With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security – related Risks Programme
European Commission – Directorate General Home Affairs

SMART CIBER –
System of Maps Assessing Risk of Terrorism against Critical Infrastructures in Big Events Rallies
Grant Agreement N. AG025
30-CE-0453363/00-22

CONCEPT PAPER
The city governance and the 'Evil Done' model for the risk assessment of the terrorism potential targets
First part: the "soft targets", i.e. symbolic/iconic sites

by Marco Lombardi*, Chiara Fonio* and Alessia Ceresa*
(Scientific Team)

This paper focalizes the attention on the terrorism aspect of the risk assessment model, considering in particular the s.c. "soft targets", intended as symbolic or iconic sites of Milan city.

29 July 2013

THE *EVIL DONE* MODEL: THE OPERATIONAL PROPOSAL

The Evil Done model[1] is based on the theories of "situational criminology" applied to terrorism and violent acts as a tool that, although still in the process of development, has already been tested by the police in various countries especially to assess the attractiveness and exposure to risk of potential targets of terrorism[2]. As far as the Smart Ciber project concerns, this model is applicable in light of some specific features:

---

* Smart Ciber Project, Scientific Coordinator, Professor of Sociology and Director of ITSTIME-*Italian Team for Security, Terroristic Issues & Managing Emergencies*, Università Cattolica del Sacro Cuore - Milan
* Smart Ciber Project, Scientific Expert, PhD in Sociology
* Smart Ciber Project, Scientific Expert, PhD in Criminology

[1] Clarke R. V., Newman G. R., *Outsmarting the Terrorists*, Praeger Publisher, Westport, 2006

[2] Özer M.M., Akbaş H. (2011) *The Application of Situational Crime Prevention to Terrorism*, in Turkish Journal of Police Studies (Polis Bilimleri Dergisi), Vol. 13 (2), pp. 179-194; Indermaur D., *Situational Crime Prevention of Violent Crimes: Theory and Practice in Australia*, in Studies on Crime and Crime Prevention, Crime Research Centre, University of Western Australia, 8, 1, 1999, pp. 71-78; Linden R., *Situational Crime prevention: Its Role in Comprehensive Prevention*

- It is set in the perspective of "Big Events" and "Critical Infrastructures", which are by definition "attractive" targets;
- It can provide operational guidance with respect to the evolution of risk scenarios, indicating the criticality of specific areas of the city.

Moreover, the following operational proposal stems from the need to use a strong theoretical model which could guide the experts. This is in fact of particular relevance if we consider a risk emerged during the MidTerm Conference (see Concept Paper 5), namely a technologically driven approach that could lead to a form of determinism. The EVIL DONE model gives the opportunity, as specified below, to obtain both a subjective and an objective perspective within a robust theoretical framework. Thus, the risk of using an overall reductive approach is minimized thanks to an assessment that is not dependent exclusively on technology. Objective and subjective evaluations concur in assessing risks of different nature.

Besides, the deterministic risk is overcome through the assessment procedure itself, as the further added value of the EVIL DONE model is the intertwined evaluation of both the experts having a strong academic background in the field, as well as the security managers responsible for the crisis rooms of the several Critical Infrastructures involved as stakeholders in the project: therefore the theoretical and the operational components represent a complementary aspect of this procedure and not a dichotomy.

Evil Done is an acronym in which each letter represents a characteristic of the analyzed object (area, place, CI, etc.) (see diagram below).

The proposal aims to use the model in a dual perspective:

- **Objective Perspective**: for each feature identified in the field, give objectively verifiable indicators that determine the value of the specific feature;
- **Subjective Perspective**: the model will be provided to the committee of experts and to the security managers of CI in order to be assessed.

Initiatives, in Revue de l'IPC Review, Department of Sociology, University of Manitoba, Vol. 1, March/Mars 2007, pp.139-159

The purpose is to obtain a double-track perspective (subjective and objective) of the same Evil Done characteristics, for a better assessment.

EVIL DONE diagram from both objective and subjective perspectives:

EVIL DONE *Definitions*	Objective indicators *Observed in the field and standardized on a scale from 1 to 4*	Subjective evaluations *Advice of experts*
E – *exposed*: the Target must be logistically visible to attack	Distance / Proximity to District 1 / Milan city center	Non-exhaustive list of targets proposed to the experts for their subjective evaluation that is expressed on a scale from 1 (min) to 4 (max) for each characteristic of the model.
	Distance / Proximity to Critical Infrastructure	
V – *vital*: the Target must be vital to society in terms of services and the functioning of the city	Minimum essential services (Critical Infrastructure)	
	Services for the smooth operation of the city (e.g, Courts, Police Stations, Consulates, etc.)	
I – *iconic*: Determines the symbolic / iconic value of the Target, relevant to the ideology of the individual terrorist organization	Symbolic value in perspective: political	
	Symbolic value in perspective: religious	
	Symbolic value in perspective: social	
	Symbolic value in perspective: economical	
	Symbolic value in perspective: cultural	
	Symbolic value in perspective: historical	

L – *legitimate*: the subversive activities carried out must be morally legitimized by civil society and is a catalyst for the media	Morally acceptable in the opinion of the public	
	The Target is an object of social dissent	
	Place of demonstrations / public events	
	Mass-media catalyst	
D – *destructible*: the Target must have the structural characteristics of "destructibility"	Size of the structure / building	
	Building material used	
O – *occupied*: some terrorist organizations seek Targets that will have a large influx of people, since the objective is to kill as many innocent people as possible	Place open to the public	
	Rate of influx of people (daily, weekly, monthly, etc.)	
N – *near*: terrorist organizations choose Targets also with regard to the proximity to the places where the terrorists are hiding in order to make it easy to escape after the act of terrorism	Proximity to places of discomfort (Aler-Erp social housing, abandoned and degraded areas, etc.)	
	Proximity to places with a high rate of immigration	
E – *easy*: the target is chosen also with regards to the ease with which an attack could be carried out and completed successfully, necessary to give a strong message to the government and civil society	Level of security and checking of the target. If so, what (CCTV, private security, intrusion detection systems, etc.)?	
	Distance from / proximity to barracks and police stations (PS, CC, etc.)	
	Distance from / proximity to links / junctions and escape routes (main roads / motorways, train stations, airports, metro, etc.)	

The aspect to consider in both evaluations (subjective and objective), is the different nature and/or feature of each letter. In particular, as emphasized in the literature, different forms of terrorism and subversion should be taken into account:

1. E (*exposed*) - D (*destructible*) - E (*easy*): constitute the set of "physical / structural" characteristics of the target
2. V (*vital*) - I (*iconic*) - L (*legitimate*): constitute the set of "ideological" characteristics of the target, which vary depending on the type of terrorist organization or subversive movement to which it refers
3. O (*occupied*) - N (*near*): represent the "strategic" characteristics of the target. In fact, it is a simple strategic choice of the individual terrorist group either to attack targets involving places / buildings with a large flaw of people or, symbolic targets, if it prefers targets that have a symbolic value in themselves, irrespective of their being "open to the public" (*occupied*).
   In addition, the proximity to places of escape or hiding for criminals appears to be a strategic and operational choice for the various terrorist organizations (*near*), often referred to typically as the "Rational-choice Theory", or from a simple assessment of costs / benefits of the strategic choice[3]. Therefore, the proximity to hiding places is determined by the fact that they opt for carefully evaluated and well known targets; instead, proximity to places of escape appears to be a pragmatic option, particularly in the planning of an attack.

A further step of operationalization of the Evil Done model implies that the characteristics of each target identified in the urban context must then be geo-located visually on the cartographic model. Therefore, this study will proceed with the identification of the logistic location of each target on the map and then move to the analysis of its features in light of the assessment made by the double-track perspective (objective and subjective) on the basis of the model detailed above (i.e. for each geo-located point that corresponds

[3] Becker G., *Crime and punishment: an economic approach*, in Journal of Political Economy, 76, 1968, pp.169-217; Cornish D. B., Clarcke R. V., *Understanding crime displacement: an application of rational choice theory*, in Criminology, Vol. 25, Issue 4, March 2006 (1987), pp. 933-948

to a target, a pop-up will be created which shows a detailed assessment of the target from the objective and subjective perspective).

The Evil Done model has been developed in two different contexts[4]: i.e. the s.c. "soft targets" indentified in this study with the several Milan city public and private sectors, i.e. symbolic or iconic sites; the s.c. "hard targets" identified in this study with the several Critical Infrastructures involved in the project through *ad hoc* Agreements for the information sharing and the sensitive data exchange.
This paper in particular focalizes its attention on an in-depth analyses of the first category: the s.c. "soft targets".

"SOFT TARGETS" (PUBLIC/PRIVATE SECTORS): SYMBOLIC/ICONIC SITES (Appendix I and Appendix II)

The s.c. "soft targets" have been generally defined as "*public or semi-public (some degree of restricted access) facilities where large number of people congregate under relatively loose security. Soft targets include various form of public transportation, shopping malls, corporate offices, places of worship, schools and sport venues, to name a few*"[5].
This study in particular, considers "soft targets" a wide *spectrum* of potential targets that, for different reasons, have an attractive effect for the different forms of terrorism, taking into consideration not only the s.c. international terrorism (i.e. the *Jihād* matrix terrorism based on religious ideologies), but also other forms of terrorism/subversion internal to the national Italian borders (e.g. the political matrix terrorism, namely the *Red Brigades* extreme left-wing terrorism or the Anarchic-Insurrectional subversive movements). According to this premise, once selected this kind of targets, the terrorist movements can obtain the same, and in some cases even stronger emotional and concrete effects, compared to the "hard targets". This issue has been evaluated by McCreight: "*Any terrorist group wishing to damage that complacency or shake up a country's 'security fatigue' could no better than hit a soft target*" [6]. This is the reason why it is essential to take into consideration *a priori* the potential targets that are not obvious according to the previous experiences of terrorist attacks within the EU borders, but that have been experienced in other Countries (e.g. Middle East Countries), on the base of a probabilistic approach, which importance has been underlined by the doctrine. In particular, Bedford & Cooke developed a risk

[4] Libicki M. C., Chalk P., Sisson M., *Exploring Terrorist Targeting Preferences*, Department of homeland Security, RAND Infrastructure, Safety, and Environment Program, 2007, RAND_MG483.pdf
[5] STRATFOR Global Intelligence, *Special Security Report: The Militant Threat to Hotels*, STRATFOR, 8 September 2009
[6] McCreight R., *Soft targets in your backyard*, in Homeland Defense Journal, 5(10), Oct., 2007, pp. 30-34

assessment on terrorism threat based on this perspective: "*Probabilistic approaches involve sophisticated notions of **release** (rate at which the hazard strikes), **exposure** (vulnerability of populations per unit time), **dose rate** (impact per person), and **background levels** (inherent natural risk levels)*"[7].

Therefore, the iconic/symbolic sites/places in a city may be target of violent events for different reasons.
In light of this premise, the Milan Municipality developed partnerships with different stakeholders, coming from private-public sectors of Milan city. From a scientific perspective, the scientific team provided them with a questionnaire aimed to make a survey of the most relevant sites and more probable targets of terrorist attacks within the Milan urban context, according to their experience. This survey has to be intended as a flexible list of sites, which can be modify through the time, as well as substituted with other iconic possible targets present in other Municipalities/Counties, to adapt this document to the specificities of the other EU Counties partners in this study (see "Evil Done Questionnaire - 1° part": **Appendix I**).

In detail, the stakeholders involved in the survey procedure, i.e. two-steps process of iconic sites analysis through the two s.c. "Evil Done Questionnaires" (1° & 2° part), are the following:
-Territorial development Dept. (Expo 2015-Milan)
-Education Sector (Municipality of Milan)
-Territorial Information System (Municipality of Milan)
-Statistic Dept. (Municipality of Milan)
-Technical and Culture Dept. (Municipality of Milan)
-Sport Sector (Municipality of Milan)
-Presidency Office (Municipality of Milan)
-Citizens Services Dept. (Municipality of Milan)
-Museum of 900 (Private Sector)
-Streets maintenance Sector (Municipality of Milan)
-Social Housing Sector (Aler/Erp)
-Training Sector (Municipality of Milan)
-Territory Sector (Municipality of Milan)
-Public Works Sector (Municipality of Milan)
-Technical Office of Public Property (Municipality of Milan)
-Museums (Private Sector)
-Cultural Sector (Municipality of Milan)

[7] Bedford T., Cooke R., *Probabilistic risk analysis*, Cambridge Univ. Press, New York, 2001

The result of this first survey has been a new list of the first ten symbolic sites in Milan, which have a higher probability in being targeted by terrorist organizations, on the base of the risk assessment (scale evaluation 1 to 5) of the stakeholders involved in the project (private and public sectors). Therefore, it is possible to mention which sites should be object of a special care from a prevention strategy perspective, as listed below:

1. Castello Sforzesco
2. Duomo
3. Corso Vittorio Emanuele e Galleria
4. Palazzo di Giustizia
5. Palazzo Marino
6. Palazzo Reale
7. Santa Maria delle Grazie
8. Stadio San Siro – Meazza
9. Stazione Centrale
10. Teatro alla Scala

The sites are listed from the site (number 1), which has a higher risk of becoming target of terrorist attacks to the last one (number 10), characterized for a lower probability level. It is also important to underline that the abovementioned list takes into consideration the first ten sites which obtained a higher score in the risk level assessment procedure by the several symbolic places stakeholders involved in the first step survey.

The second step, within the evaluation process of the risk level among the considered symbolic sites, is characterized for a further analysis, focusing the attention only on the ten most relevant in terms of risk level, iconic places (see "Evil Done Questionnaire – 2° part": **Appendix II**).
Each of these sites has been object of a more in-depth risk analysis on the base of a further questionnaire, investigating certain security aspects already adopted by each site.
In detail, the questions refer to the following main topics:

-**the technological devices component**: i.e. cctv systems, alarm systems, access control, other to be specified

-**the human resources component**: public security forces, private security agents. Besides, for both categories, it is required to specify if they operate daily and/or nightly
-**the daily flow of people** has to be quantify and in case of a Big Event occurs, it is required to specify the increment on the visitors number
-**the operative protocols component**: i.e. existent operative protocol in case of terrorism and in case of Big Event. Whether there aren't protocols for these two particular emergencies contexts, it is analyzed the possibility in developing *ad hoc* protocols for these cases
-**historical cases records** and **statistical database** of emergencies (if existent)
-**internal directives on the mass media communications management** in case of emergency (if existent)
-how it would be worth to **implement** (if necessary) **the existent operative protocols** in case of terrorism
-the probabilistic analysis a **terrorist attack** occurs (scale 1 to 5)
-the frequency through the year the site organizes a **Big Event** (scale: never-weekly-monthly-3/4 times in a year-2 or less times in a year)
-**qualities and limits** to the existent protection system (open question)
-further **suggestions and comments** on this issue (open question)

The result of the abovementioned scheme questionnaire has demonstrated that there is a diffused awareness of both public and private sectors in developing security strategies to protect these kind of targets.
In concrete, it is worth to analyze the several abovementioned aspects referred to the risk assessment for a better comprehension of the adopted safety/security issue calibrated on the ten sites exposed to a higher level of risk.
The technological component is characterized for a shared adoption of devices to guarantee the safety/security of the mentioned sites: each place adopts cctv systems for the videosurveillance, managed by different institutions, *primus inter pares* the Local Police (PL), as well as technological instruments for the access control (i.e. badges) and alarm systems to prevent unauthorized accesses and/or to monitor in case some emergency occurs.
A mirror-like situation is revealed considering **the human resources component**, as all the mentioned sites adopt private security agents (Institutes of vigilance) to strengthen the control capability for increasing the security level, since the agents patrol the site both daily and nightly.

The daily flow of people, instead depends on the features of the single site: some sites are by definition open to the public[8], some others have a higher flow of people only in certain period of the year (i.e. Marino Palace) or during certain events (*Teatro alla Scala*) or (special) Big Events (i.e. *Stadio San Siro-Meazza*) and finally there are some places that are by definition visited by many people, because of their function (i.e. the *Stazione Centrale* or *Palazzo di Giustizia*), although they also are considered historical places (in light of the architectonic features of these two buildings (Mussolini period, "Empire Style").

It is important to underline that each site has its specificity, which has to be taken into consideration to guarantee a certain level of safety/security, as demonstrated by **the operative protocols component** analysis. In fact, all the places adopted operative protocols in case of an emergency (both safety/security nature) occurs, although only some of them have implemented *ad hoc* operative protocols in case of terrorist attack, but all the stakeholders involved in the survey underline the importance to have or develop (in the next future) this kind of protocols. The same approach is valid also for the *ad hoc* operative protocols during Big Events, but the difference is that, in the course of these events, the Prefecture has the direction and coordination of the security plan, therefore the sites that do not have specific protocols to manage Big Events, adopt automatically the plans implemented by the Prefecture. Anyhow, all the stakeholders underlined the importance in developing protocols to manage the safety/security during Big Events. Besides, it is important to underline that the majority of the stakeholders underlined the necessity to update and implement the existent protocols in case of terrorist attack, as any protocol needs to be updated after a certain time, because the (internal/external) conditions may vary, as they vary, through the time. Therefore, to develop effective operative protocols, it is essential to modify and update them according to the changed conditions and variables an urban context is influenced from.

Few sites record **the historical cases** (managed emergencies), but some of them fill this gap with a database through which **the statistical data** are gathered, to analyze the frequency certain kind of emergencies occur, on the base of a classification of the emergencies typology (nature): natural hazards, sabotages, technical breakdown, etc.

The topic issue of **communication with mass media** (and third parties in general) during an emergency is an extremely important aspect, as demonstrated by the fact that the majority of the listed sites improved *ad*

[8] i.e. *Castello Sforzesco*, *Duomo* Church, *Corso Vittorio Emanuele & Galleria*, *Palazzo Reale*, *Santa Maria delle Grazie*, because they are touristic places; *Palazzo Marino* is open to the public only in certain planned period (3/4 times in a year), as it is the seat of the Milan Mayors'Office, the General Direction and the Presidency Council; the *Stadio San Siro-Meazza* has a higher flow of people during football matches or concerts (Big Events); the *Stazione Centrale* has a high flow of people as it is the main train station (tourists, passengers, occasional visitors, etc.) as well as the *Palazzo di Giusitzia*; *Teatro alla Scala* has a high flow of people during art performances (plays, concerts, ballets, etc.)

hoc directives to manage and define "what-how-when" communicate with external parties (i.e. mass media).
The valuation of the necessity to update operative protocols needs to be integrated with the information about the probability assessment for a site in being target of **terrorist attack** and the frequency the place organizes **Big Events**, as these two component are co-related. In fact, Big Event is by definition an attractor for terrorism, since it catches the attention of the mass media, increases the flow of people in a certain venue at the same moment, thereof it strengths the risk level, as the mentioned factors increases the vulnerability of the site.
Therefore, it is important to notice that in "ordinary" condition any site is characterized for a medium level of risk (scale 1 to 5: score between 2/3), while the risk level naturally increase during certain special events (i.e. concerts, sport events, art exhibitions, etc.) (scale 1 t o5: score between 4/5). On the other side, each site has its specificity in planning Big Events through the year, in some case they are regularly programmed (i.e. *Stadio San Siro-Meazza*), in some other places these kind of events are exception, planned in certain period of the year (i.e. *Palazzo Marino*): thereof each site has to be analyzed individually, as well as the risk level requires an *ad hoc* assessment, according to the specific features of the site itself.
Finally, the questionnaire wants to detect from a general perspective **the qualities and limits** of the existent security level, intended as "open questions", according to the opinion, based on the perception and experience of the single stakeholder involved in the survey. The result has been rather homogeneous in both the perspective of the assessment: the qualities in terms of value scale are largely defined as a medium level of effectiveness in the existent protection system; the limits have been unanimously identified with the objective necessity in improving the training and the update courses for the employees in general, as well as those specifically involved in the safety/security issues of the site. In few words, the stakeholders recognize that the periodical update of the employees is fundamental to reduce the risk level. Furthermore, this aspect has been underlined even in answering the **suggestions and comments** "open questions", i.e. the stakeholders specified that two forms of training are fundamental for an effective protection of the place: the training for using in a proper way the technological devices (cctv systems and surveillance instruments) and the training for an effective emergencies management, whatever is the origin of this dangerous event (sabotages, natural hazards, technical breakdown, etc.).

In conclusion, the "soft targets" are characterized for a wide variety of logistic (external), structural (internal) features which have to be taken into consideration to implement a proper prevention strategy, as well as to adapt the operative protocols to the specificities of each site in developing suitable and effective procedures to manage emergencies, whatever is the nature of the dangerous event.

With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security – related Risks Programme
European Commission – Directorate General Home Affairs

SMART CIBER –
System of Maps Assessing Risk of Terrorism against Critical Infrastructures in Big Events Rallies
Grant Agreement N. AG025
30-CE-0453363/00-22

GLOSSARY

BIG EVENT: Big Events of mega-events are "large-scale cultural (including commercial and sporting) events which have a dramatic character, mass popular appeal and international significance".
CRITICAL INFRASTRUCTURES: the EU Communication COM(2004) 702 defines Critical Infrastructures as "Those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of the government Member States".
"EVID DONE" MODEL: it is a risk assessment model based on the "Situational Criminology" by Clarke, characterized for the development of certain features that, the experience and the most diffused literature, recognize as the most determinant aspects that make a certain site/place a potential/privileged target for terrorism.
"Evil Done" is the acronym of a set of features that characterize the potential targets to analyze:
E-exposed; V-vital; I-iconic; L-legitimate; D-destructible; O-occupied; N-near; E-easy
HARD TARGETS: the predominant literature in the terrorism context defines the "hard targets" as those that have a more probability in being object of terrorism attacks, because of the intrinsic nature and function that these kind of targets have within a social context. Usually the hard targets are identified with the Critical Infrastructures. Examples of "hard targets" could be the following: electrical and gas company, public transportation company, water system, train and railway company, etc. (see also "Critical Infrastructure" definition)
OPERATIVE PROTOCOL: it is a standard procedure for managing certain emergency or risky situations that may occur within certain technical contexts.
RISK: the doctrine has not created a unique definition of "risk", since this phenomenon can occur in different contexts and it can be expressed from a wide *spectrum* of phenomena of different nature.
This research defines "risk" as is "the evidence of a (potential or real) threat of damage, injury, liability, loss or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive measures, such as surveillance practices".
RISK ASSESSMENT MODEL: a "model" is a schematic and simplified description of a phenomenon, system or process that accounts for its known or inferred proprieties and may be used for further study of its characteristics (i.e. predictions). Thereof, a "risk assessment model" is a scheme through which it is possible to analyse a set of phenomena that the experience indentifies as (quantitative and qualitative) highly probable to generate "risk" within a certain context.

SAFETY AND SECURITY POLICY: the distinction between the two terms "safety" and "security" is always ambiguous, since in many languages there is not a concrete distinction between the two words, as there is only one word to express the both concepts (e.g. German '*Sicherheit*', French '*sécurité*', Italian '*sicurezza*', Spanish '*seguridad*', etc.). In reality the doctrine defines "safety" as 'the condition of being free form harm or risk', which is basically identical to the "security" definition, i.e. 'the quality or state of being free from danger'. But in the case of "security", a further meaning has been developing, more specifically in connection with criminological aspects, i.e. 'the measures taken to guard against espionage or sabotage, crime, attack or escape'.
In light of the pervious premise, the "security and safety policy" is the set of rules and strategies to prevent/repress any form of danger, harm or risk , whatever is the nature of these phenomena.
SOFT TARGETS: the predominant literature in the terrorism context defines the "soft targets" as those that have a possibility on the base of the most recent events in being object of terrorism attacks. These targets are defined as "soft" in light of their intrinsic nature and function, since they are not essential for the functioning of a certain urban context and society at large (as it is the case, for instance, of the Critical Infrastructures). Examples of "soft targets" in both public and private sectors, could be the following: hotels, museums, sport stadium, churches and religious sites, art monuments, etc.
TERRORISM: the doctrine has not given an exhaustive and clear definition of "terrorism". In fact, both the U.S.A. and the EU created their own "terrorism" definitions, although the result is for both definitions, a list of behaviours that the experience referrers to terrorism phenomenon.
The main difficulty in defining this complex criminal activity is due to its "dynamic and flexible" capability in adequate its violent strategy to the social, political, religious, historical context of reference. Thereof, the doctrine distinguishes different forms of "terrorism": i.e. religious terrorism, political terrorism, narco-terrorism, environmental terrorism, etc.; furthermore the logistic violent operative capability influences the "terrorism" definition: i.e. national terrorism and international terrorism.
VULNERABILITY: it is a certain phenomena that has negative consequences (social uneasiness) within a certain space (urban setting) from different viewpoints: i.e. social, political, institutional, economical, cultural, religious, etc.

With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security – related Risks Programme
European Commission – Directorate General Home Affairs

SMART CIBER –
System of Maps Assessing Risk of Terrorism against Critical Infrastructures in Big Events Rallies
Grant Agreement N. AG025
30-CE-0453363/00-22

Appendix I

"Evil Done Questionnaire" provided to the private-public sectors of the Milan Municipality
"Soft targets"
1° part

The following survey aims to assess the iconic dimension of certain sites (buildings, areas, etc.), underling the probability that a violent attack may target a specific community present in this place, violating the history, memories and features that characterize the shared identity of the community itself.
This questionnaire is an "open" list of potential iconic places which characterize the "Milanese identity", which aim is to attribute a score on the base of the iconic value assessment of each mentioned site belonging to the city of Milan.
The list excludes *a priori* what is considered Critical Infrastructure, namely the vital sectors for the city governance, i.e. the electrical system, hospitals, universities and schools, (local/national) government institutions, general consulates, etc.
Nevertheless whether some CIs may be classified as "iconic sites", it is possible to add them to the following list.
As this is a qualitative survey, there is not an objective criterion to measure this "dimension" (i.e. iconic/symbolic value), as the evaluation is merely subjective in light of your experience and perception, intended as added values to this survey.
The evaluation that is required is independent from the "time" variable. For instance, the *San Siro Stadium* has an iconic value per se (what it is required for this questionnaire), but the same site may become a "sensitive target" during a football match or a concert. This evaluation from a temporal viewpoint should not be taken into consideration in the "iconic value" assessment, as it is possible to "measure" it in the specific column (see the scheme below), as a specific risk increasing level component.
On the base of this very first assessment, it is possible to elaborate a classification of the identified sites/places that allows further in-depth analysis completed also with objective data (e.g. the daily flow of people, structural feature of a building, etc.).
In this first step phase it is crucial to focus the attention on the following aspects:

- First crucial evaluation of the iconic/symbolic value of each listed site/place through the attribution of a score 1 to 5, where 1 is no/little importance and 5 is maximum importance (e.g. is the Milan

Dome according to your perception a little importance site from an iconic perspective (1-2) or is it a symbolic site of the "Milanese identity" (5)? Or again, is it a site of medium iconic value (3-4)?)

- Possible mention of a site/place with an high risk potentiality of terrorist attack, during certain particular moments (e.g. according to your perception, the terrorist attack potentiality of the site *Rho Fiera* increases during the EXPO 2015, or the site/place is always a highly possible target?)

Further empty lines at the end of the scheme allow to insert further sites/places not taken into consideration yet.

Place/site	**Iconic/symbolic level**					**In case of particular events, does the risk level increase?**
	Min.				**Max.**	**If yes, please specify the event, otherwise leave this space empty (ex. the place "stadium" please specify "football match", "concert" or some other event that can influence the risk/attractiveness of the place)**
Chiaravalle Abbey	1	2	3	4	5	
Aquarium	1	2	3	4	5	
Arco della Pace	1	2	3	4	5	
Milan Arena	1	2	3	4	5	
Duomo-Castello pedestrian area (via Dante)	1	2	3	4	5	
S. Eustorgio Basilica	1	2	3	4	5	
S. Lorenzo Basicila and Colonne	1	2	3	4	5	
Sant'Amborio Basilica	1	2	3	4	5	
Sormani Public Library	1	2	3	4	5	
Labour Chamber	1	2	3	4	5	
Casa degli Omenoni	1	2	3	4	5	
Castello Sforzesco	1	2	3	4	5	
Monumental Cemetery	1	2	3	4	5	
Corso Como	1	2	3	4	5	
Corso Vittorio Emanuele	1	2	3	4	5	
Duomo	1	2	3	4	5	
Non-Christian buildings(mosques, synagogue)	1	2	3	4	5	

Fiera Milano city	1	2	3	4	5	
Fiera Rho	1	2	3	4	5	
Fiera Sant'Amborgio	1	2	3	4	5	
Stelline Foundation	1	2	3	4	5	
Assago Forum	1	2	3	4	5	
Galleria Vittorio Emanuele	1	2	3	4	5	
Pirelli building	1	2	3	4	5	
Pac	1	2	3	4	5	
La Rinascente	1	2	3	4	5	
La Triennale	1	2	3	4	5	
Art Galleries	1	2	3	4	5	
Lido di Milano	1	2	3	4	5	
Mercati Generali	1	2	3	4	5	
Navigli (area)	1	2	3	4	5	
Unicredit new palace	1	2	3	4	5	
Palazzo dei Giureconsulti	1	2	3	4	5	
Region palace	1	2	3	4	5	
Palazzo di Giustizia	1	2	3	4	5	
Palazzo Marino	1	2	3	4	5	
Palazzo Reale	1	2	3	4	5	
Sempione park	1	2	3	4	5	
Pinacoteca di Brera	1	2	3	4	5	
Quadrilatero della moda	1	2	3	4	5	
Besana roundabout	1	2	3	4	5	
Santa Maria delle Grazie (Il Cenacolo)	1	2	3	4	5	
Milan stock-exchange	1	2	3	4	5	
San Siro Stadium	1	2	3	4	5	
Stazione Centrale	1	2	3	4	5	
Teatro degli Arcimboldi (theatre)	1	2	3	4	5	
Teatro alla Scala (theatre)	1	2	3	4	5	
Velasca tower	1	2	3	4	5	
Via Tortona	1	2	3	4	5	
Villa Belgioioso Bonaparte or Villa Reale	1	2	3	4	5	
	1	2	3	4	5	
	1	2	3	4	5	

	1	2	3	4	5	
	1	2	3	4	5	
	1	2	3	4	5	
	1	2	3	4	5	

With the support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security – related Risks Programme
European Commission – Directorate General Home Affairs

SMART CIBER –
System of Maps Assessing Risk of Terrorism against Critical Infrastructures in Big Events Rallies
Grant Agreement N. AG025
30-CE-0453363/00-22

Appendix II

"Evil Done Questionnaire" provided to the private-public sectors of the Milan Municipality "Soft targets" 2° part

The 1° part of the questionnaire (see **Appendix I**) aimed to identify which iconic sites have a higher probability in being target of terrorist attacks.
Below there is the classification of the first ten sits which have a higher probability of becoming targets of terrorism:

11. Castello Sforzesco
12. Duomo
13. Corso Vittorio Emanuele & Galleria
14. Palazzo di Giustizia
15. Palazzo Marino
16. Palazzo Reale
17. Santa Maria delle Grazie
18. San Siro – Meazza Stadium
19. Stazione Centrale
20. Teatro alla Scala

The original list to select the potential soft targets was long, thereof in future it will be possible to recalibrate the abovementioned classification, as it has to be intended always as an "open list", object of constant update and modification if the external conditions vary. Nevertheless, at the moment it is important to focalize the attention on the first ten potential targets, listed above, to gather information aimed to make a risk-assessment referred to each soft target.

The present Protocol is object of a first test, aimed to develop a standard process to gather the information also for the future implementations of this model.

Therefore we require you to answer the following questions for each of the ten mentioned sites. In case you are not the competent authority in charge to manage the information we ask for, please provide us with the name of the responsible in charge for the management of those data (natural or legal subject):

<table>
<tr><td>Castello Sforzesco</td><td>1.</td><td colspan="4" rowspan="10">Note:

1. Indicate which is the specific site object of the analysis.
2. A partial answer to this questionnaire is accepted and useful for an overall assessment.
3. Whether it is ABSOLUTELY IMPOSSIBLE to provide with certain information, please indicate which is the possible source/authority in charge to collect this information.</td></tr>
<tr><td>Duomo</td><td>2.</td></tr>
<tr><td>Corso Vittorio Emanuele & Galleria</td><td>3.</td></tr>
<tr><td>Palazzo di Giustizia</td><td>4.</td></tr>
<tr><td>Palazzo Marino</td><td>5.</td></tr>
<tr><td>Palazzo Reale</td><td>6.</td></tr>
<tr><td>Santa Maria delle Grazie</td><td>7.</td></tr>
<tr><td>Stadio San Siro – Meazza</td><td>8.</td></tr>
<tr><td>Stazione Centrale</td><td>9.</td></tr>
<tr><td>Teatro alla Scala</td><td>10.</td></tr>
<tr><td rowspan="2">Is the site protected with technological devices? (if yes, please specify)</td><td>Videosurveillance (cctv)</td><td>Alarm systems</td><td>Access control</td><td>Other</td></tr>
<tr><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td></tr>
<tr><td rowspan="2">Is the site protected through human resources (public security forces or private security agents?) (daily and nightly)</td><td colspan="2">Public security forces (PS, EEI, etc.)</td><td colspan="2">Private security agents (private security institute, etc.)</td></tr>
<tr><td>Daily patrol</td><td>Nightly patrol</td><td>Daily patrol</td><td>Nightly patrol</td></tr>
</table>

	Yes	Yes	Yes	Yes
Is it possible to quantify the daily average flow of visitors to your site? If yes, please specify the number	Yes, average number:	I do not know, possible alternative source of information:		
Do you have already adopt *ad hoc* operative protocols to manage terrorism emergences, which require an inter-forces coordination? (e.g. PS, CC, fire brigades, Ambulances/hospitals, etc.)	Yes	I do not know, possible alternative source of information:		
If there aren't specific protocols to manage terrorism events, do you think it would be worth to adopt and develop this kind of protocol within the context of your site protection?	Yes	No		
Do you already have operative protocols specifically addressed towards the possible emergences during Big Events within the context of your site protection?	Yes	I do not know, possible alternative source of information:		
If there aren't specific protocols to manage emergences during Big Events, do you think it would be worth to adopt and develop this kind of protocol within the context of your site protection?	Yes	No		
Do you keep any historical archive of the emergency events occurred through the last 10 years for the protection of your site?	Yes	I do not know, possible alternative source of information:		
Do you keep any statistical database gathering the frequency of emergency events that occurred, according to the typology of the events, for the protection of your site? (technical damage, sabotage,	Yes	I do not know, possible alternative source of information:		

natural hazards, etc.)					
Do you have specific directives to manage emergency situations in regard to the communications with external entities, i.e. mass media, institutions, etc. through the several stages to the emergency management for the protection of your site? (emergency - management of the event - recovering phase)	Yes	I do not know, possible alternative source of information:			
How do you think your operative protocol to manage terrorism events could be improved (if possible)?	Yes	I do not know, possible alternative source of information:			
Which is the probability that a terrorist attack can target your site?	Probability level				
	None				Extremely high level
	1	2	3	4	5
Which is the frequency your site manages Big Events?	Never	Weekly	Monthly	3/4 times in a year	2 or less times in a year
Quality of your existent system of protection and management of emergencies:					
Limits of your existent system of protection and management of emergencies:					

Further comments on your existent system of protection and management of emergencies:	
Suggestions to improve the existent system of protection and management of emergencies:	