VALUTAZIONE E GESTIONE DEL RISCHIO
NEGLI INSEDIAMENTI CIVILI ED INDUSTRIALI
ISTITUTO SUPERIORE ANTINCENDI,
ROMA, 20-22 SETTEMBRE 2016

VALUTAZIONE DELLA SICUREZZA DELLE INFRASTRUTTURE CRITICHE NEL SETTORE CIVILE, DEFINIZIONI E METODOLOGIA

Diego Carlo LO PRESTI[1] ; Nicola MAROTTA[2]

[1] Prof. Ass. Dipartimento di Ingegneria dell'Energia, dei Sistemi, del Territorio e delle Costruzioni (DESTeC) - Università di Pisa – Largo L. Lazzarino, 1 – 56127 Pisa, e-mail: d.lopresti@ing.unipi.it
[2] Docente a contratto Dipartimento di Ingegneria Civile e Industriale - Università di Pisa – Largo L. Lazzarino, 1 – 56127 Pisa, e-mail: nicola.marotta@dic.unipi.it

Abstract: Le società industrializzate dipendono dal corretto funzionamento di un insieme d'infrastrutture tecnologiche, quali le reti elettriche, quelle viarie e ferroviarie e le reti di telecomunicazione che, per la loro rilevanza, sono genericamente indicate come infrastrutture critiche, perché intese come quei sistemi, o parte di essi, essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale, il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello Stato, a causa dell'impossibilità di mantenere tali funzioni. Infatti, guasti tecnici, disastri naturali ed eventi dolosi, se non addirittura terroristici, potrebbero avere degli effetti devastanti. Gli eventi degli ultimi anni hanno accelerato gli sforzi di individuazione e designazione delle infrastrutture critiche a livello nazionale ed europeo e hanno rafforzato le preoccupazioni per l'aumento della protezione delle infrastrutture critiche in settori sensibili per la sicurezza dell'individuo e della comunità. Si tratta di reali pericoli per lo sviluppo e il benessere sociale di un Paese che sembrano essere accresciuti dall'estremizzazione dei fenomeni climatici e dalla tormentata situazione socio-politica mondiale. Le minacce alla sicurezza delle infrastrutture critiche nel settore civile (scuole, ospedali, stadi, teatri, cinema multisala, stazioni ferroviarie, aeroportuali, marittime ecc.) sono uno dei principali problemi delle società industrializzate negli ultimi tempi. Nei loro confronti vengono sempre più richieste garanzie di massima sicurezza, per scongiurare qualsiasi incidente che potrebbe mettere in pericolo la salute e la sicurezza dei cittadini, ma anche costituire un impatto pericoloso per l'ambiente e l'economia di un paese. L'obiettivo della presente memoria è fornire in modo semplice ma puntuale gli elementi di base per comprendere la tematica insieme alle motivazioni della sua importanza sia a livello nazionale, sia europeo, sia internazionale. In particolare, dopo aver tracciato l'origine del problema, cioè il tipo di minacce e rischi che si intendono contrastare, nonché le nuove vulnerabilità gravanti sulla nostra società, si descrivono le azioni intraprese dall'Europa finalizzate a migliorare la protezione delle Infrastrutture Critiche nel settore civile, anche in riferimento alla Direttiva 2008/114/CE e alla normativa nazionale di recepimento (D.Lgs 11 aprile 2011, n. 61).

Introduzione

I paesi maggiormente industrializzati sono dotati di sempre più estesi e sofisticati sistemi infrastrutturali, le cosiddette Infrastrutture Critiche (IC) come le reti di distribuzione dell'energia e le infrastrutture del trasporto, così come specificato nella Direttiva del Consiglio Europeo, ma che possono riguardare anche altri settori come si vedrà meglio in seguito.

Le IC possono essere soggette a vari tipi di malfunzionamento, legati a problemi tecnologici, a disastri naturali, ad attacchi intenzionali. La crescente attenzione, a livello mondiale, nei confronti della sicurezza delle IC è dovuta al fatto che lo sviluppo dei diversi settori della società e di conseguenza il benessere della popolazione nei paesi industrializzati, dipende, e dipenderà sempre di più, dalla disponibilità e dal corretto funzionamento di infrastrutture tecnologiche. In questa ottica, la preoccupazione di proteggere le infrastrutture critiche è sempre andata aumentando. Gli attacchi terroristici dell' 11 settembre 2001 negli Stati Uniti e quelli che colpirono la metropolitana e le ferrovie a Madrid nel 2004 e nel 2005 a Londra, portarono alla ribalta il problema. L'impegno profuso dai vari stati si concentrò all'inizio sulla protezione delle infrastrutture civili contro gli atti di terrorismo, questo anche se i documenti di politica generale presentavano un'impostazione multirischio che si estendeva anche alle calamità naturali e agli incidenti tecnologici. Tuttavia lo tsunami che sconvolse il Sud-Est asiatico nel 2004 danneggiando numerose infrastrutture insediate - comprese istallazioni energetiche decisive – e i vasti danni conseguenti all'uragano Katrina nel 2005 che ebbe effetti devastanti sulla città di New Orleans e gli stati della Louisiana, dell'Alabama e del Mississippi, indussero i vari stati a riorientare talune politiche. I paesi europei, nonché l'Unione europea, prendono oggi in considerazione la totalità dei rischi che possono presentarsi, anche se in molti di questi paesi europei - soprattutto in Francia e nel Regno Unito - la priorità è ancora rivolta alla minaccia posta dal terrorismo. Le minacce alla sicurezza delle infrastrutture critiche nel settore civile (scuole, ospedali, stadi, teatri, cinema multisale, stazioni ferroviarie, aeroportuali, marittime ecc.) ovvero luoghi oggetto di passaggio di grandi masse sono diventati oggi più che mai a rischio per eclatanti attentati di matrice terroristica e sono uno dei principali problemi delle società industrializzate negli ultimi tempi. Nei loro confronti vengono sempre più richieste garanzie di massima sicurezza, per scongiurare qualsiasi incidente che potrebbe mettere in pericolo la salute e la sicurezza dei cittadini, ma anche costituire un impatto pericoloso per l'ambiente e l'economia di un paese.

Interconnessione delle infrastrutture critiche

Queste infrastrutture, un tempo sistemi sostanzialmente isolati e verticalmente integrati, per ragioni di natura economica, sociale, politica e tecnologica sono divenute sempre più complesse e

interdipendenti al punto tale che un evento avverso che occorre a una di esse, in una data localizzazione geografica, può propagarsi ad altre infrastrutture amplificando gli effetti negativi e provocando danni a soggetti dislocati anche in località molto remote rispetto all'origine dell'evento iniziale.

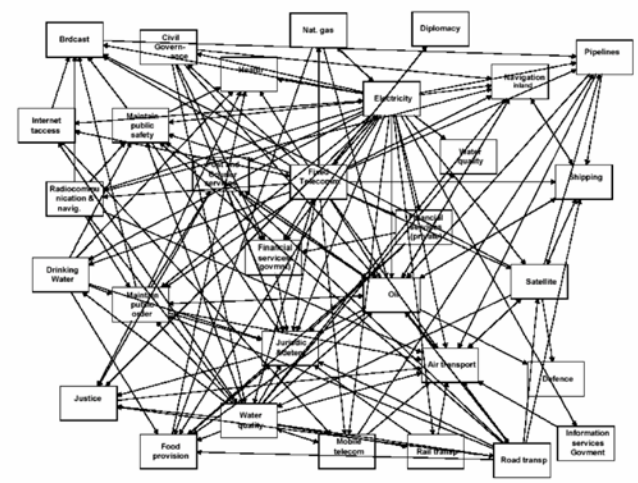

Figura 1- *Grafico delle interdipendenze esistenti fra le diverse infrastrutture operanti in Olanda (Fonte TNO). La complessità del grafico evidenzia l'elevato numero di interazioni fra le infrastrutture considerate nell'analisi.*

Questa interdipendenza ha indotto in queste infrastrutture, nuove e impreviste vulnerabilità, rischiando di causare reali conseguenze negative per lo sviluppo e il benessere sociale del Paese, anche a causa delle accresciute minacce legate all'estremizzazione dei fenomeni climatici e alla tormentata situazione socio-politica mondiale, al punto che un guasto (di natura accidentale o dolosa) in una di loro può facilmente propagarsi con un meccanismo di effetto domino alle altre, amplificando i suoi effetti e provocando disfunzioni e malfunzionamenti anche ad utenti remoti, sia dal punto di vista geografico che funzionale, rispetto al punto ove si era originariamente generato il guasto. Se a questo aggiungiamo che oggi la maggior parte delle infrastrutture critiche appartengono e sono gestite da imprese sia pubbliche che private, sulle quali ricade pertanto la responsabilità della loro protezione, è facile rendersi conto della complessità dei problemi per quel che riguarda sia la ripartizione dei ruoli e delle responsabilità tra i soggetti interessati, pubblici e privati, che la compatibilità tra obiettivi nazionali di sicurezza ed interessi commerciali. Questo comporta da un lato una maggiore vulnerabilità sistemica dovuta alla presenza di effetti domino e dalla globalizzazione delle minacce, e dall'altro una maggiore complessità che si ripercuote nella difficoltà di analisi, comprensione, e gestione del System of Systems Engineering (SoSE) che si viene a creare dalla integrazione fra le diverse infrastrutture.

È inoltre importante chiarire fin da subito che la sicurezza delle infrastrutture critiche non costituisce un settore isolato, in quanto si inserisce nel contesto più ampio delle politiche di protezione civile. Queste hanno come obiettivo generale la messa a punto di strumenti per

permettere al settore civile di far fronte alle minacce poste dalle catastrofi naturali, da incidenti tecnologici e attentati terroristici, ricorrendo generalmente a una strategia articolata su più punti: la prevenzione e la protezione delle persone e delle infrastrutture dai pericoli derivanti da calamità naturali, incidenti tecnologici e attentati terroristici, lo stato di preparazione e la gestione delle conseguenze e, infine, la reazione e il ripristino dei servizi. In tale quadro, la sicurezza delle infrastrutture critiche, nell'ottica di un approccio integrale alla protezione, contribuisce al raggiungimento di un ulteriore obiettivo, vale a dire quello della gestione della continuità operativa (ingl. «Business Continuity Management», BCM).

La continuità operativa

La consapevolezza di questa minaccia emerge nel momento in cui le infrastrutture critiche si trovano a loro volta di fronte alla necessità di garantire continuità nella fornitura dei servizi essenziali alla popolazione. Per gli aspetti della continuità dei sistemi complessi (centrali di produzione e reti di distribuzione energia, reti ferroviarie, ospedali, etc.) la continuità nell'erogazione di servizi costituisce un bene primario e pertanto deve essere adeguatamente protetto da un'ampia gamma di minacce al fine di garantire il regolare svolgimento delle attività. All'interno della ISO/PAS 22399:2007, che è lo standard di riferimento (insieme alla ISO 22301:2012) per la gestione degli incidenti e la continuità operativa, quest'ultima è definita come: "*systematic and coordinated activities and practices through which an organization optimally manages its risks and the associated potential threats and impacts there from*".

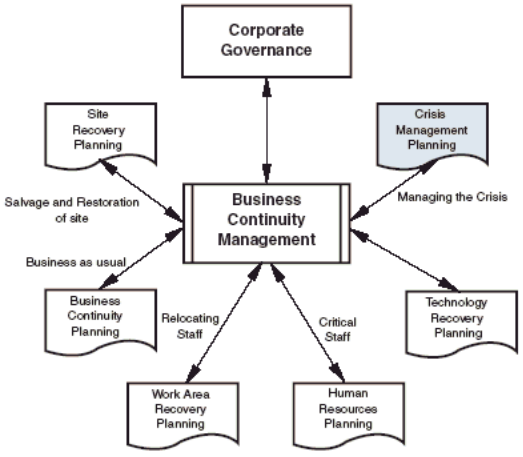

Fig. 2 – *Business Continuity Management», BCM (Tratto dalla norma BS25999)*

Lo standard enfatizza ulteriormente tale affermazione richiedendo la presenza di procedure da utilizzarsi come approccio iniziale e finalizzate all'identificazione delle minacce e dei pericoli. Per garantire tale continuità operativa è necessario quindi mettere in atto un opportuno insieme di misure, quali politiche, prassi operative, procedure e strutture organizzative, che consentano al

sistema il soddisfacimento dei propri obiettivi di continuità operativa. Questa situazione in particolare per le infrastrutture critiche civili, portano alla necessità di predisporre un Sistema di Gestione per la Continuità Operativa (SGCO) che garantisca all'organizzazione la sopravvivenza in caso di interruzione dell'operatività ed il ripristino delle attività critiche entro tempi e modalità predeterminati. La norma ISO 22301:2012 sostituisce la precedente BS25999-2 e specifica i requisiti che devono essere soddisfatti da ogni organizzazione che intenda dotarsi di un Sistema di Gestione per la Continuità Operativa (SGCO). L'applicazione di tali requisiti garantisce la riduzione degli impatti dovuti al possibile verificarsi di scenari di interruzione di processi critici aziendali e ne assicura l'affidabilità. Un SGCO comprende una struttura documentale ed operativa che prevede i seguenti punti:

1) Definizione della Politica per la Continuità Operativa;

2) Definizione dell'Ambito;

3) Definizione metodo e analisi degli impatti sull'operatività;

4) Definizione metodo e valutazione del rischio

5) Stabilire la strategia per la GCO

6) Sviluppare ed attuare la GCO di risposta: Piani di gestione degli incidenti, Piani di continuità operativa

7) Effettuare le esercitazioni

8) Monitorare e revisionare il SGCO

9) Mantenere e migliorare il SGCO

La complessità e interdipendenza unitamente alla necessità di una continuità operativa ci fanno capire come sia estremamente difficile difendere queste strutture da tutte le possibili minacce e come non sia impossibile eliminare ogni rischio per ogni individuo in ogni luogo in ogni momento. Queste considerazioni hanno portato vari Paesi, e di recente anche la Comunità Europea, a definire specifiche strategie di mitigazione del rischio atte a migliorare la sicurezza delle diverse infrastrutture critiche, sia nei confronti di eventi accidentali che dolosi o terroristici. Per tutti questi motivi tali infrastrutture dovrebbero essere ciclicamente sottoposte a processi di Security & Safety Assessment al fine di individuare eventuali falle e porvi rimedio. Una breve analisi delle politiche adottate da vari soggetti nazionali e internazionali mostra che la sicurezza delle IC presuppone una serie di passi successivi: in primo luogo, la definizione di ciò che viene considerato come infrastruttura critica, secondo, l'individuazione di quelle infrastrutture che rientrano nella definizione, terzo, una valutazione del rischio cui tali infrastrutture sono soggette e la constatazione di eventuali carenze nella loro sicurezza e, infine, l'elaborazione e l'applicazione di opportune misure di protezione per ridurre il livello di rischio.

Definizione di infrastrutture critica

Il termine Infrastrutture Critiche è definito nella sezione 1016(e) dell'USA Patriot Act del 2001 e con esso si intendono quei "*sistemi e beni, sia fisici che virtuali, così vitali alla nazione che un loro malfunzionamento o una loro distruzione produrrebbe un impatto debilitante sulla sicurezza dei cittadini, sulla sicurezza economica della nazione, sulla salute pubblica nazionale e su una qualsiasi combinazione delle precedenti*". Successivamente agli USA Patriot Act è nato il Dipartimento di Homeland Security degli Stati Uniti avente lo scopo, tra l'altro, di assicurare la protezione delle Infrastrutture Critiche Nazionali. Anche l'Europa ha emanato un proprio programma di Protezione delle Infrastrutture Critiche nel quale viene fornita una definizione di Infrastruttura Critica. Nel giugno 2004 il Consiglio Europeo prende l'iniziativa di chiedere la preparazione di una strategia per la protezione delle Infrastrutture Critiche nel territorio dell'Unione da possibili attacchi terroristici, che porta la Commissione ad emettere la Comunicazione 702 del 2004. Questo documento contiene la prima definizione di Infrastruttura Critica in Europa: *Quelle risorse fisiche, servizi e installazioni, reti e risorse informatiche le cui degradazione (disruption) avrebbe un serio impatto sulla sicurezza o il benessere economico degli Europei o sul funzionamento efficace dell'Unione Europea o dei Governi degli Stati Membri* .

Questo documento contiene un elenco delle IC individuate dalla Commissione così composto:

- impianti e reti energetiche (centrali elettriche, impianti di produzione di gas e petrolio, depositi e raffinerie, sistemi di trasmissione e di distribuzione)

- sistemi di comunicazione e di tecnologia dell'informazione (per esempio, le telecomunicazioni, i servizi radiotelevisivi, il software, l'hardware e le reti tra cui Internet)

- la finanza (per esempio, banche, strumenti finanziari e investimenti)

- il sistema sanitario (per esempio, gli ospedali, i servizi sanitari e di raccolta del sangue, i laboratori, il settore dei prodotti farmaceutici e i servizi di raccolta e salvataggio e di emergenza)

- l'approvvigionamento alimentare (per esempio, l'industria alimentare, i sistemi di sicurezza igienica, la produzione e la distribuzione all'ingrosso)

- l'approvvigionamento idrico (per esempio, i bacini, l'immagazzinamento, il trattamento, gli acquedotti)

- i trasporti (per esempio, i servizi portuali, aeroportuali e intermodali, i sistemi di trasporto collettivo su rotaia, i sistemi di controllo del traffico)

- la produzione, l'immagazzinamento e il trasporto di sostanze pericolose (per esempio, materiali chimici, biologici, radiologici e nucleari)

- l'amministrazione (per esempio, servizi cruciali, strutture, reti di informazione, beni e

patrimonio architettonico e naturale).

Questa attività della Commissione ha condotto nel 2008 all'approvazione della Direttiva 2008/114/CE che costituisce attualmente la base della legislazione UE in tema di Infrastrutture Critiche. La Direttiva contiene le istruzioni agli Stati Membri innanzitutto per l'individuazione delle Infrastrutture Critiche e in particolare delle Infrastrutture Critiche Europe (ICE), il quadro di riferimento per la collaborazione tra Stati e introduce delle misure di protezione, in particolare la valutazione dei rischi da effettuare a livello nazionale e i Piani di Sicurezza degli Operatori delle ICE. Queste ultime, che costituiscono un sottoinsieme delle IC individuate all'interno di ogni stato, sono quelle infrastrutture un malfunzionamento delle quali avrebbe impatti significativi su almeno un altro Stato Membro (quindi almeno su due Stati Membri dell'Unione). L'individuazione delle ICE è limitato nella Direttiva ai settori Energia (Elettricità, Petrolio e Gas) e Trasporti (Trasporto stradale, ferroviario, aereo, marittimo). La Direttiva consacra l'orientamento verso la gestione del rischio come approccio principe alla protezione delle IC. Quindi, oltre al piano di valutazione dei rischi a livello nazionale ogni gestore di IC designata come ICE dovrà disporre di un Piano di Sicurezza del'Operatore (PSO).

Seppur relativa alle infrastrutture critiche europee, nonché parziale, in quanto focalizzata soltanto su quelle dei settori dell'energia e trasporti, la Direttiva 2008/114/CE del Consiglio dell'8 dicembre 2008 definisce chiaramente le locuzioni: infrastruttura critica "*un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni*" e infrastruttura critica europea "*un'infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri. La rilevanza dell'impatto è valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture*".

Security Liason Officer (SLO)

Oltre alla predisposizione del PSO la Direttiva 2008/114/CE, prevede l'obbligo, per gli stati membri dell'Unione Europea, di designare uno SLO (acronimo di Security Liason Officer) per ogni singola infrastruttura critica Europea. La direttiva tuttavia, non fornisce ne indicazioni sul ruolo, né sulle responsabilità e competenze dello SLO.

Gli Stati membri devono quindi assicurare che tutte le ICE designate dispongano di un piano di sicurezza per gli operatori (PSO) e in aggiunta di un Security Liaison Officer (SLO): Funzionario

di Sicurezza che funge da collegamento tra il proprietario/l'operatore dell'Infrastruttura Critica e l'autorità nazionale responsabile della protezione dell'Infrastruttura, al fine di scambiare informazioni utili relative ai rischi e alle minacce individuati, riguardo alla ECI interessata.

Come previsto dalla Direttiva, la direzione designata dell'organizzazione deve nominare un SLO che, a prescindere dal suo ruolo principale, che è quello di punto di contatto (interfaccia), dovrà anche occuparsi della corretta attuazione della valutazione del rischio e del piano di sicurezza per gli operatori (PSO) di cui ne sarà garante.

La sua presenza è, infatti, essenziale, dal momento che, come ribadisce la Linea Guida all'implementazione della Direttiva, la loro presenza è il prerequisito per poter formulare il PSO.

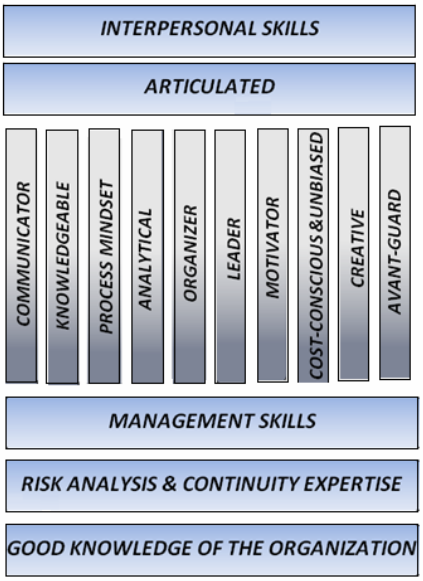

Fig. 3 – *Capacità e attitudini del Security Liason Officer (SLO)*

Una figura quindi che dovrebbe avere un'adeguata formazione tecnica, completata da spiccate capacità relazionali e gestionali (Fig. 3), fondamentali per garantire il funzionamento dei piani strategici per prevenire potenziali minacce, accidentali o indotte. Un profilo da individuare preferibilmente dentro la stessa infrastruttura per assicurare una migliore conoscenza di processi e attività interne. Essendo parte integrante della struttura aziendale, costui deve essere in grado di comunicare all'esterno le problematiche più rilevanti cui deve fare fronte l'impresa privata, e quindi di indirizzare il legislatore e gli apparati dello Stato nei processi decisionali e nell'adozione delle più efficaci strategie per la tutela del patrimonio aziendale del Paese. Tuttavia, il SLO deve possedere anche le conoscenze tecniche necessarie per comprendere appieno le informazioni provenienti dalle agenzie pubbliche, per poterle valutare efficacemente e per attuare le azioni opportune e adeguate in base al contesto di riferimento. Sono infatti definiti una serie di processi e

di scambi informativi di dati sensibili che possono essere gestiti solo da un professionista della sicurezza riconosciuto come tale, che sia in grado di parlare “lo stesso linguaggio” dell’Autorità pubblica.

Inoltre deve avere le conoscenze per poter, determinare le minacce, identificare i rischi, individuare gli elementi critici, organizzativi e collettivi, determinare la vulnerabilità di tali elementi alle minacce individuate, identificare specifici eventi e scenari e le loro possibili conseguenze. Saper effettuare una analisi del rischio in grado di valutare i controlli esistenti, determinare le conseguenze derivanti dal concretizzarsi del rischio, determinare le probabilità che da un tale rischio scaturiscano specifiche conseguenze, definire il livello di rischio su una combinazione di conseguenze e probabilità. Ed ancora poter effettuare una valutazione del rischio per determinarne la sua accettabilità e l’eventuale necessità di ulteriori misure di mitigazione. Stabilire le raccomandazioni e le strategie per i rischi residui, assegnare le responsabilità e verificare l’adeguatezza dei fondi necessari per le attività di gestione dei rischi per poi iniziare il ciclo di controllo e revisione finalizzato al rilevamento di eventuali cambiamenti.

Revisionare i rischi e le rispettive strategie di mitigazione, monitorare e revisionare i progressi compiuti e i risultati di ciascuna delle fasi del processo.

Recepimento della Direttiva e normativa nazionale

Con il D.Lgs n. 61 dell'11 aprile 2011 l'Italia ha recepito la direttiva 2008/114/CE dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione. Il decreto legislativo è entrato in vigore il 5 maggio 2011 a seguito della pubblicazione sulla Gazzetta Ufficiale (GU n. 102 del 4 maggio 2011). Quest’ultimo contiene le linee guida per l’individuazione delle ICE, istituisce il Nucleo Interministeriale Situazione e Pianificazione (NISP) e contiene la definizione del Piano di Sicurezza per gli Operatori delle Infrastrutture Critiche Europee. Al NISP (presso la Presidenza del Consiglio dei Ministri con la collaborazione dei Ministeri competenti) sono affidate l’individuazione e la designazione delle ICE, la struttura responsabile (Segreteria per le IC, “SIC”) per le attività tecniche e scientifiche necessarie per le funzioni del NISP e per i rapporti con la Commissione e gli altri Stati Membri interessati dalle ICE che l’Italia intende designare.

Tale decreto, al pari della direttiva recepita, prevede l’obbligo, per le predette infrastrutture attualmente ancora in corso di identificazione e designazione, di redigere un Piano di Sicurezza dell’Operatore (PSO).

Piano di Sicurezza dell’Operatore (PSO)

Nell’appendice “B” del D.Lgs n. 61 dell'11 aprile 2011 compaiono, in modo sintetico, alcune indicazioni circa gli elementi che il piano di sicurezza dell’operatore (PSO) deve contenere. Il PSO deve necessariamente comprendere:

1. L’individuazione degli elementi più importanti dell’infrastruttura. Cioè beni, risorse e attività la cui disponibilità dovrà essere sempre garantita e ai quali applicare le azioni preventive e difensive che permettano un’efficace protezione dell’infrastruttura.

2. L’analisi dei rischi, realizzata sulla prefigurazione degli scenari di rischio più rilevanti e allo scopo di individuare le vulnerabilità degli elementi dell’infrastruttura e le conseguenze che deriverebbero dal mancato funzionamento di ciascun elemento sulla funzionalità dell’intera infrastruttura.

3. L’identificazione delle misure e procedure più idonee alla prevenzione e protezione distinguendole tra misure permanenti (a) e misure ad applicazione graduata (b).

a) Le misure permanenti (utilizzate in modo continuativo) sono:

- I sistemi di protezione fisica (ad esempio gli strumenti di rilevazione, il controllo accessi, altre misure di prevenzione ed elementi di protezione).

- Le predisposizioni organizzative per l’allertamento comprese le procedure di gestione delle crisi (ad esempio il Crisis Management Plan, il Crisis Team).

- I sistemi di controllo e verifica esterni e interni allo scopo di testare le misure e procedure di sicurezza adottate.

- I sistemi di comunicazione (ad esempio, la comunicazione interna – esterna, il sistema di archiviazione e il trattamento dei documenti).

- Le attività di addestramento e accrescimento della consapevolezza del personale.

- I sistemi per la continuità del funzionamento dei supporti informatici (ad esempio le strategie di Disaster Recovery volte al salvataggio della tecnologia e dei dati che essa supporta).

b) Le misure ad applicazione graduata, sono quelle attivabili in relazione ai rischi e alle minacce contestualizzate nell’arco del tempo e quindi variabili al variare delle condizioni e livelli di rischio dell’infrastruttura.

Il rischio delle/nelle infrastrutture critiche

In termini generali, il rischio si definisce come il prodotto di tre variabili: la probabilità di vedere l'infrastruttura essere oggetto di minaccia, il livello di vulnerabilità della stessa e l’esposizione che rappresenta la stima del valore delle risorse a rischio presenti nell’area di danno della infrastruttura. Quest’ultima si riferisce alla natura, alla qualità e quantità degli elementi a rischio all’interno dell’infrastruttura esposta, quantificati in termini relativi (valore venale) o

assoluti (numero di persone, beni, etc.).

Risk = function (Hazard, Exposure, Vulnerability)

In formula il rischio specifico *Rj,t* rispetto all'evento j-esimo e a un prefissato valore di t, di una determinata infrastruttura, è traducibile nella seguente equazione:

$$R_{j,t} = \sum_{i=1}^{N_{j,t}} P_j . V_{i,j} . E_{i,j}$$

Dove:

Pj: Probabilità di accadimento di un evento j-esimo, in un certo periodo di tempo t, in una data infrastruttura[1] .

$V_{i,j}$: Vulnerabilità relativa allo scenario i-esimo, connesso all'evento j-esimo degli n elementi esposti;

$E_{i,j:}$ Valore degli n elementi esposti rispetto allo scenario i-esimo connesso all'evento j-esimo

Inoltre:

$N_{j,t}$ = numero degli scenari attesi relativi all'evento j-esimo nell'intervallo t

i = generico scenario atteso

j = generico evento disastroso

t = orizzonte temporale di previsione

Per rendere più agevole questa valutazione si è soliti considerare il danno *D* come prodotto della vulnerabilità *V (Vulnerability)* dell'elemento esposto e il suo valore *E* (*Exposure*).

Pertanto, se l'entità degli elementi a rischio può considerarsi indipendente dalla gravità dell'evento, abbiamo:

$$D_{i,j} = V_{i,j} \times E_{i,j}$$

dove:

- $D_{i,j}$ è il danno prodotto dallo scenario i-esimo, a seguito dell'evento j-esimo

E l'equazione precedente diviene:

$$R_{j,t} = \sum_{i=1}^{N_{j,t}} P_j . D_{i,j}$$

[1] Si tratta della probabilità che in un intervallo di tempo prefissato un fenomeno si presenti con il valore di uno dei suoi parametri caratteristici superiore ad un determinato valore di soglia. Essendo una probabilità è un numero maggiore di zero e minore di 1. Esprime il livello di attesa, il grado di fiducia, rispetto ad un evento specifico (p.es. sisma, evento meteorico, incidente, ecc.) di definita intensità (p.es. magnitudo del sisma, intensità di pioggia, entità di un incidente, ecc.) in un'area delimitata (p.es. infrastruttura, ambito urbano, ambito territoriale, area vasta, ecc.) in un determinato tempo (p.es. in un anno, in cento anni, ecc.).

Vulnerabilità delle infrastrutture critiche

La vulnerabilità di un sistema (Infrastruttura Critica) è funzione della sua suscettibilità (suscetpibility) al danneggiamento come probabilità complessiva al cambiamento conseguenza dell'evento (misura del grado di partecipazione all'evento) e della sua sensibilità (sensibility) al danneggiamento come stima probabilistica della velocità del sistema a perdere la propria configurazione iniziale (misura del tasso di cambiamento dovuto all'evento) e si manifesta quando nel sistema si vengono a determinare delle perdite di capacità. In generale, la suscettibilità non riguarda solo gli elementi fisici che caratterizzano il sistema, ma anche gli elementi antropici, le persone, intese come gruppi demografici (giovani, donne, anziani) e le comunità con i relativi mezzi di sostentamento, ossia la popolazione maggiormente soggetta a subire le conseguenze dannose del cambiamento (ad esempio i ceti più poveri). Sistemi suscettibili presentano una bassa resilienza.

Mentre la suscettibilità può configurarsi come la propensione al cambiamento in conseguenza di un evento estremo, la sensibilità stima invece la velocità con cui avviene questo cambiamento in conseguenza del quale il sistema perde la propria configurazione, a fronte di interferenze naturali e/o antropiche . Alcuni sistemi pur avendo tendenza a degradarsi si mantengono per lungo tempo in condizioni di stress e di recupero (sono suscettibili), altri invece sono sensibili al cambiamento e per ciò giungono rapidamente al collasso. Se un sistema risulta sensibile anche una modesta perturbazione può istantaneamente portare al collasso dell'intero sistema.

Un sistema dotato di alta sensibilità, una volta persi i propri caratteri, non solo velocemente collassa, ma presenta anche maggiori problematiche di recupero. I sistemi sensibili sono poco o affatto resistenti. Il termine sensibilità, sebbene si presti facilmente ad esprimere caratteri riguardanti parti od aree del territorio e per questo motivo sia ampiamente usato frequentemente in ambito territoriale e ambientale, è influenzato da diversi fattori sociologici, economici, politici e geografici, tra cui le relazioni sociali (in particolare razza, etnia, classe e genere), relazioni politico-economiche (caratteristiche istituzionali, risorse materiali a disposizione, occupazione) e gli attributi demografici (come l'età e lo stato riproduttivo). In definitiva mentre il concetto di suscettibilità è legato all'esistenza e sviluppo dei processi potenzialmente in grado di colpire un sistema e portare al cambiamento, il concetto di sensibilità è legato alla facilità con cui questi processi degenerativi possono avvenire. Qui l'enfasi è incentrata sulla rapidità del cambiamento, una sorta di "gradiente di trasformazione" per cui un dato sistema, a causa di forze naturali o artificiali, può subire una forte e repentina variazione della sua trasformazione divenendo così maggiormente vulnerabile.

L'espressione seguente ne aiuta la comprensione:

Vulnerabilità = sensibilità x suscettibilità.

La suscettibilità e la sensibilità sono concetti difficilmente quantificabili. Proprio per questo motivo anche la vulnerabilità risulta un concetto estremamente difficile da quantificare, in quanto si tratta di un processo dinamico complesso (reti sociali, economiche, politiche e naturali) e multidisciplinare che si differenzia di fatto, per ogni elemento esposto al rischio, in termini di azione e reazione verso elementi che possono manifestarsi singolarmente, ma anche simultaneamente. Tuttavia la valutazione della vulnerabilità è fondamentale per valutare il rischio e per aiutare i decisori politici ad elaborare risposte appropriate.

La vulnerabilità di un sistema può essere ridotta incrementando le sue capacità: la resistenza e la resilienza.

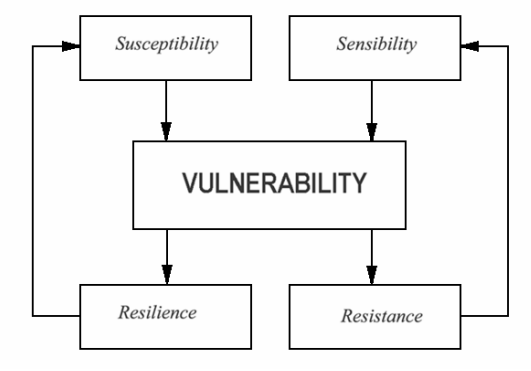

Fig. 4 – *Strategie di mitigazione della vulnerabilità*

La *resilienza* (capacità di un sistema di adattarsi all'evento) è legata alla capacità di ripristino: capacità del sistema di ripristinare le condizioni iniziali a seguito di una perturbazione causata da un evento dannoso.

La *resistenza* (capacità di un sistema di opporsi all'evento) è legata alla capacità del sistema di far fronte all'emergenza comprende sia quella istituzionale (Protezione Civile) sia quella messa in atto dai soggetti privati (Piano di Emergenza interno).

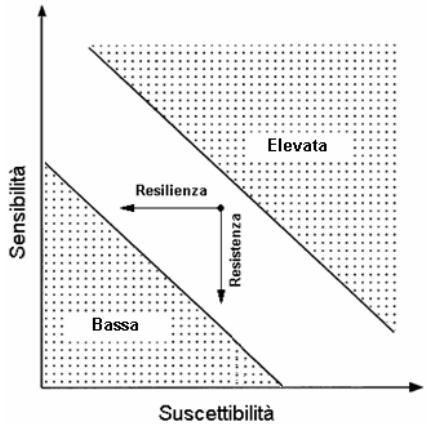

Fig. 5 – *Curve di vulnerabilità*

Non vi è ancora accordo sull'esatta terminologia e le definizioni proposte variano notevolmente a seconda del contesto tematico per il quale esse vengono utilizzate. Inoltre vi sono notevoli diversità anche quando sono usati nello stesso contesto. Le incomprensioni sono sorte quando le definizioni sono state trasferite dalle scienze fisiche e ingegneristiche alle scienze sociali.

Un risultato teorico significativo, che può essere raggiunto, consiste nel giungere a una condivisa definizione di questi concetti per attuare le migliori strategie di riduzione del rischio IC.

Resilienza delle infrastrutture critiche

La resilienza è in grado di accelerare il processo di adattamento con cui un sistema ritorna allo stato iniziale di funzionamento, rendendolo adatto al nuovo contesto dopo essere stato sottoposto a una perturbazione che l'ha allontanato da quello stato. Un sistema con bassa resilienza presenta un comportamento fragile. Dato che non è possibile proteggere permanentemente tutte le Infrastrutture Critiche e non è possibile eliminare tutti i rischi, il fattore resilienza assume particolare importanza. La condizione globale della resilienza delle infrastrutture critiche (CIR) ha subito dei drastici cambiamenti a causa della globalizzazione, del rapido progresso tecnologico, delle rivoluzioni dell'informazione e della comunicazione a cui si aggiungono anche tutte le incertezze causate dal conflitto globale e dal terrorismo. Le minacce e i rischi per la resilienza delle infrastrutture critiche stanno diventando quindi sempre più complessi. Nelle ultime ricerche riguardanti il concetto di resilienza, è evidente il crescente interesse circa lo studio degli aspetti salienti di questo fattore e di come la resilienza sia da considerare una "capacità del sistema", che è possibile costruire, sviluppare e gestire attraverso varie strategie legate al sistema e alla personalità individuale e alla cultura di chi a questo sistema fa parte.

Secondo questa prospettiva è necessario promuovere una cultura della resilienza per favorire l'investimento di programmi atti a facilitare, a seguito del verificarsi di un evento incidentale/calamitoso/doloso, l'attivazione delle risorse latenti presenti nel sistema capaci di assorbire i traumi e ripristinare le condizioni iniziali (continuare a funzionare). Sono le risorse disponibili che il sistema è in grado di mettere in campo a seguito di una perturbazione causata da un evento dannoso per migliorare la capacità di reagire, limitare i danni e ripristinare le condizioni iniziali; dall'efficacia dei piani di previsione, prevenzione e preparazione predisposti e da fattori quali le modalità di gestione dei territorio, la regolazione della densità e della distribuzione della popolazione, le iniziative di informazione e formazione delle comunità a rischio, l'affidabilità del dispositivo di protezione civile, il grado di conoscenza del rischio a tutti i livelli di governo e tra la popolazione, ecc.

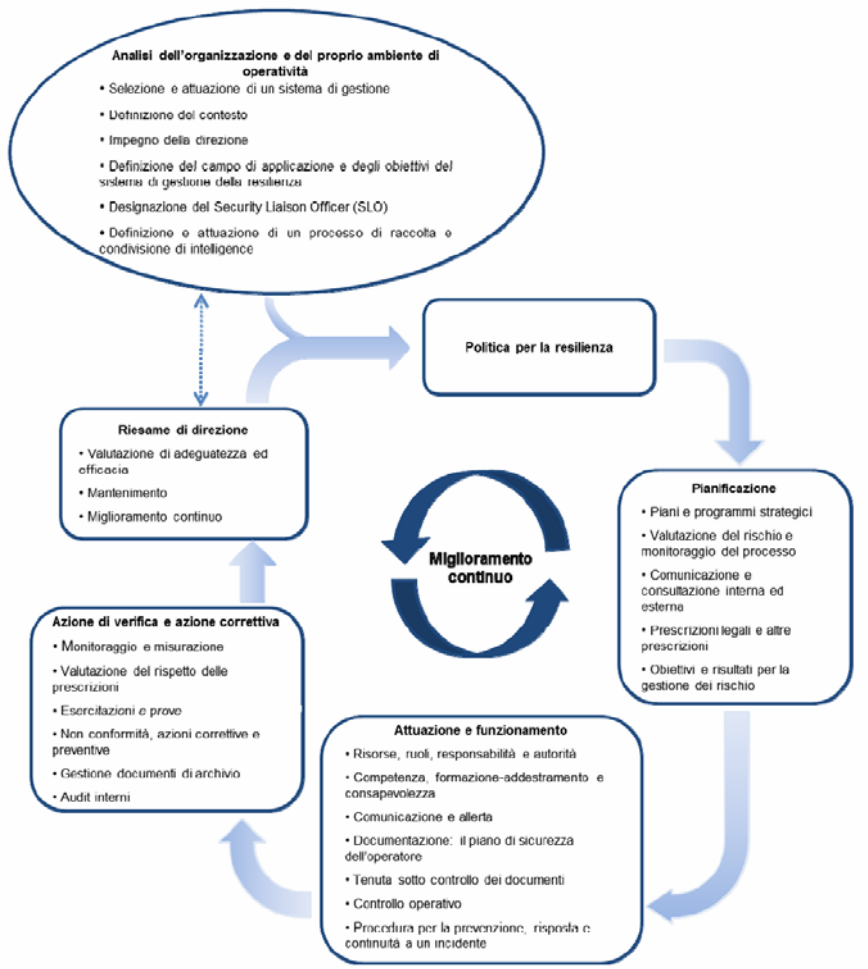

Fig. 6 – *Diagramma di flusso del sistema di gestione della resilienza (tratto da: Infrastrutture Critiche Sistema di gestione della resilienza – Requisiti - UNI/PdR 6:2014)*

Vogliamo sottolineare come quindi sia importante un *Sistema di Gestione della Resilienza delle Infrastrutture Critiche (SGRIC),* per consentire a un'organizzazione, in qualità di proprietario o operatore, di stabilire il contesto di riferimento, definire, pianificare, attuare, eseguire, verificare, riesaminare e migliorare la propria resilienza e un sistema di gestione delle emergenze.

Metodo della matrice di vulnerabilità

La vulnerabilità è un entità misurabile che tuttavia, senza un criterio di valutazione, è difficilmente quantificabile. La vulnerabilità di ogni elemento a rischio all'interno di un sistema può essere misurato con una matrice rappresentata da forme di diversa intensità corrispondenti ad altrettanto diversi stati critici del sistema.

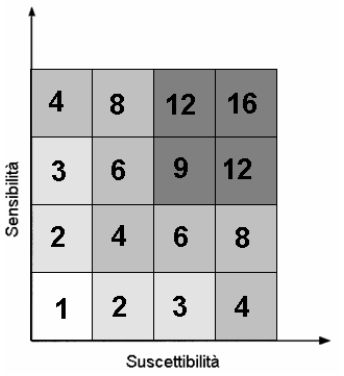

Fig. 7– *Matrice di vulnerabilità*

- V > 8 Valori elevati
- 4 < V < 8 Valori da ridurre aumentando la resilienza e resistenza del sistema
- 2 < V < 3 Valori bassi
- V = 1 Vulnerabilità trascurabile

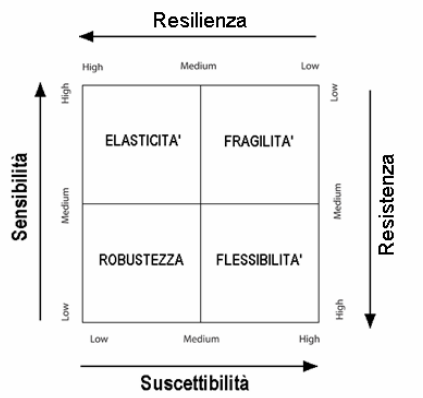

Fig. 8 – *Matrice di vulnerabilità e fattori di mitigazione*

Stati critici di un sistema: Stati di vulnerabilità

In questa memoria consideriamo un sistema capace, in funzione della sua vulnerabilità, di assumere 4 stati di vulnerabilità: flessibile o elastico, fragile o robusto corrispondenti ad altrettanti gradi di vulnerabilità. In questo caso occorre dare una definizione a questi concetti.

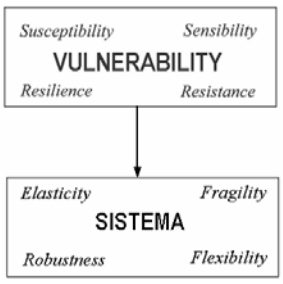

Fig. 9 – *Vulnerabilità e stati critici del sistema*

Sistemi robusti

Un sistema robusto è caratterizzato da una rete di capacità adattive, ovvero di risorse sufficientemente robuste, ridondanti e di rapido accesso da utilizzare per assorbire l'evento e riattivare un adeguato funzionamento del sistema .

Sistemi fragili

Il concetto di "fragilità" unisce due dimensioni: l'elevata attitudine di essere "ferito" da una particolare perturbazione (sia naturale o antropica), e l'elevata rapidità con cui questo avviene. In particolare, il rapporto tra l'attitudine a essere variato e la rapidità di cambiamento determina una caratteristica importante: la fragilità del sistema che influenza il grado di vulnerabilità elevandolo a valori inaccettabili. Un sistema diviene tanto più fragile quanto maggiore è la perdita della sua capacità di assorbire il mutamento diventando così molto suscettibile all'evento e quanto maggiore è la velocità con cui avviene questa perdita divenendo molto sensibile all'evento. La vulnerabilità in questo caso è rappresentata dalla "fragilità" del sistema .Emerge quindi un quadro concettuale che fornisce nuovi punti di vista e di lettura, inedite chiavi interpretative della fragilità che svelano nuove opportunità per ripensare e rinnovare nuove strategie di mitigazione del rischio delle IC.

Sistemi elastici

La vulnerabilità inoltre, è inevitabilmente associata anche alla capacità di adattamento di un sistema a seguito di un evento disastrogeno. Concetto che esprime il grado in cui un'entità riesce a conformarsi all'ambiente in cui opera manifestando un comportamento praticamente elastico. Nello specifico, si tratta di processi, che, da una parte, tendono a minimizzare le conseguenze negative della perturbazione introdotta e, dall'altra parte, tendono a sfruttare le opportunità positive di tale perturbazione. La capacità di adattamento di un dato sistema (elasticità) è tanto maggiore quanto maggiore è la resilienza e la sensibilità di tale sistema alla perturbazione introdotta o alle variazioni delle condizioni preesistenti.

Sistemi flessibili

Nell'interpretazione che viene data in questa sede, flessibilità equivale ad un adattamento variabile, mentre la rigidezza implica assenza di variabilità nel rapporto stimolo-risposta. Un sistema rigido, in conseguenza di un evento disastrogeno, non può adattarsi efficacemente per rispondere ai bisogni funzionali del sistema stesso. Un modo per ridurre la vulnerabilità è quello di incrementare la flessibilità del sistema, riducendo la sua rigidezza. In generale, elasticità non è sinonimo di flessibilità. L'elasticità è una proprietà costitutiva del sistema che sotto l'azione di determinate sollecitazioni genera deformazioni elastiche, accompagnate dal destarsi di reazioni interne, sforzi o tensioni, tendenti a far ritornare il sistema nelle condizioni primitive; la flessibilità

invece è una proprietà che dipende dal sistema e dalle condizioni al contorno che lo rendono tale, capace cioè di funzionare bene in un vasto campo di valori di perturbazione che lo potrebbero interessare.

La valutazione del rischio

La valutazione del rischio che interessa un'infrastruttura passa dunque necessariamente per un'analisi approfondita di questi aspetti. Quest'attività, ad elevato livello di specializzazione, necessita di sei passaggi operativi che consentono l'elaborazione di una adeguata analisi e valutazione dei rischi:

- comprensione dell'organizzazione operante all'interno dell'Infrastruttura Critica e determinazione delle risorse a rischio;
- individuazione dei fattori di rischio;
- determinazione delle probabilità di accadimento dell'evento ostile;
- previsione degli effetti che un evento ostile potrebbe provocare all'Infrastruttura Critica (vulnerabilità, esposizione);
- studio delle possibili strategie difensive e degli eventuali impatti sull'operatività dell'Infrastruttura Critica (misure di mitigazione);
- valutazione del rapporto costi/benefici nella strategia di protezione AS/AT applicabile al contesto.

Per rappresentare questi fattori disponiamo di varie modalità, quali ad esempio le curve F:N (frequenza/numero di eventi), le mappe di scenario, le mappe della perdita potenziale e le mappe di rischio che vengono utilizzate per regolamentare le attività di costruzione in aree vulnerabili, quali ad esempio pianure alluvionali, aree franose o sismiche, prima che le calamità si verifichino.

Anche in questo tipo di rischio è fondamentale la definizione del cd. albero dei guasti (Fault Tree Event), e l'albero degli eventi (Event Tree Analisys) cioè metodi logici che, di ogni evento, consentono, partendo dalle cause base o radici, di quantificare la probabilità di verificarsi dell'evento e dall'analisi degli scenari le conseguenze attese.

Il risultato è quello di giungere ad una valutazione quantitativa o semiquantitativa attraverso un indice sintetico, capace di misurare il rischio esistente e tale da fornire indicazioni circa gli obiettivi da raggiungere, le risorse, i mezzi ed i processi da attivare per l'integrazione del rischio nelle politiche di sviluppo.

Una volta quantificato il rischio, è poi necessario valutare la accettabilità o meno dello stesso rischio, sia sulla base delle norme vigenti che sulla base delle valutazioni rischio-beneficio. Non è infatti perseguibile, realisticamente, una politica di "azzeramento" del rischio per la insostenibilità

economica dei provvedimenti che dovrebbero essere assunti (si pensi all'intrinseca fragilità del territorio italiano, per oltre il 75% esposto a qualche rischio naturale). Si può quindi pensare, almeno in linea di principio, di arrivare a definire dei livelli di rischio accettabile, che individuino le combinazioni tollerabili del trinomio probabilità/vulnerabilità/esposizione.

Anche in questo caso si può immaginare di definire, in un diagramma, una curva di isorischio, contraddistinta dallo stesso valore delle combinazioni probabilità/vulnerabilità/esposizione, che separa due porzioni di spazio: area del rischio accettabile e area del rischio non accettabile, che consente di prendere delle decisioni per ridurre il rischio.

Fig. 10 – *Quantificazione del rischio*

La definizione di una soglia di rischio accettabile è importante nell'ambito dell'attività di prevenzione e di programmazione dello sviluppo e della salvaguardia di sistemi, poiché è il mezzo per valutare le priorità di intervento e di decidere i criteri di gestione del rischio.

Una volta che il livello accettabile di rischio è determinato, si passa alle misure di mitigazione dello stesso rischio (legali, tecniche, finanziarie, istituzionali e politiche) per ridurre il rischio al di sopra del livello di accettabilità. La valutazione dei rischi è quindi fondamentale per la attuazione di strategie di riduzione del rischio. Si tratta di un processo presente in ogni fase del processo di gestione del rischio, che consente di identificare le cause e le possibili soluzioni; per monitorare l'efficacia delle misure di riduzione del rischio ed il loro impatto reale; e valutare periodicamente le strategie globali e individuare di conseguenza gli adeguamenti necessari.

La valutazione dei rischi non è quindi un processo da fare una sola volta ma un processo da ripetere periodicamente.

Conclusioni

La strategia di sicurezza necessaria a garantire il corretto funzionamento delle Infrastrutture

Critiche (IC), sia in condizioni normali sia in condizioni di emergenza, richiede la predisposizione di misure, procedure e azioni mirate, da parte governativa, da parte delle aziende che le gestiscono, ma soprattutto da parte degli operatori del settore che agiscono all'interno di queste strutture, e che sono chiamati alla valutazione, mitigazione e gestione del rischio. Questo rischio è in qualche modo connesso con gli aspetti di fragilità intrinseca che contraddistinguono le moderne infrastrutture a causa della loro crescente complessità ed interdipendenza che, pur facendole essere robuste rispetto a tutta una classe di eventi/attacchi, risultano essere estremamente fragile nei confronti di specifici eventi estremi. L'evoluzione verso nuove forme di minacce come il terrorismo internazionale delocalizzato all'interno di contesti quotidiani, necessita di figure, sempre più competenti nella valutazione di scenari e circostanze in continuo mutamento, ossia persone le cui capacità sono tali da garantire la gestione complessiva del rilevanti processi o sotto-processi. La figura del Security Liaison Officer (SLO), che la Direttiva Europea 2008/114 prevede quale punto di riferimento per la protezione delle Infrastrutture Critiche Europee o, come dice la Direttiva stessa, di una sua figura equivalente, non esiste nel panorama formativo italiano, accademico e non.

Una figura che dovrebbe avere un'adeguata formazione tecnica, completata da spiccate capacità relazionali e gestionali, fondamentali per garantire il funzionamento dei piani strategici per prevenire potenziali minacce, accidentali o indotte. Idealmente in possesso di una Laurea o Master in Sicurezza delle Infrastrutture Critiche o altri titoli equivalenti, accompagnati dall' esperienza e/o formazione sul campo.

Per questo motivo le Università assumono un ruolo importantissimo nel momento in cui decidono di formare nuove figure professionali in grado di acquisire una conoscenza approfondita delle tecniche di decisione e gestione strategica della protezione di beni e di servizi vitali per il sistema Paese, offrendo le basi necessarie per comprendere gli scenari di rischio, individuare le tecniche di protezione ed apprendere la capacità critica di valutazione per formulare strategie aziendali e settoriali di efficace investimento preventivo. L'obiettivo è di formare il Security Manager o il Security Liaison Officer (SLO) previsto dalla Direttiva Europea, rivolto a responsabili della sicurezza di infrastrutture pubbliche e private, personale dei servizi di intelligence e funzionari istituzionali, fornendo loro gli strumenti decisionali per far fronte alle problematiche di protezione da minacce naturali e antropiche e gli elementi necessari per formulare politiche di investimento e piani per la gestione e il superamento di crisi.

Questi futuri professionisti devono essere in possesso delle capacità di management del rischio, di comunicazione e di organizzazione e delle conoscenze per l'applicazione di nuovi approcci e metodologie per ridurre le vulnerabilità e fronteggiare le nuove minacce a cui questi complessi sistemi, sempre più indispensabili per il nostro vivere quotidiano e la sicurezza e

prosperità di un Paese, sono soggetti.

Bibliografia

1) (GU n. 102 del 4-5-2011) DECRETO LEGISLATIVO 11 aprile 2011 , n. 61 Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione.

2) EUROPEAN COMMISSION-HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY-JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure CyberspacBrussels, 7.2.2013 JOIN(2013) 1 final.

3) Presidenza del Consiglio dei Ministri-Sistema di Informazione per la sicurezza della Repubblica – Relazione sulla politica dell'informazione per al sicurezza 2013-Relazione al Parlamento.

4) S. Personick, C. Patterson (Ed.), Critical Infrastructure Protection and the Law, an overview of key issues, National Academy of Engineering – National Research Council, The National Academies Press, 2003.

5) S. Rinaldi, J. Peerenboom, e T. Kelly, Identify, Understanding, and Analyzing Critical Infrastructure Interdependencies, IEEE Control System Magazine, pp. 11-25, dicembre 2001.

6) S. Ritter, J. Weber, Critical Infrastructure Protection: Survey of world-wide Activities, Critical Infrastructure Protection (CIP) Workshop, Frankfurt, 29-30 settembre, 2003.

7) D.A. Shea, Critical Infrastructure: Control Systems and Terrorist Threat, Report for Congress RL31534, The Library of Congress, 21 febbraio 2003.

8) N. Marotta, O. Zirilli, Disastri e Catastrofi, Maggioli Editore, 2015.