Provincia di Milano

PROGRAMMA DI PREVISIONE E PREVENZIONE DEI RISCHI

RISCHIO ATTI TERRORISTICI

VOL 1.9

2013

Protezione Civile
Provincia di Milano

Provincia di Milano - Settore Protezione Civile e GEV

REVISIONE E AGGIORNAMENTO DEL PROGRAMMA PROVINCIALE DI PREVISIONE E PREVENZIONE DEI RISCHI E DEL PIANO PROVINCIALE D'EMERGENZA DI PROTEZIONE CIVILE

Programma provinciale di Previsione e Prevenzione

RISCHIO ATTI TERRORISTICI

approvato	Dott. Giovanni Carra
verificato	Dott. Giovanni Carra
elaborato	Dott. Giovanni Carra

0	GV	GV	GV	Febbraio 2013
rev.	sigle			data

codice elaborato 0408-01-09-01R-00

Indice

1 RISCHIO ATTI TERRORISTICI

1.1 Premessa

L'analisi del rischio derivante da atti terroristici viene attualmente affrontata, nel rispetto della normativa vigente, nell' ambito delle funzioni convenzionalmente riferite alla "Difesa Civile" ovvero della sicurezza dello Stato comprendendo tutte le situazioni emergenziali che derivano da atti definibili "di aggressione alla nazione" e pertanto anche quelle connesse agli atti terroristici.

Essa ha il compito di assicurare la continuità dell'azione di governo, proteggendo, da un lato, la capacità economica, produttiva e logistica del Paese e, dall'altro, riducendo l'impatto degli eventi di crisi sulla popolazione. L'articolo 14 del Decreto Legislativo n. 300 del 30/07/1999 (e s.m.i.) attribuisce la competenza in materia di Difesa Civile al Ministero dell'Interno, nonché alle prefetture, che la esercitano attraverso il Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile. La Commissione Interministeriale Tecnica della Difesa Civile (C.I.T.D.C.) si riunisce presso il Ministero dell'Interno che la presiede e assicura il coordinamento delle Amministrazioni centrali dello Stato.

Negli ultimi anni la dimensione internazionale della sicurezza e la moltiplicazione delle ipotesi di rischio ha indotto il Ministero dell'Interno ad elaborare strategie di prevenzione e pianificazione mirate al soccorso in scenari complessi. Il Corpo Nazionale dei Vigili del Fuoco garantisce il soccorso specializzato con appositi nuclei, in caso di pericolo nucleare, batteriologico, chimico e radioattivo le cui iniziali vanno a formare il noto acronimo NBCR.

Per tali rischi il Piano Nazionale di difesa civile ha definito le minacce, ha individuato i possibili scenari e ha stabilito le misure da adottare. Il Piano Nazionale rappresenta la direttiva generale per la stesura dei Piani discendenti e di settore, predisposti da amministrazioni pubbliche e private erogatrici di servizi essenziali, nonché dei 103 Piani Provinciali predisposti dai Prefetti. Le pianificazioni sono sottoposte, al fine di testare la funzionalità e la capacità operativa, a periodiche esercitazioni.

La C.I.T.D.C. ha, tra l'altro, il compito di valutare le situazioni emergenti e pianificare le misure da adottare in caso di crisi, valutare altresì altre ipotesi di rischio, non direttamente riferibili ad azioni dolose, che possono determinare situazioni di crisi per la continuità dell'azione di Governo nonché danni alla popolazione e, in genere, alla sicurezza del Paese. In quest'ottica la Commissione e il Dipartimento approfondiscono le tematiche legate alle infrastrutture critiche e, in stretta collaborazione con il Ministero della Salute, le modalità di gestione di una crisi prodotta dal diffondersi di gravi malattie epidemiche.

La pianificazione e l'attività di Difesa Civile vengono sviluppate nell'ambito di un sistema protetto sottratto al decentramento e per il quale le informazioni rimangono riservate. La pianificazione di protezione civile coesiste con quella di difesa civile e, quando necessario, entra in modo autonomo nel sistema di difesa civile. La sintesi dei due sistemi, quando convergono, è assicurata a livello politico.

Il Piano Provinciale di Previsione e Prevenzione e quello di emergenza in corso di aggiornamento, possono concorrere allo sviluppo delle attività di:

- assistenza generale di supporto per le forze in prima linea;
- aiuto e soccorso a vittime;
- aiuto alla messa in sicurezza di edifici danneggiati;
- spegnimento di incendi;
- supporto psicologico alle vittime;
- servizi medici di emergenza.

Nella pianificazione di emergenza, è particolarmente difficile costruire scenari per attacchi, attentati, sommosse ecc.: i protagonisti di questi eventi cercano sempre di confondere le autorità, talvolta cambiando tattica all'ultimo momento in base ad una 'lettura' dei piani predisposti, talvolta emettendo

preavvisi falsi o confusionari. In tali casi la pianificazione di emergenza diventa ridondante (almeno parzialmente), e può aumentare la confusione rendendo più complesse le operazioni di soccorso.

Malgrado questo, i piani di emergenza progettati per affrontare il problema terrorismo devono tendere a definire i presupposti sui quali saranno sviluppate forme di collaborazione tra le forze dell'ordine e i servizi di emergenza.

La pianificazione di protezione civile deve in ogni caso essere finalizzata a:

- garantire la sicurezza del personale, delle loro condizioni di lavoro, e dei loro mezzi e attrezzature;
- garantire che gli operatori di protezione civile non siano messi in una posizione in cui potrebbero essere presi in ostaggio o diventare bersagli dei terroristi (o, per errore, delle forze dell'ordine);
- predisporre un alto livello di collaborazione tra forze di polizia (o unità militari) e unità civili di soccorso;
- allestire una catena di comando che rifletta le realtà della situazione.

1.2 Tipologie di minaccia

La letteratura specialistica ed in particolare le pubblicazioni dell'agenzia federale americana FEMA (Federal Emergency Management Agency), tra cui sicuramente vale la pena di evidenziare il documento intitolato "Managing the emergency consequences of terrorist incidents: a planning guide for state and local governments" classifica le tipologie di minaccia generate dall'uso delle cosiddette "armi di distruzione di massa" definite a loro volta come qualsiasi arma che è progettata o destinata a causare la morte o gravi lesioni corporali attraverso il rilascio, la diffusione, o l'impatto di sostanze chimiche tossiche o velenose; organismi patogeni; radiazioni o radioattività, o di esplosione o incendio.

Nel caso di agenti chimici, biologici e radioattivi, la loro presenza può non essere immediatamente evidente, rendendo difficile determinare quando e dove sono stati rilasciati, chi è stato esposto, e che pericolo è presente per i primi soccorritori e tecnici medici.

Vengono nel seguito sommariamente descritte le tipologie di minaccia terroristica, in base alla modalità di diffusione degli effetti ed alla natura e aggressività delle emissioni.

1.2.1. Esplosioni

Gli ordigni esplosivi sono una delle armi più comuni dei terroristi. I dispositivi esplodenti risultano facili da reperire e da costruire artigianalmente e le informazioni per la loro costruzione sono di dominio pubblico. Gli Esplosivi sono facilmente trasportabili, utilizzando veicoli ed esseri umani come mezzo di trasporto. Possono essere fatti esplodere da postazioni remote o da attentatori suicidi.

Alcuni dispositivi possono essere provvisti di detonatori temporizzati o innescati a distanza e possono essere progettati per essere attivati dalla luce, pressione, movimento, o la trasmissione radio.

Bombe convenzionali sono stati utilizzati per danneggiare e distruggere edifici finanziari, le istituzioni politiche, sociali e religiose. Gli attacchi si sono verificati nei luoghi pubblici e nelle strade della città con il coinvolgimento di migliaia di persone in tutto il mondo.

1.2.2. Minacce biologiche

Il riconoscimento di un pericolo biologico può avvenire attraverso diversi metodi:

- scoperta di prove di attività bioterroristica (dispositivi, agenti, laboratorio clandestino);
- la diagnosi (identificazione di una malattia causata da un agente identificato come agente di bioterrorismo);
- rilevazione (raccolta e interpretazione dei dati pubblici di monitoraggio sanitario).

Quando le persone sono esposte a un patogeno come l'antrace o vaiolo, possono non sapere di essere state esposte, e coloro che sono infetti, o successivamente infettati, possono non sentirsi male per

qualche tempo. Questo ritardo tra l'esposizione e l'insorgenza della malattia, il periodo di incubazione, è caratteristico di ciascuna malattia infettiva. Il periodo di incubazione può variare da alcune ore a una o poche settimane, a seconda dell'esposizione e patogeno. La minaccia potrebbe anche consistere in un agente biologico introdotto nei prodotti agricoli coltivati su larga scala (ad esempio, ruggine del grano) o in un virus che colpisce il bestiame, potenzialmente devastante per l'economia locale o anche nazionale.

A differenza delle vittime di esposizione ad agenti chimici o radiologici, le vittime di attacco di agenti biologici possono servire come vettori della malattia con la capacità di infettare altri (ad esempio, il vaiolo, la peste).

Gli agenti biologici sono organismi o tossine che possono uccidere o inabilitare persone, bestiame e raccolti. Un attacco biologico è l'emissione deliberata di germi o altre sostanze biologiche nocive.

I tre gruppi di base degli agenti biologici che possono essere utilizzati come armi sono batteri, virus e tossine. La maggior parte di agenti biologici sono difficili da coltivare e mantenere. Molti deperiscono rapidamente quando esposti alla luce del sole e di altri fattori ambientali, mentre altri, come le spore di antrace, sono molto longevi. Agenti biologici possono essere dispersi nell'aria, infettando animali che portano la malattia all'uomo e contaminando cibo e acqua.

Le modalità di diffusione sono:

- aerosol - agenti biologici si disperdono nell'aria, formando una nebbia sottile che può diffondersi rapidamente. L'inalazione l'agente può causare la malattia in persone o animali;
- animali - alcune malattie sono diffuse da insetti e animali, come le pulci, topi, mosche, zanzare e bestiame;
- la contaminazione di cibo e acqua - alcuni microrganismi patogeni e le tossine possono persistere nelle forniture di cibo e acqua. La maggior parte dei microbi possono essere uccisi, e le tossine disattivate attraverso la cottura di cibi e l'ebollizione;
- da persona a persona - Gli esseri umani sono stati la fonte di infezione per il vaiolo, la peste, ecc.

1.2.3. Minacce Chimiche

Gli Agenti chimici hanno lo scopo di uccidere, ferire gravemente, o inabilitare le persone attraverso effetti fisiologici. Un incidente terroristico con una sostanza chimica richiederà immediata reazione di emergenza da parte delle forze dell'ordine dei VVFF medici di emergenza e personale di elevata specializzazione.

I prodotti chimici pericolosi possono essere introdotti nell'ambiente tramite dispositivi di aerosol (ad esempio, ordigni, spruzzatori, o generatori aerosol) e con contenitori a rottura. Un attacco di questo tipo potrebbe comportare il rilascio di un agente chimico, come un nervino o una sostanza chimica industriale, che può avere gravi conseguenze.

All'inizio delle operazioni potrebbe non essere evidente se un focolaio è stato causato da un agente infettivo o di una sostanza chimica pericolosa, tuttavia, la maggior parte dei attacchi chimici saranno localizzati, ed i loro effetti saranno evidenti nel giro di pochi minuti. Esistono agenti chimici di carattere sia persistente che non persistente. Agenti persistenti rimangono nella la zona colpita per ore, giorni o settimane. Agenti non persistenti hanno un alto tassi di evaporazione, sono più leggeri dell'aria, e si disperdono rapidamente, perdendo così la loro capacità di causare vittime dopo 10 a 15 minuti, anche se possono essere più persistenti in piccole zone non ventilate.

Segni di un rilascio di sostanze chimiche sono le persone che hanno difficoltà di respiro, irritazione agli occhi; perdita di coordinazione, senso di nausea, o avere una sensazione di bruciore nel naso, della gola e dei polmoni. Inoltre, la presenza di molti insetti morti o uccelli possono indicare il rilascio di un agente chimico.

1.2.4. Esplosione nucleare

Un'esplosione nucleare è un'emissione di luce intensa e calore, un'onda di pressione, e diffusione di materiale radioattivo che può contaminare l'aria, l'acqua e le superfici a terra a grande distanza. Un dispositivo nucleare può variare da un arma portata da un missile intercontinentale lanciato da una nazione ostile o un'organizzazione terroristica, ad un sistema portatile di piccole dimensioni concepito per essere trasportato da un individuo. Tutti i dispositivi nucleari possono causare effetti letali quando esplodono, a causa di luce accecante, intenso calore (irraggiamento termico), iniziale radiazione nucleare, onda d'urto, incendi appiccati dagli impulsi di calore e gli incendi secondari causati dalla distruzione.

La minaccia nucleare presente durante la Guerra Fredda è diminuita, tuttavia permane la possibilità che un terrorista possa ottenere l'accesso a un'arma nucleare. Gli ordigni nucleari sono attualmente più piccoli.

La dispersione geografica degli effetti di un'esplosione dipendono essenzialmente da:

- dimensioni del dispositivo. Una bomba più potente produrrà effetti a maggiore distanza;
- altezza dal suolo a cui il dispositivo è stato fatto esplodere;
- natura della superficie sottostante l'esplosione; alcuni materiali presentano maggiore propensione a diventare radioattivi di altri. Aree piane sono più suscettibili agli effetti esplosione;
- condizioni meteorologiche. Velocità e direzione del vento influiscono sul tempo di arrivo del fallout, e le precipitazioni possono lavare ricadute dall'atmosfera.

Oltre agli altri effetti, un'arma nucleare fatta esplodere in atmosfera può creare un impulso elettromagnetico (EMP), ad alta densità di campo elettrico. Un EMP agisce come un colpo di fulmine, ma è più forte, più veloce, e più breve. Un EMP può seriamente danneggiare i dispositivi elettronici collegati a fonti di alimentazione o antenne. Questo include sistemi di comunicazione, computer, elettrodomestici e sistemi di accensione di auto o aerei. Il danno potrebbe variare da una interruzione di funzionamento temporanea all'esaurimento effettivo dei componenti. La maggior parte delle apparecchiature elettroniche nel raggio di centinaia di chilometri da una detonazione nucleare ad alta quota potrebbe risultare compromessa. Anche se un EMP è improbabile che danneggi la maggior parte delle persone, potrebbe danneggiare quelli con pacemaker o altri dispositivi elettronici impiantati.

Anche se le persone non sono abbastanza vicino al l'esplosione nucleare per essere colpiti dagli effetti diretti, possono essere colpiti dal fall-out radioattivo. Esplosioni che si verificano in prossimità della superficie terrestre possono creare quantità molto più elevate di fallout rispetto ad esplosioni che si verificano ad altitudini più elevate. Questo perché l'enorme calore prodotto da una esplosione nucleare provoca una corrente d'aria che forma la nube a fungo. Quando si verifica una esplosione vicino alla superficie della terra, milioni di particelle di polvere vaporizzate vanno a costituire la nube. Come il calore diminuisce, materiali radioattivi che si sono vaporizzati condensano sulle particelle e cadono di nuovo a terra. Il fenomeno si chiama fallout radioattivo. Il materiale di fallout decade per un lungo periodo di tempo, ed è la principale fonte di radiazione nucleare residua.

Le radiazioni nucleari sono invisibili, inodore, e non sono in genere rilevate dai nostri sensi. Le radiazioni possono essere rilevate solo dai dispositivi di monitoraggio delle radiazioni. Questo rende le emergenze radiologiche diverse da altri tipi di emergenze, come inondazioni o uragani. Il monitoraggio potrà prevedere i tempi di ricaduta di arrivo, che saranno resi note attraverso i canali ufficiali di avvertimento.

I tre principali fattori per proteggersi dalle radiazioni e la ricaduta sono la distanza, il tempo e la schermatura.

- Distanza – maggiore è la distanza rispetto alle particelle fallout, meglio è. Uno spazio sotterraneo, come un seminterrato di un edificio risulta più protettivo rispetto ai piani fuori terra;
- Schermatura - materiali di elevata densità come muri di cemento, mattoni, terreno possono proteggere dalle particelle di fallout;

- Tempo – le radiazioni di fallout perdono la loro intensità abbastanza rapidamente. Il fallout radioattivo costituisce la maggiore minaccia per le persone durante le prime due settimane, al termine delle quali si riduce a circa l'1 per cento il so livello di radiazione iniziale.

1.2.5. Dispositivo dispersione radiologica (RDD)

L'uso terroristico di un RDD - spesso chiamato "nucleare sporco " o "bomba sporca" - è considerato molto più probabile dell'uso di un ordigno esplosivo nucleare. Un RDD combina un dispositivo esplosivo convenzionale - come una bomba - con materiale radioattivo. Può essere utilizzato dai terroristi perché richiede limitate conoscenze tecniche rispetto a un ordigno nucleare. Inoltre, i materiali radioattivi utilizzabili in un RDD sono ampiamente utilizzati in medicina, in agricoltura nell'industria e nella ricerca, e sono pertanto più facili da ottenere rispetto uranio o plutonio.

Lo scopo principale dell'uso terroristico di un RDD è quello di provocare paura psicologica e conseguenze economiche. Alcuni dispositivi potrebbero provocare vittime da esposizione a materiali radioattivi. A seconda della velocità con cui è stata evacuata l'area della detonazione di un RDD o di quanto erano protette le persone presenti sul luogo , il numero di morti e feriti da un RDD non dovrebbe essere sostanzialmente più grande di quello derivante da una bomba convenzionale.

La dimensione della zona interessata e il livello di distruzione causata da un RDD dipenderà dalla dimensione e sofisticazione della bomba convenzionale, il tipo di materiale radioattivo utilizzato, la qualità e la quantità del materiale radioattivo, e le condizioni meteorologiche locali - principalmente vento e precipitazioni. L'area interessata potrebbe essere messa off-limits al pubblico per diversi mesi durante lavori di sgombero.

1.2.6. Cyber attacco

Spesso non ci si rende conto che le nostre azioni sul web possono mettere noi, le nostre famiglie, e anche il nostro paese a rischio. Imparare a conoscere i pericoli e intraprendere le necessarie azioni per proteggere noi stessi è il primo passo per rendere Internet un luogo più sicuro per tutti. La sicurezza informatica è una responsabilità condivisa e ognuno di noi ha un ruolo da svolgere.

Cybersecurity implica la protezione delle infrastrutture per prevenire, individuare e rispondere agli incidenti informatici. A differenza di minacce fisiche le minacce informatiche sono spesso difficili da identificare e comprendere. Tra questi pericoli i maggiori sono i virus in grado di cancellare interi sistemi, le intrusioni e irruzioni nei sistemi per modificare i file, intrusioni per utilizzare i nostri computer per attaccarne altri, o intrusioni per rubare informazioni riservate. Lo spettro dei rischi informatici è senza limiti, le minacce, alcune più gravi e sofisticate rispetto ad altre, può avere effetti ad ampio spettro su individui, comunità, organizzazioni, anche a livello nazionale.

Tali rischi comprendono:

- criminalità organizzata, sponsorizzata dallo stato hacker, e spionaggio informatico possono creare rischi di sicurezza nazionale per il nostro paese;
- servizi di trasporto, di energia, e altri potrebbero essere disturbati da grandi incidenti informatici su larga scala. L'entità della perturbazione è molto incerta in quanto determinata da molti fattori ignoti come il bersaglio e dimensioni dell'incidente;
- vulnerabilità dei dati e loro perdita se la rete è compromessa. Informazioni su una società, i suoi dipendenti ei suoi clienti possono essere a rischio;
- dispositivi di proprietà individuale come computer, tablet, telefoni cellulari e sistemi di gioco che si collegano a Internet sono vulnerabili alle intrusioni. Le informazioni personali possono essere a rischio senza sicurezza adeguata.

1.2.7. Altri pericoli di natura terroristica

La pianificazione deve tenere in debita considerazione anche la possibilità che si verifichino attacchi terroristici di natura insolita.

Anche se è impossibile prevenire ed evitare ogni tipo immaginabile di terrorismo o attacco, la pianificazione dovrebbe considerare che i futuri approcci terroristici potrebbero avere differenti livelli di complessità e di coordinamento. Pertanto, i programmi sviluppati per attentati terroristici dovranno essere di ampia portata ma sufficientemente flessibili per affrontare l'imprevisto. In questi casi, la formazione e l'esperienza dei soccorritori possono essere più importanti di procedure dettagliate.

1.3 Le infrastrutture critiche

Le infrastrutture critiche sono le risorse materiali, i servizi, i sistemi di tecnologia dell'informazione, le reti e i beni infrastrutturali che, se danneggiati o distrutti, causerebbero gravi ripercussioni alle funzioni cruciali della società, tra cui la catena di approvvigionamenti, la salute, la sicurezza e il benessere economico o sociale dello Stato e della popolazione.

Il Libro Verde adottato a Bruxelles il 17 novembre 2005 (Programma europeo di protezione delle infrastrutture critiche) ha suddiviso le Infrastrutture Critiche in 11 settori:

Amministrazione Civile	Funzioni di Governo, Forze Armate, Servizi dell'amministrazione civile, Servizi di emergenza, Servizi postali, Corrieri postali
Salute	Ospedali e Centri di cura, Produzione di medicine, sieri, vaccini, Case farmaceutiche, Laboratori biologici e Agenti biologici
Trasporti	Strade, Ferrovie, Traffico aereo, Condotte sotterranee di acqua, Trasporti marittimi ed oceanici
Energia	Produzione di oli e gas, raffinerie, trattamento e stoccaggio incluse le condotte, Centrali elettriche, elettrodotti, oleodotti e gasdotti, Impianti di distribuzione di elettricità, gas, olio
Informazione, tecnologia e comunicazione	Protezione di sistemi di informazione e reti, Sistemi automatici di controllo, Internet, Forniture di comunicazione fissa, Fornitura di comunicazione mobile, Comunicazione radio, comunicazione satellitari, broadcasting
Spazio e Ricerca	Centri spaziali, Centri di ricerca
Finanza	Servizi di pagamento e strutture di pagamenti privati, Assegnazione finanziarie di governo
Sicurezza Pubblica ed Ordine legale	Mantenimento della sicurezza dell'ordine e legale, Amministrazione della giustizia, carceri
Acqua	Fornitura di acqua potabile, Controllo della qualità dell'acqua, Prelievo e controllo della quantità dell'acqua
Alimenti	Forniture alimentari e controlli alimentari
Industrie chimiche e Nucleari	Produzione e Stoccaggio e trasformazione di sostanze chimiche e nucleari, Condutture di sostanze pericolose

1.4 Scenari di evento

Un attentato terroristico potrà, in linea di massima, evidenziarsi come fatto immediatamente evidente: l'emergenza segnalata presenta fin dall'inizio le caratteristiche tipiche dell'offesa nucleare, batteriologica, chimica radiologica (NBCR), quali

- sversamenti o dispersioni di polveri, liquidi, gas non giustificati nell'ambiente o noti come tossici o comunque dannosi;
- malessere, evidenze cutanee o di altro tipo, segnalati da più persone in un ambiente;
- odori non abituali o non motivati nell'ambiente;

- scenario di altro tipo, ma coinvolgente obiettivi sensibili o sostanze pericolose: l'evento segnalato od accertato è di tipo tradizionale (incendio, incidente stradale, atto di vandalismo …), ma coinvolge ambienti, mezzi o contenitori in grado di provocare emissioni pericolose, ad esempio;
- incendio all'interno di uno stabilimento che produce od impiega sostanze tossiche od in grado di liberare sostanze tossiche, laboratori, ospedali;
- incidente stradale in area urbana associato alla emissione di sostanze;
- esplosione senza effetti evidenti all'interno di un luogo affollato;
- evento caratterizzato da assenza di danno, ma tale da creare notevole richiamo di persone e soccorritori: nella considerazione che la pratica della "duplicazione" riguarda circa il 50% degli attentati, particolare attenzione dev'essere dedicata agli eventi che provocano richiamo senza iniziali evidenze di danno, soprattutto all'interno od in prossimità di obiettivi sensibili; ad esempio;
- esplosione, fragore, lampo, sibilo, fumo all'aperto, all'interno od in prossimità di luoghi affollati;
- esplosione, incendio, rumore, odore in prossimità di stabilimenti o depositi di sostanze pericolose;
- allarme, fumo, incendio in prossimità di cisterne, veicoli furgonati, depositi di materiali;
- segnalazioni ripetute di effetti analoghi, non riferiti ad un preciso scenario: caso tipico delle conseguenze di contaminazione di alimenti, bevande, oggetti, riguarda in particolare i rischi suscettibili di produrre effetti differiti rispetto al contatto con l'agente contaminante ;
- presentazione alle strutture sanitarie o richieste di soccorso di più persone che presentano gli stessi sintomi, non riferibili alla epidemiologia ordinaria;
- decessi ripetuti con causa non accertata o comunque sospetta, avvenuti in circostanze simili.

Non deve esser trascurata, inoltre, l'ipotesi che un'offesa NBCR sia apportata mediante azioni apparentemente riferite a scenari ordinari, eventualmente di matrice vandalistica o malavitosa tradizionale.

1.4.1. Indicatori di rischio

Sulla base della casistica disponibile è possibile definire una serie di tipologie di indicatori di rischio, ovvero di circostanze che possono venirsi a verificare prima dell'accadimento di un atto terroristico, o nelle fasi iniziali di sviluppo dello stesso.

- scoppio o esplosione con limitati effetti, specialmente in luogo affollato;
- segnalazione di un dispositivo, un contenitore od un veicolo che ha disperso una sostanza gassosa o nebulizzata o una polvere;
- segnalazioni di odori insoliti provenienti da liquidi o sostanze nebulizzate;
- segnalazioni di dispositivi, contenitori o tubi estranei all'ambiente o comunque sospetti;
- animali morti;
- indumenti o dispositivi di protezione individuale abbandonati.

1.4.2. Indicatori di evento

Tra gli indicatori di evento, particolare rilevanza assumono alcune tipologie di chiamata di emergenza, sia in relazione al luogo di accadimento dell'evento, sia in relazione al giorno e all'ora di accadimento.

In relazione al luogo di accadimento, può essere considerata indicatore di evento una segnalazione proveniente da:

- edifici e monumenti storici e/o simbolici;
- edifici pubblici, stazioni (ferroviarie, aeroportuali, marittime);
- scuole, ospedali, stadi, teatri - cinema multisale, ecc.;

- edifici sedi di organi governativi, militari, partiti politici, enti religiosi, ecc.;
- ipermercati, centri commerciali, ecc.

Dal punto di vista del giorno di accadimento ed anche dell'ora, può essere considerata indicatore di evento una segnalazione che coincide con:

- feste religiose;
- feste nazionali;
- date storiche – politiche;
- manifestazioni sportive, culturali, sociali.

Altri indicatori di evento riconoscibili direttamente sulla scena e riferibili essenzialmente alla matrice terroristica possono essere:

- inaspettato numero di morti, feriti o malati;
- sintomi e segni clinici inspiegabili (molte persone che presentano sintomi similari);
- presenza sospetta di mezzi, apparecchiature, persone inusuali in quel luogo;
- eventi (uguali o diversi) disseminati nella stessa area o inspiegabili in quel luogo;
- più persone che segnalano un effetto apparentemente senza una causa precisa o traumatica.

1.5 Attività di Previsione e Prevenzione

Il Programma di Previsione e Prevenzione, rispetto all'analisi ed alla definizione del rischio terroristico, è orientato alla individuazione delle principali tipologie di evento rispetto alle quali potranno essere definite le procedure di intervento, nel rispetto delle competenze specifiche definite per il rischio terroristico. Poco o nulla la pianificazione Provinciale in materia di Protezione Civile è in grado di aggiungere all'attività svolta dalle forze di polizia e di intelligence per quanto riguarda l'attività di previsione e di prevenzione. Particolare rilevanza, ai fini previsionali assume per l'area Milanese, lo sviluppo del progetto europeo Smart Ciber.

1.5.1. Il progetto Smart Ciber

SMART CIBER è l'acronimo di System of Maps Assessing Risk of Terrorism against Critical Infrastructures in Big Events Rallies, un progetto europeo che ha l'obiettivo di creare un sistema di mappatura per la prevenzione dei rischi sia di security sia di safety (Protezione Civile) in occasione dei grandi eventi. Tale progetto è sviluppato nell'ambito del programma europeo "Prevenzione, preparazione e gestione delle conseguenze in materia di terrorismo ed altri rischi legati alla sicurezza".

Il Comune di Milano, in qualità di applicant organization, è affiancato da quattro partners nazionali ed internazionali: Università Cattolica del Sacro Cuore (UCSC), Municipality of Varna, Municipality of Budapest e Safety Region Rotterdam Area. Inoltre, come partners associati, partecipano al progetto Regione Lombardia, A2A, ATM, AMSA, Ferrovie Nord, Ferrovie dello Stato, SEA, MM, UNICRI. L'unione e la condivisione delle esperienze dei diversi partners consente l'elaborazione di un modello condiviso di risk assessment grazie alla creazione di una mappa integrata dei rischi e alla costruzione di indici dei rischi, (garantendo così una base scientifica al progetto).

L'obiettivo del sistema è la geolocalizzazione di luoghi, strutture e aree che riportano criticità relative alla sicurezza e quindi maggiormente sottoposte a rischi. Seguendo questo obiettivo si realizzerà una mappa in grado di indicare i diversi livelli di rischio presenti sul territorio in tempo reale, grazie all'attività di aggiornamento della mappa in modo dinamico e operativo. Proprio la dinamicità e l'operatività renderanno la mappa uno strumento utile per indirizzare gli interventi di più soggetti, quali Forze dell'Ordine, Regioni, aziende che gestiscono i trasporti, l'erogazione di elettricità e gas, i servizi ambientali e infine istituti di ricerca. A questo proposito la condivisione della mappa avviene all'interno di una rete privata che comprende tutti i soggetti coinvolti elencati precedentemente; la scelta di una rete intranet è motivata dalla manipolazione di informazioni che, in primo luogo hanno un notevole

impatto sulla percezione della sicurezza del cittadino e in secondo luogo potrebbero essere utilizzate per fini anti-sociali, criminali o di terrorismo.

La gestione di grandi eventi, quale Expo 2015, sarà supportata e agevolata dall'utilizzo del sistema di mappatura, in grado di fornire informazioni integrate del territorio relative a rischi e criticità esistenti; grazie a tale strumento gli enti coinvolti in grandi eventi disporranno di maggiori informazioni al fine di prendere le necessarie decisioni, decisioni che riguardano piani di sicurezza sia ordinaria sia di contingenza. Il fine ultimo del progetto SMART CIBER è quindi assicurare al cittadino una sicurezza, intesa come security e safety, che sia il prodotto di una sentita e motivata collaborazione tra enti ed istituzioni.

L'attuazione del progetto è prevista per fasi, secondo il seguente schema:

- Fase 1 - Individuazione degli indicatori di rischio terroristico e analisi comparativa; successiva condivisione tra i partner delle esperienze sui sistemi e sulle metodologie in atto per la valutazione del rischio terroristico;
- Fase 2 - Elaborazione del modello di valutazione integrata dei rischi, programmazione e definizione degli aspetti operativi, procedurali e tecnologici in grado di adeguare il modello ai contesti locali dei partner così come di altri Stati membri della UE;
- Fase 3 - Test del Modello nei quattro paesi di appartenenza dei partners (Italia, Bulgaria, Ungheria, Olanda);
- Fase 4 - Elaborazione del modello finale con finalizzazione e valutazione della fattibilità utile per replicare il modello;
- Fase 5 - Comunicazione e diffusione dei risultati attraverso una serie di apposite azioni che verranno svolte per tutta la durata del progetto.