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
Second part: the "hard targets", i.e. Critical Infrastructures

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. "hard targets", i.e. the Critical Infrastructures of Milan city.

30 September 2013

INTRODUCTION

The previous paper (see Concept Paper 6) focalized the attention on the s.c. "Soft Targets" analyzed in light of the "Evil Done" model, developed through a questionnaire provided to the most symbolic sites of the Milan city, considering their iconic value, because of cultural, social, religious, historical, economical, political implications which characterize these (public and private) places.
This second part of the EVIL DONE model analysis for the development of a risk assessment map against terrorism potential targets, focalizes its attention on the s.c. "Hard Targets", i.e. the Critical Infrastructures of the Milan city. In particular in this study the main CIs of Milan have been contacted: i.e. ATM (public transportation service), A2A (electric and gas system) and AMSA[†] (public dumps and environmental issue), MM (water system), SEA (airport company), RFI (train railway company), FN (local train company).

[*] 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

[†] AMSA is part of the A2A company, for this reason this paper considers A2A integrating data also for the AMSA experience. Therefore when A2A is mentioned, it is implicit the extension to the AMSA case.

"HARD TARGETS": CRITICAL INFRASTRUCTURES

The definition of Critical Infrastructure (CI), as a due premise to this paper, has already been analyzed in the Concept Paper 3 from both European and national perspectives.
Therefore, a further evolution of the CIs analysis, as possible terrorist targets, in light also of the weak signals, social vulnerabilities and early warnings which characterize an urban context, requires to focalize the attention specifically on the terrorism phenomenon. In particular, on the base of the EVIL DONE model for the terrorism threat risk assessment, it is possible to develop an operative system. Thereof, this study adopted as model the one widely utilized for the protection of the s.c. "*soft targets*" against terrorism (e.g. international hotels), since the risk map that this research intends to implement is based on indicators referred even to the weak signals, intended as social vulnerabilities.

In detail, the agreement with the Milan CIs implies also an active participation to the model development, through a self risk assessment process, i.e. a questionnaire (see "Evil Done Questionnaire 1": **Appendix I**). In fact the questionnaire has been provided to the *security managers* of the several CIs, able to make an assessment of the reaction capability and the security level in the existent conditions in case of an emergency occurs (the s.c. "*self check and risk assessment*"). The added value of this approach is characterized for an *ex ante* risk assessment (considering any form of risk, from terrorism to the natural hazards or technical/technological devices break down), as it is able to evaluate the response capability even before the emergency/event occurs, implementing the already existent protocols and improving also a better inter-forces cooperation capability, that an emergency situation unavoidably requires.
The results obtained from the 1° round interviews on the base of this first questionnaire are both quantitative and qualitative data, so that the risk assessment for each CI is as complete as possible.

The further aim of making a comparative afford among the CIs to understand the gap among the several risk assessment systems has been solved through a 2° round interviews with the infrastructures *security managers* (see "Evil Done Questionnaire 2": **Appendix II**). In fact this second questionnaire is calibrated to gather specific and comparable quantitative data on the risk assessment issue in the safety/security management of each CI.

It is evident that a risk assessment for the development of a city governance model requires a complex and wide analysis of elements that in a different way can influence the prediction capability to manage emergencies on the base of previous experiences: from "early warning" signals (i.e. vulnerabilities) to the s.c. "red flags" ones (i.e. emergencies, among which terrorist attacks).

In light of this premise, it is essential to analyze the feedback of the two questionnaires considering each CI (vertical analysis approach) and its specific experience in assessing risks and managing emergences on the base of the already existent system and in light of a comparative approach among the several involved infrastructures (horizontal analysis approach).

"EVILD DONE QUESTIONNAIRE 1"

1-Critical Infrastructure (CI) security level assessment:

The first part of the questionnaire is divided in several sub-groups of questions referring to the topic safety/security aspects, considering the nature of any Critical infrastructure. Thereof, It is possible to classify the several aspects as follow:

-**logistic aspect**
-**strategic aspect**
-**risk and vulnerability aspect**

Therefore, it is essential to deeply analyze each aspect separately, considering that the gathered data have both a quantity and qualitative nature.

The **logistic** aspect is a fundamental component for an effective risk assessment and the consequently development of a prevention policy, as this perception is generally shared among the several CIs in Milan.
In fact, the majority of the CIs are logistically located or the supplied services are in a position which guarantees a proximity to the city center, intended as a sensitive area, as usually within an urban context, like the one of Milan, is characterized for a big flow of people (i.e. people who are resident, working or tourist in this area) and a high concentration of symbolic/iconic buildings, institutions, monuments, etc..

In detail, the feedback of this first part of the questionnaire has determined that the majority of the CIs pay attention to their logistic location in relation to the reality that surrounds the infrastructure itself, as a delicate aspect is the management of the safety and security factors referred to the central part of Milan city. Therefore, the maximum value, i.e. in a scale 1 to 5, the maximum score -5-, attributed by the security managers to the assessment of the security in relation to the proximity to the city center has been expressed by ATM (public transportation company), as this CI reaches any part of the city in light of the intrinsic nature of the supplied service. The same situation has been assessed by MM (water system) and A2A (electrical and gas systems) and finally by FerrovieNord (FN), as this local train company has a station in *Cadorna*, which is an area already considered closed to the historical part of the city.

A medium level of risk (score: 3) has been attributed by RFI (national train railway company), as its railway has no direct access to the city center of Milan, as its main service is focused in linking Milan with external areas (cities, regions, countries), therefore the aim is to link the passengers to the most important connections with the public transportation system. Nevertheless, a medium level of risk implies that there is a certain degree of risk connected to the city center, in fact the assessment has been motivated by the fact that some portion of the train railway are closed to areas considered part of the historical center of the city.

Finally, a minimum proximity to the city center (score: 1) has been attributed to the SEA (airport company), as the nature of its service objectively hampers the location in an area closed to the city center. In detail, the two main airports linked to the Milan city, i.e. *Linate* and *Malpensa*, are located in different areas outside the city: *Linate* is in the east suburban area of Milan; while *Malpensa* is 40 km. outside Milan, being under a different province (Varese province).

The second logistic aspect considered in the risk assessment is the proximity to symbolic/iconic sites of the city (not necessary located closed to the city center), the result of the survey confirmed the previous importance of certain CIs which aim is to link, supplying different services for the city functioning, the different sensitive areas of the city: this is the case of ATM, A2A and MM, (score: 5) as they play a key role inside the city, covering almost any part of Milan. RFI also determined a maximum proximity to the symbolic places of the city, as for this CI it is necessary to consider not only the direct relation to these sites, but also the indirect link, as the train stations are connected with other transportation systems (ATM), i.e. underground, bus, tram, etc., which cover the most important sites of the city.

The FN local train company, instead defined a medium level of proximity to the most important symbolic/iconic sites of the city (score: 4), as there is only the station of *Cadorna* that covers an areas surrounded by symbolic sites (historical places, museums, cultural centers, etc.).

Finally, SEA has a minimum proximity with symbolic sites of the city (score: 1), because of the previous explanation referred to its logistic location of both the *Linate* and *Malpensa* airports.

The third parameter of risk assessment to be considered is the proximity to other CIs, the risk in this situation is the logistic interdependency among the several main CIs of Milan.

The special correlation among the CIs can be explained with two different motivations: firstly, there is a synergy between certain CIs (e.g. the train stations –RFI- and the relevant public transportation vehicles –ATM- , which aim is to connect the station with the main sites inside the Milan city). A second reason of a logistic proximity is rooted in the intrinsic nature of the supplied services by each CI (e.g. the water system –MM- or the electric/gas system –A2A- need to cover the whole urban context, as well as the public transportation system –ATM-), in this case is unavoidable an overlap of the different services from a cartographic perspective (Milan city map).

The feedback analysis, from this point of view, therefore reveals that the majority of the CIs interlink each other, since the aim to supply an essential service to the city requires an overall presence of the infrastructure system in the city. Thereof, all the main CIs (i.e. A2A, ATM, FN, MM and RFI) underlined a direct logistic proximity with other CIs, while SEA, as the airport is a very sensitive site and because of its logistic location is the one more isolated from the other CIs, due also to a responsible choice in avoiding any proximity with other infrastructures that may, under certain conditions, increase the risk level.

The last parameter of evaluation of the logistic risk assessment is the proximity to other essential services, not officially classified as “Critical Infrastructures”, i.e. tribunals/courts, hospitals, police stations and police headquarter, general consulates, etc.

In light of this perspective, the majority of CIs have revealed having a direct proximity with some or many of this particular category of sites. In fact, A2A, MM, ATM underlined their logistic location closed to certain essential services for the city (score: 5); while RFI and FN have a medium level of proximity to these buildings (score: 4), as the number of sites is limited to the station location, closed to police stations (PS, CC and GdF) and hospitals, although there is not a direct link with these sites. Finally, SEA is not surrounded by essential sites, because of its logistic location within the Milan urban context and because of a specific choice not to increase the risk level, managing an airport closed to other sensitive potential safety/security targets.

From a **strategic** perspective, this research has taken into consideration the two main components to prevent first, and then to control potential risks, i.e. the technological devices and the human resources.

In detail, unanimously all the main CIs interviewed in the course of the present study utilize both these measures, as a shared concept is that the technological devices are useless whether there is not the human component, which can filter and give and interpretation to the contingent situation for determining the risk level in case an event occurs. On the other side, the use of technological devices facilitates the everyday work of the employees and/or persons responsible for the safety/security of any infrastructures.

Each infrastructure adopts a wide typology of technological devices (alarm systems, access monitoring, videosurveillance of different kind, badges for the access control of the employees and in certain cases also of the occasional visitors, etc.) active both daily and nightly. Each tool is calibrated according to the nature of the site to control, as well as the typology of the service supplied by each CI. Sometimes the technological devices are shared with the public security forces (e.g. cctv systems), to improve the security level.

Human resources is a fundamental aspect for an effective safety/security strategy, it could be both internal and external to the CI company, in fact there are different cases: the internal employees are trained also for managing events when the safety or the security is compromised, other infrastructures prefer to manage the security issue through private security agents (Institutes of vigilance) and some others prefer to integrate both the solutions.
Furthermore, the main CIs share the policy of planning training and update courses for the internal employees, as it is perceived as a fundamental part of the whole strategy of prevention/management of risks (intended as any form of risks, involving the safety issue and/or the security one).

The **risk/vulnerability** aspect is characterized for two main focuses of attention: i.e. the social uneasiness interlinked with the logistic location of the CI and the contact with a (daily) flow of people that, for different reasons, expose the CI to risks.
This analysis is run through a sociological perspective and not only from a criminological point of view, strictly related to the safety and security aspects.

In detail, the social uneasiness can be revealed through different phenomena, i.e. what has been defined in this research as “weak signals” or “early warnings” (see Concept Paper 5). These particular human phenomena have a wide variety of concrete expressions. It is possible to underline that the majority of the CIs share similar phenomena belonging to this category of risk.
In light of this consideration, it is possible to classify the most common expressions of social uneasiness, as follow:
1-Roma camps
2-unauthorized occupations (buildings, trains wagons or private properties in general)
3-abandoned/isolated areas
4-thefts of particular materials (iron, copper, batteries, etc.)

5-proximity to social housing buildings (*Aler*, *Erp*), as the experience reveals being places of particular social uneasiness
6-illegal immigrants
7-areas where there is a lack of lightening or it is insufficient

The first four phenomena are commonly experienced by the majority of the CIs, while there are other forms of social uneasiness which can be considered as specificities of certain infrastructures (e.g. unauthorized permanence on the railway –RFI and FN-; lack of lighting in galleries –RFI and FN-, etc.). the problem of illegal immigrants usually has not direct consequences on the CI functions, as well as the proximity with social housing, but this phenomena causes indirect problems, because of the progressive degradation of the area or some criminal behaviors which have a higher probability in presenting their effects in these contexts: i.e. drug dealing, prostitution, gangs of youth or ethnical gangs and so forth.

Finally, as far as the direct contact with people is concerned, it is possible to distinguish two categories of infrastructures:
-CIs that, because of the nature of the supplied service, requires a direct contact with people: i.e. ATM (public transportation system); SEA (airport company); RFI (national train railway company) and FN (local train company). In this case the contact with the public is both with customers of the service and occasional people
-CIs that, because of the modality of supplying the service, implies an indirect contact with people: i.e. A2A (electrical and gas company) and the related AMSA (dump company and environmental issue); MM (water system). In this case the contact with the public is indirect because the electricity, gas and water distribution functions independently from the customers presence, besides there could be an occasional contact with people in the administrative offices (complains, bills payment, utility charges, etc.) or when a technical intervention is required by customers.

2-Existing protocols assessment:
This part of the questionnaire focalizes its attention on the already existent operative protocols in case an emergency occurs. The analysis refers to the practical approach that each CI adopts in case of emergency, and in particular the two main aspects taken into consideration are the inter-forces coordination component and the specific case of terrorism attack during an emergency by the employees specialized in safety/security management.

The results lead to a common shared experience from this perspective, as all the major CIs have operative protocols that foresee an inter-forces coordination with the public security forces (i.e. PS-national police, CC-*carabinieri*, PL-local police, VVF-fire brigades, Civil Protection, ambulances and hospitals), some of them have also direct contacts with special police, such as the RFI and FN, since in the major train stations there is a fix police station (PolFer-special police for the train stations, which is a branch of PS-national police).
The majority of CIs adopt even *ad hoc* operative protocols in case a terrorist attack occurs (NATO and EU Protocols, Leonardo Da Vinci plan) and some of them are updating their protocols in line with the EU Directives on this issue. It is likewise important to notice that in case of Big Event, all the CIs security plans are directed and coordinated by the Milan Prefecture, as *ad hoc* meetings are scheduled in order to plan the security and the coordination before-during-after (i.e. briefings and debriefings activity) the event itself.

3-Potential emergencies assessment

This part of the questionnaire is developed on the base of the past experience for each CI and their modality in valuating previous emergencies events.
The focus of attention is "how" each infrastructure elaborates a feedback analysis after certain events, taking into consideration two particular aspects: i.e. the communication management with third parties (i.e. external entities: mass media, institutions, etc.) and the valuation of the efficiency in terms of time from the phase of the emergency occurs to the recovery moment, i.e. the achievement of the *status quo ante* condition (i.e. 3 phases procedure: emergency-emergency management-recover to the *status quo ante*).

In detail, all the CIs have an historical archive that collect the reports of past emergencies. Obviously each infrastructure has developed an archive in conformity to the nature of the supplied service: from this perspective, it is important to distinguish archives that record the technical breakdown from those that collect reports of emergencies of different nature (natural hazards, sabotages, terrorism, etc.). Besides, some infrastructure adopted this system of risk assessment analysis in recent times or the system has been recently updated for contingent reasons to make more effective the internal operative protocols.
The historical archive is completed with statistical database adopted by all the CIs, as there is an objective necessity in gathering data on relevant events, from the technical breakdown to the emergencies of different nature. Similarly to the historical archive, the statistical systems can cover both the safety and security events, since each infrastructure has its modality in gathering the data (usually there are specific departments inside the company which are responsible in updating the database). Likewise the archive system, the statistical database in some case has been recently updated (MM in march 2012) to improve

the effectiveness of the operative protocols, besides some databases distinguish the typology of the emergency on the base of a scale of danger that attribute a certain level of seriousness to each event occurred and managed by the infrastructure.

The other aspect taken into consideration in the third part of the questionnaire is the CI communication capability with third parties (mass media, institutions, etc.) in case an emergency occurs.
In this case, the majority of the CIs have specific directives *a priori* defined in the operative protocols, besides the infrastructures share the common rule, according to which there is a scale of value attributed to each emergency, so that the coordination with external entities for communication on the event are defined only under certain circumstances (the level of danger, the interruption of the service, if there are human victims or wounded people, etc.). All the CIs agree in defining two different kind of mass media communication, and sometime the two forms overlap: i.e. the use of mass media for diffusing a message about the service supply to the customers (from the infrastructure perspective) and the communication to diffuse a news by the mass media channels (from the mass media perspective).

Finally, all the CIs share the importance to evaluate the "timing" aspect to manage and recover after an emergency occurred. Details on this aspect have not been diffused for security reasons.

4-Assessment of the impact and vulnerability on the CI in case of emergency
The assessment of the impact and vulnerability has been structured through the gather of both quantitative and qualitative data, as the aim is to understand the risk level of each infrastructure of being involved in a certain kind of emergency, through a scale value (quantitative) and the explanation in light of the past experience and the operative protocols (qualitative).

In detail, from the "vulnerability" perspective, the questionnaire specifically requires to the infrastructure to attribute a value (scale 1 to 5) to the possibility of being victim of a terrorist attack. The general perception is a medium level of possibility, due to different variables: i.e. the historical moment that can influence the probability level, according to the national/international political events; the fact that "terrorist attacks" are by definition unpredictable events, therefore it is always implicitly taken into consideration in the development of operative protocols; the fact that "terrorism" is also a flexible phenomenon which can express its violence in different forms, that is why, through the last years, the CIs addressed their attention towards new phenomena, i.e. cyberterrorism (the target is the software and/or hardware) and electronic terrorism/sabotages (the target are electronic devices).

The further aspect, interlinked with the previous issue, is the probability that an emergency may involve the safety/security of people. This aspect it also related to the direct or indirect contact that the nature of the supplied service by a certain infrastructure has with people (customers, occasional visitors, people involved by chance). Therefore, the infrastructures that supply a service through a direct contact with customers (i.e. ATM, SEA, RFI, FN) obviously underlined the maximum exposure to risk of people (score: 5); while the other infrastructures (i.e. A2A, AMSA, MM), which service is supplied independently from the customers contact, reduced the risk level (score: 3).

A further distinction has been defined, as the people involved in an emergency situation may be not only customers or people “external” to the company, but in these cases the experience underlines that the “internal” employees of the infrastructure have the maximum exposure to risk in any moment. In fact, this second category of people (employees) who have a probability in being involved in emergencies is generally mentioned as the one with the maximum probability (score: 5).

From the “impact” perspective, the questionnaire refers to the economical aspect involved in an emergency for the CI and the mass media impact, as certain emergencies become mass media attention attractors.

Therefore, as far as the economical consequences of an emergency concerns, it is important to analyze the probability that a CI property may be involved and damaged in case of emergency: all the CIs take into consideration this aspect in developing a policy of prevention and management of emergencies of any nature, as all of them can risk a direct damage to their infrastructures (i.e. buildings, trains, gas pipelines, water system, etc.) in case this kind of event occurs (score: 5). On the contrary, not all the CIs can involve properties belonging to third parties (public or private sectors) when an emergency occurs, as this factor is interlinked with the logistic location of the infrastructure and its related systems: this is the case for instance of SEA, since the airport requires being in a logistic position isolated from the rest of the city.

A further economical aspect, is the pure esteem of the different kind of costs the CI needs to deal with in case an emergency occurs. In fact, the questionnaire defines the following typology of costs:

-direct cost
-indirect costs
-image costs

The assessment of the “direct costs” is implicit in a policy of risk assessment for all the CIs, the “indirect costs” need to be calibrated according to the infrastructure, as the nature of the services vary according to the infrastructure. Finally the “image costs” are the most difficult to calculate *a priori*, according a shared opinion to all the CIs, since they are the most dangerous in terms of credibility and diffused perception of the offered service quality. In fact, many infrastructures underlined that the image costs are always higher than the real costs to restore the *status quo ante* situation.

The impact that an emergency has on the attraction capability of the mass media is proportional to the emergency nature and related effects. Furthermore, it is evident that all the CIs share the same topic issue of managing the communications with the mass media, as it is a sensitive issue during a dangerous event for different reasons: the image cost due to the public opinion, the diffused panic among the customers and the public at large that could be generated from a wrong communication strategy, the amplification of the real effects produced by the emergency, the reliability of the supplied service, the quality and credibility of the service supplied by the CI, etc.. On the other side, in reality the mass media interest for certain events, can be interpreted also in a positive perspective, as it is a valid instrument to give a proper communication about the situation or to inform the customers and the public at large about the potential dangers (security and safety aspects), it is also a valid instrument to plan surveys involving the public to gather information about the general satisfaction of the service or to diffuse “security campaign” for the customers especially in certain period of the year (e.g. RFI in collaboration with PolFer periodically organizes prevention campaigns during the Christmas time or during the summer holidays to reduce the risk for its customers of being victim of crimes while they are travelling).
There is a shared opinion that the aspect of external communications with third parties, especially referred to mass media, requires a special care, therefore the majority of the CIs have an *ad hoc* office (usually the public relation office or the press release office) competent to manage the communications with the mass media in the course of an emergency. This is due also to the fact that our society is more and more dependent on the communication channels and instruments, not only the traditional ones (i.e. TV, radio and newspapers), but through the last years, new technology has been implementing the communication capability (i.e. internet, social networks, iphones, smart phones, tablets, etc.).

5-Proposals for the implementation of the existent system

The general assessment of the existent situation in the safely and security polices is characterized for a shared opinion among the CIs: i.e. the operative protocols should never be considered “exhaustive solutions”, as the experience indicates that they can always be improved and updated. The majority of the infrastructures in fact, *a priori* schedule a periodical update of the operative procedures, in some other cases the protocols are updated only when there is a concrete necessity, as basically they correspond to an already tested high security standard.

The recent violent facts at an international level (i.e. terrorist attacks), indicate that it is impossible to ignore an objective risk of terrorism, considering CIs as one of the privileged target of this subversive phenomenon, according to the common literature. Therefore, the CIs are aware that two are the main factors helping the development of a proper prevention strategy: a constant activity of training for the internal employees and the diffusion through different channels of a "security culture" (mass media, training courses, update courses, information sharing with institutions, the creation of a network among the CIs, etc.). Finally, the CIs underline the importance of developing flexible operative protocols, which becomes an essential component in case of terrorism, as this phenomenon is by definition a dynamic and flexible form of crime.

"EVILD DONE QUESTIONNAIRE 2"

A special focus has been devoted to the gather of quantitative data, to complete the risk assessment evaluation of the Milan CIs. In fact, an *ad hoc* EVIL DONE questionnaire has been provided to the security managers of the CIs for a second round interviews, aimed specifically in attributing numerical data (scale 1 to 5) to the several aspects related to safety/security issues (see "Evil Done Questionnaire 2": **Appendix II**).

The CIs answered the protocol from a general perspective first (ATM, A2A/AMSA, RFI, FN), besides some of them specified the quantitative data for each topic site, which has a strategic logistic position because of the aim of the CI service provided (i.e. ATM, RFI, FN, A2A/AMSA)

In details, the questionnaire is divided into three parts, as follow:

1- **Security level assessment of the Critical Infrastructure**
2- **Assessment of the existent protocols**
3- **Potential emergencies assessment**

It is important to underline that form a general perspective the quantitative results are almost similar, as the level of security perception, as well as the emergencies management are shared issues among all the CIs. The assessment of the protocols is also considered an essential component, not only in case an emergency occurs, but even before, as a prevention tool aimed in *a priori* defining the procedures and the several phases in managing an emergency.

On the contrary, from a single CI site analysis perspective there is a wide *spectrum* of numerical values, attributed by each CI, till the point that the score defined by the security managers of each CI varies from site to site within the same Critical Infrastructure, according to several internal/external components: namely, the logistic location of the specific site, the urban features of that area, the social situation (social uneasiness, integration level of non-citizens, proximity to social housing buildings, etc.) and so forth.

1-Security level assessment of the Critical Infrastructure

In particular, focalizing the attention on the "security level" issue, in general the numeric attribution (scale 1 to 5) on both the technological and human components in defining the security level of the CI is between 3/4 (i.e. medium level). The urban context that surrounds the CI is taken into consideration as well, as the knowledge of the territory where the CI is logistically located is fundamental to understand the potential risks and the resources that a certain part of the city can offer. The impact of certain vulnerabilities is determinant also to develop *ad hoc* operative protocols, shaped on the specificities of the urban context: i.e. Roman camps, high rate of immigration (regular, semi-regular, illegal), social uneasiness (i.e. social housing impact: Aler, Erp), etc.. In consequence, the urban aspect is also interpreted from a quantitative perspective as an issue that has a medium-level impact on the security policies development (score between 2/3).

2-Assessment of the existent protocols

The operative protocols issue has been analyzed through a single specific question: i.e. "How do you assess the efficiency level of the existent operative protocols for the management of emergencies which implies an inter-forces cooperation (e.g. national police, fire brigades, ambulances/hospitals, etc.)". Thereof, the assessment has been defined in terms of efficiency of the inter-forces capability in managing an emergency. The result from a quantitative perspective is a shared awareness of the importance in developing and improving operative protocols, as the score attributed to this issue by the security managers is commonly between 3/5, therefore the operative protocols have a medium-high level of efficiency and effectiveness in managing emergencies.

3-Potential emergencies assessment

The last set of questions focalizes the attention on the analysis of potential emergencies. The questionnaire provided the security managers with a list of possible threats that the shared experience at an international level recognized as the most probable risks a CI can run: namely, cyberterrorism (hacking/cracking), electronic terrorism, terrorism attacks, CBRNE (i.e. Chemical, Bacteriological/biological, Nuclear and Enhance highly explosive material) or mass-destruction weapons, employees harassments, natural hazards, others to be specified.

The security managers attributed a score (scale 1 to 5) for each threat and the general result is a medium-low level of risk in relation to the mentioned list of potential dangerous events: i.e. score between 3/1.

The case of Big Events and related potential increasing risk level is characterized for a inhomogeneous numerical value attribution, as it depends on the logistic where the big event has been organized within the urban context, therefore the proximity with the CI: the railway companies are logistically more distant to the topic areas where big events usually are organized, therefore they have a minimum risk in being involved in emergencies, because of a big event takes place (score: 1), while the public transportation system is highly involved in big events, therefore there is an increasing level of risk occurring under this circumstance (score: 5).

The last two questions refers to the communication issue, focalizing the attention on the capability and effectiveness in developing communication strategies by the CIs with mass-media, institutions, etc. in case an emergency occurs.

The first focus refers to the capability in terms of technological and human resources to manage the communication issue with external entities (i.e. mass-media, institutions, etc.), taking into consideration the three main phases of an emergency: namely, 1°-the emergency; 2°-emergency management; 3°-recovering to the *status quo ante*.

The result has been diversified, some CI did not provided with their data because of security reasons, others underlined a medium-high level of resources (both technological and human) in managing the communication strategy with external entities (score: 4/5).

The last question refers to the effectiveness in an inter-offices/departments coordination terms to communicate with external entities (i.e. mass-media, institutions, etc.), always considering the abovementioned 3 phases of an emergency.

The result is similar to the previous one, as some did not provide with a numerical value for security reasons, others defined a medium-high level of capability in coordinating the several internal departments to achieve a more effective communication capability with external entities (mass-media *in primis*).

In conclusion, it is possible to underline the importance to gather both quantitative and qualitative data aimed to draw a clear picture of the safety/security perception in all its several aspects, in light of a more and more complex urban context, to develop and improve more effective strategies for the risk assessment and the management of an emergency when occurs.

Furthermore the quantitative gathered data are intended to be uploaded to the risk-assessment software, through a geo-localization approach on the Milan city map, visible through a “pop-up” system able to show for each CI the main features in its risk assessment system and strategy, till the point of providing with further details at the level of the single site within the single CI organization, as a sort of identikit/profiling that characterize each (more or less sensitive) site of each CI.

GLOSSARY

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.

SOCIAL UNEASINESS: see “vulnerabilities” and “weak signal or early warning”

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.

WEAK SIGNAL or EARLY WARNING: it is a phenomenon present in a certain setting, that apparently has not a negative consequences but in concrete it generates social uneasiness, also at the simple level of “social perception” (i.e. there is not a real and concrete risk, but there is a diffused sense of vulnerability within a certain community).

Appendix I

“Evil Done Questionnaire 1” provided to the Milan Critical Infrastructures: qualitative and quantitative data
“Hard targets”
1° part

It is possible to make a risk assessment on the base of the following set of questions, according on the existing situation and available resources. The following list of question is not exhaustive, as it is an “open list”, which can be modify according to the context of application, on the base of these basic questions:

- **Who**: which CI is involved in the risk assessment procedure
- **How**: which instruments (technical devices/human resources) are involved in the risk assessment analysis
- **Why**: the reason/motivation according to which the *ex ante* risk assessment is done
- **When**: it has already mentioned that the list of questions is provided before an emergency event occurs, as it is an *ex ante* assessment procedure

1-Critical Infrastructure (CI) security level assessment:

=Logistic aspect: scale 1 to 5 (1=minimum proximity – 5= maximum proximity)
a) is the CI logistically locate in a position of proximity to the city centre? (Milan: District 1)
b) is the CI logistically located in a risky position, according to the iconic/symbolic sites/places of the city? (cultural, historical, religious, institutional sites/places)
c) is the CI logistically located in a risky position, because of its proximity to other CIs?
-If yes, please specify which CI/s
d) is the CI logistically located in a risky position, because of its proximity to other fundamental services for the city?
-If yes, please specify which services (Courts, Police Headquarter, General Consulates, etc.)

=Strategic aspect:
a) is the CI already protected with technological control systems?
-If yes, please specify which ones (ex. CCTV, anti-intrusion systems, alarm systems, etc.)

b) is the CI protected through the support with private security agents? (daily and nightly)
c) does the CI adopt systems of access control?
-If yes, please specify which kind of systems (human resources/technological devices)
d) do the internal stuff and employees attend training course specifically oriented to manage emergency situations? If yes, how frequently they attend them? Do they attend also update courses?

=Risk/vulnerability aspect:
a) is the CI logistically located in an particularly social vulnerable urban context?
-proximity to the social housing buildings?
-abandoned areas?
-depredated, isolated or lack of lighting areas/insufficient lighting areas?
-high impact of immigration areas?
-other…
b) is the CI open to the public?
c) does the CI provide a pubic service that involves a high flow of people or public daily?

2-Existing protocols assessment:

a) do you already have operative protocols on emergency situations management that define an inter-forces cooperation? (ex. Police, Fire brigades, Ambulances/Hospitals, etc.)
b) do you already have operative protocols specifically oriented towards the management of terrorist violent attacks?
-If yes, is there any difference with the other operative protocols in case of different emergency (technical break down, natural hazards, etc.)?
-If no, have you ever thought or evaluate the possibility to develop specific operative protocols in case of terrorist attacks

3-Potential emergencies assessment:

a) do you keep records on the emergencies occur during the last 10 years?
b) do you have statistical data on the emergency cases frequency, according to the typology of managed events? (technological devices break down, sabotage, natural hazards, etc.

c) do you have any directive during the emergency how to communicate with external parties, such as mass media, institutions, etc. during the several stages of the event? (emergency-management of the event-restoration to the status quo ante of the situation)
d) do you have evaluations in terms of timing in managing an emergency situation, from the moment the emergency occurs to the restoration of the *status quo ante* condition?

4-Assessment of the impact and vulnerability on the CI in case of emergency: scale 1 to 5 (1=minimum probability – 5=maximum probability)

a) what is the probability that a terrorist attack could target your infrastructure?
b) which is the probability that people could be involved in?
-employees and staff
-public and/or customers of the service
c) what is the probability that damages to the infrastructure properties occur?
-properties or goods belonging to the company
-properties or goods belonging to third parties (subject/s external to the company)
d) what is the probability that an emergency could attract the mass media attention?
e) which are the economical consequences whether an emergency occurs?
-direct costs
-indirect costs and costs related to the company image

5-Proposals for the implementation of the existent system

a) how is it possible to implement (whether it is necessary to implement) the already existent Protocols in case of terrorism attacks occur?
b) how i sit possible to implement (whether it is necessary to implement) the already existent Protocols in case of emergencies in general occur?
c) do you think it would be worth to implement Operative Protocols specifically focalized on emergencies referred to terrorism attacks or subversive activity for your Critical Infrastructure?
d) do you think it would be worth to implement Operative Protocols focalized on emergencies referred to terrorism attacks or subversive activity, which share the management of the situation with other Critical Infrastructures?

e) do you think it would be more effective to develop Operative Protocols for emergency situations, characterized for being more generic and flexible to be calibrated case by case on the base of the emergency nature? Or do you think it would be more effective to develop *ad hoc* Operative Protocols, calibrated on each specific emergency a priori predetermined?

f) Strong and weak aspects of the already existent procedure of emergency management utilized by your Critical Infrastructure

g) Comments, critics, and/or suggestions on the base of the already existent system utilized by your Critical Infrastructure

Appendix II

"Evil Done Questionnaire 2" provided to the Milan Critical Infrastructures: quantitative data "Hard targets" 2° part

1-Security level assessment of the Critical Infrastructure:

a) Think about the protection level of the CI you work for. How do you assess the protection level on the base of the existent technological and surveillance devices (e.g. cctv)?

scale 1 to 5 (1= minimum protection 5= maximum protection)

b) How do you assess the access monitoring system on the base of the existent human resources and technological devices?

scale 1 to 5 (1= minimum monitoring activity 5= maximum monitoring activity)

c) According to your experience, may the context where the infrastructures is located be considered as a particularly vulnerable one? i.e. is the CI located in a proximity space where there are critical or abandoned areas or it is located in an urban context characterized for a general problem of uneasiness and insecurity?

(e.g. *1= minimum risk 5= maximum risk*)

2-Assessemnt of the existent protocols:

a) How do you assess the efficiency level of the existent operative protocols for the management of emergencies which implies an inter-forces cooperation (e.g. national police, fire brigades, ambulances/hospitals, etc.)

su scala da 1 a 5 (1=minimo – 5=massimo)

3-Potential emergencies assessment:

a) We ask you to assess each of the following emergencies, through the assignment of a numerical value on the base of the probability level that each emergency occurs:

- □ Cyberterrorism (sabotages)
- □ Electronic terrorism (sabotages)
- □ Terrorism (attacks)
- □ CBRN terrorism (non-conventional weapons: bio/bacteriological, chemical, radiological/nuclear attacks)
- □ Harassment to internal employees
- □ Natural hazards
- □ Other: please, specify …

scale 1 to 5 (1=minimum – 5=maximum) for each abovementioned emergency

b) How do you assess the general risk level related to the CI, on the base of part experienced where the infrastructure was involved in Big Events?

scale 1 to 5 (1=minimum – 5=maximum)

c) How do you assess the capability level in terms of human resources and devices adopted to manage the communication system with external entities, i.e mass media, institutions, etc. within the several phases of an emergency?

scale 1 to 5 (1=few – 5=optimum)

-1° emergency:
-2° emergency management:

-3° recovering to the *status quo ante*:

d) How do you assess the efficiency level in terms of coordination capability among the infrastructure internal offices/departments for the management of the communications with external entities, i.e. mass media, institutions, etc. within the several phases of an emergency?

scale 1 to 5 (1=few – 5=optimus)

-1° emergency:
-2° emergency management:
-3° recovering to the *status quo ante*: