "**access control and surveillance in the BE**" according to the considered documents and to the organization criteria given by Section 2.2. The main references according to Table 2 ID codes. "-" refers to no specific associable data.*

RMRS identification	Access control	Security services	Illumination
BE application elements	buildings, open spaces	buildings, open spaces	open spaces
Specific components	spaces (depending on their use), BE furniture	BE widespread infrastructures for surveillance	lighting systems
RMRSs strategy definition	Access control for pedestrians and vehicles, people counter for occupant capacity, weapons and banned items inspections	Security service, Video surveillance CCTV	Nightly illumination of buildings perimeter and BE areas prone to attacks
Main attacks typologies faced (qualitatively ordered)	Whatever attack typologies could be foil, but limited to a circumscribed area	These measures could discourage terrorists or supporting authorities to reveal possible threats	These measures could discourage terrorists or supporting authorities to reveal possible threats
Soft/hard targets application	Hard targets	Security service for hard targets, while CCTV should be use for Soft targets as well	Wherever it could be considered a deterrent for terrorist acts
Visibility classification	Invasive, visible and invisible in relation to the employed technology	Visible	Visible
Applicability to BE main intended use	Public spaces, BEs for education, religion and health, BEs for transportation, BE as working places	Public spaces, BEs for education, religion and health, BEs for transportation, BE as working places and residential	Public spaces, BEs for education, religion and health, BEs for transportation, BE as working places and residential
Significant effects on crowded places	Impeding the access in crowded places to vehicles and banned items such as maintain a sustainable capacity of spaces might have ab elevate impact on citizens' security	CCTV in crowded places can be useful for investigations after the attack	The illumination of overcrowding places could avoid accident and collision in case of disordered evacuation
Effectiveness before/during the attack	Such measures can be defined as preventive, reducing the possibility of sudden attack	Surveillance systems allow detecting possible aggressors and suspected behaviours before the attack	The illumination allows detecting possible aggressors and suspected behaviors before the attack
Layer of defense	L1+L2+L3	L1+L2+L3	L1+L2+L3
Permanent/temporary solution	Permanent for hard targets and specific soft targets where security forces operations are constantly applied; temporary for soft targets and mass gathering events	Generally permanent; temporary for mass gathering events	Generally permanent; temporary for mass gathering events
Main interactions with other key factors and related RMRSs	Design in the BE: *Building Shape, Safe perimeter* BE layout: *Standoff, Area division, Emergency layout* Safety and security management of the BE: *Emergency plan, Security personnel*	Design in the BE: *Building Shape, Façade protection, Safe perimeter* BE layout: *Area division* Safety and security management of the BE: *Emergency plan, Security personnel, Coordination*	Design in the BE: *Building Shape, Safe perimeter* BE layout: *Standoff, Area division, Emergency layout* Safety and security management of the BE: *Security personnel*
Refs – ID codes	IT1 IT3 AU3 UK3 FR3 US1	IN1 AU3 UK3 FR3	US4

3.4. RMRSs by safety and security management of the BE

Table 6 groups the main RMMs concerning the *"safety and security management of the BE"* by dividing them according to the BE application elements. Each RMRS is also discussed according to the classification criteria of Section 2.2.The "*Security personnel*" (i.e. LEAs, Security Forces, including surveillance bodies in soft targets) should perform all the actions mainly related to security issues (compare Section 2.1.1) (Bernardini et al. 2017; Jore 2019). They are active, before the event, to mainly deter and detect possible attackers, and, during the attack, to mainly support First Responders and detect the assaulters, thus being supported by access control and surveillance RMRSs (compare with Section 3.3). They should be adequately trained to face the effective conditions, and so they need to be one of the core elements in the "*coordination*" measures (Bernardini et al. 2017; NaCTSO - National Counter Terrorism Security Office 2017; Sommer et al. 2017; Joint Counterterrorism Assessment Team (JCAT) 2018).In this sense, "*coordination*" actions in the BE prone to a terrorist act is essential before and during the event, thus including all the elements related to the safety of the hosted users, by including "*first aid*" solutions in the immediate aftermath. From a procedural point of view, while responding to the attack conditions in the BE, these three RMRSs should be strongly supported by *emergency plan* and *emergency layout*, and by tools to estimate the damages caused by the attack itself (by both including direct fatalities due to the event and crowd-related and behavioral based phenomena, e.g. crushing effects in the crowd (Bernardini et al. 2017; Li et al. 2017; Abreu et al. 2019)).

In view of the above, it is important to underline the role of two main RMRSs. Firstly the "*Emergency plan*" becomes a key element in the management-oriented RMRSs. This is the sum of subsequently indications for emergency personnel and for users about the employment of the predisposed emergency facilities (see *emergency layout* in Section 3.2). Therefore, emergency plans have to be strictly related to the other RMRSs and able to organize and create interactions among them. Who directs this plan should have the capability to comprehend every key aspect and potentiality of each emergency measure and to take advantages from them by putting each RMRS into communication, in order to prevent and discourage the attack and to work jointly in case of it occurs. Emergency plans have to face with the soft target typologies, with their intended use, with the possibility that specific activities take place and in case of mass gathering events in relation to the number of expected people (which can sensibly vary in soft targets and, especially, in open spaces in the BE).

It is worthy of notice that such kind of measures is well codified in the literature when they are referred to a single part of the BE (e.g. single building) or to the BE as a whole during specific events, such as organized mass-gatherings, festivals and so on. In case of "daily" use of the BE, it cannot be possible to define an overall system for safety and security management, since this can be related only to those activities which involves a safety plan according to the current regulation. Nevertheless, it is important to evidence how future efforts in defining common actions plan between all the BE stakeholders will can improve the coordination of counterterrorism measures in this sense.Secondly, the "*user's involvement*" concerns all the actions aimed at improving the awareness, the preparedeness and the correct response of citizens to the risk of possible terrorist attacks (Bernardini et al. 2017), as for other kind of SUODs. Nowadays, in earthquake-prone regions inhabitants generally know what are the actions that should perform to take shelter during a seismic event, but terrorism is a novel hazard, that people are not able to understand which are the best procedures to comply. Promoting initiative such as the provision of booklets or guidelines to common people can improve their awareness and preparedness in case of necessity (before the event). How to take shelter from armed attacks, where escaping toward, how to call designated authorities asking for help or intercept practical information are just some notion that each of us should know. Repetitive actions and training exercise especially for hard targets should be performed such as to bring people to right behaviors in an emergency

(Ministère de la Culture et de la Communication 2016), while emergency personnel and emergency facilities (i.e. wayfinding systems, individual devices, intelligent emergency management systems) could be used to leading people to adopt correct choices in emergency conditions, such as for other kind of emergencies (e.g. fires or earthquakes, both indoors and outdoors) (Sato et al. 2014; Ibrahim et al. 2016; Galea et al. 2017). Some European countries (i.e.: Belgium, United Kingdom, and Germany) has supported the development of counterterrorism measure for individual devices (mainly smartphone application). Some of these Apps constitute a tool to provide detailed indications of the right behaviors to perform linked to the types of a terrorist attack (e.g.: the virtual platform *iNFO-R!SQUES.be*[9]). Other Apps inform users about ongoing terrorist attacks integrating the alert message system to the users' location thanks to the WLAN networks for smartphones (e.g.: the *KATWARN*[10] mobile application). Further supplementary material can be found in Annex I at Section 7.

[9] Available at: https://www.info-risques.be/fr (last access: 30/04/2020)
[10] Available at: https://www.katwarn.de/en/system.php (last access: 30/04/2020)

*Table 6 RMRSs concerning "**safety and security management of the BE**" according to the considered documents and to the organization criteria given by Section 2.2. The main references according to Table 2 ID codes. "-" refers to no specific associable data.*

RMRS identification	Security personnel	Coordination	First aid	Emergency plan	Users' involvement
RMRSs strategy definition	Employ security personnel with adequate professional training depending on the target/threats	All the involved actors should adopt communication, information sharing, consultation, cooperation and training, being supported by a coordination center (i.e. emergency center)	First aid, ambulance and medical services	Planning and managing of protective measure (mainly, for safety purposes) to face the attack	Providing preventive instructions to citizens; Manuals about what to do in case of terrorist attack
Main attacks typologies faced (qualitatively ordered)	Security personnel can be useful to monitor and to intervene in case of necessity for all typologies of counter terrorism	The management of whatever attack typologies can be improved through the communication	First aid teams face all type of attack where victims and injuries could be	All typologies of attacks require a specific and detailed emergency management plan	Adequate instruction could be provided for each type of emergency
Soft/hard targets application	Security personnel with specific training (i.e. LEAs, military forces) are required for hard targets; their presence in soft targets is established by national regulations in relation to the targets entity	Communication between parts have to be guaranteed both for soft and hard targets.	Medical personnel should be present within a hard target and ready to intervene in soft target situations	Specific plans are developed for hard targets, meanwhile general strategies have to be preventively guaranteed for soft targets	Informing citizen about the right behaviors to practice could be useful for both soft and hard target, according to specific indications depending on the possible restricted access by the public
Visibility classification	visible	visible	visible	visible	invisible
Applicability to BE main intended use	Public spaces, BEs for transportation, BE as working places	Public spaces, BEs for transportation, BE as working places	Public spaces, BEs for transportation, BE as working places	Public spaces, BEs for education, religion and health, BEs for transportation, BE as working places	Public spaces, BEs for education, religion and health, BEs for transportation, BE as working places and residential buildings
Significant effects on crowded places	Many regulations define specific limits of overcrowding above which the employment of security personnel is required	The possibility to communicate became necessary in case of crowded condition to coordinate real time strategies for response, rescue (first aid) and evacuation	Medical personnel have to be present in case of mass gathering events	Recent regulations confirm the necessity to predispose ad hoc measure to prevent incident and attack in crowded places	If the major part of the crowd was aware of the actions to be undertaken in case of terrorism attack, accidents could be reduced

Effectiveness before/during the attack	The professional training for personnel improves the effectiveness of the emergency management during the attacks	Before the attack, coordination between the LEAs is essential. During an attack the communication have to be guaranteed between stricken populations and emergency personnel (alarms and indications), and among personnel too for coordination	Medical service effectively take place after the attack, but if it is already predisposed in the site it could reduce times to intervene	The emergency planning before a specific event or to respond to a sudden attack reflect its effects during all the duration of the emergency	A preventive informative campaign for citizens helps them to follow the right behavior in case of a terrorist attack
Layer of defense	L1+L2+L3	L1+L2+L3	L1+L2+L3	L1+L2+L3	L1+L2+L3
Permanent/temporary solution	Generally permanent, but with possible variations depending on the specific conditions of the target (i.e. for soft targets); temporary for mass gathering events	Generally permanent; temporary for mass gathering events	Generally permanent, but with possible variations depending on the specific conditions of the target (i.e. for soft targets); temporary for mass gathering events	Generally permanent, but with possible variations depending on the specific conditions of the target (i.e. for soft targets); temporary for mass gathering events	-
Main interactions with other key factors and related RMRSs	*ALL* of them as necessity to know the BE features to better operate against attacks	*ALL* of them as necessity to know the BE features to better operate against attacks	*ALL* of them as necessity to know the BE features to better operate against attacks	Design in the BE: *ALL* BE layout: *ALL* Access control and surveillance in the BE: *ALL*	BE layout: *Sheltering, Area division, Emergency layout* (i.e. to induce correct emergency response behaviors)
Refs – ID codes	AU1 IT1 IT2 IT3 FR1	AU1 US1 US2 AU3	AU3 IT3	AU1 AU2 UK1 US1 IN1 US2 UK2 US4 AU3 IT1 IT2 IT3 UK3 FR1 FR2 FR3	FR1 FR2 FR3

4. Discussion: RMRSs analysis from a "sustainability perspective"

The RMRSs discussed below are finally discussed according to the "sustainability perspective" introduced by previous works and discussed in Section 1 (John Garrick et al. 2004; Coaffee et al. 2009; Bernardini et al. 2017; Gayathri et al. 2017; Li et al. 2017; Festag 2017; Ahmed and Memish 2019; Beňová et al. 2019; Ghazi and Abaas 2019; Laufs et al. 2020; Zhu et al. 2020). In particular, after considering which BE element is the main target for the RMRS, the key elements for discussion are outlined in

Table 7-PART1 (the possibility to ensure redundancy over different attacks and over time (before/during); the possibility to include a human-centered perspective or support human behaviors by the RMRS; the possibility to sharing the capabilities of the BE by the RMRS, by considering the internal part of the BE, which are indoor/buildings and outdoor/open spaces in the BE, or by considering the surrounding BEs) and

Table 7-PART2 (Perceptive aspects of the users in terms of safety and livability of the BE, and of the terrorists in terms of deterring potential of the RMRS; potentialities of application in the BE, by mainly point out existing scenarios, and linear and areal BEs, according to the D1.1.1 schematization).

Table 7. Discussion of the RMRSs according to the a "sustainability perspective". Colors of the cells imply: green-possibility to apply the RMRS (OK=as it; additional improvement suggestions pointed out); yellow-possibility to apply the RMRS but including the suggestion or by considering the limitations defined; red-difficulties to apply the RMRS, by including reasons or suggestions. According to Section 2and Section 3 discussion, as well as on D1.1.1 results, main BE elements towards the RMRSs are oriented are: Open spaces (OS); Building (BU); Urban scale (US).

PART 1

			Redundancy			Sharing the capabilities of the BE	
		Main BE element towards they are oriented	directly facing more than 1 attack typology	effective before & during the attack	**Human centered-approach prone**	indoor/outdoor	neighboring
design of the physical elements in the BE	*Safe perimeter*	OS	improved by standoff and access control				only in case of shared solutions in different BE
	Building shape	BU	improved by standoff and access control	facilitate evacuation/sheltering/rescuers' access			
	Façade protection	BU	OK			by emergency layout (invacuation)	
	Structure	BU	OK			by invacuation	
BE layout	*Standoff*	OS	improved by safe perimeter and access control	combined to areas division		in case of more safe perimeter inside the same BE	only in case of shared solutions in different BE
	Sheltering	BU	OK		simulation-based tools suggested to plan sheltering	by invacuation	
	Areas division	OS		facilitate evacuation/rescuers' access	simulation-based tools needed	identifying different functional parts of the BE areas	
	Emergency layout	OS+BU			simulation-based tools needed	identifying different functional parts of the BE areas; by invacuation	only in case of shared solutions in different BE
access control and surveillance in the BE	*Access control*	OS	OK				
	Security services	OS+BU	OK	before: to detect; during: to manage and support the emergency response and plan		only in case of interconnected (e.g. internet of things-based) systems in different buildings	only in case of interconnected (e.g. internet of things-based) systems in different BE
	Illumination	OS		OK	simulation-based tools suggested to plan illumination	OK	only in case of shared solutions in different BE
safety and security management of the BE	*Security personnel*	OS+BU+US	improved by access control and security services	OK		collaboration with LEAs/first responders at urban scale	collaboration with LEAs at urban scale
	Coordination	OS+BU+US	OK	OK		collaboration with LEAs/first responders at urban scale	collaboration with LEAs/first responders at urban scale
	First aid	OS+BU	OK		simulation-based tools needed (fatalities, effects of the crowd)	collaboration with LEAs/first responders at urban scale	collaboration with LEAs/first responders at urban scale
	Emergency plan	OS+BU	improved by security services; coordinated with emergency layout		simulation-based tools needed	collaboration with LEAs/first responders at urban scale	collaboration with LEAs/first responders at urban scale
	Users' involvement	OS+BU+US	OK	OK	better moving towards interactive solutions		collaboration with LEAs/first responders at urban scale

PART 2

		Main BE element towards they are oriented	Perceptive aspects			BE application		
			Users' safety	Users' liveability	Deter terrorists	existing (i.e. historical)	linear	areal
design of the physical elements in the BE	*Safe perimeter*	OS		limiting invasive solutions	improved by access control and security personnel	invisible recommended	borders of the BE, distinguishing main effective access along the linear space and secondary access (lateral streets)	borders of the BE, distinguishing effective accesses
	Building shape	BU	depending on the functional areas division	depending on the functional areas division	analize possibiliy of views inside the buildings			
	Façade protection	BU				potentially invasive	buildings in correlation to the emergency layout and plan strategies	buildings in correlation to the emergency layout and plan strategies
	Structure	BU				generally invasive	strategic buildings in the BE	strategic buildings in the BE
BE layout	*Standoff*	OS			improved by safe perimeter, access control, security personnel			
	Sheltering	BU	individuals' engagment, layout signaling and emergency personnel support should be guaranteed					
	Areas division	OS	crowding phenomena to be limited	depending on the functional areas division				
	Emergency layout	OS+BU	perceived but individuals' engagment and layout signaling should be guaranteed	depending on the functional areas division				
access control and surveillance in the BE	*Access control*	OS	OK	generally invasive	improved by safe perimeter, access control, security personnel			
	Security services	OS+BU	perceived but potentally invasive	only in case of interconnected (e.g. internet of things-based) systems which can supply useful information to the hosted individuals		integrated (aesthetic BE furniture) solutions recommended		
	Illumination	OS	better if integrated in the BE	OK	improved by safe perimeter, access control, security personnel	integrated (aesthetic BE furniture) solutions recommended		pay attention to the open spaces configuration
safety and security management of the BE	*Security personnel*	OS+BU+US	perceived but invasive	potentially invasive	OK	OK	OK	OK
	Coordination	OS+BU+US				OK	OK	OK
	First aid	OS+BU	perceived but individuals' awareness should be guaranteed			OK	OK	OK
	Emergency plan	OS+BU	individuals' awareness should be guaranteed			OK	OK	OK
	Users' involvement	OS+BU+US	individuals' engagment should be guaranteed			OK	OK	OK

Conclusions

This deliverable pursues the aim to collect a conspicuous state of the art on the terrorism menace in the view of the existing and affirmed risk-mitigation and reduction measures to face this risk for the users of the Built Environment. In this view, the activates traced by this deliverable complete the risk matrix definition of D1.3.1 by moving from risk assessment to risk management and reduction.

A classification of possible strategies to implement against terrorism is achieved through the definition of a complete methodology based on classification analysis and comparisons, to finally outline the applicability of them into the BE, by focusing on the elements characterizing the BE and the possible classifications (i.e. linear versus areal BEs) as defined in D1.1.1.

Firstly, the possible targets of terrorist acts are discussed, and then a classification of attack typologies is pursued from previously occurred events. Different strategies are related to the time when they show their effectiveness, and to the place where they are placed. These measures can refer to the distribution and disposition of security elements and furniture merged into the BE or properly belonging to the buildings structures and to their design rather than the employment of facilities and novel technologies to support emergency phases.

The classification inspects all the activities related also to the emergency planning the employment of trained personnel, the communication, and coordination among parts. The results discussion also evidences how the strategies selection should be supported by a simulation-based approach and by including human-factors (behavioural as well as perceptive elements) into the required analysis.

This work put the basis for the subsequent task where risk matrixes factors will be combined to the activity results so as to outline strategies of analysis and planning of counter terrorism measures to be implemented into the BE.

6. References

Abreu O, Cuesta A, Balboa A, Alvear D (2019) On the use of stochastic simulations to explore the impact of human parameters on mass public shooting attacks. Saf Sci 120:941–949. https://doi.org/10.1016/j.ssci.2019.08.038

Ahmed QA, Memish ZA (2019) From the "Madding Crowd" to mass gatherings-religion, sport, culture and public health. Travel Med Infect Dis 28:91–97. https://doi.org/10.1016/j.tmaid.2018.06.001

ANZCTC (2017) Australia's Strategy for Protecting Crowded Places from Terrorism

Australian Institute for Disaster Resilience (AIDR) (2018) Safe and Healthy Crowded Places. 96

Bálint K (2018) UAVs with Biometric Facial Recognition Capabilities in the Combat Against Terrorism. SISY 2018 - IEEE 16th Int Symp Intell Syst Informatics, Proc 185–189. https://doi.org/10.1109/SISY.2018.8524800

Bennett B (2017) Understanding, Assessing, and Responding to Terrorism. John Wiley & Sons, Inc., Hoboken, NJ, USA

Beňová P, Hošková - Mayerová Š, Navrátil J (2019) TERRORIST ATTACKS ON SELECTED SOFT TARGETS. J Secur Sustain Issues 8:453–471. https://doi.org/10.9770/jssi.2019.8.3(13)

Bernardini G, Quagliarini E, D'Orazio M (2017) Grandi eventi e terrorismo: la progettazione consapevole della sicurezza delle persone. Antincendio 12 anno 69:12–28

Coaffee J, O'Hare P, Hawkesworth M (2009) The visibility of (in) security: The aesthetics of planning urban defences against terrorism. Secur Dialogue 40:489–511

Consiglio Nazionale delle Ricerche - COMMISSIONE DI STUDIO PER LA PREDISPOSIZIONE E L'ANALISI DI NORME TECNICHE RELATIVE ALLE COSTRUZIONI (2018) Istruzioni per la valutazione della robustezza delle costruzioni (in Italian)

Cozzolino A (2012) Humanitarian Logistics. Springer Berlin Heidelberg, Berlin, Heidelberg

Cuesta A, Abreu O, Balboa A, Alvear D (2019) A new approach to protect soft-targets from terrorist attacks. Saf Sci 120:877–885. https://doi.org/10.1016/j.ssci.2019.08.019

Federal Emergency Management Agency (2009) Risk Management Series. Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks (FEMA 455)

Federal Emergency Management Agency (2011) Buildings and Infrastructure Protection Series. Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA-426/BIPS-06), 2nd edn.

Federal Emergency Management Agency (2006) Risk Management Series. Safe Rooms and Shelters. Protecting People Against Terrorist Attacks (FEMA 453)

Festag S (2017) Counterproductive (safety and security) strategies: The hazards of ignoring human behaviour. Process Saf Environ Prot 110:21–30. https://doi.org/10.1016/j.psep.2017.07.012

Galea ER, Xie H, Deere S, et al (2017) An international survey and full-scale evacuation trial demonstrating the effectiveness of the active dynamic signage system concept. Fire Mater 41:493–513. https://doi.org/10.1002/fam.2414

Gayathri H, Aparna PM, Verma A (2017) A review of studies on understanding crowd dynamics in the

context of crowd safety in mass religious gatherings. Int J Disaster Risk Reduct 25:82–91. https://doi.org/10.1016/j.ijdrr.2017.07.017

Ghazi NM, Abaas ZR (2019) Toward liveable commercial streets: A case study of Al-Karada inner street in Baghdad. Heliyon 5:e01652. https://doi.org/10.1016/j.heliyon.2019.e01652

Gordon TJ, Sharan Y, Florescu E (2017) Potential measures for the pre-detection of terrorism. Technol Forecast Soc Change 123:1–16. https://doi.org/10.1016/j.techfore.2017.05.017

Government I (2015) Occupational Safety and Healthcare on work places (D.lgs. 9 aprile 2008, n. 81, Testo coordinato con il D.Lgs. 3 agosto 2009, n. 106) (in Italian)

GSA (2007) The Site Security Design Guide

Home Office in partnership with the Department for Communities and Local Government (2012a) Crowded Places: The Planning System and Counter-Terrorism

Home Office in partnership with the Department for Communities and Local Government (2012b) Protecting Crowded Places: Design and Technical Issues

Ibrahim AM, Venkat I, Subramanian KG, et al (2016) Intelligent evacuation management systems: A review. ACM Trans Intell Syst Technol 7:. https://doi.org/10.1145/2842630

John Garrick B, Hall JE, Kilger M, et al (2004) Confronting the risks of terrorism: making the right decisions. Reliab Eng Syst Saf 86:129–176. https://doi.org/10.1016/j.ress.2004.04.003

Joint Counterterrorism Assessment Team (JCAT) (2018) Planning and Preparedness Can Promote an Effective Response to a Terrorist Attack at Open-Access Events

Jore SH (2019) The Conceptual and Scientific Demarcation of Security in Contrast to Safety. Eur J Secur Res 4:157–174. https://doi.org/10.1007/s41125-017-0021-9

Kalvach Z, et al. (2016) Basics of soft targets protection - guidelines (2nd version). Prague

Karlos V, Larcher M, Solomos G (2018) Review on soft target/public space protection guidance. Publications Office of the European Union, Luxemburg

Kılıçlar A, Uşaklı A, Tayfun A (2018) Terrorism prevention in tourism destinations: Security forces vs. civil authority perspectives. J Destin Mark Manag 8:232–246. https://doi.org/10.1016/j.jdmm.2017.04.006

Lapkova D, Kotek L, Kralik L (2018) Soft Targets – Possibilities of Their Identification. In: Katalinic B (ed) Proceedings of the 29th DAAAM International Symposium. DAAAM International, Vienna, Austria, pp 0369–0377

Laufs J, Borrion H, Bradford B (2020) Security and the smart city: A systematic review. Sustain Cities Soc 55:102023. https://doi.org/10.1016/j.scs.2020.102023

Li Piani T (2018) Progettazione strutturale e funzione sociale dello spazio (quale) vulnerabilità e soluzione al terrorismo urbano. Sicurezza, Terror e Soc - Int J - Ital Team Secur erroristic Issues Manag Emergencies (in Ital ISSN 2421-4442) 7–15

Li S, Zhuang J, Shen S (2017) A three-stage evacuation decision-making and behavior model for the onset of an attack. Transp Res Part C Emerg Technol 79:119–135. https://doi.org/10.1016/J.TRC.2017.03.008

Lin J, Zhu R, Li N, Becerik-Gerber B (2020) How occupants respond to building emergencies: A systematic

review of behavioral characteristics and behavioral theories. Saf Sci 122:104540. https://doi.org/10.1016/j.ssci.2019.104540

Marchment Z, Gill P (2019) Modelling the spatial decision making of terrorists: The discrete choice approach. Appl Geogr 104:21–31. https://doi.org/10.1016/j.apgeog.2019.01.009

Matsika E, O'Neill C, Battista U, et al (2016) Development of Risk Assessment Specifications for Analysing Terrorist Attacks Vulnerability on Metro and Light Rail Systems. Transp Res Procedia 14:1345–1354. https://doi.org/10.1016/j.trpro.2016.05.207

Miko FT, Froehlich C (2004) Germany's Role in Fighting Terrorism: Implications for US Policy. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE

Ministero dell'interno (2018) Circolare del 18 luglio 2018 - Modelli organizzativi e procedurali per garantire alti livelli di sicurezza in occasione di manifestazioni pubbliche (in italian)

Mistretta P, Garau C, Pintus S (2014) Beni Comuni dello Spazio Urbano

NaCTSO - National Counter Terrorism Security Office (2017) Crowded Places Guidance. United Kingdom

National Consortium for the Study of Terrorism and Responses to Terrorism (START) (2019) Global Terrorism Database Codebook: Inclusion Criteria and Variables

National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD) |

National Research Council (1987) Infrastructure for the 21st Century: Framework for a Research Agenda. National Academies Press, Washington, D.C.

Ruiz Estrada MA, Koutronas E (2016) Terrorist attack assessment: Paris November 2015 and Brussels March 2016. J Policy Model 38:553–571. https://doi.org/10.1016/j.jpolmod.2016.04.001

Sato T, Izumi T, Nakatani Y (2014) Tourist Evacuation Guidance Support System for Use in Disasters. In: Kurosu M (ed) Human-Computer Interaction, Part III, HCII 2014. Springer International Publishing, pp 494–501

Sommer M, Njå O, Lussand K (2017) Police officers' learning in relation to emergency management: A case study. Int J Disaster Risk Reduct 21:70–84. https://doi.org/10.1016/J.IJDRR.2016.11.003

UNDRR Disaster Definitions - Global Disaster Loss Collection Initiative

US department of Homeland Security (2018) Planning Considerations: Complex Coordinated Terrorist Attacks

Walker C (2000) Briefing on the terrorism act 2000. Terror Polit Violence 12:1–36

Woo G (2015) Understanding the Principles of Terrorism Risk Modeling from Charlie Hebdo Attack in Paris. Def Against Terror Rev 7:1–11

Zhu R, Lin J, Becerik-Gerber B, Li N (2020) Human-building-emergency interactions and their impact on emergency response performance: A review of the state of the art. Saf Sci 127:104691. https://doi.org/10.1016/j.ssci.2020.104691

Zoli C, Steinberg LJ, Grabowski M, Hermann M (2018) Terrorist critical infrastructures, organizational capacity and security risk. Saf Sci 110:121–130. https://doi.org/10.1016/j.ssci.2018.05.021

7. Annex I – Analysis of most exposed European Countries to the terrorism threat. Normative frame, strategies and citizen education.

7.1 France

Regarding the terrorist attacks taken place in France in recent years, the State has reacted by maximizing the level of security, in concordance with the respect of citizens freedom and through a series of anticipatory and reactive actions. In particular, Government institutions and public authorities act on three different fields, summarised in prevention, knowledge and planning, with the aim of avoiding the occurrence of an attack.

A supporting system of knowledge of the French experience was the *Gérer la sureté et la sécurité des événements et sites culturels*[11] treatise, drafted in 2017.

The response to the terrorist threat is planned through the creation, in 1978, of a general security plan, *Vigipirate Plan*[12], subjected to various modifications until 2016. It can be explained as a management tool, available to the State, used to contrast terrorism actions, engaging institutions, law enforcement agencies and citizens to operate through surveillance measures aimed at understanding the terrorist threat and adopting correct behaviours. In addition, the same introduces prevention rules to increase user's awareness with respect to the knowledge of the terrorist threat and the devices to banish each danger situation and amplify the system of protection measures to be adopted in reference to the situation of reducing risks and victims. A fundamental highlighted parameter is the measure of education which, considering all the accounted passive prevention measures, represents the most complex procedure in the management and control phase.

In the design process, the *Vigipirate Plan* indirectly identifies three different levels of exposure in relation to the criteria of active surveillance, - "*supervision*", "*reinforced security - risk of attack*" and "*urgent attack*" -, by switching from continuous and extensive monitoring on the whole territory, to the reinforced one, located in the place affected by the imminent terrorist assault and restricted only to the crisis period.

With the *Gérer la sureté et la sécurité des événements et sites culturels* treaty, the French State highlights the need to educate all users of urban BEs, especially when public outdoor meeting places happen or during major events.

The French government, among other management education actions of the terrorist event, has developed an app tool for smartphones, called *SAIP (Système d'alerte et d'information des populations)*, which allows to all users to send alert messages in case of attack. This system has a dual function: first of all, it geolocates the terrorist event (by reporting), identifies and changes the alert level of the reference area, and provides to user's rules concerning the correct behaviours to be taken in relation to the level of alert.

[11] Available at: https://www.culture.gouv.fr/Media/Actualites/Autres-dossiers/Plan-vigipirate/Gerer-la-surete-et-la-securite-des-evenements-et-sites-culturels (last access: 22/05/2020)
[12] Available at https://www.gouvernement.fr/vigipirate (last access: 22/05/2020)

7.2 United Kingdom

According to a chronological classification, United Kingdom was the first European country to adopt regulatory instruments against terrorism. The Terrorism Act, implemented in 2000 (Walker 2000), defines the meaning of terrorism and a list of legally protected and criminally relevant legal assets.

However, following the traumatic events of 2001 in U.S.A- and the multiple explosions happen in London in 2005, the government intensified the analysis and security procedures, defining the current monitoring tool, the Counter-Terrorism and Border Security Act 2019[13]. This regulatory instrument focuses the attention mainly on conferring greater powers to terrorist activities repression for community.

In addition to the regulatory framework, the British counter-terrorism strategy is a forefront measure for the management and reduction of the risk associated with this type of phenomenon. The CONTEST 2018[14], name of the British anti-terrorist strategy, aims to define a well-structured protocol. This protocol is summarized in 4 ***Key Actions*** with a specific objective linked to the 4 main phases of the strategy itself. The 4 actions are listed as follow:

[KA-UK.1] ***Prevent***, acting on the control of the formation of new terrorist associations;
[KA-UK.2] ***Pursue***, through the strengthening of the investigation systems aimed at identifying possible terrorist actions in preparation or occurring;
[KA-UK.3] ***Protect***, strengthening British protections against terrorist attacks;
[KA-UK.4] ***Prepare***, identifying actions that mitigate impacts of terrorist attacks by informing and training citizens.

It is evident that, in addition to the control systems strictly connected to intelligence actions, United Kingdom has moved in the identification of two main lines of action: *Active Strategies* (AS) for the management of the terrorist attack and *Passive Measures* (PM) acting directly on citizens through their education.

The population educational process as a passive counter-terrorism measure tool has been implemented through 3 programs, currently active:

[PM-UK.1] ACT[15] (ACTION COUNTERS TERRORISM), based on the creation of an e-learning platform (developed by the British police) aimed at training citizens;
[PM-UK.2] SCaN[16] (SEE, CHECK and NOTIFY), developed for the creation of training packages useful to companies and organizations for the management and emergency education of all users (divided by the role assumed in the associations);
[PM-UK.3] information advertisement RUN, HIDE, TELL[17] (Annex 1 - Figure 1**Errore. L'origine riferimento non è stata trovata.**), aimed at spreading awareness of the terrorist threat among citizens. It educates societies to respect correct behaviours in vulnerable places and amplify the knowledge about the surrounding environment, allowing to decrease the magnitude of the attacks.

[13] Available at: http://www.legislation.gov.uk/ukpga/2019/3/contents/enacted (last access: 22/05/2020)
[14] Available at: https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2018 (last access: 22/05/2020)
[15] Available at: https://act.campaign.gov.uk/ (last access: 22/05/2020)
[16] Available at: https://www.gov.uk/government/news/security-training-package-empowers-staff-to-see-check-and-notify-scan (last access: 22/05/2020)
[17] Available at: https://www.gov.uk/government/publications/stay-safe-film (last access: 22/05/2020)

The technological response, as a tool for citizens education and terrorist event smart management, is identified in a free app: *citizenAID*®[18]. It constitutes an open source database of guidelines directly available for citizens that explains procedures for the management of the event, considering the type of weapon used, as well as first aid actions.

Annex 1 - Figure 1 - Advertising campaign of RUN, HIDE, TELL

7.3 Belgium

Belgium represents the European country that has set up specific risk analysis, prevention and management measures, resulting from terrorist attacks. The Crisis Centre, born in 1986, is currently one of the 5 Belgian Service Public Federal and develops, since 2009, proactive approaches to risk education. Even in the Belgian country, the activity and reactivity of urban users are essential for the optimal management of terrorist events.

Therefore, Belgium improves activities and educates population to manage risks in vulnerable situations. The *Communiquer Sur Les Risques*[19] was the first awareness campaign in which citizens' education englobes all the 4 communication levels [20] in relation to the risk exposure assessed by the Crisis Centre. According to this, the training/information activity has the aim to promote self-protection and solidarity in citizens.

Belgium, like UK, has supported communication campaigns through smart network systems.

[PM-BE.1] The virtual platform *iNFO-R!SQUES.be*[21] constitutes the tool for the definition alert levels and education to risk management in Belgium. The platform differs from UK apps, providing detailed indications of the behaviour linked to the types of terrorist attack (explosion or weapons attack);

[PM-BE.2] *BE-Alert*[22] can be compared, instead, to a communication tool used to prevent a terrorist attack. This smart program, managed by superordinate control government associations (regional, municipal or statute), informs the registered users about ongoing terrorist attacks through messages and independently of the user's location.

[18] Available at: https://www.citizenaid.org/home (last access: 22/05/2020)
[19] Available at:https://centredecrise.be/sites/default/files/brochure_team_d5_communiquer_sur_les_risques_fr_0.pdf (last access: 22/05/2020)
[20] Available at: https://centredecrise.be/sites/default/files/guide_fr.pdf (last access: 22/05/2020)
[21] Available at: https://www.info-risques.be/fr (last access: 22/05/2020)
[22] Available at: https://www.be-alert.be/fr/ (last access: 22/05/2020)

7.4 Germany

The geographical position and the political weight assumed in the European Union by its members are the dominant characteristics of the approach to terrorism in Germany (Miko and Froehlich 2004).

Focusing the attention on the political point of view, Germany, like UK, has built a restrictive framework of measures to prevent and counter terrorist activities through legal disposals. In addition, Germany is well structured and advanced for the use of innovative technologies in the supervision of people and groups, potentially involved in terrorist scenarios. The development and installation of "mass" facial recognition control systems in surveillance devices strengthen the security measures in airports[23] and train stations[24].

As in the other European countries, Germany institutions define procedures aimed at educating citizens to manage the traumatic event, promoting cognitive projects also in schools. The *COTRA project*[25] aims to sensitize young citizens about this type of brutal event and identify messages containing hatred and encouragement to violence. With these measures, people are able to recognize extremist manipulation actions.

The management of the traumatic event through the education of citizens has involved the creation of two main applications:

[PM-GE.1] *NINA*[26], a smart software that collects and displays in the app interface warnings and communications from government and public safety profiles, as well as meteorological stations data;

[PM-GE.2] *KATWARN*[27] allows users to receive alert notifications. This app, compared to the others mentioned above, integrates the alert message system to the location of users through data stations and WLAN networks for smartphones, decreasing the sense of alarmism to the only people present in the surroundings of the terrorist event ("Guardian Angel" function - Annex 1 - Figure 2). All information, as in the previous app, comes from official and certified sources. Starting from 2015, these alert systems have been implemented in the light signs of subways, trams and buses, as well as integrated in specific on-board computers of some cars.

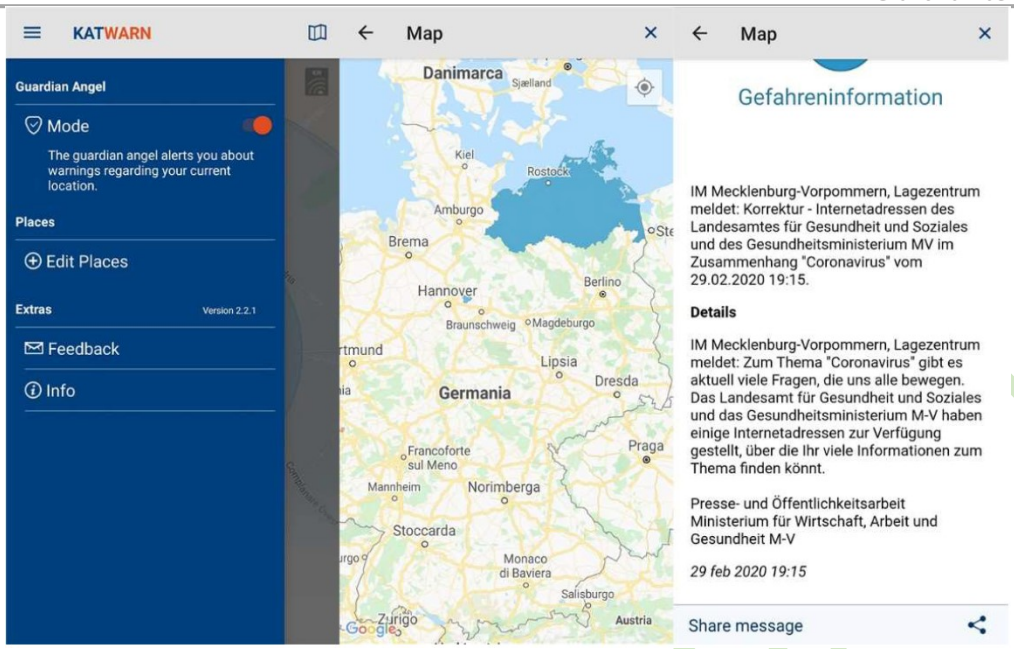
[23] Available at: https://digit.site36.net/2019/07/12/german-airports-face-recognition-now-also-for-children/ (last access: 22/05/2020)

[24] Available at: https://www.euractiv.com/section/data-protection/news/german-ministers-plan-to-expand-automatic-facial-recognition-meets-fierce-criticism/ (last access: 22/05/2020)

[25] https://www.project-contra.org/Contra/EN/Manual/190215ManualContraEN.pdf?__blob=publicationFile&v=7 (last access: 22/05/2020)

[26] https://www.bbk.bund.de/DE/NINA/Warn-App_NINA_node.html (last access: 22/05/2020)

[27] https://www.katwarn.de/en/system.php (last access: 22/05/2020)



Annex 1 - Figure 2 "Guardian Angel" function in the KATWARN APP