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 experience of Milan Critical Infrastructures

by Alessia Ceresa[*] and Chiara Fonio[*]
(Scientific Team)

This paper focalizes the attention on the topic terrorism target, i.e. the "Critical Infrastructures", as the EU devoted a special attention to this issue, through ad hoc *EU Directives, in light of previous experiences that demonstrated how the risk (both safety and security) level increases from the interaction of two urban components: i.e. Big City and Critical Infrastructures.*
In light of this premise, the aim of this paper is to present the already existent "risk assessment model" within the Milan urban context (taken as basic example for a shared approach at a European level) and its related Critical Infrastructures. In fact the knowledge of the status quo, *facilitates the further implementation of a risk assessment system flexible enough to be shared also with other EU Countries and its specific Critical Infrastructures.*

21 September 2012

INTROCUDCTION

The Critical Infrastructures protection is a crucial issue both at a European and national level, in light of the interaction of the most recent events that occurred in several EU Counties after the 9/11 terrorist attack in the U.S.A., i.e. the bombing in Madrid (2004), involving the train system and the one in London (2005), involving the underground and the bus systems[1], as both regarding topic transportation critical infrastructures.

[*] Smart Ciber Project, Scientific Expert, PhD in Criminology
[*] Smart Ciber Project, Scientific Expert, PhD in Sociology
[1] Fonio C., "Londra 2005: la lezione e le pratiche apprese", a cura di Lombardi M., Le nuove sfide metropolitane, Ed. FrancoAngli, Milano, 2007, pp. 101-111

In detail, after the terrorist attacks experience in Madrid and London, the European Countries felt being as touchable as the U.S.A., and the EU institutions reacted against the violent capability of the s.c. international terrorism. In light of this emergency situation, the Justice and Home Affairs Council called on the Commission to make a proposal for a *European Programme for Critical Infrastructure Protection* (EPCIP)[2], focalizing its attention on the protection of the Critical Infrastructures (CIs) against the terrorism threat within the internal EU borders, not excluding at the same time, other forms of threats, included criminal activities, natural hazards and other causes of accidents, through an all-hazards approach[3]. This proposal has been integrated with a complex Action Plan, i.e. "*Prevention, Preparedness and Consequent Management of Terrorism and other Security related risks*", characterized for a program to develop between the years 2007 and 2013[4].

Therefore, to achieve the abovementioned aim, the very first crucial aspect to implement among the EU Countries was the definition of Critical Infrastructure itself, as it could be considered the starting point to develop an homogeneous prevention/repression program against any form of disruption or destruction perpetrated against any CI, wherever logistically located.
The EU Communication COM(2004) 702 on the Critical Infrastructure Protection plan, in fact, developed a definition of "Critical Infrastructures"[5], according to the EU experience, as follow:
"*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*" (paragraph 3.1).

The mentioned definition has been integrated with a list of CIs, which owner could be both public and private sector, generally recognized at a EU level:

[2] Commission of the European Communities, Communication form the Commission to the Council and the European Parliament COM(2004) 702 final, *Critical Infrastructures Protection in the fight against terrorism*, Brussels, 20.10.2004, in OJ C. 52, 02.03.2005
[3] http://europa.eu/legislation_summaries/justice__freedom_security/fight_against_terrorism/133260_en.htm#
[4] European Council, Decision 2007/124/EC of 12 February 2007 establishing for the period 2007 to 2013, as part of the General Programme on Security and Safeguarding Liberties, the Specific Programme '*Prevention, Preparedness and Consequent Management of Terrorism and other Security related risks*', in OJ L. 58/1-6, 24.02.2007
[5] Commission of the European Communities, Communication from the Commission to the Council and the European Parliament COM(2004) 702 final, *Critical Infrastructures Protection in the fight against terrorism*, Brussels, 20.10.2004, in OJ C. 52, 02.03.2005

- *Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system)*
- *Communications and Information Technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet)*
- *Finance (e.g. banking, securities and investment)*
- *Health Care (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services)*
- *Food (e.g. safety, production means, wholesale distribution and food industry)*
- *Water (e.g. dams, storage, treatment and network)*
- *Transport (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems)*
- *Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)*
- *Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments)*

Afterwards, the EU Commission Communication on the Critical Infrastructures protection plan has been extended to the specific protection against cyber-attacks, as a further specification of the possible violent strategies perpetrated by any form of terrorism (real or virtual), i.e. terrorist organizations and/or hacking/cracking phenomena, as a brand new growing threat: i.e. the s.c. cyber and electronic terrorism[6].
The outcome has been a topic EU Communication, i.e. the EU Commission COM(2009) 149 on Critical Information Infrastructure Protection (CIIP)[7], specifically addressed towards the Information and Communication Technologies (ICT's) systems, services, networks and infrastructures. The EU Commission in fact, declares that the ICT devices are becoming more and more vital components of our everyday life, both

[6] Ceresa A., "New Technology. Terrorism and an international prevention/repression strategy", Nova Science Publishers, Inc., New York, 2009, pp. 157-170; Berkowitz B.D., "Information Warfare", in Rattray G.J. *Strategic Warfare in Cyberspace*, Boston: MIT Press, pp. 517ss.; Berkowitz B.D., "Warfare in the information age", in *Science and Technology*, Fall 1995, Vol. 12, n. 1, pp. 59-66; Szafranski R., "A theory of information warfare: preparing for the 2020", in *Airpower Journal*, Spring 1995, pp. 56-65, www.cdsar.af.mil/apj/szfran.html

[7] Commission of the European Communities, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2009) 149 final, *on Critical Information Infrastructures Protection – "Protecting Europe from a large-scale cyber-attack sand disruptions: enhancing preparedness, security and resilience"*, Brussels, 30.03.2009

as private citizens and private/public institutions, therefore, any disruption and/or destruction of these systems would provoke "[…] *a serious impact on vital societal functions […]*".

In light of these due premises, the Smart Ciber study aims to involve the major Critical Infrastructures of the city of Milan in the development of a system of integrated maps for risk assessment against terrorism threats within the urban context, with a special focus on both Critical Infrastructures and Big Events, intended as two particular components which could be intertwined, given a certain space and time.

The collaboration of the Milan major CIs has been double: they provided the scientific team with their topic lists of indicators, utilized by each CI and calibrated on each specificity (i.e. the particular service provided by each infrastructure); the scientific team conducted several interviews with experts of each CI company, i.e. the security managers employed in the several companies responsible for the crisis rooms of each infrastructure.
Besides, from a methodological perspective, the output is a qualitative result of an in-depth analysis of the risk assessment indicators lists matched with the theoretical framework and its related specific indicators lists (see *Concept Paper n. 1*), intertwined with the outcome of the several interviews to privileged witnesses, i.e. CIs experts (see *Appendix*).

In detail, it is important to analyze each CI separately, profiling the topic risk assessment indicators lists integrated with the feedback of the several interviews, as an added value to the collected qualitative data.

1. RFI: RETE FERROVIARIA ITALIANA

The RFI is the company which manages at a national level the train railway, thereof, it is evident this is a crucial infrastructure because from its organization depends the whole train transportation system and the development of the train network that links the several Italian regions inside and outside the national borders. It is implicit how the security from both prevention and repression perspectives, is crucial to guarantee the transportation service in the city of Milan. This topic situation is similar to other big cities in Italy (Rome, Turin, Naples, etc.), although the geographic and logistic specificities require a special attention to calibrate a security policy in each local context.

Although the RFI never experienced specific terrorism threats, this company has to manage several safety problems of different nature, with an eye open to the security aspects within topic situation (e.g. the visit in

Milan of public authorities, such as the Pope or Government representatives or any kind of Big Event that often occurs in a big city like Milan).

The wide *spectrum* of emergency events that may occur in the course of the everyday operational activity, from the technical/technological devices breakdown/damages to the several criminal behaviors targeting the RFI systems, requires the development of operative protocols to manage these situations through an inter-forces cooperation activity: the PolFer-Polizia Ferroviaria (train special police), VVFF-fire brigades, PS-Polizia di Stato (national police), PL-local police, ambulances and hospitals, civil protection, etc. are in constant contact to exchange information in topic events. Therefore, besides a general emergency operative protocol, the RFI developed *ad hoc* protocols for emergencies that may occur in specific logistic contexts, qualified as particularly sensitive according to the best practice and experience, i.e. the galleries, sensitive sites or crucial railway crossroads from a logistic perspective.

The crisis room covering Milan and the surrounding area, is based on an operational electronic system able to geolocate the different problems that may occur on the base of a list of several indicators that the best practice identified as the major vulnerabilities related to the RFI activity. This system is able to foresee possible solutions in the risk assessment procedure through an algorithmic program, although the human factor, through a case by case analysis on the base of the experience component, is crucial to evaluate the level of danger and how to react to the contingent situation.

In particular, the most frequent vulnerabilities that RFI company needs to face and manage are listed as follow:
-special material stealing, i.e. copper, utilized for the train electric railway, as it is an expensive material that can be easily sold at the black-market
-unauthorized occupations (e.g. workers' strikes)
-nomad/roman camps, as they usually settle down closely to the railway in dangerous logistic position. Besides their presence often is related to the copper stealing, as it is one of their main criminal activity
-big flows of people, especially customers during certain period of time (e.g. summertime/national holidays or during big events)
-the use of trains by football clubs fans (ultra and hooligans) and/or people during particular demonstrations
-lost/found objects

The interaction of the mentioned vulnerabilities is evident, where the logistic component is matched with a topic critical situation: e.g. the railway that is closed to *Aler* buildings (social housing), characterized for being highly sensitive sites, as they are catalyst factors of social uneasiness (i.e. drug and alcohol abuse, gangs of youths, prostitution, abandoned areas, etc.). The weak signals of vulnerability, characterized for a lack of control and a progressive development of micro-criminality, could become factors of radicalization, as the sociological studies in this field has demonstrated[8] (see *Concept Paper n. 1*).

2. FN: FERROVIE NORD

The FN company covers the train system from a regional (Lombardy Region) and local perspectives.
FerrovieNord manages the transit of 100 trains for each of the 8 railway lines (an average transit of 800 trains in 24 hours), covering 420 Km (i.e. FerrovieNord Milano – 320 km. plus FerrovieNord Ramo d'Iseo 100 km). Although it is not a big transportation company, the management of its trains and railway lines is crucial because the majority of its logistic activity develops in the surrounding metropolitan area of Milan, where there is the interaction and overlap of several crucial infrastructures, i.e. the train system covers the Linate airport area, closed to the underground system (managed by ATM company) or the railway lines intertwined with the RFI ones.

The Security Department has been created 5 years ago and it is structured within the context of the "quality and environment" sector. In the original hierarchy this department was the leader of the FN company, afterwards this company has been fragmented in several smaller companies under the name of FerrovieNord, i.e.:
1-FN Rete
2-FN Treni, subdivided as follow:
-Trenord (passenger trains)
-Trenitalia (Freccia Rossa, created 2 years ago)
-Nord Cargo (goods trains)

[8] Silber, M. D. & A. Bhatt. (2007) 'Radicalisation in the West: The Homegrown Threat', New York City Police Department; Radicalization, Recruitment and the EU. Counteradicalization Strategy http://www.transnationalterrorism.eu/tekst/publications/WP4%20Del%207.pdf

In particular, the crisis room of this infrastructure is characterized for an electronic operational system, able to reveal in real-time problems connected with the function of the train system, i.e. trains delay or cancellation, technical breakdown and so forth.

A similar situation to the RFI one has to be manage by FN, as this train company shares with the RFI some railway crossroad lines, besides they share the experience of managing a sensitive service, such as the transportation system and the related safety and security issues, in abandoned areas or places characterized for a diffused problem of social vulnerabilities (i.e. social disease).

In particular, the major vulnerabilities managed by FN, shared also with RFI, are the following:
-presence of nomad/roman camps (average 20 people per camp) settled down closed to the railway lines. This phenomenon is highly dangerous both for safety reasons (e.g. arsons of garbage, unauthorized dumps which block the regular trains transit on the railway, etc.) and security ones (e.g. damages of different nature –electric system-, stealing of copper, stealing of personal belongings, begging, prostitution, etc.). A prevention plan has been created through the building of walls 7 mt. high, gates and enclosures along the railway line, although it is impossible to cover all the 8 lines managed by FN. Besides, it has been discovered that in some areas the nomad groups succeeded in braking the walls an access close to the railway to settled down their unauthorized camps. Therefore, a definitive solution to prevent/repress this phenomenon has to be found
-graffiti both inside the stations buildings and inside/outside the trains, to control this phenomenon the FN has adopted two solutions, first of all this company immediately removes the graffiti to discourage the reiteration of this criminal behavior and a constant private security agents patrol (daily and nightly) in specific areas that are more vulnerable according to the experience through the time
-aggressions against the employees
-stealing of particular materials (i.e. technical keys and pass-partout, technical material)

A synergic plan to reduce and prevent vulnerabilities has been developing in cooperation with RFI-Rete Ferroviara Italian, PL-local police, PolFer-train special police, the Municipality of Milan, private security institutes aimed to improve the control capability at list of the most sensitive areas.

FN adopts *ad hoc* operative protocols according to the logistic location and nature of the event, acting in cooperation with PolFer, PL, PS (national police), ambulances and hospitals, VVFF-fire brigades, the Municipalities of two small cities in Varese province (Busto Arsizio and Gallarate), civil protection, SEA, RFI:

-galleries
-Linate/Malpensa airports proximity
-natural hazards
-Cadorna station, being a topic area characterized for a big flow of passengers in Milan city centre
-terrorism attack or cyberterrorism (included electronic sabotages)
-earthquake

The safety and security systems are jointly monitored through a list of indictors divided within 5 levels, according to the focus of the safety/security issues (i.e. technical/technological devices and related disruptions, trains operational capability and efficiency, safety, security, environment), this system is quite recent, as it has been adopted in 2011 for qualitative and quantitative data gathering on the FN company overall management. The collected data are analyzed by a centralized system to optimize the information and improve the reaction and resilience capability in case of emergency of any nature in any time. This database is completed with *ad hoc* written reports for each event, characterized for a detailed description of the situation and the feedback of the facts: both the database information and the written reports contribute to implement a statistical system that represents from a chronological perspective, the "history" of the FN most important events.

3. ATM: AZIENDA TRASPORTI MILANESI

ATM company is a holding of 20 different sub-companies that supplies a wide variety of services, i.e. underground transportation, public transportation (tram and bus), municipal car parking, car-sharing service, bike-sharing service, bar and coffee services (e.g. inside the underground stations).
In particular, only the public transportation sector covers a wide flow of people per day, therefore, it is evident how the safety and security issues are vital for the effective function of this company, that is the reason why there is a closed cooperation with PS (national police) and PolMetro (special underground police), since they are in contact H24 with.

In light of the mentioned organizational premises, ATM created an *ad hoc* internal s.c. Security Committee, competent for the risk assessment analysis, which developed a network of connections with PS, PolMetro, CC-carabinieri, ambulances and hospitals, GdF-Guardia di Finanza (fiscal police), reorganizing the urban context of Milan, through a distinction into 4 main areas the whole geography of the city of Milan. In each area there is a fix presence of PS (3 locations) and CC (1 location), such a closed and constant control of the

flow of people is justified in light of the fact that the basic difference between the company that manages the airports in the surrounding area of Milan, and the public transportation system is the fact that people utilizing the transportation system have a direct and immediate access to the vehicles (underground trains, trams or buses), without passing through direct control accesses, like in the airports, i.e. ATM needs to face a higher level of (safety and security) risks compared to other CIs because of the nature of the services they supply, although many CIs share the same feature, i.e. the management of a big flow of people per day.

Because of the dynamic nature of the urban transportation system, ATM developed a unique "open" operative protocol for emergencies, flexible enough to be integrated case by case on the base of the nature of safety/security situation involved in, according to the topic event. The analysis of any emergency event is run through a three-phase risk assessment. In other wards they adopt an action-reaction strategy:
1) before the event (risk assessment)
2) in the course of an event (response to the emergency)
3) after the event (restoration of the *status quo ante* situation and feedback analysis through a s.c. "incident reporting", collected in a database for statistical reasons)

There are several crisis rooms according to the transportation typology (underground system or tram/bus, etc.), while the technological alarm (e.g. technological or electrical sabotages) is managed in synergy with the several crisis rooms involved in.

The ATM risk management approach is much more oriented towards the simulation/study of potential risk scenarios (i.e. "case studies"), rather than the development of indicators lists, able to test the efficiency level of the system functions, because of the already mentioned peculiar nature of the public transportation system, which implicitly requires to be flexible to manage any event/problem in a short time, in light of the high number of people (not only customers) who might be involved in a dangerous situation. The analysis of risk scenarios, determined on the previous cases experience at an international level, provided with a wide *spectrum* of scenarios, which have been operationalised through statistical data, according to the everyday ATM concrete experience.

The major vulnerabilities identified by ATM are as follow:
-vandalism behaviors of different nature
-damages of different nature against the ATM properties
-graffiti

-"penetration test" run by micro-criminality to test the ATM capability to recover the system (e.g. sabotages of CCTV)
-cyberterrorism
-lost/found objects

4. SEA: SOCIETA' DI GESTIONE AEROPORTUALE

SEA manages the two major airports in the north of Italy, i.e. Milano Linate and Milano Malpensa. Linate, which is the smaller airport, manages 300 of flights per day, although, compared to Malpensa, it has a sector dedicated to the commercial flights (cargo airlines) and not only to the passengers, as it is for Malpensa. It is important to underline the fact that, although the name of the two airports is related always to the city of Milan, in reality the Malpensa airport is logistically located 40 km outside Milan, as it is in an other province (Varese province). The result is a complex management of a wide territory, where the logistic factor is crucial also from a safety and security viewpoint.

The risk assessment system of this company is based on the National Security Handbook (2012), as SEA security and safety department is not used to adopt software able to collect data through an indicators list of possible vulnerabilities; for this reason statistical data gathering and analysis are not available, although they adopt a "case reporting" system, through the drafting of reports on specific events. The risk assessment, in fact, is based on a "lesson learned policy", where each case already managed is analyzed and the operative protocol can be modified according to the topic experiences.

In detail, there is a permanent presence of PS national police agents in certain areas of the airport, as in case of highly dangerous situations they are the leaders of the task force in charge of managing the emergency. Operative protocols in fact, have been developed as "open" sources, as they can be modified according to the experience: the human resource is a key factor according to SEA security/safety policy to make a risk assessment in a concrete or potential emergency situation and learn from the "case study" analysis of previous events. Therefore, the protocols are based on a cooperation activity of emergencies management, as in the topic event many stakeholders are involved in, i.e. SEA security (responsible for the crisis room management), PS (national police), Polizia Penitenziaria (prison special police), VVFF-fire brigades, CC (carabinieri), GdF (fiscal police) and private security agents.

The major vulnerabilities, which have been experienced by SEA, are the following:

-attempted stealing or robberies
-stealing of personal belongings (e.g. luggage)
-big flow of people
-counterflows (e.g. wrong exits or emergency exits)
-lost/found objects

SEA needs to face also contingent situation, such as "sensitive flights", i.e. the flights where the passenger is a public person (e.g. a Government representative or a religious one). In this case, there are *ad hoc* operative protocols able to manage the situation, i.e. to guarantee the security of the passenger and at the same time to reduce the discomfort of the "ordinary" passengers due to the higher level of security measures: in few wards to guarantee even in this peculiar situations the efficiency of the system.

5. AMSA: AZIENDA MILANESE SERVIZI AMBIENTALI

AMSA is part of the a2a holding (the company that manages the electricity and gas system in Milan and surrounding areas). This company is specifically oriented to the management of the garbage dumps and ecological/environmental related services.

AMSA manages 4 urban areas of Milan and 16 garbage dumps within the city and the security department has been recently developed and improved.

The security/safety management of this company is based on a software, the s.c. "security matrix", composed of an indicators list divided in several sectors, according to the phenomena it is important to observe. Because of the nature of this system, statistical data are available, as well as "case reporting" of previous events and emergencies of different nature, so that there is an historical perspective of the events that AMSA has managed through the time: some events are definitely closed, other are still open cases or brand new dangerous phenomena could be recorded by the system.

AMSA supplies also transversal services, i.e. it operates in cooperation with other CIs for instance during big events: e.g. in the course of the visit of some public representative, the AMSA employees are in charge to monitor the manhole covers or the public rubbish bins, or AMSA supplies barriers to control the crowd, etc. In detail, AMSA cooperates with PS (national police), the PL (local police), the private security agents. Besides, it operates in synergy with the prefecture and the police headquarter in the course of big events,

as under these circumstances, the security factor plays a key role in the AMSA main organizational and operational tasks.

The major vulnerabilities faced by AMSA are the following:
-thermodestruction of confiscated materials
-vandalism
-arsons
-stealing of particular materials (e.g. copper, iron, paper, batteries, etc.)
-information protection
-illegal dump trafficking (e.g. poison material or toxic products)
-presence of semi-convicted people (internal employees, as they are working on the base of a resocializing program planned by a magistrate)
-employees aggression (daily and nightly)

A special role has this company in case of natural hazards: i.e. snowfalls, water overflowing, garbage emergencies or in case of moving buildings because when the police intervenes in unauthorized occupations of houses or buildings in general, AMSA afterwards is in charge to clean up the place, etc.

6. a2a: ELECTRIC & GAS COMPANY

The company that manages the energy (electricity and gas) supply in the city of Milan is characterized for a highly capability in monitoring the urban territory, as it manages a wide networks of devices from the electric power distribution to the gas lines, which cover the whole metropolitan area and surrounding areas. In fact, this company manages the electricity and the gas line from the city center to the suburban areas of Milan.

The safety and security issues are managed through the support of technological devices (cctv, alarms, etc.) and private security agents. Besides, the a2a is constantly in contact with CC-carabinieri and Civil Protection in case any kind of emergency occurs (i.e. from natural hazards to sabotages and so forth).
There are already existent operative protocols that define the inter-forces coordination, according to the emergency nature, although there is a project to implement *ad hoc* protocols in case of specific kind of emergencies occur.

The two different services (electricity and gas) are autonomously managed, according to the specific law within each sector, as well as the emergencies are managed in a different way, in light of the specific exigencies that each service requires. In fact, the aim is to restore the service in the shorter time, as the electrical and gas systems are vital for the functioning of both the citizens everyday life, as well as for the other CIs activities.
In case of big events, where the eclectic and gas systems are involved in the security aspect, the police headquarter gives *ad hoc* directives to the a2a company to guarantee a higher standard of security in topic areas directly or indirectly involved in the specific big event.

In general, the gather of data on the events and emergencies have been managed by a2a through the time, as they are collected by the operative center, to centralize the information about any safety and security issue. In is important to underline that a2a noted an increase in social uneasiness through the last years, that requires a further effort in adapting their response capability to several and different situations, as this infrastructure covers the whole Milan territory till the suburban areas of the city.

The major vulnerabilities that a2a has experienced are listed as follow:
-stealing of particular material (e.g. copper, brass, etc.)
-nomad/roman camps closed to the electrical power stations
-vandalism
-graffiti
-damages of different nature
-suspect activities and/or permanence of people (e.g. unauthorized access, suspicious photos taken to particular electric power station or gas station, etc.)

7. MM: METROPOLITANA MILANESE

MM manages the water system in the city of Milan and surrounding areas. This company is responsible for the storage, the treatment and the network of the water system, as there are 32 water storage centrals in Milan, which distribute the drinking water along 2.400 km of water line system.

The safety and security issues are crucial aspects in the management of this infrastructure, fundamental for the city. Therefore, the waterworks is monitored H.24, as the major danger is the possibility of a water pollution with poison or toxic (chemical, bacteriological) products.

In fact, the security of the waterworks is closely linked to the management and supply of the service to the city of Milan, for this reason there is a close cooperation with the public security forces (i.e. PS national police, CC carabinieri, PL local police, etc.), calibrated case by case on the base of the danger level.
In case of big event management, the MM receives the operative protocol and related procedures directly from the police headquarter, according to an *a priori* risk assessment.

In detail, the major vulnerabilities that MM has experienced are the following:
-damages
-stealing of material of different nature
-unauthorized access
-communication problems (lack of communication and info sharing between the central site and the surrounding ones)

The *excursus* of the safety and security profiling of the several CIs located in Milan can lead to some considerations. Firstly, a transversal analysis of the several sets of vulnerabilities they experienced through the time, reveals that there is a certain homogeneity, as it is evident the repetition of certain criminal phenomena within the Milan urban context, i.e. microcriminality or phenomena that could be considered "border line" between criminal behaviors and social uneasiness, or even peculiar criminal behaviors connected with special events (e.g. big events) intertwined with the logistic position of the CIs perceived as potential targets to illegal/criminal activities.

Focalizing the attention on the terrorism issue, although the deep differences among the several CIs, due to the different nature of the services supplied by each company, the security managers of the crisis rooms located in each infrastructure, agreed on the basic problem in developing prevention/repression plans against the terrorism phenomenon. In fact, they adduced there is an objective difficulty in developing and improving *ad hoc* operational protocols against terrorist attacks, because of the implicit nature of the terrorism phenomenon. The doctrine and legislative framework at both National and European level demonstrated how difficult is the improvement of a unique and clear definition of "Terrorism"[9], as it is an

[9] Definition of Terrorism according to the Italian legal sources: art. 270 c.p. (criminal code) defines the national terrorism/subversion, art. 270-*sexies* p.c. (criminal code) defines the international terrorism. Definition of Terrorism according to the EU legal sources: EU Council Framework Decision of 13.06.2002 *on combating terrorism*, 2002/475/JHA, in O.J. L. 164/3-7, 22.06.2002

extremely flexible and dynamic phenomenon, characterized for a wide *spectrum* of different scenarios of possible attacks by any kind of terrorism (national or international terrorism and subversion, cyberterrorism and electronic terrorism), given the variables of time/space, i.e. the main two factors to analyze for the development of an effective prevention/repression strategy against this peculiar criminal behavior.
Therefore, as the security managers of the CIs underlined, it is necessary to adopt a pragmatic approach, implementing operative protocols flexible enough to be calibrated case by case on the topic situation and emergency that they are required to manage.

Besides, there is a diffused need to improve the information sharing system among the several CIs to optimize the resources and to better understand the problems that surround sensitive sites connected with each infrastructure. In fact, the knowledge of the (potential/real) problems inside and outside the perimeter of each CI can deeply influence the ordinary activity, as well as the safety/security level of each infrastructure. Thereof, this study should be intended as the first step in facilitating the development in future of closer collaborations among the Milan CIs.

Finally, it has to be specified that the EU partners of the project, i.e. the Safety Region of Rotterdam (Holland), the Municipality of Budapest (Hungary) and the Municipality of Varna (Bulgaria), are developing in parallel the same partnership with their own CIs, to be in line with the information sharing aim and also to match the test phase through the final software, intended as the output of the risk map development for the EU big cities governance (i.e. the acronym SMART CIBER).

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 CITY: it refers to a metropolis or a complex urban setting, characterized for a big flow of people living and/or working within a specific urban context.
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".
CYBERTERRORISM: it is a subversive activity perpetrated by individuals with a high skill and knowledge in technology, who are able to find first and then to exploit the weak-points of IT programs (*software*), through the use of technological devices (*hardware*). Thereof, the technological instrument is both the mean and the end.
The doctrine identifies a wide typology of this "virtual" terrorism: i.e. hacking, cracking, phreaking, phishing, etc.. Although the main theory considers "cracking" the real form of "cyberterrorism" from a criminological perspective, as this illegal activity aims not only to violate a software, but even to steal, manipulate the information and data content in a technological device.
ELECTRONIC TERRORISM: the doctrine often confuses "cyberterrorism" with the "electronic terrorism", but through the recent years the main theory distinguishes the two forms of terrorism, since the "electronic terrorism" aims to target the "electronic devices" and not the IT ones. Some other theories consider this phenomenon much more a form of "sabotage", rather than a form of "terrorism. It means that the sabotage is a violent strategy from an operative perspective, rather than a criminal phenomenon itself.
OPERATIVE PROTOCOL: it is a standard procedure for managing certain emergency or risky situations that may occur within certain technical contexts.
RADICALIZATION THEORY: it is a theory according to which an individual can develop an inner process "through which an individual changes from passiveness or activism to become more revolutionary, militant or extremist, especially where there is intent towards, or support for, violence".
It is important to underline that "radicalization" is not "terrorism", as the inner psychological process of radicalization not always leads to terrorism, while terrorism is always the result of a radicalization process.
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.

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

INDICATORS of THE CITY OF MILAN "CRITICAL INFRASTRUCTURES" (CI)

The following list is the result of the integration of several indicators lists utilized by the major Critical Infrastructures in Milan (i.e., RFI: national train railway company, a2a: electricity and gas systems company, SEA: airport company, ATM: public transportation system company, AMSA: garbage dumps and ecological matter company, FN: regional/local train system company, MM: water system company)*:

Stealing
Stealing of copper, iron etc.
Stealing of personal belongings (i.e. badge)
Nomad camps
Unauthorized occupation
Vandalism
Graffiti
Arson
Attempted stealing or robberies
Robberies
Damages
Lost objects
Found objects
Employees aggressions (daily & nightly)

	Big flows of people
	Counterflows (i.e. wrong exits)
	Faults (i.e. malicious or accidental -technical, sabotage-)
	Cyberterrorism

**Source*:
a2a[10] – Azienda elettrica e gas
AMSA[11] – Azienda Milanese Servizi Ambientali (Gruppo a2a)
ATM[12] – Azienda Trasporti Milanesi
FN[13] - FerrorvieNord
MM[14] – Metropolitana Milanese
RFI[15] – Rete Ferroviaria Italiana (Gruppo FS - Ferrovie dello Stato)
SEA[16] – Società di gestione aeroportuale (Milano Linate e Milano Malpensa 1 e 2)

[10] www.a2a.eu
[11] www.amsa.it
[12] www.atm-mi.it
[13] www.ferrovienord.it
[14] www.metropolitanamilanese.it
[15] www.rfi.it
[16] www1.seamilano.eu