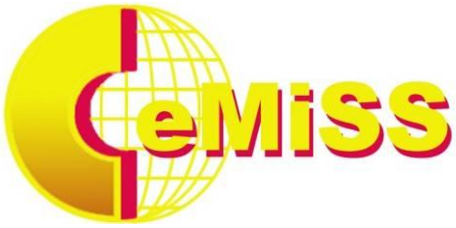


**Centro Militare di Studi Strategici**

**Rapporto di Ricerca 2011 - STEPI AE-SA-18**

# La strategia globale di protezione delle infrastrutture e risorse critiche contro gli attacchi terroristici

**di Prof. Roberto SETOLA**

**data di chiusura della ricerca: Settembre 2011**

*A mia moglie e mia figlia per il tempo e per l'affetto che ho sottratto loro.*

# INDICE

**LA STRATEGIA GLOBALE DI PROTEZIONE DELLE INFRASTRUTTURE E RISORSE CRITICHE CONTRO GLI ATTACCHI TERRORISTICI**

# SOMMARIO

## LA STRATEGIA GLOBALE DI PROTEZIONE DELLE INFRASTRUTTURE E RISORSE CRITICHE CONTRO GLI ATTACCHI TERRORISTICI

Le società industrializzate dipendono dal corretto funzionamento di un insieme di 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. Tali infrastrutture, un tempo sistemi sostanzialmente isolati e verticalmente integrati, sono divenuti sempre più interdipendenti al punto tale che un evento avverso che occorre ad una di esse, in una data localizzazione geografica, può propagarsi ad altre infrastrutture amplificando gli effetti negativi ed affliggendo soggetti dislocati anche in località molto remote rispetto all'origine dell'evento iniziale.

Diversi episodi occorsi nell'ultimo decennio hanno evidenziato come la crescente complessità di queste infrastrutture ha fatto sì che esse siano fragili rispetto ad eventi estremi al punto che, alcuni studiosi, ritengono quasi ineluttabile eventi catastrofici ai loro danni.

In questo contesto terroristi, o più in generale criminali, potrebbero effettuare attacchi contro tali infrastrutture, identificate come target attrattivi, sia per gli effetti materiali e psicologici legati al venir meno dei servizi essenziali che esse erogano alla popolazione, sia per la relativa facilità di individuazione ed accesso alle stesse.

L'estensione e la quantità di asset che compongono tali infrastrutture rende praticamente impossibile una loro protezione di tutti i singoli elementi costituenti, ciò anche in relazione al fatto che la tipologia delle minacce si va, a causa dei fenomeni di interdipendenza, amplificando e generalizzando.

La constatazione di tali minacce e la vulnerabilità delle infrastrutture critiche, ha portato a sviluppare specifiche strategie genericamente indicate come CIP – Critical Infrastructure Protection. Tali strategie, adottando un approccio All-Hazard, mirano a sviluppare metodologie, strumenti e norme che puntano in primo luogo a ridurre l'impatto negativo che un malfunzionamento, accidentale o doloso, di queste infrastrutture ha sulla

popolazione, sull'economia e sulla società e a favorire il ripristino delle normali funzionalità.

Questo mutato contesto è analizzato nei **Capitoli 2** e **3** con l'obiettivo di illustrare quali sono le problematiche connesse con l'attuale scenario architetturale sotteso alle infrastrutture critiche.

Il **Capitolo 4** è dedicato ad introdurre strumenti per la valutazione del rischio connesso con la sicurezza di tali infrastrutture e, nello specifico, con eventi caratterizzati da una bassissima probabilità di accadimento (eventi estremi), quali appunto le azioni terroristiche o dolose, nonché con la qualificazione e quantificazione delle conseguenze di tali eventi in scenari complessi caratterizzati da ampi e diffusi fenomeni di interdipendenza.

Tale aspetto è analizzato in maggior dettaglio nella seconda parte del documento dove, nel **Capitolo 6**, è effettuata una disamina del fenomeno delle interdipendenze scomponendolo nelle diverse dimensioni che caratterizzano questo complesso fenomeno.

Il **Capitolo 7** si sofferma su quelle che sono le problematiche connesse con la cyber sicurezza di queste infrastrutture, andando a dettagliare le problematiche relative alla minaccia cyber per i sistemi di monitoraggio e controllo utilizzati per la supervisione delle diverse infrastrutture.

Il successivo **Capitolo 8** affronta, invece, il problema della qualificazione e quantificazione degli effetti secondari dovuti ai fenomeni di propagazione a cascata delle conseguenze di eventi negativi. Nello specifico il capitolo illustra tre diverse, e per certi aspetti complementari, metodologie di analisi.

La valutazione dell'attrattività dei diversi asset che compongono le diverse infrastrutture critiche quali possibili obiettivi di azioni terroristiche è analizzato nel **Capitolo 9** che termina la sezione.

I **Capitoli 10** e **11** raccolgono una disamina di alcune delle "best-practice" a livello internazionale, con uno speciale focus, sul ruolo del Ministero delle Difesa e, più in generale sulle strategie adottate dai diversi governi per la protezione delle Infrastrutture Critiche.

L’analisi della situazione italiana è effettuata nel **Capitolo 12** dove, nell’evidenziare l’assenza di uno specifico piano strategico, si illustrano quelli che sono i ruoli assunti dai diversi organismi e si delineano quelle che dovrebbero essere le responsabilità ed i ruoli del Ministero della Difesa.

Il successivo **Capitolo 13** effettua un'analisi di quelli che sono i costi per la protezione delle infrastrutture critiche evidenziando la necessità, a casa dell’impossibilità di sostenere gli attuali costi sociali della security, di delineare diversi modelli di business che rendano sostenibili nel tempo tali oneri.

Il **Capitolo 14** chiude il lo studio con alcune considerazioni conclusive.

**Le Infrastrutture Critiche**

**GENERALE**

# 1 Introduzione

Da più parti si è consolidata l'affermazione che il tragico attentato alle Twin Towers del 2001 abbia "cambiato" il mondo, ed infatti l'eco di quell'evento a dieci anni dal suo accadere è ancora molto forte al punto che è ancora indicato, soprattutto in ambito anglosassone, come semplicemente (o terribilmente) il "9/11"[1] senza alcuna necessità di specificare in che anno è accaduto. Questo per una serie di motivi "generalisti", che vanno dal tragico bilancio di morti innocenti che ha comportato, alle modalità di esecuzione, al simbolismo dell'obiettivo (il cuore economico del 'Satana Americano'). A questi aspetti, in un'ottica più tecnica, occorre aggiungerne almeno altri due che, dal punto di vista delle strategie di anti-terrorismo (o più in generale di sicurezza nazionale), rappresentano elementi di estrema rilevanza che riguardano la *weapon*[2] utilizzata e i così detti effetti secondari (o effetti di secondo ordine).

Infatti, mentre di per sé le azioni terroristiche contro l'infrastruttura aeronautica, ed in particolare i dirottamenti di aeromobili, sono una tragica realtà fin dal 1961 quando ci fu il primo dirottamento di un aereo civile di risonanza internazionale, con il 9/11 l'azione contro i velivoli non è stato un fine, bensì un mezzo. Ossia l'infrastruttura aeronautica ha assunto il ruolo di **vettore** da sfruttare per portare a compimento un attacco contro un obiettivo non direttamente legato al mondo aeronautico.

L'altro aspetto, sebbene non sia ben chiaro fino a che punto previsto dai terroristi, ma sicuramente da essi successivamente ampiamente cavalcato, è stato quello dei così detti effetti secondari. Purtroppo il bilancio di oltre 3.000 morti è stato solo uno degli effetti dell'attentato e, per quanto sia cinico a dirsi, per molti analisti non quello più impattante.

[1] Si ricorda che nel mondo anglosassone la data è nel formato mese-giorno-anno.
[2] Arma di distruzione di massa.

Infatti, il crollo delle Twin Towers provocò l'interruzione della fornitura di energia elettrica, gas e servizi telefonici ad un'ampia zona di Manhattan. La presenza nelle vicinanze dell'evento d'importanti nodi di telecomunicazione provocò disservizi nelle comunicazioni e nella fruizione di Internet ad una platea di utenti molto ampia (anche in Italia si ebbero delle ripercussioni) e questo anche a causa dell'impossibilità di operare in loco da parte dei tecnici e/o di rifornire di gasolio i generatori di emergenza. L'azione terroristica indusse immediatamente sui mercati finanziari mondiali ripercussioni sia dirette (a causa della distruzione di parte dell'infrastruttura telematica a servizio di Wall Street) che indirette (legate al crollo di fiducia degli investitori), e sull'intero comparto del trasporto aereo con danni diretti ed indiretti dell'ordine di centinaia di miliardi di dollari[3].

Questi effetti secondari sono stati possibili, indotti e amplificati a causa del mutato contesto socio-tecnologico che caratterizza le attuali società post-industrializzate. Infatti, la necessità di offrire servizi innovativi a costi contenuti con una sempre maggiore attenzione all'efficienza, ha imposto profondi cambiamenti sul piano architetturale, tecnologico ed economico con l'affermazione del paradigma della globalizzazione.

Tale fenomeno, unitamente alla consequenziale liberalizzazione di molti mercati, un tempo esclusivo appannaggio di aziende monopolistiche di stato, ha comportato da un lato una frammentazione concorrenziale con un aumento esponenziale dei soggetti coinvolti in modo più o meno diretto nella gestione e nel controllo delle diverse infrastrutture tecnologiche alla base delle economie occidentali e, dall'altro, la necessità che ogni singolo operatore si concentri in modo pressoché esclusivo sulle attività specifiche del proprio core-business esternalizzando tutti i servizi ancillari (spesso anche, purtroppo, quelli strettamente connessi con la sicurezza e la continuità di esercizio delle proprie infrastrutture – come evidenziato anche con il black-out in Italia del settembre 2003).

Gli stessi fenomeni, unitamente alla pervasiva e omogenea diffusione delle tecnologie proprie del settore ICT (Information and Telecommunication Technologies), hanno fatto sì, per altro, che il funzionamento di tali infrastrutture fosse sempre più mutuamente dipendente non solo  su scala nazionale, ma planetaria, con la conseguenza che subiamo gli effetti di eventi che occorrono a diverse migliaia di chilometri da noi.

[3] Statement of Brian Jenkins to the National Commission on Terrorist Attacks Upon the United States http://www.9-11commission.gov/hearings/hearing1/witness_jenkins.htm

Nel breve spazio del primo decennio del millennio abbiamo avuto diversi episodi che evidenziano come le nostre infrastrutture siano fragili rispetto a categorie di eventi fino ad ora non adeguatamente considerate e che potrebbero, come purtroppo già accaduto, essere sfruttate da gruppi criminali, terroristici o anche da nazioni avversarie per determinare situazioni di pericolo, panico, carenza di fiducia ovvero destabilizzare e creare danni al nostro paese.

# 2 Infrastrutture e Risorse Critiche

Le società moderne dipendono sempre di più dall'esistenza e dal corretto funzionamento di un insieme d'infrastrutture tecnologiche quali: reti di telecomunicazione, reti di calcolatori, reti di trasporto (automobilistico, ferroviario, aereo, ecc.), sistema sanitario, circuiti bancari e finanziari, sistemi idrici, ecc. Per la loro rilevanza queste infrastrutture sono generalmente indicate come **Infrastrutture Critiche (*Critical Infrastructures*)**[4] poiché un loro non corretto funzionamento, anche per un periodo di tempo limitato, può incidere negativamente sull'economia di singoli o di gruppi, comportando perdite economiche se non addirittura mettendo a rischio la sicurezza di cose e persone. Secondo una definizione:

> *Critical Infrastructures are **systems and assets**, whether **physical or virtual**, so vital for a state that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*

**[US Patriot Act 2001[5]]**

ossia un insieme di siti/risorse e sistemi, tanto fisici che cyber il cui non corretto funzionamento potrebbe comportare un impatto sulla sicurezza nazionale, l'economia del paese, la salute e la sicurezza dei cittadini.

[4] Elgin M. Brunner and Manuel Suter, *International CIIP Handbook 2008/2009*, Center for Security Studies (CSS), ETH Zurich, 2008.
[5] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

La seguente definizione del termine “infrastruttura”

> An **infrastructure** is *“a network of independent, mostly private-owned, man-made systems that function collaboratively and synergically produce and distribute a continuous flow of essential goods and services”.*

**[PDD-63, 1998[6]]**

evidenzia la natura per lo più privata della proprietà/gestione di tali complessi sistemi.

Una definizione leggermente diversa di Infrastruttura Critica è quella proposta dal *Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche* istituito presso il Dipartimento per l’Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri che, nel suo rapporto conclusivo sulla situazione italiana così definiva le infrastrutture critiche:

> ***Complesso di reti e sistemi*** *che includono industrie, istituzioni, e strutture di distribuzione* ***che*** *operando in modo sinergico* ***producono un flusso continuato di merci e servizi essenziali*** *per l’organizzazione, la funzionalità e la stabilità economica di un moderno paese industrializzato e la cui distruzione o temporanea indisponibilità può indurre un impatto debilitante sull’economia, la vita quotidiana o le capacità di difesa di un paese.*

**[PIC, 2004[7]]**

Questa definizione evidenzia maggiormente l’aspetto di network e sistemico che caratterizza tali infrastrutture, ciò a sottolineare, in qualche modo in contrapposizione alla consolidata dottrina della protezione degli “obiettivi sensibili”, che l’aspetto “critico” non è tanto nel valore del singolo componente, quanto piuttosto nella sua valenza sistemica o, in

[6] Presidential Decision Directive 63 (PDD 63) on May 22, 1998.
[7] Presidenza del Consiglio dei Ministri, Dipartimento per l’Innovazione e le Tecnologie, *Protezione delle Infrastrutture Critiche Informatizzate*, Marzo 2004.
http://www.infrastrutturecritiche.it/aiic/index.php?option=com_docman&task=doc_view&gid=38&tmpl=component&format=raw&Itemid=103

altri termini, in relazione alla capacità della specifica infrastruttura di erogare ai "clienti" i propri servizi essenziali.

Volendo fare un'esemplificazione che evidenzi come sia andata aumentando la rilevanza della tematica nel corso degli anni, si può far riferimento al sistema finanziario e, nello specifico, alla sicurezza di una banca. Se fino a qualche decennio fa era "sufficiente" garantire la sicurezza del CED (Centro Elaborazione Dati), delle diverse filiali e dei collegamenti proprietari che connettevano le filiali con il CED, con l'introduzione del home-banking limitarsi a garantire la sicurezza di questi soli elementi non è più sufficiente, in quanto esso non garantisce che gli utenti remoti possano fruire del servizio di home-banking. Per ottenere ciò è necessario che l'utente finale abbia la necessaria connettività (oltre che altri servizi quali l'elettricità), servizio questo che è per lo più al di fuori della sfera di controllo dell'operatore bancario, ma un cui malfunzionamento incide profondamente sulla capacità di erogazione del servizio di home-banking. Il tutto si complica ulteriormente nel momento in cui il servizio in Italia è erogato appoggiandosi a operatori e/o infrastrutture collocati al di fuori dei confini nazionali.

Di per sé ognuna delle infrastrutture critiche è un sistema complesso (complex network) distribuito geograficamente, caratterizzato da un comportamento dinamico fortemente non lineare (ovvero che in situazioni particolari, anche piccoli eventi che in condizioni nominali sarebbero assorbiti senza conseguenze palesi, possono provocare una forte alterazione nelle funzionalità del sistema) e che interagisce sia con le altre infrastrutture critiche sia con diversi soggetti: gestori, utenti, ecc. Per molte di queste infrastrutture non esiste nessuna singola entità che abbia il completo controllo o anche solo la completa conoscenza del sistema, né esiste alcuna entità in grado di monitorare globalmente il sistema, né di gestirlo in modo centralizzato.

Sebbene diversi tentativi siano stati fatti, non esiste una definizione operativa di quali siano le infrastrutture critiche per una nazione[8]. Nel corso degli anni i vari governi hanno stilato elenchi che individuano settori nell'ambito dei quali operano le infrastrutture critiche.

[8] In Italia, alla data di compilazione del presente studio, il tema di individuare quali siano le Infrastrutture Critiche Nazionali è delegato alla Commissione Interministeriale Tecnica della Difesa Civile (CITDC) del Ministero dell'Interno i cui lavori non sono ancora conclusi.

Nello specifico, questi sono gli 11 settori individuati come critici dal governo americano:

1. Agriculture and Food
2. Water
3. Public Health
4. Emergency Services
5. Defense Industrial Base
6. Information and Telecommunications
7. Energy
8. Transportation
9. Banking and Finance
10. Chemical Industry and Hazardous
11. Postal and Shipping

**[US Physical Protection, 2003[9]]**

a cui occorre aggiungere le cinque aree indicate inizialmente come *key-assets* (successivamente etichettate come *key-resources*): National Monuments and Icons, Nuclear Power Plants, Dams, Government Facilities, and Commercial Key Assets.

[9] Department of Homeland Security, *Phisical Protection of Facilities and Real Properties*, Aprile 2003.

Dal canto suo la Commissione Europea, dopo un ampio dibattito, con la promulgazione della Direttiva Comunitaria COM(2006)787 ha individuato i seguenti 11 settori critici con i relativi sotto-settori:

| Sector | | Sub-sector | |
|---|---|---|---|
| I | Energy | 1 | Oil and gas production, refining, treatment, storage and distribution by pipelines |
| | | 2 | Electricity generation and transmission |
| II | Nuclear industry | 3 | Production and storage/processing of nuclear substances |
| III | Information, Communication Technologies, ICT | 4 | Information system and network protection |
| | | 5 | Instrumentation automation and control systems (SCADA etc.) |
| | | 6 | Internet |
| | | 7 | Provision of fixed telecommunications |
| | | 8 | Provision of mobile telecommunications |
| | | 9 | Radio communication and navigation |
| | | 10 | Satellite communication |
| | | 11 | Broadcasting |
| IV | Water | 12 | Provision of drinking water |
| | | 13 | Control of water quality |
| | | 14 | Stemming and control of water quantity |
| V | Food | 15 | Provision of food and safeguarding food safety and security |
| VI | Health | 16 | Medical and hospital care |
| | | 17 | Medicines, serums, vaccines and pharmaceuticals |
| | | 18 | Bio-laboratories and bio-agents |
| VII | Financial | 19 | Payment and securities clearing and settlement infrastructures and systems |
| | | 20 | Regulated markets |
| VIII | Transport | 21 | Road transport |
| | | 22 | Rail transport |
| | | 23 | Air transport |
| | | 24 | Inland waterways transport |
| | | 25 | Ocean and short-sea shipping |
| IX | Chemical industry | 26 | Production and storage/processing of chemical substances |
| | | 27 | Pipelines of dangerous goods (chemical substances) |
| X | Space | 28 | Space |
| XI | Research facilities | 29 | Research facilities |

**[COM(2006)787[10]]**

[10] Proposta di direttiva del Consiglio relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, COM(2006)787. Dicembre 2006.

È immediato costatare che, oltre ad una differenza sul numero dei settori critici, esistono alcune differenze nella loro identificazione che rispecchiano la diversa rilevanza che i diversi settori ricoprono nella cultura e nella società americana rispetto a quella europea. Infatti, mentre nella lista predisposta dal governo americano troviamo settori quali l'industria per la difesa, i servizi postali, l'industria chimica e, esplicitamente, l'agricoltura, nella lista dei settori critici europei compare in modo esplicito un riferimento ai servizi erogati dalla Pubblica Amministrazione.

A livello internazionale l'intera problematica riguardante la protezione di queste infrastrutture, nella loro globalità, è genericamente indicata con il termine **CIP** – ***Critical Infrastructure Protection***. Nell'ambito della problematica della CIP, quando si focalizza l'attenzione principalmente sugli aspetti connessi con la presenza (e la vulnerabilità indotta e/o costituita) del cyberspace, si tende a parlare di **CIIP** – ***Critical Information Infrastructure Protection***. In realtà il confine fra CIP e CIIP è molto labile a causa delle strettissime interrelazioni esistenti fra il mondo fisico (tangibile) e il mondo virtuale (delle informazioni) al punto che, a prescindere dalla causa prima, un guasto tende sempre ad affliggere entrambi i mondi. Per questo motivo in letteratura i due termini sono usati spesso come sinonimi ed alcuni autori hanno suggerito l'uso dell'acronimo CI(I)P. Ciononostante, tale suddivisione è utile in quanto favorisce la percezione della necessità di considerare, parallelamente agli aspetti di sicurezza fisica, anche la problematica indotta dalla presenza del cyberspace.

Una disamina delle principali attività che i diversi governi hanno o stanno mettendo in atto in tale ambito è contenuto nel "**CIIP Handbook**" del ETH di Zurigo[11].

Gli Stati Uniti furono i primi, nel 1996, a percepire l'importanza della problematica iniziando una serie di analisi e studi che si concretizzarono, nel 1998, nell'emanazione da parte del presidente Clinton delle ***Presidential Decision Directives 62*** *e* ***63***.

[11] http://e-collection.library.ethz.ch/view/eth:31123

Esse, nell'identificare 8 settori critici[12], si ponevano quale obiettivo lo sviluppo di un programma mirato alla salvaguardia e protezione di queste infrastrutture per far sì che, come si legge nella prefazione della Direttiva a firma del presidente Clinton:

> *Any interruption or manipulation of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.* **[13]**

**[PDD-63, 1998]**

LA PDD 63 richiamò un ampio interesse oltre che negli Stati Uniti anche in Germania e in tutti i paesi anglofoni. Purtroppo, possiamo dire con il senno di poi, che l'attenzione sollevata dalle giuste considerazioni portate dal rapporto finirono con confluire nell'alveo delle attività per il cosiddetto *Millennium Bug (Y2K)*[14] con la conseguenza che si confusero le due problematiche. Il tutto comportò che, sebbene a livello mondiale il passaggio del millennio non comportò (grazie alle azioni di ammodernamento e sostituzione di molti dei sistemi legacy in esercizio) alcun reale problema ai sistemi informativi, le soluzioni adottate contribuirono, invece, ad acuire il problema (come vedremo meglio in seguito) delle infrastrutture critiche in quanto nel brevissimo volgere di meno di un lustro la stragrande maggioranza delle infrastrutture critiche dismise l'uso di hardware, software, protocolli e linee dedicate per passare rapidamente a soluzioni "standard".

Gli eventi dell'11 settembre hanno fornito un drammatico impulso a tutte le attività connesse con la sicurezza nazionale. In particolare, la difesa delle infrastrutture critiche è divenuta uno degli elementi basilari dell'impianto del Department of Homeland Security, come specificato dal **HSPD-7 "*Critical Infrastructure Identification, Prioritization, and Protection*"**[15], le cui linee strategiche erano state delineate nei due documenti emanati

[12] PDD 63 identificava quali settori critici: telecomunicazioni, sistemi di produzione dell'elettricità, gas e petroli, attività bancarie e finanza, trasporti, forniture idriche, servizi pubblici e servizi di emergenza. La differenza fra quanto successivamente individuato nel documento "Homeland Security Presidential Directive 7" del dicembre 2003 aiuta a cogliere la complessità della tematica visto che il solo concetto di quali siano gli ambiti "essenziali" per una nazione varia anche con l'evoluzione del contesto sociale e tecnologico.

[13] La PDD 63 concedeva alle agenzie governative cinque anni di tempo per mettere in atto quanti necessario. Per uno scherzo del destino esattamente cinque anni dopo, nel 2003, gli USA hanno sperimentato il più grande black-out della loro storia.

[14] Ovvero il problema legato al fatto che in molti sistemi informatici sviluppati fino alla metà degli anni '80 la data era codificata solo con due cifre, per cui al passaggio di millennio potevano insorgere problemi di incoerenza legati al fatto che la data 00 sarebbe stata interpretata come 1900 e non come 2000.

[15] Homeland Security Presidential Directive-7 on Critical Infrastructure Identification, Prioritization, and Protection, December 2003.

contemporaneamente dalla Casa Bianca nel febbraio del 2003 per la protezione, rispettivamente, del **mondo fisico**[16] e **di quello cyber**[17].

Nel contempo, con il duplice obiettivo di salvaguardare la sicurezza nazionale e la sicurezza ed operatività delle basi militari esistenti nei diversi paesi, gli USA attivarono un'azione di *moral suasion* nei confronti dei governi alleati, affinché anch'essi ponessero il problema della Protezione delle Infrastrutture Critiche nelle rispettive agende con un'attenzione preliminare e prevalente per la minaccia cyber (e quindi per le attività di Critical Information Infrastructure Protection – CIIP).

Tali iniziative portarono il G8 ad approvare gli "*eleven principles*", che dovrebbero ispirare la politica dei singoli stati in tema di protezione delle infrastrutture critiche informatizzate, principi che vennero poi ripresi e ribaditi nella risoluzione ONU n. 58/199 "***Creation of a global culture of cybersecurity and the protection of critical information infrastructures*"**[18] adottata dall'Assemblea Generale delle Nazioni Unite il 23 dic 2003.

L'azione degli USA ottenne solo in parte gli effetti sperati dal governo americano, in quanto solo alcune nazioni (nello specifico Canada, UK, Australia, in parte Germania ed i paesi scandinavi) attivarono specifiche iniziative per innalzare la protezione delle loro infrastrutture critiche (informatizzate).

Lo scarso successo di tali iniziative era, in parte, dovuto al tipo di obiettivo che con esse si voleva perseguire, ovvero un contrasto al terrorismo di natura confessionale individuato come l'unico pericolo per la sicurezza delle singole nazioni. Una tale impostazione, essendo estranea alla cultura europea, ebbe a trovare maggiore resistenza, tanto è vero che nella consultazione che avviò la **Commissione Europea**[19] vi era la richiesta di evidenziare quale sarebbe dovuto essere il focus della redigenda normativa, ossia se prendere in considerazione in via esclusiva la minaccia di origine terroristica oppure se adottare l'approccio più ampio del ***All-Hazard***.

Gli attentati di Madrid e, successivamente, quello di Londra, evidenziando come il rischio del terrorismo medio-orientale fosse concreto anche in Europa, convinsero la

[16] Office of the President. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. February, 2003
[17] Office of the President. The National Strategy to Secure Cyberspace. February, 2003.
[18] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf
[19] EU Commision Green Paper on a European Programme for Critical Infrastructure Protection COM(2005)576, 2005- http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

Commissione Europea ed i vari Stati Membri della necessità ed urgenza di fare qualcosa. Ciononostante, anche alla luce dell'esperienza dei black-out del 2003 in Nord America ed in Italia, la tematica ebbe ad assumere da subito in Europa la più ampia connotazione del ***All-Hazard*** (sebbene con un'attenzione prioritaria alla minaccia terroristica).

Dal suo canto la politica statunitense mantenne invariato il focus, tanto che ancora nel documento "*Interim National Infrastructure Protection Plan*" del febbraio 2005 l'obiettivo era specificato come

> *Build a safer … America by enhancing protection of the CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy.*

**[Interim National Infrastructure Protection Plan, 2005]**

Sulla scorta, però, del disastro dovuto all'uragano Katrina, nel breve volgere di un anno l'amministrazione americana fu costretta ad un totale ripensamento di quelli che dovevano essere gli obiettivi della strategia per la difesa delle infrastrutture critiche nazionali, tanto è che nel documento *National Infrastructure Protection Plan,* emanato nel 2006, l'obiettivo diventa:

> ***Direct terrorist attacks*** *and* ***natural***, ***manmade***, *or* ***technological hazards*** *could produce catastrophic losses …. Attacks using components of CI/KR as weapons could have even more devastating physical and psychological consequences.*

**[National Infrastructure Protection Plan, 2006[20]]**

dove, quindi, alla minaccia terroristica (indicata ancora quale la prima minaccia) si affiancano, praticamente sullo stesso piano e nell'ambito delle stesse finalità, anche tutti quegli eventi di carattere naturale, causati dall'uomo o dovuti a guasti delle infrastrutture tecnologiche che potrebbero minare il corretto funzionamento delle diverse infrastrutture critiche.

[20] http://www.dhs.gov/files/programs/editorial_0827.shtm

Oggi si è quindi consolidata a livello mondiale un'impostazione più generale per quella che è la protezione delle infrastrutture critiche, il cui obiettivo è quello di prevenire e contrastare minacce di qualunque origine nei confronti delle diverse infrastrutture con il fine di preservarne le capacità di erogazione dei relativi servizi e favorire, in caso di anomalie, il rapido ripristino delle condizioni di normalità.

In quest'ottica il termine All-Hazard ha assunto la seguente valenza:

> ***All-hazard:*** *naturally occurring event, human induced events (both intentional and non-intentional) and technology caused events with potential impact on organization, community or society and environment on which it.*

**[ISO/CD 22300[21]]**

[21] http://www.iso.org/iso/home.html ISO/TC223 Social Security.

# 3 Cambiamento di Contesto

La prima domanda che ci si pone imbattendosi nell'ambito della "Protezione delle Infrastrutture Critiche" è se questa tematica è "solo" una nuova etichetta per quelle attività di protezione, antiterrorismo e, più in generale, di sicurezza già da sempre in atto, oppure se essa sottende qualcosa di nuovo e/o diverso.

Fondamentalmente le diverse infrastrutture critiche sono state, fin dalle loro origini, oggetto di attentati e azioni terroristiche e per esse si è sviluppata negli anni una consolidata cultura della sicurezza.

L'impressione, però, è che tutto questo non sia più sufficiente.

Ciò è dovuto al fatto che tutte queste infrastrutture, un tempo sistemi sostanzialmente indipendenti e verticalmente integrati, sono divenute sempre più connesse/dipendenti le une dalle altre al punto che, il singolo gestore/proprietario, non è più in grado di garantire in maniera autonoma l'operatività ed il corretto funzionamento della propria infrastruttura e della relativa filiera. Per queste ragioni è obbligato a dipendere dalle capacità dei suoi "fornitori" di fare altrettanto in situazioni in cui, il più delle volte, questi ultimi a loro volta dipendono, in modo diretto o indiretto, dal corretto funzionamento della prima infrastruttura.

Una serie di motivazioni di carattere sociale e tecnologico, quali la globalizzazione dei mercati e la liberalizzazione degli stessi con il conseguente venir meno degli operatori monopolistici nazionali, hanno fatto sì che i singoli operatori si siano dovuti sempre più concentrare su quello che era il loro core-business esternalizzando la gran parte dei servizi ancillari.

Il tutto ha comportato, come illustrato nella figura 1, una forte crescita dell'integrazione delle diverse infrastrutture in termini di interoperabilità.

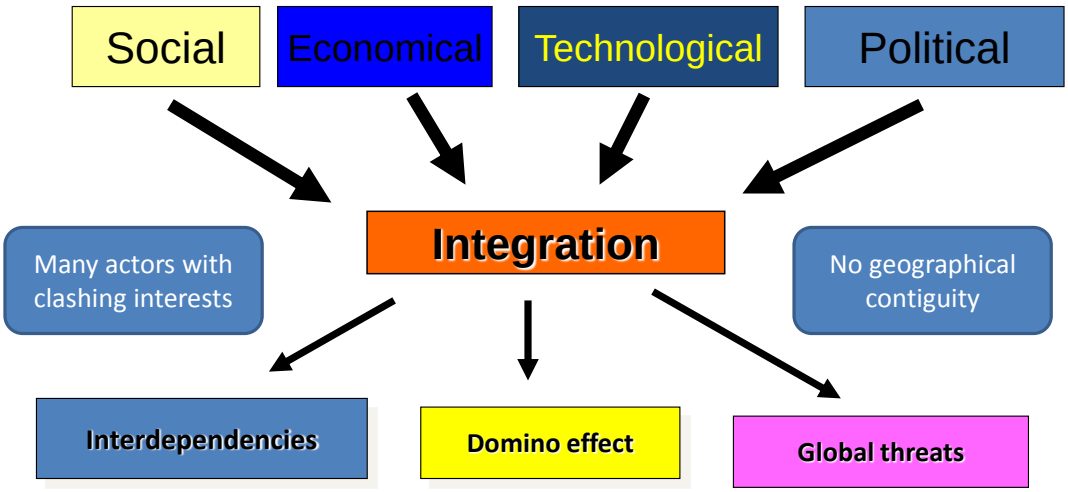


Figura 1. Leve che spingono all'integrazione delle diverse infrastrutture e aspetti negativi per la sicurezza da ciò indotto.

Se di per sé il fenomeno dell'integrazione ha comportato una serie di benefici dal punto di vista dell'efficienza, della qualità dei diversi servizi e, soprattutto, della riduzione dei costi, essa introduce, a causa della crescente complessità sistemica, una vulnerabilità intrinseca e nuove tipologie e forme di minacce.

In prima battuta possiamo affermare che, in questo contesto, il fenomeno delle ***interdipendenze*** è il rovescio della medaglia rispetto ai summenzionati fenomeni della globalizzazione e della liberalizzazione dei mercati. Si tratta di un fenomeno con cui dovremmo imparare a convivere, comprendendone le problematiche e gestendone le implicazioni negative per la nostra società.

Le varie infrastrutture tendono, infatti, ad essere sempre più strettamente connesse, al punto che esse risultano fortemente correlate. Ciò comporta che, un guasto/disservizio (di natura accidentale o dolosa) in una di loro, possa facilmente propagarsi con un 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/disservizio (accidentale o doloso).

La figura 2, sviluppata dal *US Office of Critical Infrastructure Protection*[22], presenta un quadro di ciò che potrebbe verificarsi in una nostra città (o anche in una base o un insediamento militare di notevoli dimensioni).

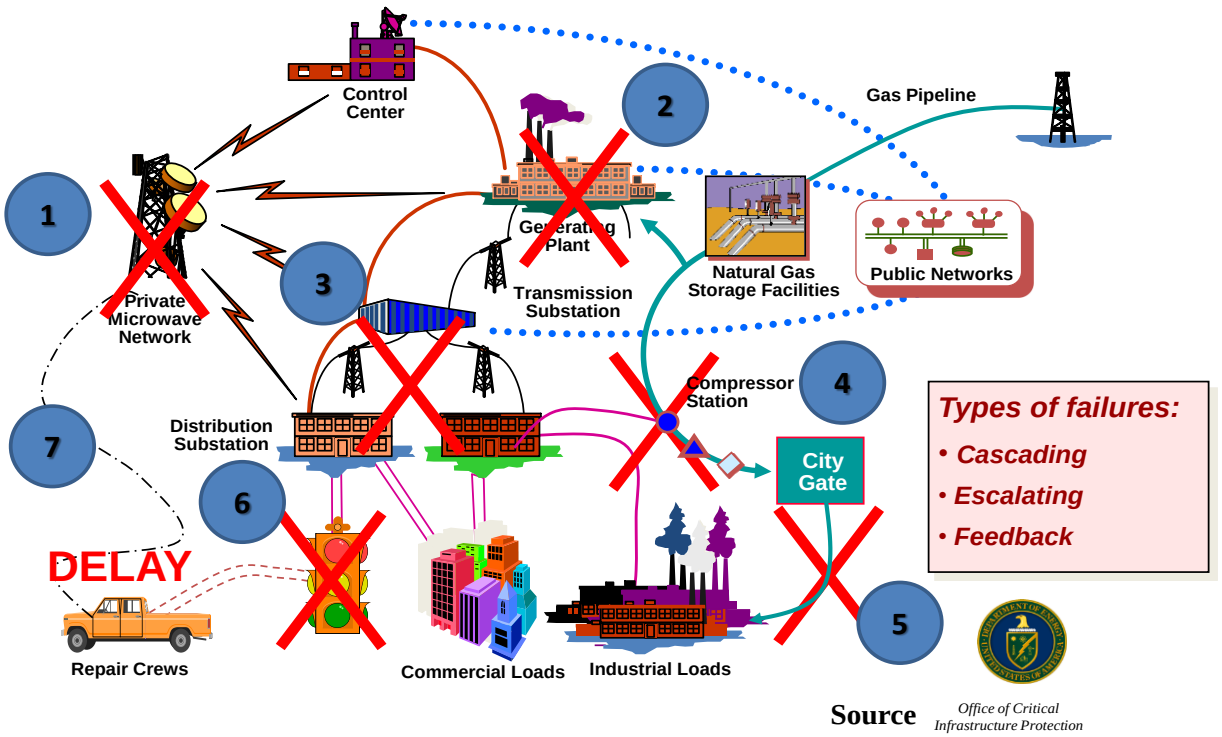


Figura 2. Esempio di interdipendenze tra assets fisici e cyber nel settore energia (Fonte: US Office of Critical Infrastructure Protection).

A causa del guasto ad una antenna per comunicazioni ad onde corte (1), si ha che il Centro di Controllo non è più in grado di tele-monitorare la rete elettrica e, nello specifico, non è più in grado di effettuare quelle modulazioni nell'impianto di produzione e sulla rete di distribuzione necessarie per gestire le variazioni di carico e/o le normali anomalie (2). La conseguenza di ciò (3) è (effetto secondario di primo livello - cascading) l'insorgere di problemi nella rete di distribuzione elettrica con conseguenti black-out in una o più aree. Ciò comporta che (effetti secondari di secondo livello o effetto domino - escalating) da un lato, a causa dell'assenza di energia elettrica anche le pompe a servizio delle pipeline del gasdotto (4) non possano operare, con conseguente paralisi dell'area industriale (5), e dall'altro (6) la congestione del traffico cittadino a causa del non funzionamento degli impianti semaforici e della non operatività delle pompe di benzina. A tutto questo si deve aggiunge che i problemi di circolazione causano ritardi nell'intervento delle squadre di

[22] Oggi assorbito nel Department of Homeland Security.

soccorso con conseguente dilatazione dei tempi di ripristino del guasto (7) (effetto a contro-reazione o feedback).

Quello descritto potrebbe sembrare un caso di studio non realistico, ma purtroppo negli ultimi anni si sono avuti diversi episodi emblematici del livello di interdipendenza esistente fra le diverse infrastrutture tecnologiche. Uno dei primi è certamente quello occorso nel 1998 al Galaxy IV (un satellite per telecomunicazioni in orbita geo-stazionaria sulla costa occidentale degli Stati Uniti). Il suo guasto comportò che circa 40 milioni di pagers andarono immediatamente fuori servizio, circa 20 voli della United Airlines in fase di decollo subirono ritardi di diverse ore a causa della mancata comunicazione del clima in quota, alcune emittenti radiofoniche rimasero oscurate, ma ancor più sorprendenti furono le conseguenze sul sistema di trasporto viario. Infatti, a causa dell'impossibilità di processare le carte di credito nelle aree di servizio lungo le autostrade (che utilizzavano le comunicazioni satellitari per la connessione con i circuiti degli enti emettitori) vi furono notevoli difficoltà nell'effettuare i rifornimenti di carburante con conseguente congestione lungo quelle arterie viarie[23].

Un episodio più vicino a noi si è verificato il 2 gennaio 2004, quando un guasto all'impianto di condizionamento di un importante nodo di Telecom Italia a Roma ha provocato la paralisi del traffico telefonico sia fisso che mobile (anche degli altri operatori) per diverse ore in una vasta area della Capitale e nel litorale laziale. L'incidente ha anche avuto ripercussioni sul sistema finanziario (circa 5.000 filiali bancarie e 3.000 uffici postali sono rimasti privi di connessione telematica) e sul trasporto aereo (il 70% dei banchi di accettazione dell'aeroporto di Fiumicino è stato costretto a ricorrere a procedure manuali per le normali operazioni di check-in). Si sfiorò anche il black-out elettrico in quanto il gestore elettrico dell'area (ACEA) perse la sua capacità di monitoraggio e controllo di circa la metà dell'intera rete elettrica che serve la città di Roma. Senza entrare in dettagli tecnici, qui si vuole solo ricordare come, a seguito della liberalizzazione del mercato dell'energia elettrica, l'allora operatore monopolista ENEL fu costretto a dismettere, fra le altre cose, tutta la propria componente della rete di distribuzione. Nello specifico quella relativa all'area di Roma fu acquisita da ACEA, che per rendere maggiormente efficiente la gestione della rete decise di remotizzare presso la propria sala di controllo tutta la

[23] Per una descrizione di questo e degli altri episodi citati si veda (e le reference lì citate) S. Bologna, and R. Setola, "The Need to Improve Local Self-Awareness in CIP/CIIP", Proc. of First IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005), pp. 84-89, November 2005.

gestione anche della ex-rete di distribuzione ENEL. L'incidente, di cui si è fatto menzione precedentemente, comportò l'impossibilità di avere informazioni nella centrale operativa di ACEA circa l'evoluzione di tutta la rete ex-ENEL. Fortunatamente non vi fu necessità di dover procedere a nessuna manovra sulla rete.

Un aspetto interessante che è emerso da episodi come questo è che non sempre i gestori delle singole infrastrutture hanno ben chiare le criticità e la rilevanza dei servizi da essi erogati. Con la conseguenza che, pur di limitare le conseguenze negative sul piano dell'immagine ed economico, difficilmente rendono partecipi i propri utenti di incidenti incipienti con la conseguenza che questi ultimi, come nel caso del black-out telefonico di Roma, non hanno elementi per presagire la criticità della situazione e, quindi, mettere in atto attività di alleggerimento e di allerta.

Tornando alla **figura 1**, si nota che le conseguenze dirette dell'integrazione sono, oltre alla presenza delle interdipendenze, l'effetto domino e la globalizzazione della minaccia. Ciò è legato al fatto che la natura della minaccia che può affliggere uno specifico target non è più solo ed unicamente quella specifica del target stesso, ma in una qualche misura essa eredita tutte le vulnerabilità anche dai suoi fornitori (come evidenziato dall'episodio di ACEA).

Un altro esempio di ciò è fornito dal worm "slammer" che il 25 gennaio 2003 si è rapidamente diffuso su Internet. Questo worm sfruttava una nota vulnerabilità nel sistema SQL 2000 server di Microsoft e comportò un incremento anomalo nel traffico IP. Questo ha causato, oltre ai prevedibili problemi di accessibilità a molti siti e ai servizi erogati tramite Internet, anche conseguenze al sistema bancario e finanziario (negli USA circa 13.000 apparecchi bancomat andarono fuori servizio, in Italia in 11.000 Uffici Postali non fu possibile eseguire operazioni finanziarie e l'intero sistema bancario e finanziario del sud-est asiatico rimase quasi completamente bloccato), ai trasporti aerei (diversi voli in partenza dall'aeroporto di Houston subirono pesanti ritardi o furono cancellati) ed ai sistemi di emergenza (il call-center per chiamate di emergenza di Seattle andò fuori servizio lasciando scoperto un bacino di utenza di circa 165.000 persone). Il worm ha causato anche problemi ai sistemi di tele-controllo in alcune società di utilities negli USA. Nello specifico, in un caso, il worm pur non penetrando nella rete informatica della società (che era ben protetta) ne comportò comunque l'inoperatività in quanto provocò la

saturazione della banda della dorsale e, conseguentemente, la paralisi del traffico del sistema di tele-controllo.

Questo episodio evidenzia anche come, a causa di quelle non linearità a cui si accennava precedentemente, le conseguenze non rimangono confinate in specifiche aree geografiche, ma si propagano a “macchia di leopardo”.

Da questo punto di vista è estremamente emblematico ricordare quanto occorso il 4 novembre del 2006. In quella sera era programmato che una nave da crociera (la Norwegian Pearl) dovesse attraversare il fiume Ems nel nord della Germania. Per problemi di sicurezza era necessario disalimentare[24] 2 linee a 380 kV per consentire il passaggio della nave. Quella sera vi era una vera e propria tempesta di vento nel Mare del Nord e questo causò un ritardo di circa 2 ore rispetto a quanto originariamente programmato. Nel momento in cui si staccarono le due linee, si ebbe, nella porzione di rete a nord del fiume, a causa della grande quantità di energia immessa dai parchi eolici presenti nel mare del Nord, un rapido aumento della frequenza di rete fino a superare i 51 Hz con conseguente distacco di tutti i generatori. Nella parte a sud del fiume, a causa dell’eccessivo carico, la frequenza crollò rapidamente sotto i 47 Hz comportando, anche qui, lo stacco automatico di tutti i carichi rotanti. Il black-out si propagò immediatamente colpendo a macchia di leopardo la Francia (in pratica solo l’area di Parigi), il Belgio, la Spagna, e gran parte del Nord Africa. In Italia si ebbero problemi solo in Puglia. Alla fine furono colpiti dal black-out oltre 15 milioni di cittadini in 11 nazioni con tempi di ripristino che arrivarono anche alle 2 ore.

Un altro episodio emblematico connesso con il mondo elettrico è quanto occorso in Italia il 28 Settembre del 2003. Quella notte, a causa di una configurazione eccessivamente fragile della nostra rete elettrica con una forte componente di importazione di energia dall’estero, la concomitanza della necessità di procedere ad alcune attività di manutenzione programmata su alcune linee verso l’estero, di un guasto su una linea in Svizzera, e di una serie di incomprensioni fra gli operatori italiani e quelli svizzeri innescò un black-out che coinvolse l’intera nazione con oltre 56 milioni di utenti disalimentati, più di 110 treni bloccati, con oltre 30.000 persone a bordo, cancellazioni di tutti i voli, danni alle produzioni ed alle derrate alimentari, ecc. L’aspetto da sottolineare è quello che ha

[24] È il termine usato nel mondo elettrico per indicare che le linee elettriche sono staccate dalla rete (ossia che sono aperti i relativi interruttori e sezionatori) e che, quindi, per esse non fluisce la corrente elettrica.

contribuito a causare il forte ritardo nella riaccensione nel Sud Italia. È necessario premettere che non tutte le centrali elettriche sono in grado di avere un *black-start*, ossia la possibilità di riaccensione in assenza di elettricità fornita dalla rete. Nel piano nazionale di riaccensione è infatti previsto che le prime centrali ad essere riaccese siano quelle idroelettriche (molto più presenti al Nord che al Sud Italia). Per altro queste centrali sono poste in genere in luoghi non facilmente accessibili e per lo più controllate da remoto. Nello specifico non fu possibile tele-comandare dalla sala di controllo di Napoli l'accensione della centrale di Presenzano a causa della non operatività della rete di telecomunicazione utilizzata. La conseguenza fu (effetto feedback) la necessità di inviare operatori nella centrale affinché eseguissero la procedura manuale con ovvia dilatazione dei tempi di ripristino che, nell'Italia Meridionale, arrivano in alcune aree anche ad oltre 9 ore dall'inizio del black-out.

Cosa era successo? A causa della razionalizzazione delle spese, indotta dalla liberalizzazione e dalla concorrenza, l'allora operatore monopolista ENEL, che aveva steso chilometri di fibra ottica per sviluppare una propria rete di telecomunicazione, aveva deciso uno sfruttamento maggiormente remunerativo/efficiente di tale rete, creando la società WIND per poi esternalizzarla ed immetterla sul mercato. La WIND, perseguendo obiettivi diversi rispetto a quelli che potevano essere i dettami di una rete esclusivamente di servizio, sottodimensionò le batterie tampone a servizio di alcune tratte (confidando nella presenza della rete elettrica) con conseguenza che tali tratte non furono più operative dopo poche ore di black-out.

La **figura 3**, che raffigura il risultato del progetto "**Quick-scan** Bescherming Vitale Infrastructuur"[25] finanziato dal governo olandese, nella sua illeggibilità da un'idea della complessità e numerosità di interrelazioni esistenti fra i diversi settori critici.

[25] Eric A.M. Luiijf, Helen H. Burger and Marieke H.A. Klaver, 2003, "Critical Infrastructure Protection in the Netherlands: A Quick-scan", in Urs E. Gattiker, Pia Pedersen and Karsten Petersen (eds), EICAR Conference Best Paper Proceedings 2003.

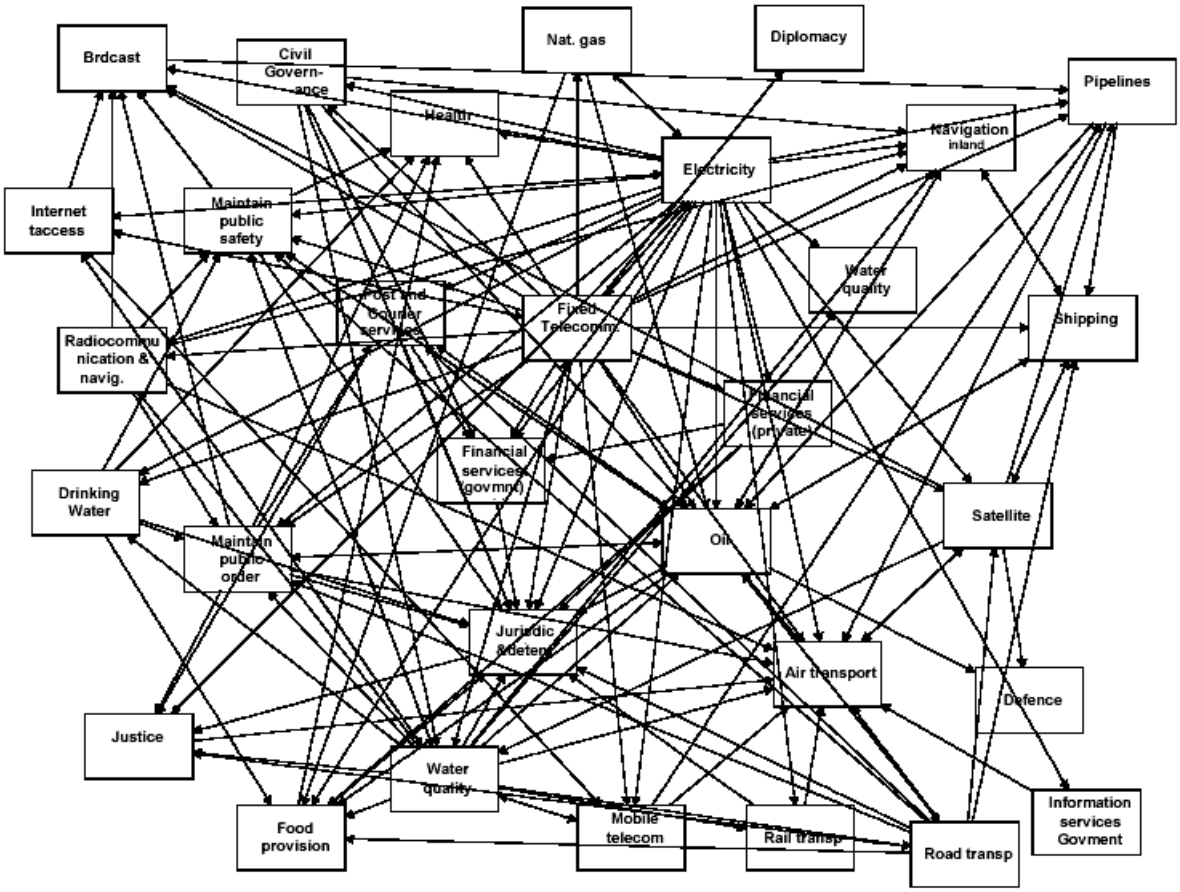


Figura 3. Interdipendenze tra infrastrutture critiche (Fonte: progetto Quick-scan).

Purtroppo stiamo tradendo, o meglio siamo stati costretti a tradire, quello che è uno dei principi che hanno ispirato da sempre le scienze ingegneristiche e sperimentali: quello del riduzionismo, ovvero il “divide et impera”, che vedeva nella decomposizione di ogni problema complesso nelle sue costituenti elementari la strada maestra per ricercare il bandolo della matassa.

Questi episodi, ed altri occorsi in questi anni, evidenziano come riducendo la scala alcuni fenomeni non son più percepibili in quanto “emergono” dall’aggregazione di una pluralità di fenomeni elementari, senza che però siano, dalla sola conoscenza di questi, prevedibili. Occorrono approcci maggiormente olistici in grado, cioè, di cogliere l’essenza del tutto e non solo il valore della singola parte, approcci che al momento non trovano nei nostri bagagli metodologici e matematici strumenti adeguati.

# 4 Risk-profiling relativo alle minacce delle infrastrutture critiche

Sulla scorta di quanto avvenuto nell'ultimo decennio, possiamo affermare che l'evoluzione tecnologica ed ingegneristica sta facendo sì che le diverse infrastrutture siano sempre più robuste rispetto ai guasti (cioè a rotture accidentali di uno o più componenti) e, quindi, si osserva una riduzione costante dell'incidenza di questa classe di minacce; tuttavia, altre tipologie di minacce stanno acquisendo una maggiore rilevanza. Queste sono sia quelle di carattere "naturale", legate alla presenza di fenomeni climatici sempre più estremizzati e violenti, sia quelle connesse con il verificarsi di eventi complessi (ossia una serie di eventi, ognuno dei quali caratterizzati da una bassa probabilità di occorrenza, che si concatenano nel tempo in modo imprevedibile), sia le minacce connesse con azioni dolose e terroristiche[26].

Quello che si evidenzia è che stanno acquisendo una sempre crescente rilevanza i così detti ***extreme event*** (eventi estremi – da qualcuno indicati anche come Black Swan Event – eventi del "cigno nero"), eventi che sono caratterizzati da una probabilità di occorrenza talmente piccola che vengono assunti come impossibili, eppure accadono.

Da un punto di vista prettamente matematico questi eventi, come illustrato nella **figura 4**, si collocano lontano dalla mediana della distribuzione di probabilità[27] e risultano quindi

[26] Su questo punto il governo canadese nel 2003 ha elaborato un interessante documento, generalizzabile a molte altre realtà internazionali, nel quale evidenzia i trend delle principali minacce "Threats to Canada's Critical Infrastructure" http://www.publicsafety.gc.ca/prg/em/ccirc/_fl/ta03-001-eng.pdf

[27] La curva in figura 4 riporta sull'asse delle ascisse i diversi eventi e sull'asse delle ordinate, per ciascun evento specifico, la probabilità di occorrenza (ogni quante volte l'evento si verifica in un dato periodo di tempo). Le code (parti estreme) sono caratterizzate da una probabilità di occorrenza così piccola che in genere è assunta come nulla (evento molto poco probabile).

caratterizzati da una bassissima probabilità di occorrenza. Infatti gli eventi più probabili (cioè quelli che si caratterizzano per il maggior numeri di casi rispetto all'universo esaminato) sono raggruppati intorno al valor medio.

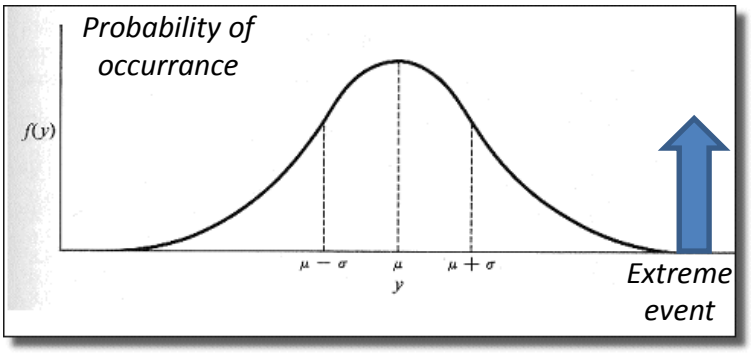


Figura 4. Probabilità di occorrenza ed "eventi estremi".

Questo aspetto ha un immediato impatto su quelle che sono le modalità di analisi del rischio connesso con i diversi eventi. Infatti la classica equazione per la caratterizzazione del rischio:

$$R = P \times V \times C$$

lega il rischio "**R**" a tre fattori che, nello specifico, sono:

- **la probabilità P di occorrenza** di un evento (cioè quanto è "probabile" che una data minaccia si concretizzi/manifesti);
- **la vulnerabilità V del sistema** allo specifico evento (che rappresenta una misura di robustezza del sistema rispetto alla specifica minaccia);
- **le conseguenze (impatto) C prodotte** dal verificarsi dell'evento (ossia quali sono le conseguenze negative in termini di vite umane, danni economici, di immagine, ecc.).

Ora è evidente che se un evento si caratterizza per una bassa probabilità (evento raro) ad esso si tende ad assegnare un basso rischio e, quindi, a escluderlo (o quanto meno trascurarlo) rispetto ad eventi/minacce che, invece, anche se caratterizzati da un minor impatto, presentano una probabilità di occorrenza più elevata.

Le possibili conseguenze di un'impostazione che non tiene conto dell'esistenza e della rilevanza degli eventi estremi è stata codificata nella metà degli anni ottanta dal sociologo americano Charles Perrow, che con la sua teoria dei "**Normal Accident**"[28] sosteneva che per sistemi sufficientemente complessi un incidente rilevante è "normale" (nel senso di non evitabile) per cui è superfluo porsi la domanda se un incidente catastrofico possa verificarsi, ma occorre solo chiedersi quando ciò avverrà. Per Perrow un sistema è complesso se per esso è possible che esistano due o più guasti che, concatenandosi temporalmente in modo "imprevedibile", rendano superflue le ridondanze, facendo sì che un *failure* catastrofico diventi inevitabile. In altri termini per Perrow la fragilità intrinseca del sistema è nella sua stessa **complessità**.

Una tragica conferma di quanto la visione di Perrow fosse corretta si è avuta con il black-out che nell'agosto del 2003 ha colpito la costa occidentale degli Stati Uniti e del Canada.

Tale black-out è stato indotto, infatti, da un serie di eventi "banali" che presi singolarmente non avrebbero potuto causare alcun pericolo, ma che si sono ordinati nel tempo creando una sequenza drammatica. Per capire le cause la commissione **congiunta istituita dal governo americano**[29] e da quello canadese ha dovuto considerare eventi occorsi sia sul piano fisico (a livello della rete elttrica) che di quello cyber (il comportamento dei vari computer) che di quello umano (cosa hanno o non hanno fatto i diversi operatori).

Infatti, tale analisi ha evidenziato che contemporaneamente ad un evento "banale" sulla rete elettrica (un fulminazione verso il suolo a causa del carico eccessivo su una rete) lo stesso si è ingigantito in quanto gli operatori nella sala di controllo non hanno avuto modo di gestire il fenomeno a causa, da un lato di due distinti problemi con il sistema SCADA (nello specifico il blocco della funzionalità del modulo di allarmi e una degradazione nel funzionamento del modulo deputato a raccogliere i dati dal campo), ma anche in conseguenza di un errore di un operatore che aveva disabilitato la funzionalità di predizione (ovvero il sistema che forniva una valutazione di come si sarebbe evoluto il carico sulla rete).

[28] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, 1999 http://press.princeton.edu/titles/6596.html
[29] U.S. - Canada Power System Outage Task Force, U.S. - http://www.nerc.com/docs/docs/blackout/ch1-3.pdf

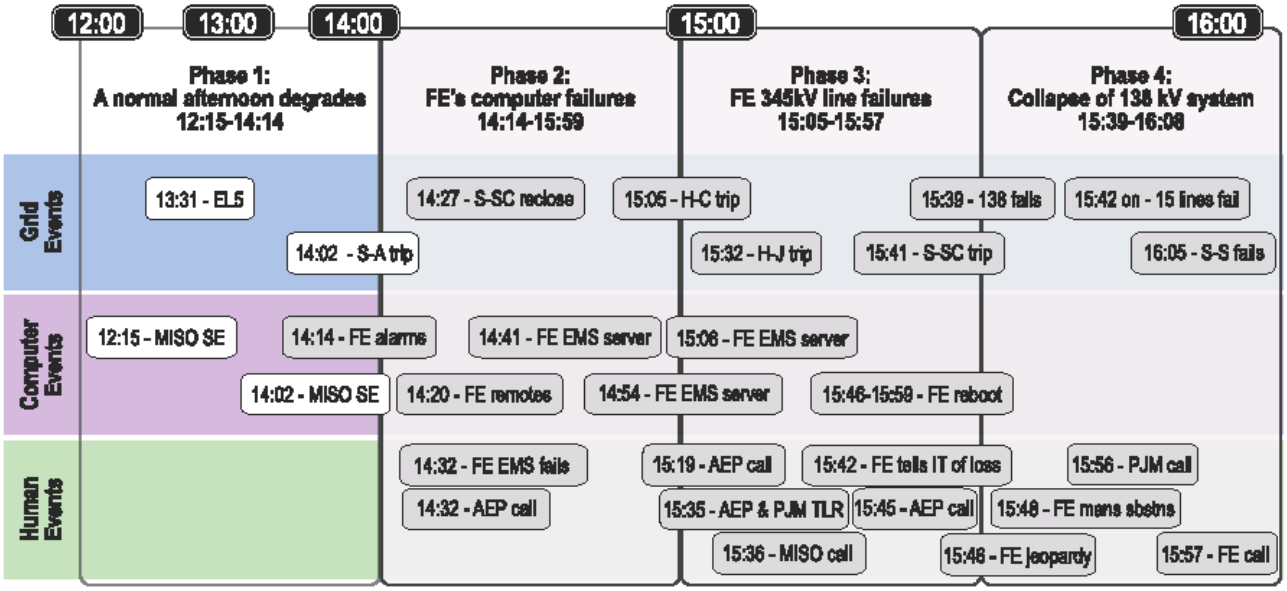


Figura 5. Sequenza degli eventi, fisici, informatici ed umani, che hanno portato al black-out del 2003 in USA e Canada (Fonte Commissione Congiunta USA-Canada **black-out del 2003 in US e Canada**).

A proposito dei black-out elettrici, è interessante notare che negli ultimi anni si è osservata una costante diminuzione nel numero dei loro episodi, a dimostrazione di una maggiore affidabilità del sistema elettrico. Nello stesso tempo, si registra l'aumento dell'ampiezza del bacino di utenze che soffrono di tali eventi. Ciò evidenzia come il sistema elettrico, che pure ha acquisito negli anni una elevata capacità di fronteggiare con efficacia i guasti di routine, a causa della sua crescente complessità, risulta maggiormente vulnerabile nei confronti di alcuni (rari) eventi le cui conseguenze risultano però difficilmente circoscrivibili, tanto che alcuni studiosi sono arrivati a sostenere **"l'inevitabilità" dei grandi black-out**[30].

Tornando all'**equazione del rischio**, si ha che la sua applicazione al mondo delle infrastrutture critiche è resa complessa non solo perché è necessario prendere in considerazione anche gli eventi estremi, ma anche perché la identificazione di quelle che sono le conseguenze dell'evento non è di semplice determinazione, in quanto occorre tener presente, oltre che gli effetti diretti, anche quelli di secondo (o superiore) livello.

Giusto per dare un'idea della complessità di questo tipo di valutazione, basta ricordare che le **stime dei danni provocati dal black-out del 2003** negli Stati Uniti oscillano fra i 4,5 ed

[30] P. Fairley, "The Unruly Power Grid", IEEE Spectrum, agosto 2004 - http://spectrum.ieee.org/energy/the-smarter-grid/the-unruly-power-grid

i 10 miliardi di dollari, sebbene la maggior parte degli economisti ritenga la stima più corretta pari a 6 miliardi di dollari[31].

A tal fine nel **capitolo 8** verranno descritte alcune metodologie e strumenti utili per la determinazione e la quantificazione di tali effetti di ordine secondario.

Continuando l'analisi **dell'equazione del rischio** occorre evidenziare che anche la determinazione della valenza dell'ultimo fattore, ovvero la vulnerabilità, implica considerazioni e valutazioni differenti rispetto a quanto storicamente fatto, in quanto la crescente integrazione fra mondo fisico e mondo cyber e le modifiche architetturali occorse a quest'ultimo nell'ultimo decennio, inducono nelle infrastrutture critiche vulnerabilità, come illustrato nel **capitolo 7**, prima non conosciute.

[31] http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf

**Strumenti e tecniche per il risk-profiling**

**SPECIALISTICA**

# 5 Introduzione al risk-profiling

Prima di addentrarci nelle tecniche e negli strumenti utili per un'analisi del rischio connesso con la minaccia terroristica, e più in generale criminale, verso le infrastrutture critiche, occorre fornire alcuni elementi di caratterizzazione delle stesse che ne evidenzino le peculiarità e gli aspetti di maggiore rilevanza. A questo sono dedicati i prossimi due capitoli, che forniranno un inquadramento teorico del problema delle interdipendenze (**capitolo 6**) e delle implicazioni connesse con il cambio di paradigma operato nel campo dei sistemi di monitoraggio e controllo (**capitolo 7**).

Il **capitolo 8** illustra tre distinti approcci utili per l'analisi e la qualificazione del possibile impatto. Tali strumenti si differenziano per la complessità del modello sotteso, che implica una maggiore o minore necessità di disporre di dati di dettaglio. Come illustrato nella **figura 6**, tratta da uno dei **pochi articoli**[32] scientifici in cui si analizza il problema della quantificazione del livello di interdipendenza esistente fra le diverse infrastrutture, gli strumenti più "semplici" hanno per lo più una valenza strategica, mentre quelli maggiormente di dettaglio possono avere anche una valenza operativa.

[32] R. Setola, "How to Measure the Degree of Interdependencies among Critical Infrastructures", Int. J. of System of Systems Engineering, (IJSSE), vol. 2, No. 1, pp. 38 -59, 2010
http://www.inderscience.com/search/index.php?action=record&rec_id=35380&prevQuery=&ps=10&m=or

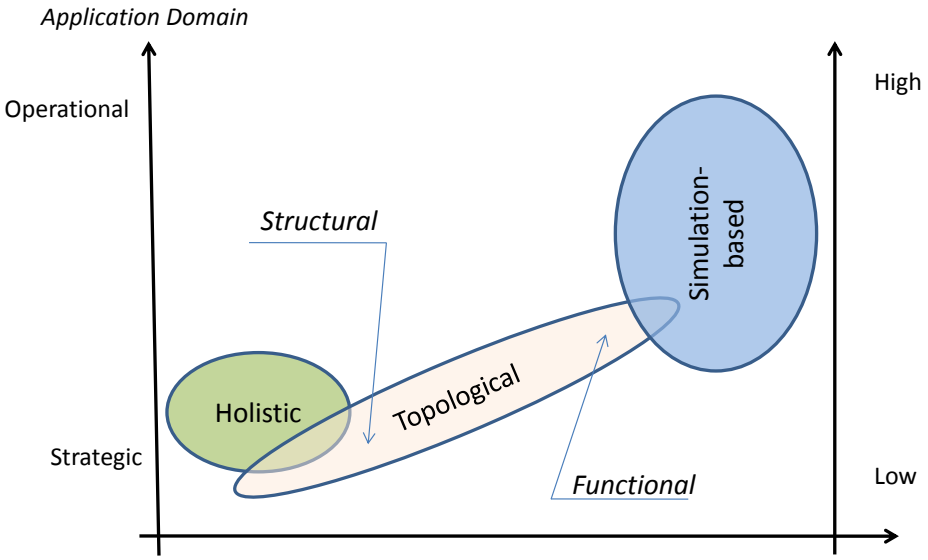


Figura 6. Caratterizzazione delle diverse metodologie di modellistica in funzione della complessità e della funzionalità (Fonte: R. Setola “La Protezione delle Infrastrutture Critiche Informatizzate”, Automazione e Strumentazione, luglio 2003).

Il **capitolo 9** si concentra in modo più specifico sul perché un’infrastruttura critica sia un possibile obiettivo per azioni eversive e, nello specifico, per azioni commesse in ambito di terrorismo di matrice confessionale, ma anche per ciò che attiene attività di “pressione” (se non apertamente di ostilità) da parte di stati.

# 6 Interdipendenze

Uno degli aspetti che caratterizza la problematica delle infrastrutture critiche è la presenza di “interdipendenze”, ovvero del fatto che un evento occorso in una infrastruttura può ripercuotersi su un’altra andando ad amplificare gli effetti negativi dell’evento originario.

Si noti che, sebbene per alcuni tipi di relazioni potrebbe sembrare maggiormente corretto parlare di *dipendenza*, in questo contesto si fa generalmente ricorso al termine *interdipendenza* in quanto, a causa dell’elevato numero di interazioni e dipendenze funzionali esistenti fra le diverse infrastrutture, per ogni coppia di infrastrutture esistono meccanismi, diretti e/o indiretti (cioè mediati tramite dipendenze su altre infrastrutture), tali per cui l’evoluzione dell’una influenza l’altra e viceversa.

Nella formulazione proposta da **Rinaldi, Peerenboom e Kelly**[33] le interdipendenze sono analizzate considerando sei diverse “dimensioni” al fine di cogliere i diversi elementi che caratterizzano sia il comportamento legato alla presenza dell’interdipendenza che il suo insorgere (**figura 7**).

[33] S. Rinaldi, J. Peerenboom, e T. Kelly, “Identify, Understanding, and Analyzing Critical Infrastructure Interdependencies”', IEEE Control System Magazine, pp. 11–25, 2001.

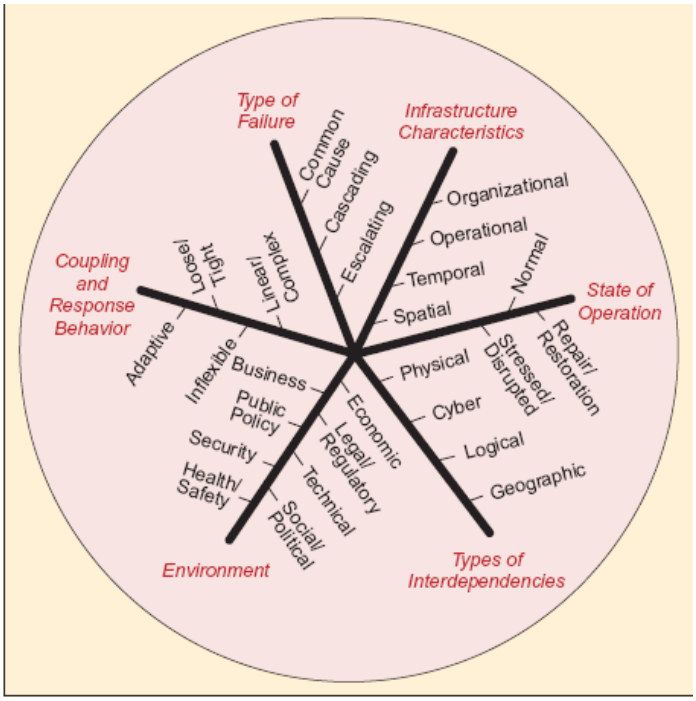


Figura 7. Dimensioni per descrivere le interdipendenze tra infrastrutture (Fonte: S. Rinaldi, J. Peerenboom, e T. Kelly, "Identify, Understanding, and Analyzing Critical Infrastructure Interdependencies"', IEEE Control System Magazine, pp. 11–25, 2001).

In particolare esse individuano lungo quali direzioni occorre sviluppare l'analisi:

**Ambiente**: cioè la struttura entro la quale proprietari e operatori stabiliscono finalità e obiettivi, costruiscono sistemi di valori per definire il loro business, ecc. Ovviamente lo stato operativo e le condizioni di ciascuna infrastruttura influenzano l'ambiente circostante e, a sua volta, l'ambiente influenza l'infrastruttura stessa.

**Tipi di Interdipendenza**: un'interdipendenza può essere classificata come:

- *Fisica*: Due infrastrutture sono fisicamente interdipendenti se lo stato di una è dipendente dall'output materiale (fisico) dell'altra. Ad esempio una centrale elettrica a carbone e la sua rete ferroviaria di adduzione mostrano un'interdipendenza fisica, giacché ognuno dei due sistemi dipende dall'output dell'altro: la centrale ha bisogno della rete ferroviaria per la fornitura del combustibile e dei componenti di ricambio dei generatori, mentre la rete ferroviaria necessita dell'energia elettrica generata dalla centrale per il proprio funzionamento e controllo.
- *Cyber*: Un'infrastruttura ha una cyber-interdipendenza se il suo stato dipende dalle informazioni trasmesse attraverso il cyberspace.

- *Geografica*: Due o più infrastrutture sono geograficamente interdipendenti se un evento ambientale locale può provocare cambiamenti nello stato delle altre infrastrutture. Questo accade quando le varie infrastrutture condividono lo stesso luogo fisico, quale un ponte, una stanza, ecc. In tal modo un evento naturale o doloso può provocare un guasto comune alle varie infrastrutture.
- *Logica*: Due infrastrutture sono logicamente interdipendenti se lo stato di ognuna di loro dipende dallo stato dell'altra tramite un meccanismo che non è nessuno di quelli precedentemente esplicitati. Questa tipologia di interdipendenza, tipicamente legato a scambi di servizi tra infrastrutture, consente di modellare quei legami connessi con fenomeni socio-economici, culturali o indotti da vincoli normativi e legislativi. In genere le decisioni umane sono predominanti nella creazione di questo tipo di interdipendenza.

Tale classificazione può essere estesa includendo anche le relazioni d'interdipendenza sociologica[34] causate dal comportamento (irrazionale) degli utenti/operatori. In questo modo è possibile modellare fenomeni quali la saturazione dei canali di comunicazione in presenza di eventi di crisi o il fatto che operatori possano disattendere ai propri compiti per ragioni di natura etica o sociale.

Si noti che, a differenza delle altre, la *Cyber interdipendenza* è una proprietà assoluta e non relativa. Ciò sottolinea come, questo tipo di interazione, possa comportare un'estesa interdipendenza (sostanzialmente) con qualunque altra infrastruttura che utilizza il cyberspace.

**Stato operativo**: Per comprendere appieno le interdipendenze è necessario determinare, per ogni infrastruttura, da quali essa dipende sia in condizioni di normale funzionamento, sia in situazioni anomale, che durante la fase di ripristino a seguito di un guasto/malfunzionamento.

**Caratteristiche dell'infrastruttura**: In quest'ambito vanno considerati elementi quali la *scala spaziale*, a proposito della quale si può definire una gerarchia di elementi:

*Parte*: il componente più piccolo distinguibile in un'analisi;

[34] U.S. - Canada Power System Outage Task Force, U.S. - http://www.nerc.com/docs/docs/blackout/ch1-3.pdf.

*Unità*: un insieme di parti funzionalmente correlate (ad esempio un generatore di calore);

*Sottosistema*: una linea di unità (ad esempio un sistema di raffreddamento);

*Infrastruttura*: un insieme completo di sistemi simili.

La *scala spaziale* ha implicazioni importanti sul modo in cui le interdipendenze sono considerate nell'analisi. Si noti che, generalmente, a livello di parti ed unità le interdipendenze hanno un ruolo minore rispetto a tutti gli altri casi. Tale scala spaziale è strettamente connessa alla scala geografica, dato che le infrastrutture possono essere considerate a livello di città, regione, nazione o sovra-nazionale a seconda dell'obiettivo che l'analisi si propone.

Altra caratteristica importante è la *scala temporale*. L'orizzonte di interesse può variare dai secondi (per le operazioni del sistema energetico ad esempio), alle ore (per le operazioni connesse con la fornitura di acqua, gas o per il sistema di trasporto), agli anni (per i miglioramenti o per l'aumento di capacità di un'infrastruttura).

Al variare dell'orizzonte temporale, alcune delle tipologie di interdipendenze acquisiranno una maggiore o minore importanza. Ad esempio, se si esamina un processo molto veloce, qual è quello della propagazione di un guasto nella rete elettrica, sarà particolarmente rilevante la cyber interdipendenza, soprattutto in considerazione delle implicazioni che ciò impone ai sistemi di tele-controllo, mentre le interdipendenze di tipo logico non avranno quasi alcun tipo di ruolo. Dualmente, queste giocheranno un ruolo primario per comprendere le conseguenze indotte da modifiche nella tipologia dei servizi scambiati (ed in questo caso le interdipendenze di tipo cyber potranno anche essere del tutto trascurate durante l'analisi).

A questi elementi caratterizzanti un'infrastruttura, vanno affiancate anche considerazioni circa i *fattori operativi* e i *fattori di carattere organizzativo* che caratterizzano il funzionamento della singola infrastruttura.

**Tipi di guasto**: Le interdipendenze tra infrastrutture possono costituire il mezzo attraverso il quale un guasto può propagarsi. In quest'ottica si parla di propagazione:

- *a cascata*: quando il malfunzionamento provoca un guasto in una seconda infrastruttura, il che comporta a sua volta l'insorgere di un'anomalia in una terza e così via;
- *intensificante*: quando il malfunzionamento in un'infrastruttura rende più gravoso un malfunzionamento, indipendente dal primo, in una seconda infrastruttura;
- *a causa comune*: quando due o più infrastrutture subiscono danni nello stesso momento e per lo stesso motivo.

**Livello di accoppiamento**: in funzione del grado di accoppiamento (stretto o lasco), varia sia il tempo di propagazione che l'intensità trasmessa di un eventuale malfunzionamento. Tali interazioni possono essere sia di tipo *lineare*, se sono il risultato del processo di progettazione (generalmente note, visibili e generate da una sequenza prevista di operazioni), che *complesse*, quando si manifestano inaspettatamente a seguito di sequenze di operazioni non previste.

Per meglio comprendere il problema delle dipendenze tra i vari elementi di un'infrastruttura e delle interdipendenze tra infrastrutture diverse, è opportuno modellare ciascuna di esse come un oggetto composto logicamente da tre distinti layer: **organizzativo**, **cyber** e **fisico** (**figura 8**). All'interno di ciascuna infrastruttura ogni elemento interagisce, oltre che con gli elementi al suo livello, anche con elementi posti nei livelli contigui (tramite legami funzionali indicati come intra-dependency), mentre gli omologhi strati delle diverse infrastrutture interagiscono fra loro attraverso legami indicati come inter-dependency.

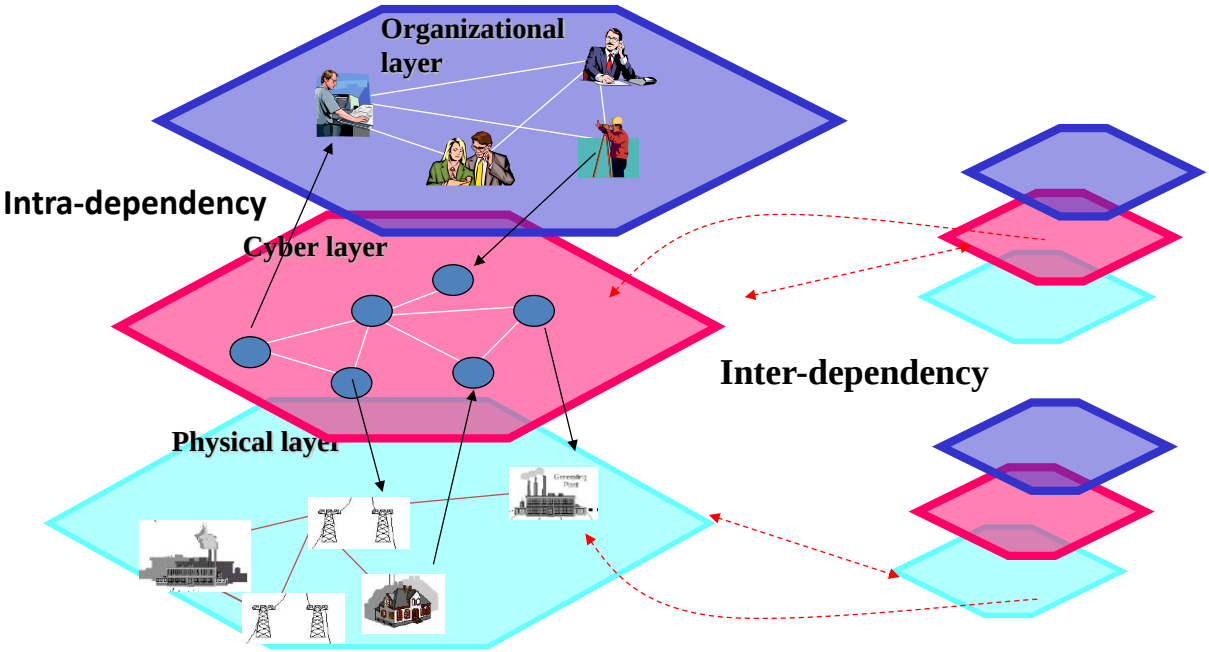


Figura 8. Intra e inter-dipendenze tra i layer delle infrastrutture[35].

[35] S. Bologna, and R. Setola, "The Need to Improve Local Self-Awareness in CIP/CIIP", Proc. of First IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005), pp. 84-89, November 2005.

# 7

# Sistemi di Monitoraggio e Controllo e la minaccia Cyber

In questo contesto un'attenzione particolare meritano i sistemi di monitoraggio e controllo, ovvero quei sistemi informatici utilizzati per la gestione di tutte le infrastrutture critiche.

In modo semplificato, lo scopo di tali sistemi è quello di raccogliere dal campo le informazioni che caratterizzano lo stato delle diverse grandezze di interesse, oltre che lo stato dei singoli apparati, e fornirne una rappresentazione aggregata e/o di dettaglio ad un operatore collocato all'interno di una sala di controllo posta anche a centinaia di chilometri di distanza dalla sorgente. A questa funzionalità, che va in genere sotto il nome di monitoraggio, con il tempo si è poi aggiunta quella relativa al controllo (o usando un termine più tecnico all'attuazione), ossia all'invio di comandi atti a modificare l'assetto sul campo al fine di soddisfare requisiti di ottimalità e sicurezza.

Tali sistemi SCADA (Supervisory Control And Data Acquisition) sono normalmente costituiti da una sala di controllo connessa, tramite link di diversa natura, ad un certo numero di RTU (Remote Terminal Unit) distribuite su un territorio più o meno vasto. Queste si occupano della raccolta delle informazioni e dell'esecuzione delle azioni gestite dal sistema centrale. La distribuzione sul territorio delle RTU assume diverse caratteristiche a seconda del tipo di impianto e può essere a carattere geografico (ad esempio, per il monitoraggio di pipeline o di sistemi di trasporto e distribuzione dell'energia elettrica), a carattere locale (pensando alla gestione della fornitura del gas nelle città), fino a dimensioni estremamente ridotte (sistemi che sovrintendono la produzione in impianti industriali) . A loro volta, le RTU possono essere connesse al sistema centrale in vari modi: si va da collegamenti punto-punto per le grandi distanze e per le zone ove le infrastrutture di comunicazione non hanno un buon grado di sviluppo (pipeline), a collegamenti che invece sfruttano le infrastrutture esistenti làddove queste siano economicamente vantaggiose (distribuzioni a livello urbano). In particolare, per gli impianti

industriali, sono state sviluppate reti di comunicazione dedicate (bus di campo) che, con protocolli aperti ma sicuramente di ridottissima diffusione, consentono un interfacciamento veloce e flessibile tra i sistemi di misura e quelli di controllo. Si parla, più spesso in questo caso, di **DCS**[36] (Distributed Control System) nei quali gioca un ruolo determinante sia la capacità di monitorare migliaia di punti di misura e attuazione (Input/Output - I/O), sia la possibilità di reagire a particolari eventi in tempi rapidissimi.

I sistemi SCADA sono stati tradizionalmente progettati come elementi separati rispetto alle altre infrastrutture telematiche aziendali, anche in considerazione dell'utilizzo, quale strato di trasporto, di protocolli dedicati come il MAP (Manufacturing Application Protocol), più adatti alla gestione di unità remote relativamente poco intelligenti, spesso connesse tramite collegamenti peer-to-peer. Tali sistemi operavano su reti isolate, avevano reti di alimentazione dedicate e ridondati, utilizzavano protocolli di comunicazione e ambienti operativi generalmente proprietari.

Questo isolamento ha avuto come prima conseguenza la scarsa attenzione riposta nella sicurezza IT dei sistemi SCADA, ritenendosi sufficienti da un lato le semplici procedure per il controllo degli accessi e dall'altro la registrazione dei diversi eventi in appositi log-file.

Tuttavia, le mutate esigenze del mercato hanno imposto una maggiore integrazione dei sistemi di produzione con le reti telematiche aziendali (intranet, extranet, internet) e ciò ha causato una forte crescita dell'esposizione dei sistemi SCADA verso il cyberspace e, quindi, nei confronti delle vulnerabilità e delle minacce di natura informatica.

Le cause di questo mutato scenario sono differenti, in molti casi concorrenti, e dovute ad aspetti legati sia al mutato contesto socio-economico, sia alla liberalizzazione dei mercati, sia alle operazioni di fusione societarie e scorporo di servizi ed attività non centrate sul core-business aziendale (con la conseguente attivazione di servizi di outsourcing), sia alla maggiore necessità di condividere le informazioni con le diverse funzioni aziendali, con conseguente integrazione delle reti di monitoraggio in quelle aziendali, fino all'interconnessione di questi sistemi con Internet per la realizzazione di servizi legati all'e-commerce.

[36] http://en.wikipedia.org/wiki/Distributed_control_system

Ora, mentre gli aspetti connessi con la *safety* sono da sempre stati considerati nel progetto di questi sistemi, anche in virtù del fatto che essa è oggetto di specifiche norme (ad esempio la IEC 61508), solo negli ultimi anni il problema della *security* (soprattutto per ciò che riguarda possibili azioni terroristiche e minacce provenienti dal cyberspace) ha cominciato a ricevere l'attenzione dovuta.

Si pensi che ancora nel 1994 la IEEE dava la seguente definizione di sicurezza delle comunicazioni nei sistemi SCADA:

> *"Security is the ability to detect errors in the original information transmitted, caused by noise on the communication channel".*
>
> **[IEEE 1994[37]]**

Questo limitato interesse nei confronti dei potenziali eventi dolosi era dovuto al fatto che, rispetto alle usuali reti informatiche, i sistemi di monitoraggio e controllo storicamente si basavano su protocolli e sistemi proprietari utilizzando reti di comunicazioni dedicate con, praticamente, nessun collegamento all'esterno. Questo faceva sì che l'unica reale minaccia fosse quella di natura interna (insider) in quanto sarebbe stato praticamente impossibile per un soggetto esterno entrare fisicamente in contatto con il sistema di monitoraggio e controllo, e avere le conoscenze e le informazioni di natura tecnica necessarie per perpetrare azioni criminali.

Con la rapida diffusione di Internet (e quindi del **protocollo IP**[38]), la necessità di aumentare l'efficienza, consentendo al management aziendale di poter avere in tempo reale informazioni sullo stato dei singoli impianti, oltre che la necessità dell'integrazione dei sistemi di produzione con le reti telematiche aziendali (intranet, extranet, Internet) per condividere le informazioni con fornitori e clienti e poi con un platea sempre più ampia di soggetti (in aggiunta al citato effetto dovuto al millennium bug), hanno fatto sì che gran

[37] IEEE Tutorial Course: Fundamentals of Supervisory Systems, 94 EH0392-1 PWR, Sponsored by the Data Acquisition, Processing, and Controls Systems Subcommittee of the Substations Committee of the IEEE Power Engineering Society, 1994. http://openlibrary.org/books/OL1229649M/Fundamentals_of_supervisory_systems
[38] http://it.wikipedia.org/wiki/Protocollo_di_rete

parte dei sistemi proprietari fossero dismessi a favore di soluzioni off-the-shelf, basati su sistemi e protocolli standard.

Tali modifiche hanno comportato che questi sistemi, un tempo praticamente scevri dai rischi connessi con l'informatica, si siano ritrovati a dover subire le medesime minacce dei "normali" sistemi IT senza, però, poter mettere in atto le medesime strategie di contrasto.

Gli studi condotti presso il BCIT nell'ambito dell' Industrial Security Incident Database[39], evidenziano come negli ultimi anni si sia avuta una profonda modifica in quelle che sono le minacce di natura informatica.

L'analisi delle serie storiche evidenzia diverse attribuzioni, illustrate in **figura 9**.

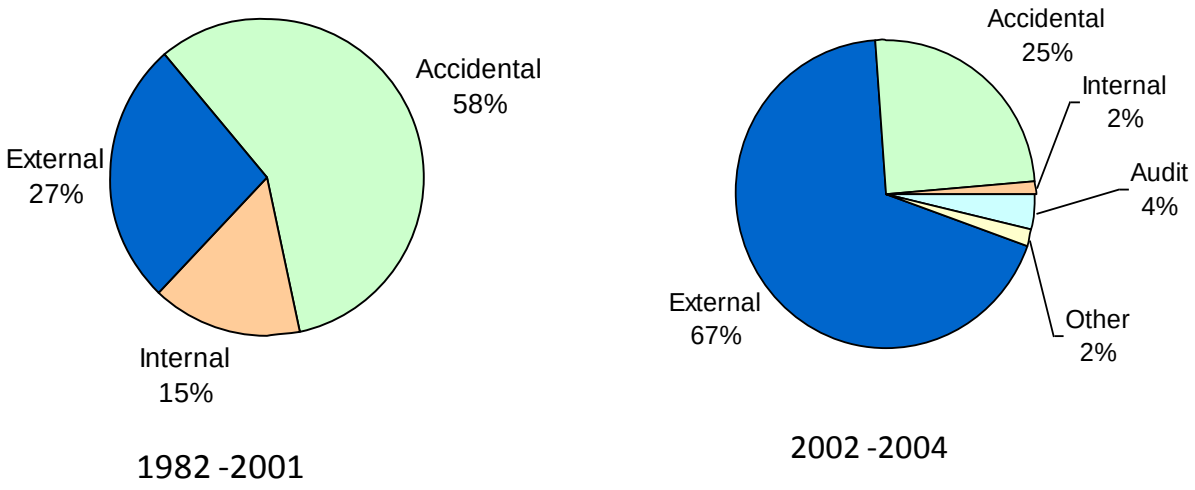


Figura 9. Incidenti informatici dei sistemi di monitoraggio e controllo industriali (Fonte: Industrial Security Incident Database).

L'aumento di tali azioni può essere ricondotto sia alla crescente disponibilità e facilità d'uso degli strumenti di attacco, che alla possibilità di perpetrare anche azioni broadband (come ad esempio la diffusione di virus o worm, che, anche se non specificatamente mirata contro il sistema di monitoraggio e controllo, affliggendo i sottostanti sistemi operativi ne comporta ripercussioni), ovvero con azioni di Denial of Service che bloccano le comunicazioni dalla periferia alla sala di controllo [40].

[39] Purtroppo i dati sono aggiornati solo fino al 2004. Successivamente l'istituto ha smesso di gestire il database. Recentemente un analogo DB è stato predisposto dal RISI (The Reposity of Security Incident) http://www.securityincidents.org/

[40] Come accaduto nel caso del worm slammer (Capitolo 3).

Come evidenziato precedentemente (**Capitolo 2**), tale scenario portò gli USA ad individuare come prioritario il contrasto alla minaccia cyber, adottando una specifica **strategia nazionale**[41] all'interno della quale una specifica attenzione era stata posta proprio sulla sicurezza dei sistemi di monitoraggio e controllo. Attenzione che, nel corso del tempo, si è andata rafforzando con lo sviluppo di tutta una serie di iniziative che vanno dalla creazione di uno specifico CERT nazionale dedicato ai sistemi **industriali**[42], allo sviluppo di **tool per l'autovalutazione** da parte dei diversi utenti del proprio livello di esposizione al rischio cyber[43], all'emanazione di raccomandazioni su come introdurre nei **capitolati di gara**[44] le specifiche relative alla sicurezza cyber, oltre che cospicui finanziamenti alle attività di ricerca e sviluppo (fra le altre cose costituendo anche un **National SCADA Testbed**[45]).

Il tutto con l'obiettivo principale di aumentare la conoscenza e l'awareness della realtà della minaccia cyber per i sistemi industriali da parte di tutti i soggetti coinvolti.

[41] The National Stategy to Secure Cyberspace, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf
[42] US CERT - Control Systems Security Program (CSSP) http://www.us-cert.gov/control_systems/
[43] CSET Cyber Security Evaluation Tool http://www.us-cert.gov/control_systems/satool.html
[44] Department of Homeland Security: Cyber Security Procurement Language for Control Systems http://www.us-cert.gov/control_systems/pdf/SCADA_Procurement_DHS_Final_to_Issue_08-19-08.pdf
[45] http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf


Figura 10. Video realizzato dall'Idaho National Lab[46] su commissione del DHS che evidenzia come un attacco cyber sia in grado di distruggere fisicamente una turbina[47].

Occorre, però, rilevare che fino al 2010 l'unico episodio documentato di sabotaggio di una infrastruttura critica mediante azione cyber è stata quella occorsa nel 2000 in Australia a Maroochy Shine, allorquando un dipendente infedele penetrò, tramite una connessione wireless, nel sistema di controllo del sistema di gestione delle acque (di cui era stato uno dei progettisti) provocando una serie di comportamenti anomali/guasti a scopo estorsivo.

Nel contempo non esiste alcuna evidenza concreta che gruppi terroristici stiano preparando azioni cyber contro infrastrutture critiche[48] sia a causa delle conoscenze necessarie per perpetrare tali azioni, che per la aleatorietà (ovvero non certezza delle conseguenze) e poca appariscenza dei risultati.

Questo, però, non vuol dire che non esistano minacce cyber per queste infrastrutture; anzi, quanto occorse con il **worm StuxNet**[49] dimostra, infatti, la possibilità, non solo teorica, che un'azione cyber possa affliggere danni notevoli a sistemi industriali.

[46] INL è uno dei principali centri di ricerca governativa per quel che riguarda l'energia elettrica e dove, utilizzando un test-bed di oltre 30 kmq, si effettuano anche studi (e certificazioni) di cyber security dei sistemi SCADA (di produttori sia americani che europei) https://inlportal.inl.gov/portal/server.pt/community/home/255

[47] http://www.liveleak.com/view?i=5de_1190957474

[48] È interessante a tal proposito la lettura dell'articolo di J. Green "The Mythos of Cyberterrorism" http://www.washingtonmonthly.com/features/2001/0211.green.html

[49] Questo worm alterava il comportamento di una specifica famiglia di PLC della Siemens http://it.wikipedia.org/wiki/Stuxnet

# 8 Strumenti per la qualificazione e quantificazione degli effetti secondari

Come evidenziato nel capitolo 3, a causa della presenza delle interdipendenze esistenti fra le diverse infrastrutture, agli effetti diretti indotti da un guasto o da un'azione dolosa su una specifica infrastruttura/componente occorre aggiungere quelli prodotti dagli effetti secondari (o di ordine superiore) legati alla propagazione del danno ad altre infrastrutture/componenti ed alle conseguenti ripercussioni sulla prima infrastruttura/componente di queste ultime degradazioni (effetto feedback).

Nel seguito si delineeranno gli aspetti fondamentali di alcune metodiche utili per tale analisi.

***Metodi olistici***

Questi strumenti hanno quale primo obiettivo quello di supportare l'analista nel comprendere, catalogare e qualificare le dipendenze esistenti fra i diversi settori/infrastrutture. Essi sono metodi generalmente qualitativi che forniscono indicazioni di tipo strategico. Il loro pregio principale consiste nella loro semplicità che si traduce, da un lato nella loro facile comprensione anche da parte di utenti non esperti e dall'altro nel fatto che il set-up di tali modelli richiede una quantità di informazioni limitate (e generalmente aggregate) e quindi reperibili con relativa facilità.

Nonostante la loro semplicità, alcuni approcci consentono di ottenere indicazioni ed elementi utili per la determinazione di scelte strategiche.

In questo contesto, uno degli approcci che ha acquisito maggior rilevanza nel corso degli anni per lo studio degli effetti secondari indotti dalla presenza delle interdipendenze fra le

diverse infrastrutture che insistono su un dato territorio è il così detto modello **IIM (Input-output Inoperability Model**[50]) proposto dal prof. Haimes della Università della Viriginia.

La metodologia IIM prende spunto dalla teoria degli equilibri economici, proposta dal premio Nobel Wassily Leontief, riadattandola all'analisi della propagazione di disservizi e/o guasti in uno scenario tecnologico. Secondo il modello IIM, le conseguenze di eventi negativi possono essere stimate introducendo il concetto di inoperabilità (definito come l'incapacità di un elemento di svolgere regolarmente il proprio compito) e analizzandone la dinamica diffusiva attraverso legami di varia natura, come quelli funzionali, geografici o sociali.

Nella sua approssimazione, la metodologia IIM assume che la sopravvivenza (o benessere) di ogni singola infrastruttura dipende dalla disponibilità di "risorse" garantite dalle altre infrastrutture. Un evento negativo che riduca la capacità operativa della *i*-ma infrastruttura può, quindi, indurre effetti negativi anche nei settori che dipendono dalle risorse prodotte dall'infrastruttura colpita per prima. Seguendo lo schema, dunque, le degradazioni possono, via via, propagarsi in cascata ad un grande numero di settori diversi e, in presenza di cicli, ridurre ulteriormente la capacità operativa del settore che per primo aveva subito l'evento negativo.

Nel modello, le degradazioni subite da ciascun settore/infrastruttura sono descritte tramite il relativo grado di *inoperabilità* $x_i$ (ovvero una variabile il cui valore è compreso nell'intervallo [0,1], dove $x_i$ =0 indica la piena funzionalità, mentre $x_i$ =1 indica il completo annichilimento delle capacità operative).

Il calcolo di quello che è l'effetto, sia diretto che di ordine superiore, indotto sul sistema da un evento esterno è effettuato tramite l'equazione matriciale:

$$\mathbf{x}(n+1) = \mathbf{A}\,\mathbf{x}(n) + \mathbf{c}$$

dove **A** è una matrice *m x m* dei coefficienti di Leontieff (con *m* pari al numero di infrastrutture prese in esame), ed i cui elementi $a_{ij}$ rappresentano la frazione di inoperabilità che dalla infrastruttura *j*-ma è trasmessa alla infrastruttura *i*-ma .

[50] http://ascelibrary.org/iso/resource/1/jitse4/v11/i2/p67_s1?isAuthorized=no

Per valutare, ad esempio, l'impatto complessivo che un evento negativo può avere sul sistema, che viene a crearsi dalle interdipendenze fra una rete elettrica, un ospedale, il sistema dei trasporti viari e il sistema di telecomunicazioni operanti in una data area geografica, occorre come prima cosa individuare il grado di dipendenza esistente fra le diverse infrastrutture (vedi **Tabella 1**).

| | Rete elettrica | Trasporti | Ospedali | Telco |
|---|---|---|---|---|
| Rete elettrica | 0 | 0.2 | 0 | 0 |
| Trasporti | 0.4 | 0 | 0 | 0.1 |
| Ospedali | 0.6 | 0.8 | 0 | 0.2 |
| Telco | 1 | 0.2 | 0 | 0 |

Tabella 1. Matrice dei coefficienti di Leontief. La colonna i-sima descrive l'impatto che la distruzione della i-sima infrastruttura comporta sulle altre infrastrutture.

Nel caso della Tabella 1, la prima colonna indica che la distruzione totale della rete elettrica (livello di inoperabilità pari ad 1) avrebbe un impatto diretto sul sistema viario, rendendone non funzionante il 40%, il 60% del sistema ospedaliero rimarrebbe bloccato, mentre il sistema di telecomunicazione sarebbe completamente fuori uso.

Le conseguenze secondarie si ottengono, invece, risolvendo l'equazione (che nel caso semplice si ottiene anche in forma chiusa).

Volendo valutare, ad esempio, gli effetti provocati da un evento che renda non-operativa l'80% della rete elettrica, si ha che

$$\bar{\mathbf{x}} = \left(I - \mathbf{A}\right)^{-1}\mathbf{c} = \left(\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} - \begin{bmatrix}0&0.2&0&0\\0.4&0&0&0.1\\0.6&0.8&0&0.2\\1&0.2&0&0\end{bmatrix}\right)^{-1}\begin{bmatrix}0.8\\0\\0\\0\end{bmatrix} = \begin{bmatrix}0.89\\0.46\\1\\0.98\end{bmatrix}$$

ossia, a causa della presenza delle interdipendenze, aumenta l'effetto di degradazione (che per la rete elettrica sale fino al 89%), e si hanno ripercussioni anche sulle altre infrastrutture (quella sul sistema di trasporto è del 46%, sulle telecomunicazioni del 98%, mentre il sistema ospedaliero è completamente fuori uso).

Tale modello, pur nella sua semplicità, è stato utilizzato per analizzare svariati scenari di crisi tra cui le conseguenze di esplosioni atomiche in alta quota, l'effetto di terremoti o uragani, così come eventi pandemici.

Uno degli aspetti più critici nella messa a punto di questo modello risiede nella determinazione degli elementi che caratterizzano le interdipendenze (ossia i coefficienti della matrice di Leontief). Ciò è dovuto sia al fatto che molte dipendenze risultano poco percepite e comprese, sia alla pluralità di elementi da cui esse sono caratterizzate, rendendo difficile, oltre che la formalizzazione, anche, molto spesso, la loro semplice comprensione. Nella formulazione originale, presentata da Haimes, tali termini erano determinati sulla base del valore economico di inter-scambio esistente fra i diversi soggetti. Una **soluzione alternativa** è quella di utilizzare direttamente la valutazione degli effetti diretti con l'ausilio di esperti dei diversi settori[51].

Nella **figura 11** sono riportate le conseguenze indotte sul sistema infrastrutturale nazionale da un evento in grado di degradare del 50% l'operatività della rete elettrica, tenendo conto non solo delle interdipendenze esistenti fra le diverse infrastrutture, ma anche della presenza di gruppi elettrogeni o altri tipi di risorse di back-up, il cui funzionamento va a ridursi nel tempo.

[51] R. Setola, S. De Porcellinis, and M. Sforna "Critical Infrastructure Dependency Assessment Using Input-output Inoperability Model", Int. J. Critical Infrastructure Protection (IJCIP), pp. 170 - 178, 2009 http://www.sciencedirect.com/science/article/pii/S1874548209000390

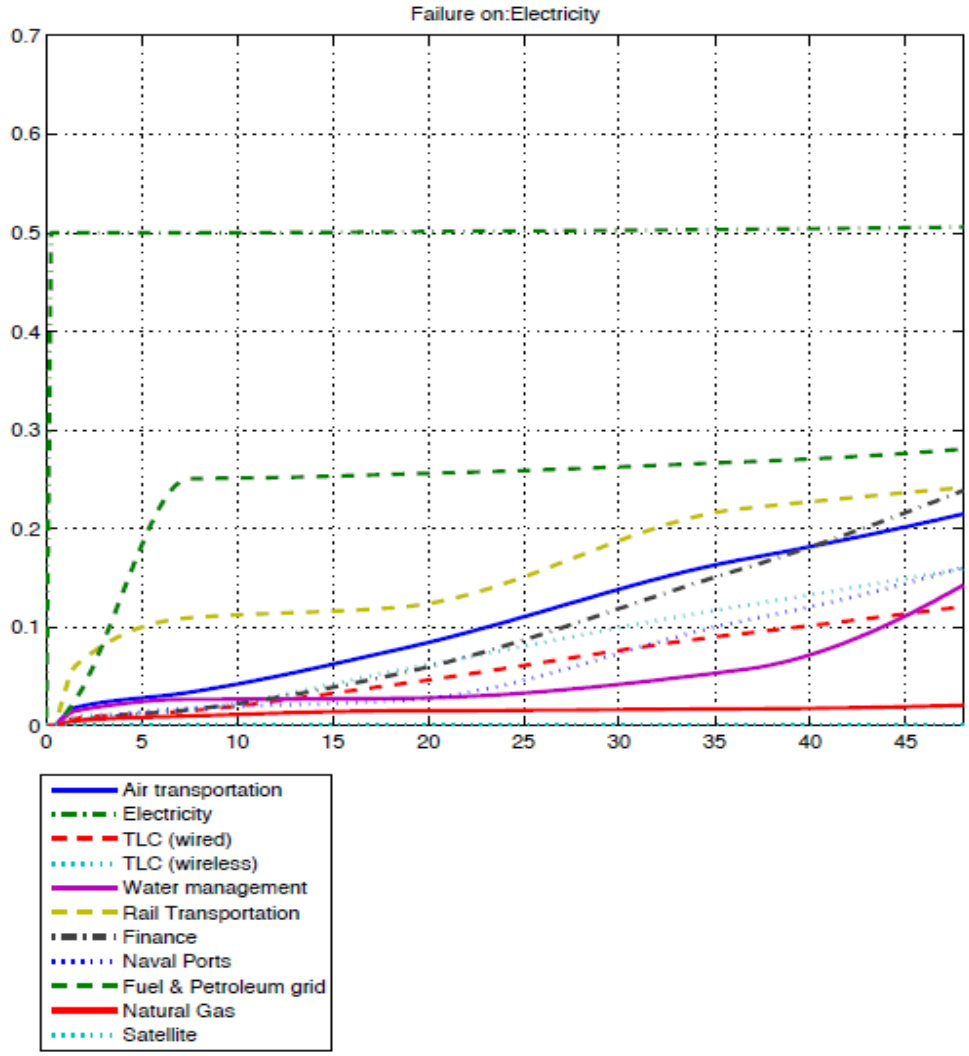


Figura 11. Applicazione del modello IIM alla realtà italiana per la determinazione degli effetti diretti e secondari di un evento che comporti una inoperabilità del 50% della rete elettrica (il modello tiene conto della presenza di scorte ed elementi di back-up considerando i parametri di accoppiamento dipendenti dalla severità e durata dell'inoperabilità).

Tale tipologia di analisi può quindi essere utilizzata sia per una prima quantificazione di quello che potrebbe essere l'impatto di un evento, sia per la definizione delle modalità di allocazione delle risorse, tenendo conto non solo della rilevanza/criticità diretta, ma anche di quella sistemica (legata agli effetti di incidenza secondari), nonché all'articolazione delle attività in fase di ripristino.

Ad esempio la **figura 12**, sempre con riferimento allo scenario italiano, mostra come il grado di dipendenza (ovvero la fragilità di un'infrastruttura dalle risorse prodotte dalle altre) non solo cresce monotonamente con la durata dell'evento negativo, ma le fragilità relative delle diverse infrastrutture cambiano nel tempo (le diverse curve si intersecano) evidenziando come, al venir meno degli elementi di back-up, le conseguenze dirette si

amplificano velocemente, e questo deve indurre a modulare in modo duale le priorità di intervento in fase di ripristino.

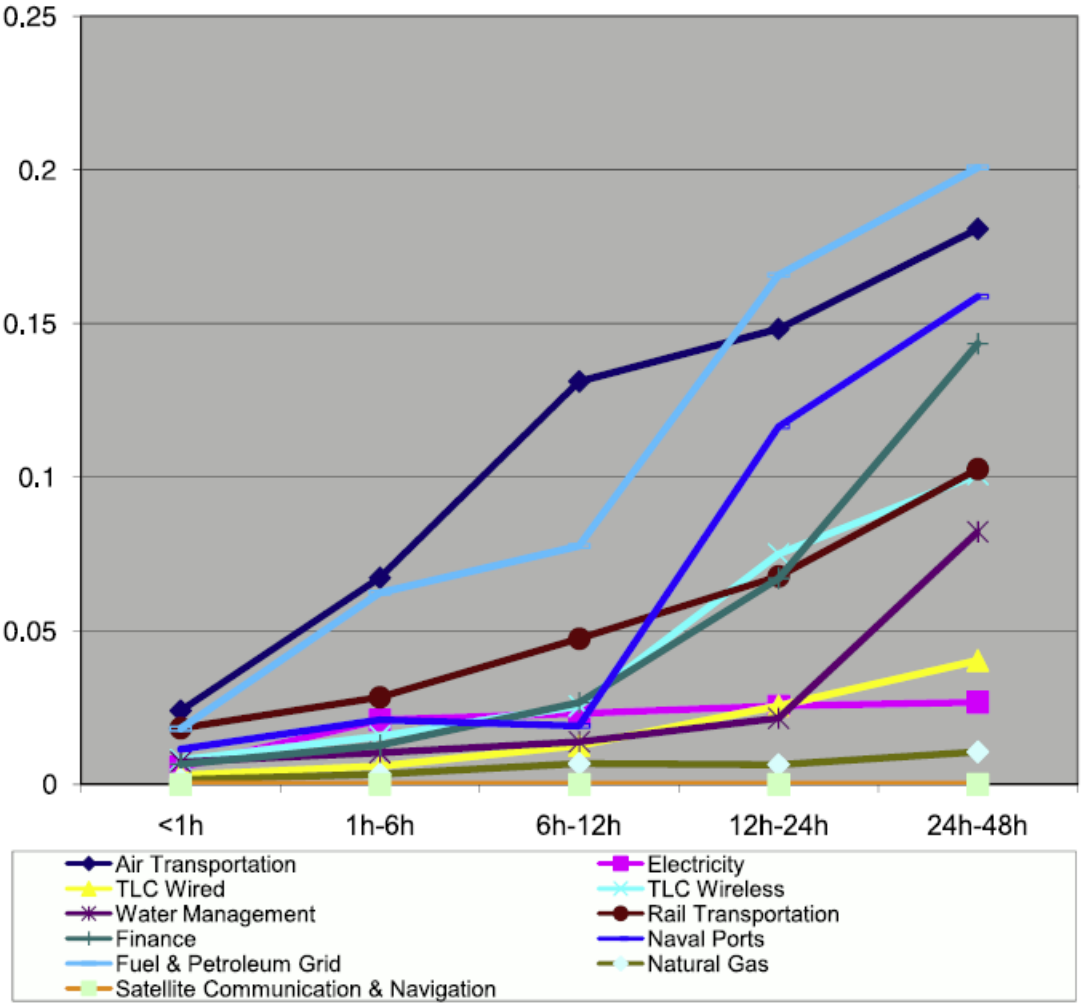


Figura 12. Indici di dipendenza delle principali infrastrutture italiane in funzione della durata del failure[51].

## ***Approcci topologici***

Un diverso approccio per la determinazione degli effetti prodotti da un evento negativo su un'infrastruttura è l'analisi delle conseguenze in termini di alterazione delle proprietà topologiche della rete e, specificatamente, degli aspetti di robustezza.

L'analisi topologica consiste nello schematizzare l'infrastruttura in termini dei suoi elementi costituenti (i nodi della rete) e negli elementi fisici e/o logici che li connettono (archi o link).

Su questo modello è possibile compiere tutta una serie di analisi che consentono di caratterizzare l'importanza e la rilevanza di ciascun nodo e/o link all'interno della rete.

Ad esempio nella **figura 13** sono individuati, per la rete elettrica italiana ad alta ed altissima tensione, i nodi con il maggior numero di link incidenti.

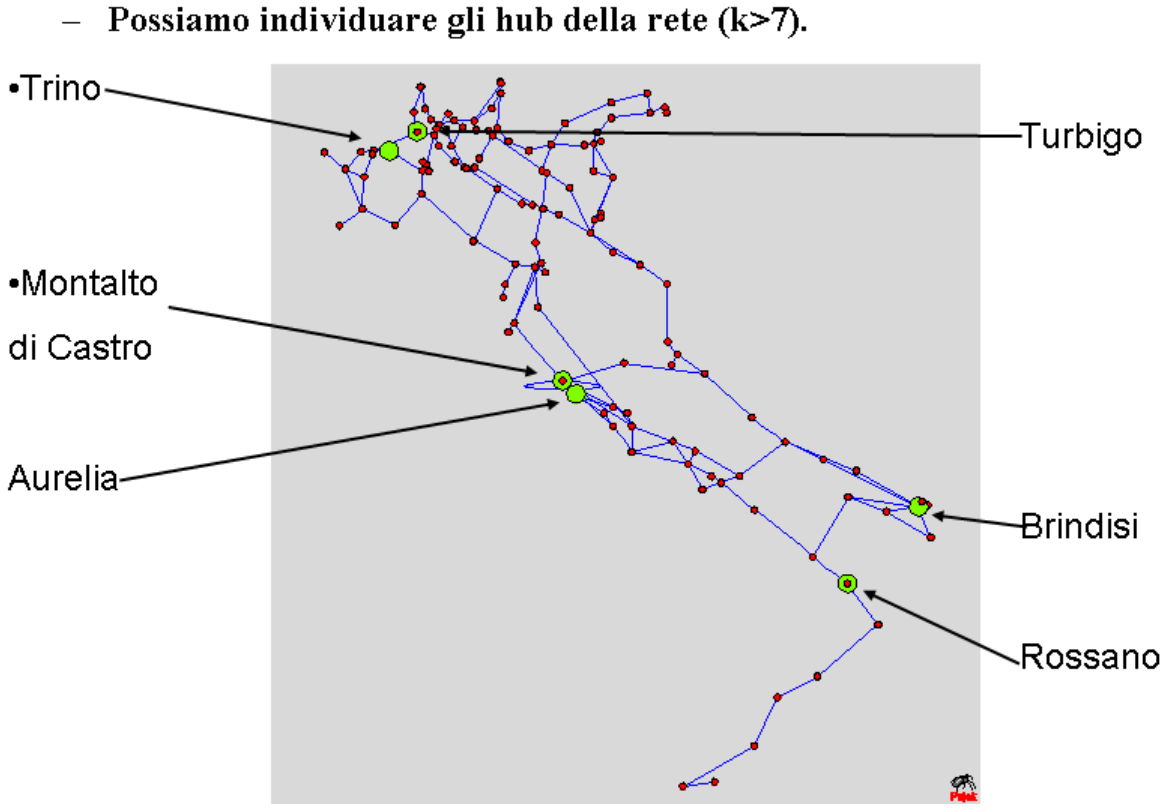


Figura 13. Schematizzazione della rete elettrica italiana ad alta ed altissima tensione con i nodi con il maggior numero di link in evidenza.

In modo analogo è possibile individuare, ad esempio, il taglio minimo, cioè il minor numero di link e/o nodi da eliminare (eventualmente con un'azione dolosa) per provocare la disconnessione della rete, con tutte le conseguenze che ciò comporta in termini di degradazione del servizio[52]. Nello specifico, l'impatto è valutato in termini di degradazioni sofferte dalla rete sia considerando il numero di nodi affetti (con diverse metriche che tengano conto della rilevanza dello specifico nodo) sia con metriche più globali in grado, cioè, di valutare l'effetto complessivo (alterazione della lunghezza del cammino medio, del diametro, ecc.).

[52] Per ovvie ragioni in queste pagine non verranno riportati i relativi risultati che evidenziano, per altro, che il numero di elementi teorici da eliminare è estremamente esiguo. Per inciso si segnala che la localizzazione e le caratteristiche anche di dettaglio della rete elettrica italiana ad alta ed altissima tensione sono informazioni di pubblico dominio, essendo state, fra le altre cose, pubblicate anche sulla Gazzetta Ufficiale.

Un aspetto interessante emerso recentemente, connesso con questi studi, è quello legato alle proprietà intrinseche che caratterizzano la rete. Infatti i lavori pionieristici di Watts e Strogatz verso la fine degli anni novanta, e quelli di Barabasi agli inizi del 2000, hanno evidenziato che in molte situazioni la schematizzazione delle reti complesse come gra[53]fi random non è aderente ai dati empirici.

In particolare i lavori di Barabasi hanno evidenziato che in molte reti il numero dei link afferenti ad uno specifico nodo, anziché seguire una legge di distribuzione di tipo gaussiano (per la quale tutti i nodi hanno mediamente lo stesso numero di link, come è prevedibile in un grafo di tipo random), ha una distribuzione che varia con legge di potenza (cioè la stragrande maggioranza dei nodi ha pochi link, mentre una esigua minoranza ha un numero enorme di nodi, si veda **figura 14)**. Questi grafi hanno pertanto una struttura poco "democratica": alcuni nodi, genericamente indicati come hub, possiedono un numero di connessioni decisamente superiore rispetto agli altri e per tale motivo essi rivestono un ruolo fondamentale nella topologia della rete stessa.

Per tali sistemi, denominati sistemi Scale-Free, si può supporre che le caratteristiche topologiche della rete derivino direttamente dalle leggi sottese alla loro evoluzione. Le caratteristiche sottese ai sistemi Scale-Free fanno sì che essi risultino particolarmente robusti rispetto a guasti casuali: il numero di nodi che è necessario eliminare (statisticamente) prima che il grafo perda la sua connessione è decisamente superiore rispetto a quanto accade nel caso di un grafo random. Il prezzo da pagare è un'elevata fragilità rispetto all'eliminazione selettiva dei nodi più importanti della rete. Se l'ordine di eliminazione è scelto in funzione del numero di link che afferiscono al singolo nodo (grado del nodo), un grafo scale-free diviene disconnesso eliminando un numero di nodi inferiore rispetto ad un grafo random.

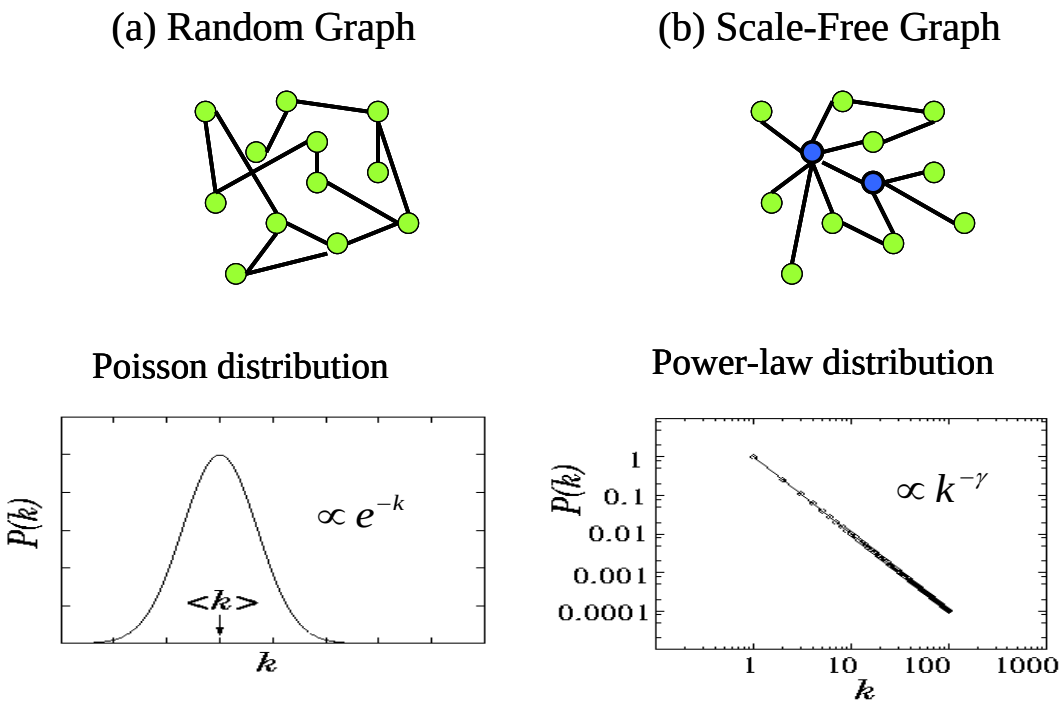


Figura 14. In un grafo random il numero di link per nodo ha una distribuzione gaussiana ($\propto e^{-k}$) centrata intorno al valor medio <k>. In un grafo scale-free vi è una distribuzione meno uniforme che varia con legge di potenza ($\propto k^{-\gamma}$): molti nodi hanno pochissimi link e solo alcuni sono connessi con un grandissimo numero di link.

Traducendo questo su un piano più operativo si ha che un grafo Scale-Free è più robusto rispetto a guasti accidentali (eventi naturali o comunque aleatori), e questo spiega anche la sua diffusione in natura, ma è decisamente più vulnerabile ad attacchi mirati (potremmo dire terroristici), ossia ad azioni che coscientemente mirano a ridurne l'efficienza e che pertanto hanno la capacità/possibilità di colpire nei punti cruciali.

Uno dei principali vantaggi di questo tipo di approccio metodologico è che lo sforzo di modellistica è relativamente semplice in quanto è facile, in molti casi, individuare quali sono i nodi e come essi sono "fisicamente" connessi. Alcuni autori hanno però evidenziato che spesso, come nel caso elettrico ed in quello delle telecomunicazioni, la sola struttura topologica fisica non rappresenta in modo esaustivo le proprietà e le caratteristiche della rete, ma a questa è necessario sovrapporre dei modelli di flusso in grado, cioè, di rappresentare come le diverse quantità fisiche/logiche che fluiscono lungo la rete.

L'introduzione dei flussi, oltre a complicare i modelli ed a richiedere la conoscenza di dati non sempre facilmente reperibili, mostra come in molte situazioni la rilevanza/criticità evidenziata nell'analisi strutturale non sempre coincide con i risultati ottenuti considerando anche le dinamiche di flusso. In altri termini non sempre la sola analisi topologica offre indicazioni corrette sulla effettiva rilevanza di un singolo nodo.

Ulteriori evoluzioni riguardano la capacità di valutare, oltre che le conseguenze dirette su una specifica rete, anche quelle che sono le conseguenze indotte su altre network (ad esempio gli effetti indotti da una alterazione della rete elettrica in quella di telecomunicazione da questa servita). In questo caso, oltre alla necessità di dotare di modelli di flusso le singole reti, è necessario modellare le modalità con cui gli effetti di una rete si ripercuotono su un'altra. Ad esempio, in **figura 15** sono riportati i risultati di uno studio che analizza, con riferimento alla realtà italiana, le conseguenze dell'eliminazione di uno o più nodi sulla rete elettrica sia in termini di allocazione di potenza ai diversi nodi, sia per quel che riguarda le ripercussioni su una specifica rete IT in termini di degradazione delle prestazioni (numero di pacchetti persi e tempo medio di consegna).

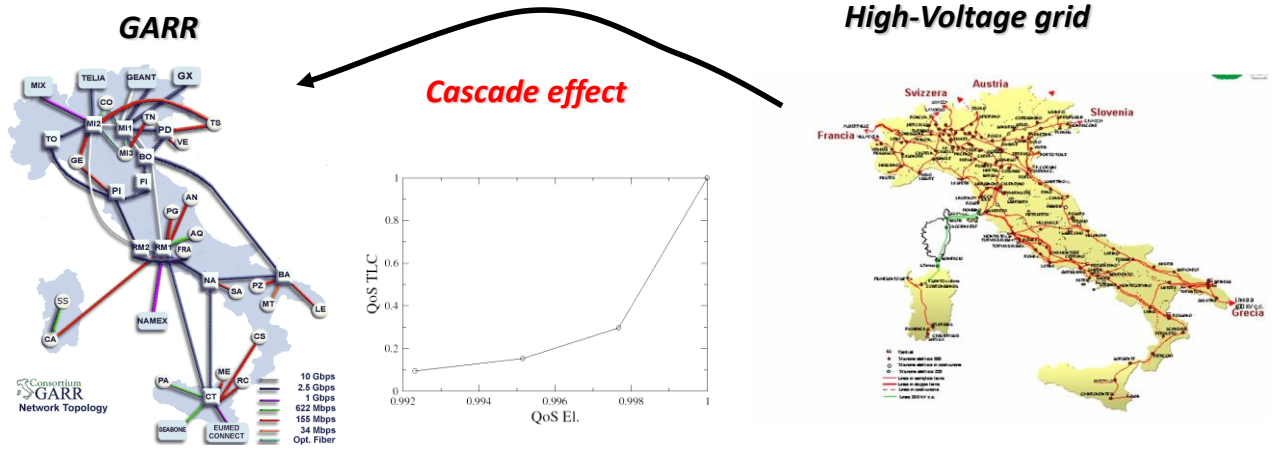


Figura 15. Studio dell'effetto indotto sulla rete GARR dall'eliminazione di uno, due o tre nodi nella rete elettrica ad alta tensione[54].

[54] S. De Porcellinis, L. Issacharoff, S. Meloni, V. Rosato, R. Setola, F. Tiriticco, "Modelling interdependent infrastructures using interacting dynamical models", Int. J. Critical Infrastructure (IJCI), pp. 63-79, 2007

Questa tipologia di approccio consente, inoltre, di formulare il problema dell'ottimizzazione dell'allocazione delle risorse per individuare, ad esempio, la dislocazione ottimale dei diversi servizi al fine di garantire un livello adeguato di intervento, in termini di riduzione degli effetti secondari, in caso di attacco singolo o multiplo[55].

***Approcci simulativi***

È evidente che gli approcci precedentemente descritti si basano su modelli molto semplificati rispetto alla complessità della realtà che caratterizza le dinamiche di una singola infrastruttura e rispetto alle relazioni di interdipendenza esistenti fra di esse.

L'approccio simulativo è l'unico strumento che appare in grado di gestire questa complessità e di supportare l'analisi di tipo what-if e, quindi, la stima degli effetti diretti e di ordine superiore connessi con eventi accidentali e/o dolosi.

Orbene, mentre lo sviluppo di simulatori per specifiche infrastrutture è un campo di ricerca sostanzialmente consolidato con prodotti commerciali e/o di ricerca sufficientemente attendibili, in grado, cioè, di effettuare analisi di predizione sul comportamento di una specifica infrastruttura con un determinato dettaglio, lo stesso non può dirsi per quel che riguarda lo studio di scenari composti da più infrastrutture.

Esistono diversi approcci a partire dall'ambizioso progetto NISAC (**National Infrastructure Simulation and Analysis Center**[56]) che ha lo scopo di fornire strumenti in grado di prevedere le conseguenze sulle diverse infrastrutture USA di eventi di natura accidentale e/o dolosa, al progetto CIPSim (**Critical Infrastructure Protection / Resilience Simulator**[57]), a soluzioni quale, ad esempio, la piattaforma **CISIA**[58] sviluppata dall'Università Campus Bio-Medico di Roma in cooperazione con l'Università di Roma Tre,

[55] Church, R.L. and Scaparra, M.P. Protecting critical assets: The r-interdiction median problem with fortification. Geographical Analysis, 39 (2). pp. 129-146, 2007.
[56] http://www.sandia.gov/nisac/
[57] http://www.inl.gov/nationalsecurity/criticalinfrastructure/
[58] S. De Porcellinis, S. Panzieri, R. Setola, and G. Ulivi, "Simulation of Heterogeneous and Interdependent Critical Infrastructures", Int. J. Critical Infrastructures (IJCIS), vol. 4, n. 1/2, pp. 110 – 128, 2008. http://www.inderscience.com/search/index.php?action=record&rec_id=16095

come anche il progetto DIESIS (**Design of an Interoperable European Federeted Simulation network for Critical Infrastructures**[59]) il cui scopo era lo studio di fattibilità di un *European Critical Infrastructure Simulation Center*.

Un' interessante disamina dei diversi progetti in atto è illustrata nel report prodotto dal **INL nel 2006**[60] ed in quello all'interno del progetto **DIESIS**[61].

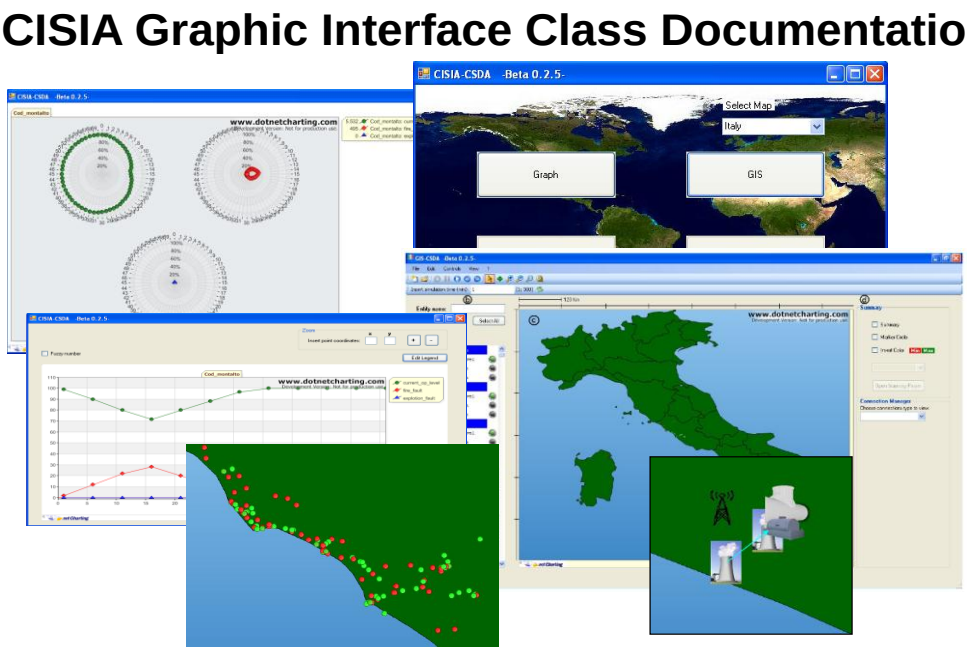


Figura 16. Alcune schermate della piattaforma CISIA.

Sostanzialmente gli approcci che si stanno seguendo sono di due tipi. Da un lato si cerca di rendere interoperanti simulatori nati per l'analisi di specifiche infrastrutture (esempi di questi approcci sono DIESIS e CIPSim). L'altro approccio è quello di sviluppare simulatori specificatamente progettati per lo studio di scenari composti da infrastrutture interdipendenti (come è il caso di CISIA). Il primo approccio ha l'indubbio vantaggio di consentire di riutilizzare quanto già fatto (oltre che una gran massa di dati ed esperienze). Il limite principale è che i meccanismi di interdipendenza che si possono modellare con questi approcci sono sostanzialmente limitati.

[59] http://www.diesis-project.eu/
[60] P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann, "Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research", INL, 2006 http://cipbook.infracritical.com/book3/chapter2/ch2ref2a.pdf
[61] EU project DIESIS, Deliverable "D2.3 Report on available infrastructure simulators" http://www.diesis-project.eu/

La strada di utilizzare simulatori di nuova generazione, sebbene abbia una capacità di modellistica in grado di gestire in modo più efficiente i fenomeni di interdipendenza (ad esempio nella piattaforma CISIA è possibile considerare una pluralità di concetti di prossimità, ognuno utilizzato per modellare uno specifico fenomeno di interdipendenza), come rovescio della medaglia, ha il problema del set-up del modello stesso che risulta più complesso, così come la validazione.

Allo stato attuale, pur con i limiti ed i problemi legati all'utilizzo di strumenti sostanzialmente ancora "giovani", l'approccio simulativo è l'unico che appare in grado di supportare una analisi operativa di quelli che possono essere gli impatti di un evento avverso all'interno di uno scenario composto da diverse ed eterogenee infrastrutture.

# 9 Determinazione dell'attrattività del target

L'altro termine da considerare nell'**equazione del rischio** è quello relativo alla probabilità di occorrenza di un determinato evento. Come evidenziato, la probabilità di accadimento di un'azione dolosa non è facilmente determinabile in quanto essa è intrinsecamente un evento estremo.

In questo contesto la determinazione della probabilità (basata su una analisi di eventi in relazione alla cardinalità degli eventi possibili) va sostituita da due diversi concetti che sono l'attrattività del target (quanto un obiettivo è "appealing") e, nel contempo, le competenze che l'attaccante deve possedere per portare a termine con successo l'azione.

In linea generale si può affermare, anche sulla scorta di quanto propagandato dagli stessi terroristi, che la scelta ottimale di un obiettivo è quella che fornisce la certezza del risultato:

> *The main point is to select targets where success is 100% assured.*
>
> **[Dr. George Habash, Founder Popular Front for the Liberation of Palestine]**

Ciò si traduce nel fatto che le azioni terroristiche sono congegnate in modo da minimizzare il rischio d'insuccesso ed al tempo stesso di massimizzare il "contro-valore" simbolico/effettivo. Da qui il fatto che normalmente le azioni terroristiche sono compiute

utilizzando il minor numero possibile di attaccanti[62] e ricorrendo alla specifca *weapon* che, fra tutte quelle disponibili, assicuri la maggior efficacia.

Questo, come verrà meglio evidenziato in seguito, ha ripercussioni su quella che è l'identificazione delle infrastrutture critiche quale obiettivo di azioni terroristiche o, più in generale, degli obiettivi da sabotare.

Con il termine sabotaggio, infatti, si intende la distruzione di un'infrastruttura e/o di un equipaggiamento dell'avversario con lo scopo di infliggere danni sia materiali che psicologici mediante incidenti in grado di creare un gran numero di vittime e/o produrre severi danni a servizi essenziali per la popolazione (ovvero per le forze avversarie). Questo perché la distruzione di servizi essenziali da un lato esalta, nell'immaginario collettivo, la potenza dell'attaccante mentre dall'altro crea nella popolazione colpita un senso di frustrazione legata all'inefficienza delle autorità governative.

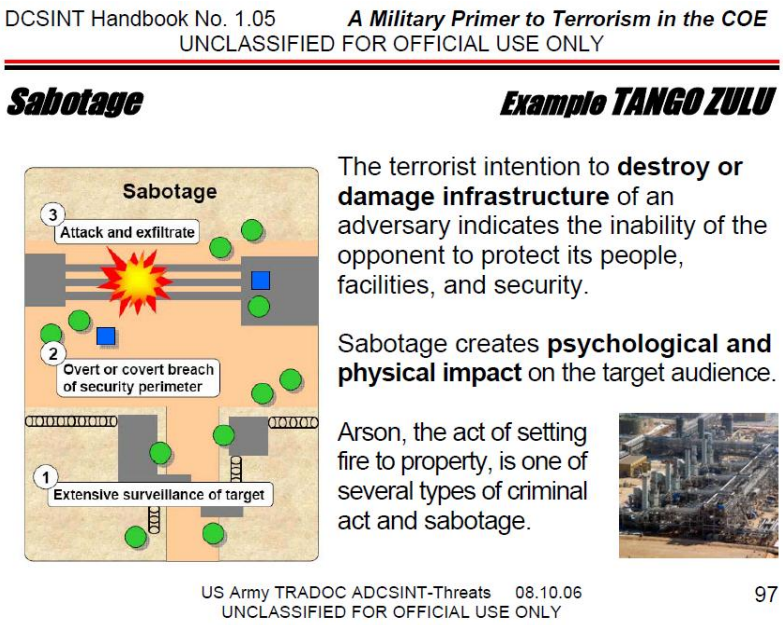


Figura 17. Esempio di un attacco terroristico ai fini di sabotaggio (fonte DCSINT – A Military Primer to Terrorism in COE - Handbook 1.05)[63].

In questo contesto, gruppi terroristici possono perpetrare azioni contro singoli elementi di infrastrutture quali gasdotti, impianti di trattamento delle acque, tralicci, sottostazioni

[62] Questo anche per limitare la circolazione delle informazioni.
[63] http://www.fas.org/irp/threat/terrorism/sup5.pdf

elettriche, antenne per telecomunicazioni, ecc. al fine di creare la percezione che "nulla è al sicuro".

Questa situazione è resa possibile anche dal fatto che la gran parte delle infrastrutture critiche sono disperse sul territorio, molte volte anche in aree rurali e/o di difficile accesso, facilmente individuabili (si pensi ad esempio una linea ferroviaria o ad un traliccio elettrico) e con una scarsa possibilità di sorveglianza.

In questo contesto, come evidenziato nel DCSINT Handbook n. 1.02 dell'agosto 2006 "**Crititical Infrastructure – Threats and Terrorism" del US Army Training and Doctrine Command**[64]", ed in accordo con la schematizzazione a tre livelli illustrata nel **capitolo 6** per ciascuna infrastruttura critica occorre tener presente che i possibili obiettivi di azioni dolose sono gli assets di natura:

> ***Physical*** *– Gli assets fisici includono tanto elementi tangibili (come componenti, apparati, edifici, prodotti, animali, etc.) che beni intangibili (come, ad esempio, le informazioni).*
>
> ***Human*** *– Le risorse umane includono sia il personale, che è necessario proteggere, che tutti coloro che possono rappresentare un insider threat (ossia soggetti con accessi privilegiati ai sistemi informativi, personale di ditte di manutenzione, ecc.).*
>
> ***Cyber*** *– l'ambito Cyber comprende sia gli apparati (hardware) che la componente di applicazioni (software) ed i relativi dati oltre che le reti che garantiscono la funzionalità.*

**[DCSINT Critical Infrastructure – Threats and Terrorism – Handbook n. 1.02]**

[64] http://www.fas.org/irp/threat/terrorism/sup2.pdf

Tenendo presente l'estensione e la complessità di ogni infrastruttura critica è immediato constatare che i possibili obiettivi sono talmente tanti da rendere praticamente impossibile una loro protezione di tutti i singoli elementi costituenti.

Per meglio comprendere l'attrattività di un possibile target, occorre delineare un profilo, per quanto sintetico, del potenziale attaccante.

L'immagine usuale del terrorista è quella di un soggetto che opera all'interno di un gruppo perseguendo una specifica agenda politica e motivato da un'ideologia o desiderio di "liberazione" di un gruppo etnico e/o nazionale. Orbene, se questa visione è corretta per alcune frange del terrorismo, il fenomeno è maggiormente complesso e variegato spaziando da organizzazioni sovra-nazionali fortemente para-militari come al-Qaida fino a gruppi locali (domestici) con limitate capacità ed obiettivi specifici.

Una tassonomia dei vari gruppi dovrebbe includere:

**Separatisti**. Gruppi che ricercano l'autonomia politica o religiosa, ovvero l'indipendenza rispetto ad una situazione di dominazione/oppressione.

**Etnocentrici.** Sono gruppi che promulgano la superiorità di specifici gruppi etnici, dove la componente etnica è anche assunta quale elemento di coesione e di identificazione.

**Nazionalisti**. Gruppi il cui fattore motivante è la lealtà e la devozione ad una nazione, la cui coscienza nazionale è posta al di sopra della cultura di altri gruppi o realtà nazionali.

**Rivoluzionari**. Gruppi il cui obiettivo è il rovesciamento di un ordine stabilito, e la sostituzione con una nuova struttura politica o sociale.

**Gruppi eversivi di estrema destra**. Gruppi generalmente descritti come reazionari che propugnano l'uso della violenza per l'affermazione di un'identità ideologica superiore. Esempio ne sono le associazioni Fasciste o Neo-fasciste.

**Gruppi eversivi di estrema sinistra**. Gruppi a volte descritti come radicali che propugnano la violenza quale strumento per la lotta di classe e l'emancipazione del

proletariato. Esempio ne sono i socialisti o comunisti di tradizione Maoista o Marxista-Leninista.

**Religiosi.** Molti importanti culti religiosi nel mondo sono esempi di estremismo. Alcune persone usano la violenza ed il terrore quale dottrina essenziale della loro religione, anche per contrastare l'altrui ovvero promuovere il proprio credo.

**Anarchici**. I gruppi anarchici si pongono come anti-autorità e anti-governo, e supportano fortemente la libertà individuale e le associazioni volontarie e i gruppi cooperativi. Spesso veicolano messaggi anti capitalisti e comunisti, e promuovono le piccole comunità come le migliori organizzazioni politiche.

**Estremisti Animalisti o Ambientalisti**. Per quanto paradossale, questi gruppi sono divenuti uno dei movimenti più significativi di terrorismo domestico, questo particolarmente in USA, dove gruppi con tali matrici ideologiche perpetrano azioni di sabotaggio verso quei sistemi/soggetti che a loro dire danneggiano l'ambiente e/o torturano gli animali. L'Earth Liberation Front (ELF) è un esempio di tali gruppi.

La tipologia di gruppo terroristico influenza fortemente il valore simbolico del singolo obiettivo, e quindi la relativa scelta dello stesso. Gruppi anarchici (ed analogamente per i gruppi animalisti o ambientalisti), ad esempio, prediligono azioni contro infrastrutture finanziarie (soprattutto banche) ed energetiche, in quanto espressione diretta del sistema antagonista e, al tempo stesso, sono obiettivi che consentono di minimizzare il potenziale effetto diretto sulle persone (la volontà, in genere, non è quella di colpire le persone, ma solo il sistema).

Approccio diametralmente opposto si ha per i gruppi con una forte connotazione religiosa/politica, il cui fine destabilizzante viene perseguito con una scelta di obiettivi in grado di creare il massimo panico nell'avversario, attraverso l'annientamento fisico del maggior numero di soggetti possibile.

Gruppi nazionalistici (anti-occupazione) puntano ad obiettivi che hanno un diretto e concreto impatto sugli interessi e/o sull'operatività dei soggetti occupanti. Ciò si traduce nell'individuazione di obiettivi quali arterie viarie, ferroviarie ed energetiche (in particolare infrastrutture Oil&Gas) che, oltre ad un effetto diretto in termini di perdite di vite umane, comportano ingenti tempi e risorse per il ripristino.

A tutto ciò occorre aggiungere che, negli ultimi anni, anche a seguito della guerra al terrorismo condotta su scala planetaria, si è osservato un cambiamento organizzativo profondo nelle galassie terroristiche con una progressiva disgregazione di organizzazioni articolate ed estese (come al-Qaida) a vantaggio di strutture composte da piccoli gruppi o da singoli individui, che operano in modo autonomo ed isolato perseguendo obiettivi e finalità autonome pur condividendo strategie e fini comuni.

Sulla scorta dei dati raccolti dal **National Counterterrorism Center**[65] nel solo 2010 ci sono stati più 11.500 attacchi terroristici in 72 nazioni che hanno provocato oltre 50.000 vittime ed almeno 13.200 morti.

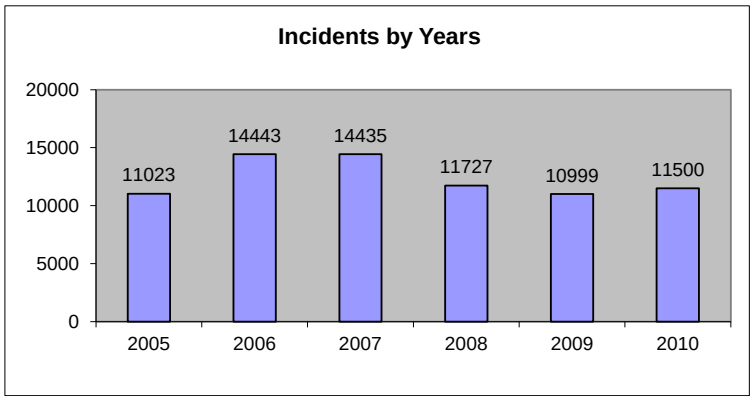


Figura 18. Numero di attacchi terroristici per anno (elaborazione dell'autore sui dati del National Counterterrorism Center).

Come evidenziato nella **figura 18**,ciò si traduce in un aumento di circa il 5% rispetto al precedente anno relativamente al numero di attacchi, a cui corrisponde, fortunatamente, una riduzione di circa il 12% nel numero delle vittime (**figura 19**).

[65] http://www.nctc.gov/

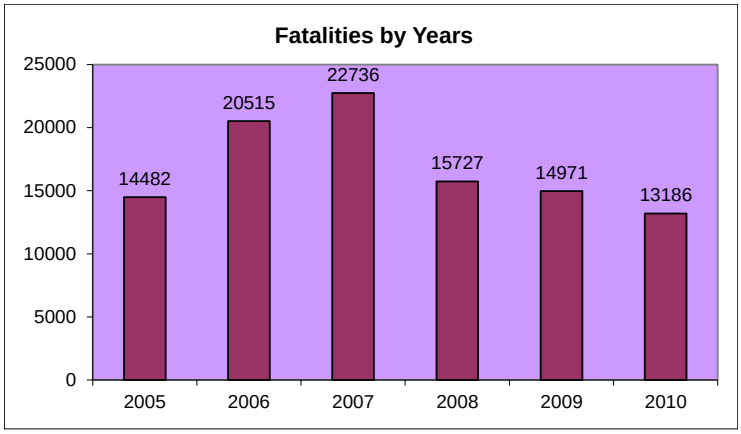


Figura 19. Numero di vittime dovute ad attacchi terroristici per anno (elaborazione dell'autore sui dati del National Counterterrorism Center).

Nel quadro generale occorre rilevare l'aumento degli attacchi in Afghanistan ed in Iraq. Nel solo Iraq sono avvenuti quasi un quarto del numero complessivo di attacchi terroristici nel 2010 (con oltre 12.087 vittime, di cui 2.704 morti).

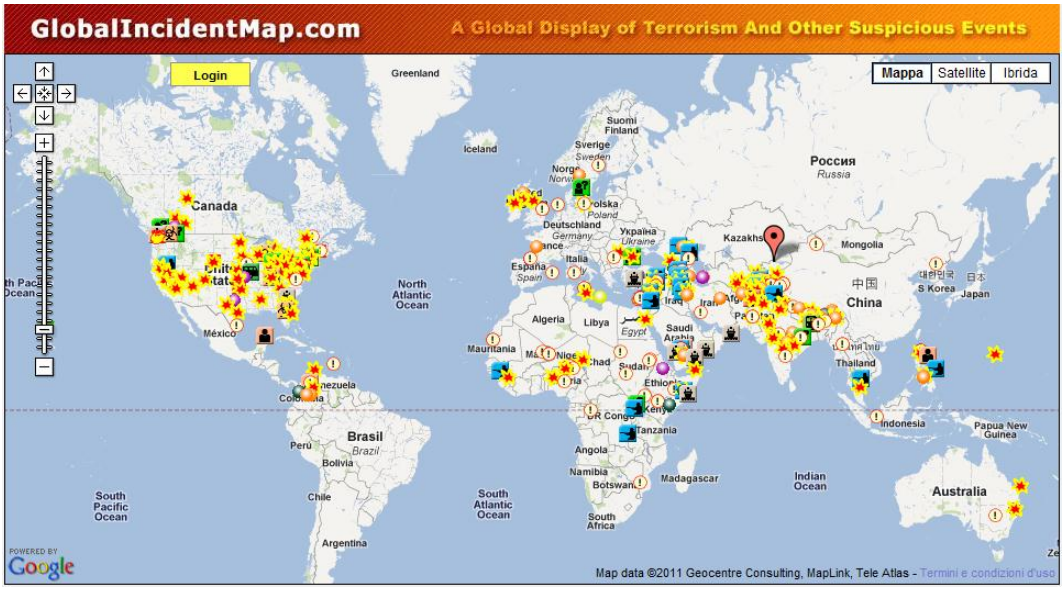


Figura 20. Il sito **http://www.globalincidentmap.com/** fornisce in tempo (quasi) reale una mappa con i principali incidenti/attacchi terroristici nel mondo (oltre che mappe tematiche relative ad eventi/incidenti che riguardano specifiche infrastrutture).

Volendo considerare gli obiettivi si ha, come evidenziato nella **figura 21**, che nel 2010 circa 500 attacchi (pari a poco più del 3%) hanno interessato in modo diretto infrastrutture critiche (per la stragrande maggioranza impianti energetici e reti di trasporti).

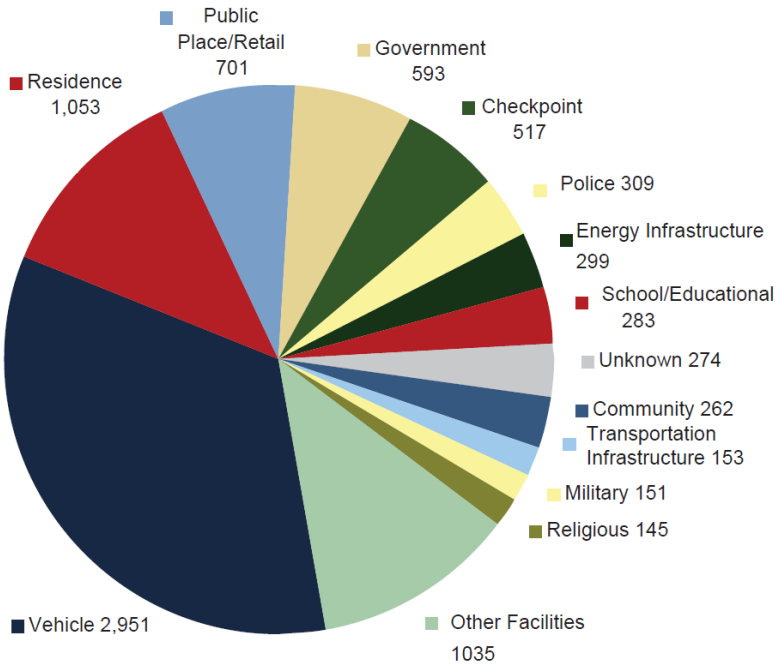


Figura 21. Attacchi terroristici nel 2010 contro "Facilities" suddivise per tipologia di facility (Totale attacchi 15.954 contando più volte attacchi a più facility) (Fonte: **NCTC- 2010 Report on Terrorism**[66]).

Un'analisi più dettagliata degli attacchi verso le infrastrutture critiche, nonché delle relative motivazioni, è stata condotta dall'**Università della California**[67], che nel 2007 ha pubblicato un rapporto in cui sono analizzati 1.084 attacchi occorsi ad infrastrutture critiche nel periodo dal 1933 al 2004. Tale studio evidenzia in primo luogo un aumento del numero di attacchi nel corso degli anni fino ad un picco massimo nella decade 1980-89.

La quasi totalità degli attacchi è stata perpetrata con l'utilizzo di esplosivi (82% del totale). Tale dato è coerente con quanto riportato nel *NCTC 2010 Report on Terrorism* che evidenzia come quasi un terzo della totalità degli attacchi terroristici (inclusivi delle azioni suicide) è stata condotta utilizzando esplosivi e che questa tipologia di attacco è quella che risulta contraddistinta dagli esiti maggiormente letali (quasi il 70% delle morti in attacchi terroristici è dovuto ad attacchi con esplosivi).

La preferenza da parte dei terroristi nell'utilizzo dell'esplosivo quale arma di distruzione trova una sua genesi, oltre che nell'efficienza del mezzo e nella relativa facilità di

[66] http://www.nctc.gov/witsbanner/docs/2010_report_on_terrorism.pd
[67] G. Ackerman, P. Abhayaratne, J. Bale, A. Bhattacharjee, C. Blair, L. Hansell, A. Jayne, M. Kosal, S. Lucas, K. Moran, L. Seroki, S. Vadlamudi, "Assessing Terrorist Motivations for Attacking Critical Infrastructure", UCRL-TR-227068, 2007, https://e-reports-ext.llnl.gov/pdf/341566.pdf

reperimento e trasporto, anche in ragioni storiche ed ideologiche per le quali, soprattutto in ambienti anarchici e rivoluzionari, la dinamite era vista come una forza equilibrante capace, cioè, di mettere uno stato ed un individuo sul medesimo livello[68].

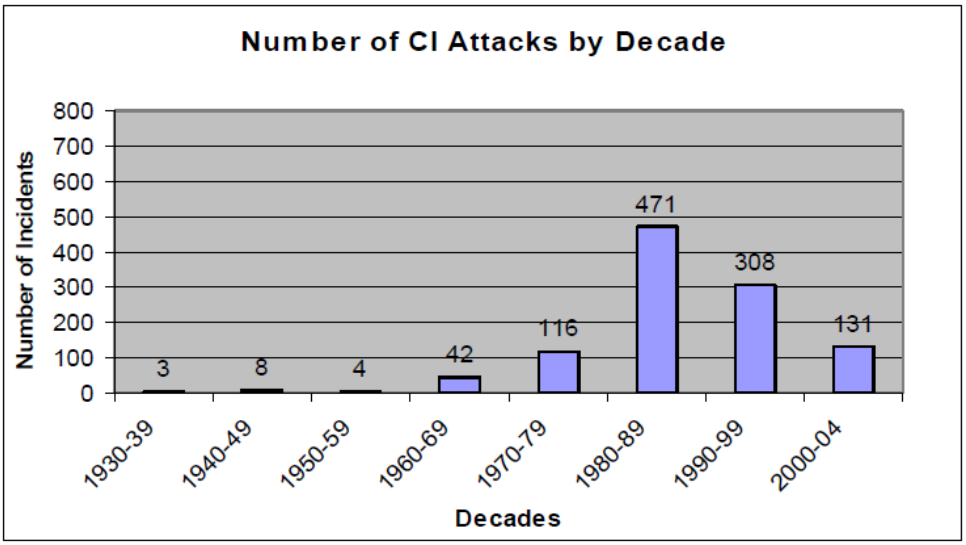


Figura 22. Numero di attacchi alle infrastrutture critiche per decade.
(Fonte: **Assessing Terrorist Motivations for Attacking Critical Infrastructure**).

Lo studio condotto dalla University of California evidenzia che ben il 29% delle azioni terroristiche perpetrate contro infrastrutture critiche è avvenuto in Europa e che, globalmente, l'infrastruttura critica maggiormente interessata è stata quella finanziaria contro di cui si è concentrato circa l'11% degli attentati.

Se, invece, si vanno a considerare gli effetti di tali azioni, si vede che quelle che hanno causato il maggior numero di vittime (escludendo gli attacchi del 9 /11 e quello perpetrato con il SARIN nella metropolitana di Tokio del 1995) sono le azioni contro le infrastrutture Gas&Oil, che hanno comportato da sole il 36% dei 1.814 morti globalmente causati da tutti questi attacchi.

Questi dati evidenziano come nella stragrande maggioranza degli attacchi verso infrastrutture l'obiettivo primario è quello simbolico e/o funzionale.

Infatti, soprattutto in Europa, la maggior parte delle azioni terroristiche perpetrate contro infrastrutture critiche ha una valenza antagonista e quindi orientati verso obiettivi con una

[68] Walter Reich, ed., Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind, rev. ed. (Washington: Woodrow Wilson Center Press, 1998), 264-265.

forte valenza simbolica (azioni contro le infrastrutture finanziarie ed energetiche), in molti casi scegliendo obiettivi che limitano il rischio di vittime.

Contrariamente, le azioni in medio oriente, Iraq in testa, si concentrano invece contro le infrastrutture Oil&Gas, che rappresentano bersagli di difficile, se non impossibile, protezione la cui distruzione comporta danni economici estremamente rilevanti per gli interessi delle forze "straniere". Per questa tipologia di attacchi, le perdite di vite umane assumono quasi una valenza collaterale, rispetto al primario obiettivo che è la volontà di colpire gli interessi patrimoniali delle forze straniere.

In questo quadro gli aspetti sistemici sembrano essere per i terroristi meno essenziali se non addirittura quasi del tutto trascurati, così come la valenza di utilizzo dell'infrastruttura stessa come weapon per infliggere un danno maggiore all'avversario.

Rispetto a ciò, fanno eccezione gli attacchi più devastanti degli ultimi anni, includendo tra questi sia gli eventi del 9/11, sia gli attacchi di Madrid (2004) e Londra (2005), sia l'azione del 1995 nella metropolitana di Tokio.

Nello specifico i terroristi hanno sfruttato, tanto negli attacchi di Madrid, quanto in quelli di Londra e di Tokio, le caratteristiche dell'infrastruttura ferroviaria/metropolitana con l'obiettivo di ottenere, oltre che il più elevato numero di vittime possibili, anche un forte disorientamento da parte dei primi soccorritori. Ciò ha comportato non solo azioni di soccorso meno efficienti, ma anche comunicazioni disorientanti all'opinione pubblica, con conseguente amplificazione del senso di frustrazione legata all'inefficienza delle autorità governative. Infatti, soprattutto nell'attacco londinese ed in quello di Tokyo, gli attacchi multipli verificatisi in rapida e sincronizzata successione in più punti della rete metropolitana, hanno dato adito, nella confusione dell'immediatezza, ad una ridda di ipotesi su quanto stava succedendo.

L'episodio del 9/11 rappresenta, invece, un salto di qualità, in quanto non solo si è utilizzata un'infrastruttura (quella aera) quale arma (weapon) per sferrare un attacco ad un diverso obiettivo, ma anche le modalità di esecuzione e gli obiettivi scelti, e nello specifico le Twin-Towers, oltre ad avere una forte valenza simbolica si caratterizzavano per la capacità di produrre effetti secondari. Infatti il solo verificarsi di quattro dirottamenti contemporanei nei cieli americani, con una fine tragica per tutti i passeggeri, ha avuto un

impatto sulla propensione a volare a livello mondiale riassorbita solo dopo diversi anni. In modo analogo, gli attentatori avevano messo in conto quali conseguenze del loro attacco non tanto i crolli delle torri stesse, il cui cedimento ha sorpreso molti esperti, quanto le ripercussioni sulla finanza mondiale, giocando in particolare sulla prossimità geografica di Wall Street all'area dell'impatto (interdipendenza geografica). Il fatto che, nell'area, operassero anche tantissime altre infrastrutture (fra cui importanti nodi di telecomunicazioni), ha ulteriormente amplificato gli effetti dell'attentato.

**Esperienza internazionale**

**GENERALE**

# 10 Il ruolo della Difesa per la salvaguardia delle Infrastrutture Critiche

In questo capitolo verrà analizzato in particolare il ruolo che i corpi militari hanno in alcuni paesi per ciò che concerne la protezione delle infrastrutture critiche e, nello specifico, la gestione della minaccia terroristica[69].

In questo contesto occorre sottolineare, come evidenziato anche da Lord Michael Jopling nel suo intervento **all'assemblea della NATO del 2007**[70], che il ruolo svolto dai militari è prevalentemente di supporto, con una maggiore focalizzazione nella gestione delle conseguenze dell'evento dopo il verificarsi dello stesso. Alcune nazioni hanno, però, iniziato ad affidare ai militari ruoli di "extra patrolling force" con lo specifico compito di affiancare e/o sostituire le forze di polizia nei compiti di sorveglianza di obiettivi e siti sensibili (aeroporti, stazioni ferroviarie, ecc.). Lo scopo di queste misure è quello di aumentare la capacità di deterrenza e, nel contempo, di recuperare risorse per le attività investigative.

Un secondo aspetto importante delle attività che vedono convolti i militari nell'ambito della CIP, riguarda la protezione di tutte quelle infrastrutture necessarie per l'assolvimento dei compiti imputati alle forze militari stesse, con riferimento alle attività da condurre sia sul territorio nazionale che all'estero.

In questo capitolo, dopo una breve disamina delle attività messe in atto dalla NATO, ci si soffermerà in modo più esteso sull'analisi dell'organizzazione adottata dagli USA. Nel capitolo successivo si illustreranno brevemente le attività messe in atto da altre nazioni.

[69] Informazioni più generali sul ruolo e l'organizzazione che i singoli stati si sono dati per la più ampia tematica della Protezione delle Infrastrutture Critiche possono essere reperite nel CIIP Handbook pubblicato dal ETH di Zurigo http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

[70] http://www.nato-pa.int/default.asp?SHORTCUT=1165

***NATO***

Il tema della protezione delle infrastrutture critiche è stato oggetto, nel 2003, di un Concept Paper del **Senior Civil Emergency Planning Committee (SEPEC)**[71], che ha delineato una roadmap e sei aree di lavoro che spaziano dallo sviluppo di strumenti e metodologie per il contrasto ad attacchi/incidenti CBRN, alla gestione di disastri naturali ed incidenti occorsi alle infrastrutture critiche stesse. Gli obiettivi principali di tali iniziative riguardano l'incentivo ad un maggiore e migliore information sharing, l'assistenza e la promozione ad attività di training ed esercitazione, oltre che lo studio delle vulnerabilità delle infrastrutture critiche e degli strumenti/metodi per aumentarne la robustezza e la sicurezza.

L'approccio adottato dalla NATO è in qualche misura differente da quanto fatto dalla Comunità Europea così come da molti stati, in primo luogo gli USA, per gli aspetti riguardanti l'impostazione della problematica e anche per ciò che attiene agli strumenti operativi. La tematica è posta sotto il cappello **Civil Emergency Planning CEP**[72] e, di conseguenza, le attività della NATO non sono rivolte a definire uno specifico quadro regolatorio, quanto piuttosto a supportare le attività messe in atto autonomamente dai singoli stati, promuovendo l'adozione di standard e l'interscambio di esperienze e competenze.

***Esperienza USA***

Negli Stati Uniti il Department of Homeland Security (DHS) è la principale autorità preposta alla protezione delle infrastrutture critiche a livello governativo per tutta la nazione. Il DHS, fra le altre attività, sovrintende alla messa in atto di quanto previsto dal **National Infrastructure Protection Plan**[73] che delinea la strategia nazionale per il contrasto alle minacce di natura terroristica, accidentali e naturali verso le diverse infrastrutture critiche. Tale azione è basata sull'identificazione di 11 settori critici, per ognuno dei quali è individuata un'entità governativa che opera come "lead agency", che ha il compito di coordinare tutte le attività messe in atto dalle diverse autorità governative a livello federale, statale e locale, nonché di raccordare tali attività con quelle portate avanti dal settore privato.

[71] http://www.nato.int/issues/scepc/index.html
[72] http://www.nato.int/cps/en/SID-69E4811D-D2CDA608/natolive/topics_49158.htm?selectedLocale=en
[73] http://www.dhs.gov/files/programs/editorial_0827.shtm

In questo quadro, la **Homeland Security Presidential Directive 7** (HSPD-7)[74] assegna al *Department of Defence* (DoD) due distinti compiti nell'ambito della Protezione delle Infrastrutture Critiche statunitensi. Da un lato il DoD è l'agenzia responsabile per la definizione di un approccio collaborativo e coordinato che miri a identificare, valutare e incrementare la sicurezza per quel che concerne le infrastrutture critiche che operano nel settore della Defense Industrial Base (DIB)[75]. L'altro compito è quello, analogamente a tutte le agenzie federali del governo americano, dell'identificazione, della prioritizzazione e della protezione di tutte quelle infrastrutture essenziali al DoD affinchè esso possa garantire la capacità di esecuzione delle proprie funzioni e missioni.

Per dare corso a tali responsabilità, nell'agosto del 2005 il DoD emise la **Directive Number 3020.40**[76] con l'obiettivo di definire le attività ed il ruolo che il DoD deve avere nell'ambito della responsabilità ad esso attribuito dal governo americano per la protezione delle infrastrutture critiche. A tal fine la Direttiva 3020.40 identifica 10 settori critici, di seguito elencati, individuando i corrispondenti soggetti, all'interno delle diverse articolazioni del DoD, che ne hanno la responsabilità.

| DEFENSE SECTOR | LEAD AGENT |
|---|---|
| Defense Industrial Base (DIB) | Director, Defense Contract Management Agency |
| Financial Services | Director, Defense Finance & Accounting Service |
| Global Information Grid (GIG) | Director, Defense Information Systems Agency |
| Health Affairs | Assistant Secretary of Defense of Health Affairs |
| Intelligence, Surveillance, and Reconnaissance (ISR) | Director, Defense Intelligence Agency |
| Logistics | Director, Defense Logistics Agency |
| Personnel | Director, DoD Human Resources Activity |
| Public Works | Chief, U.S. Army Corps of Engineers |
| Space | Commander, U.S. Strategic Command |
| Transportation | Commander, U.S. Transportation Command |

[Fonte **Directive Number 3020.40**]

[74] http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm
[75] Uno degli 11 settori indentificati quali critici a livello governativo.
[76] http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf

Si tenga presente che per DoD, per Protezione delle Infrastrutture Critiche si intende

> *The actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc.*

**[DoD Directive 3020.40, 2005]**

Si noti che il concetto assunto per l'individuazione di infrastruttura e/o risorsa critica dal DoD è quello del *Mission Based Screening*[77], ossia in termini individuazione di quelle risorse essenziali allo svolgimento delle funzioni proprie del DoD stesso.

La **figura 23** fornisce un organigramma delle responsabilità e dipendenze funzionali dei diversi soggetti coinvolti nell'ambito del DoD per la protezione delle Infrastrutture Critiche.

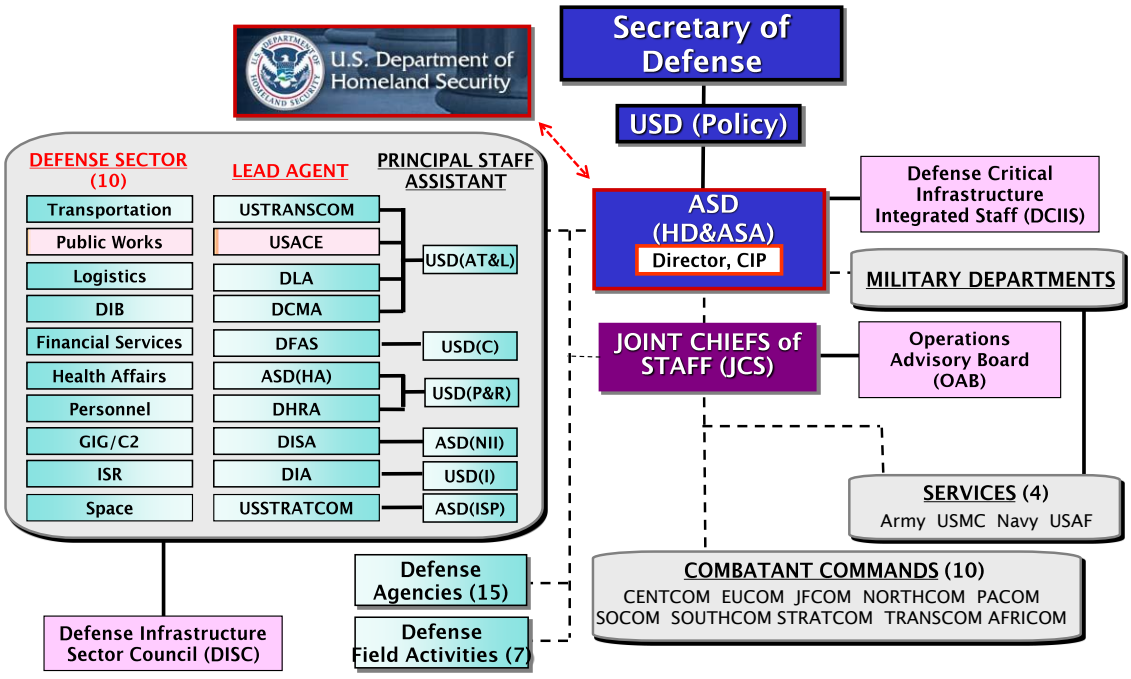


Figura 23. Organigramma dell'organizzazione e dei legami del DoD (Fonte: N. Kathir presentazione al 7th Annual Readiness and Homeland Security Seminar, 2010.

[77] Si ricorda che per l'individuazione delle infrastrutture critiche a livello nazionale, invece, l'approccio seguito dal governo americano, analogamente a quello portato avanti dalla Commissione Europea, è una valutazione sulla base delle potenziali conseguenze connesse con la loro failure (Consequences based Screening).

Come si evidenzia dalla **figura 23**, l'organizzazione proposta si basa da un lato su una precisa individuazione di responsabilità per i singoli aspetti (potremmo dire con una competenza settoriale) che però sono raccordati da una struttura centrale che ha il compito di gestire gli aspetti di interdipendenza (inter-settoriali) sia fra i sotto-settori del DoD che per quel che riguarda il raccordo con le altre autorità esterne al DoD.

In questo quadro, un elemento centrale è il ***Defence Critical Infrastructure Progam*** (DCIP)[78] il cui obiettivo è quello di aumentare la capacità di risk-management e decision making per far sì che le diverse infrastrutture critiche siano in grado di erogare i relativi servizi consentendo al DoD di svolgere le proprie funzioni e missioni.

Il processo decisionale messo a punto dal DCIP è schematizzato nella **figura 24**.

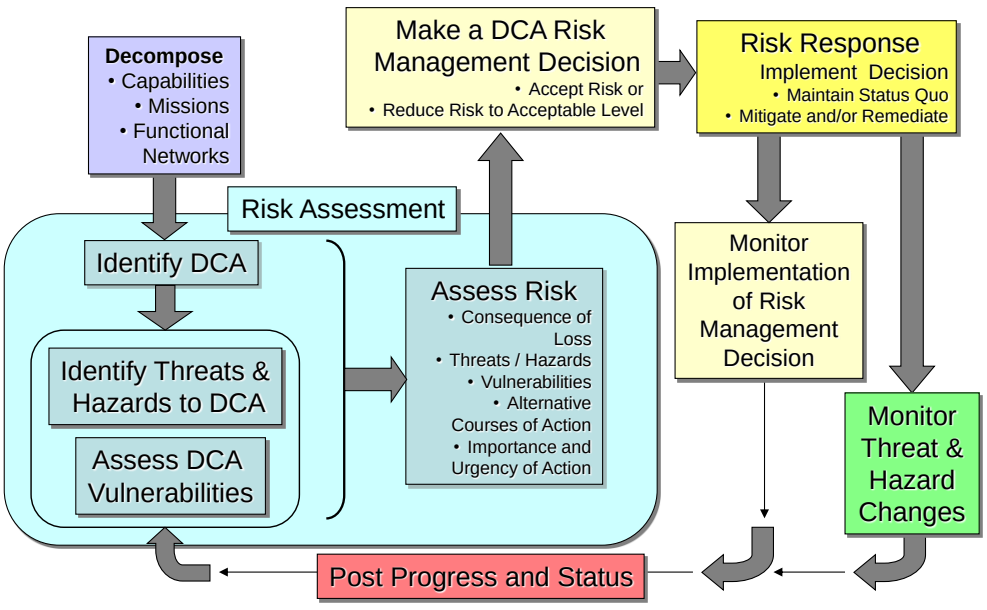


Figura 24. Schematizzazione dei principi elementari del processo di Identificazione, Prioritizzazione, Valutazione definizione delle Risposta (Mitigazione/Rimedio/Accettazione) (Fonte: N. Kathir presentazione al 7th Annual Readiness and Homeland Security Seminar, 2010).

Esso particolarizza alla realtà del DoD l'approccio generale proposto nel **National Infrastructure Protection Plan** (NIPP)[79].

[78] http://policy.defense.gov/hdasa/dcip/
[79] http://www.dhs.gov/files/programs/editorial_0827.shtm

Nello specifico il “DoD CIP life cycle”, che mira ad assicurare l’integrità della DCA/TCA[80], è composto da sei fasi, che hanno applicazione prima, durante e dopo un evento che può compromettere o degradare l’infrastruttura stessa.

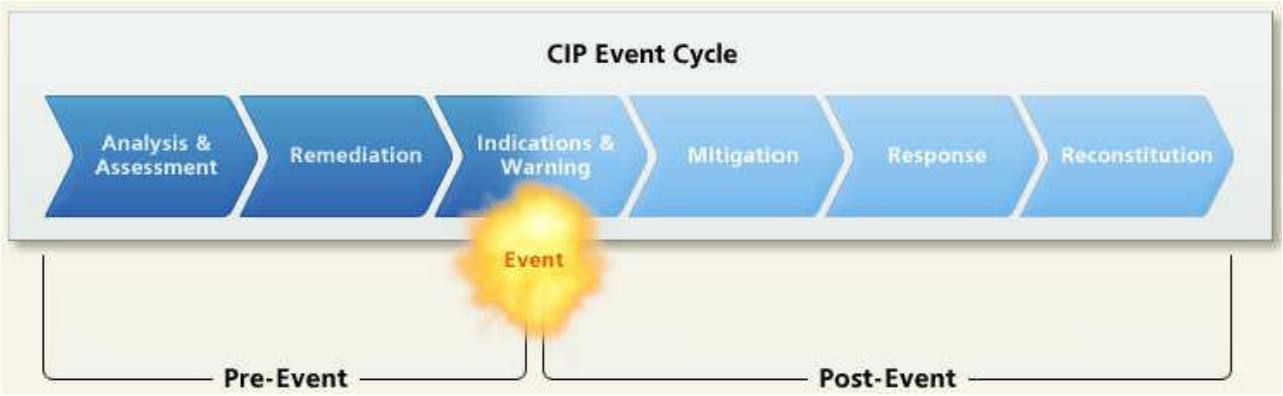


Figura 25. CIP life cycle (Fonte: National Infrastructure Protection Plan).

*Phase 1: Analysis & Assessment* (prima dell’evento)

Essa mira ad identificare, in ciascuno dei dieci settori critici per il DoD, gli assets fondamentali, determinandone le vulnerabilità, le interdipendenze, le configurazioni e le caratteristiche. Si valuta quindi l’impatto operazionale di un’eventuale degradazione o totale perdita dell’infrastruttura. Questa operazione, semplice per risorse geograficamente localizzate in un area ristretta e ben definita, diventa complicata se esse si estendono lungo link e nodi geograficamente dispersi.

Questa prima fase viene a sua volta divisa in quattro passi:

- Identificazione degli asset critici: la criticità di una risorsa è funzione sia del tempo che della particolare situazione, valutata basandosi sul valore operativo o economico;
- Operational Impact Analysis: sviluppo di matrici di dipendenza operazionale e applicazione di metodi di ricerca operativa;
- Vulnerability assessment;
- Analisi delle interdipendenze: finalizzata a mappare funzioni e risorse critiche. Come risultato di questa analisi, le criticità dei vari assets possono essere aggiornate o aggiunte rispetto a quelle precedentemente individuate.

[80] Defence Critical Asset/Task Critical Asset.

Tale approccio prevede che, stante il fatto che la protezione di tutti gli assets è pressoché impossibile, la priorità è data a quei componenti fisici, umani e cyber la cui distruzione ha un impatto debilitante sulla funzionalità del DoD. Essi rappresentano i ***Defence Critical Asset*** (DCA), ossia:

> ***Defence Critical Asset (DCA)****: un asset di straordinaria importanza per l'operatività del DoD in condizioni di pace, crisi e guerra tale che la sua indisponibilità o distruzione potrebbe avere seri e debilitanti effetti nella capacità del DoD di svolgere correttamente le sue funzioni.*
>
> **[DoDD 3020.40]**

Per rendere maggiormente operativa l'analisi con la DoDI 3020.45 è stato introdotto il concetto di ***Task Critical Asset (TCA)***

> ***Task Critical Asset (TCA)****: è un elemento (fisico, umano o cyber) di tale importanza che l'incapacità del suo corretto funzionamento o la sua distruzione potrebbero avere un serio e debilitante impatto sulle capacità di uno o più componenti/strutture del DoD di eseguire le loro funzioni/missioni.*
>
> **[DoD 3020.45]**

Nello specifico, i comandanti di ciascuna unità che operano all'interno dei 10 settori critici individuati dal DoD devono considerare le conseguenze dell'assenza temporanea/permanente dei servizi erogati da ciascuna infrastruttura, da cui essi dipendono per gli effetti sulla capacità di portare a termine le relative missioni. Per ciascuna risorsa valutata critica va quindi eseguita un'analisi di vulnerabilità per verificare quale sia il relativo livello di fragilità. Tale attività va eseguita sia per quel che riguarda le componenti del sistema interne al controllo del DoD, sia per ciò che riguarda le componenti esterne ad esse. Dopo questa analisi "dal basso" le varie informazioni

vengono centralizzate al fine di analizzare le problematiche di interdipendenza ed individuare le priorità.

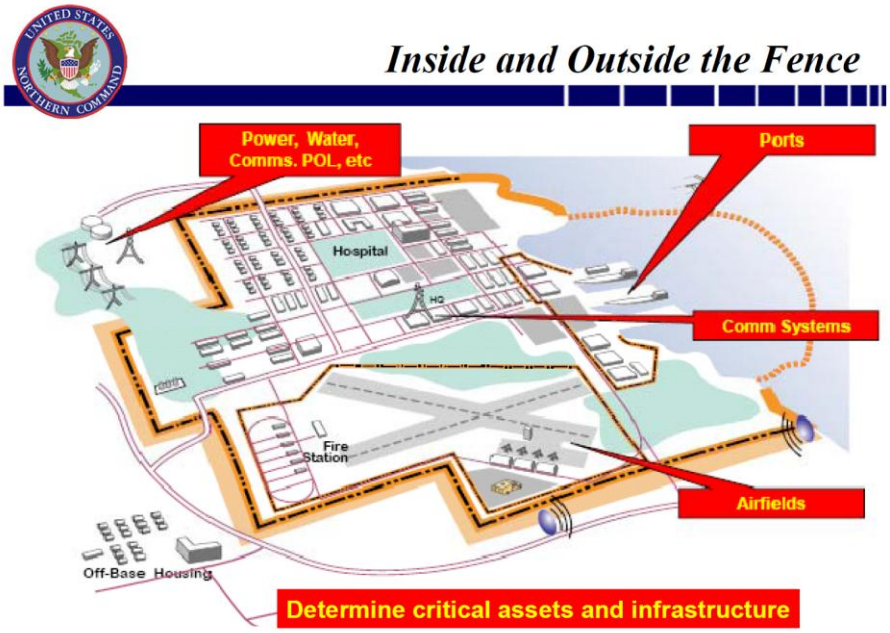


Figura 26. La determinazione degli assets critici va effettuata sia con riferimento alle risorse interne al dominio militare che rispetto alle funzionalità esterne al perimetro militare la cui assenza o degradazione può, però, compromettere la capacità operativa miliare (Fonte: B. Brech, USNORTHCOM Defense Critical Infrastructure Program (DCIP) & Critical Infrastructure Protection (CIP)).

*Phase 2: Remediation* (prima dell'evento)

Tale fase riguarda la messa in atto di misure precauzionali necessarie per rimediare alle vulnerabilità fisiche, organizzative e cyber precedentemente rilevate. Questa fase include la formazione e la awareness, e produce cambiamenti nei processi operativi, nelle procedure, nelle configurazioni e nelle singole componenti. L'obiettivo è il miglioramento dell'affidabilità, disponibilità e sopravvivenza degli assets critici e delle infrastrutture, indipendentemente dalla causa della vulnerabilità e dal tipo di minaccia.

*Phase 3: Indications and Warnings* (prima e/o durante l'evento)

Tale attività consiste nel monitoraggio costante di ciascun settore, per determinare se ci sono evidenze di eventi potenzialmente pericolosi da riportare. Le *Indications* sono segnali preparatori che indicano l'imminenza di un evento, programmato o meno, che riguarda un'infrastruttura. Esse sono basate su input a livello tattico (provenienti dai proprietari dell'asset), funzionale, operazionale (da strutture "regionali", come NATO, intelligence, enti di governo, ecc.), o strategico (se provengono dall'intelligence, dalle forze dell'ordine e dal settore privato). Se viene individuata una *Indication*, una notifica di *Warning* indicante la possibilità di una minaccia o pericolo viene inviata ai proprietari degli assets. Ciascuno dei dieci settori deve quindi sviluppare un Defense Sector Assurance Plan che determina quali condizioni ed azioni sono monitorate e contiene un compendio di incidenti da monitorare e riferire, composto da tre tipologie di incidenti:

- *Nationally-defined reportable incidents;*
- *DoD-defined reportable incidents;*
- *Sector-defined reportable incidents.*

in funzione del potenziale impatto e della relativa minaccia.

*Phase 4: Mitigation* (prima e durante l'evento)

Comprende le azioni intraprese prima e durante un evento in risposta ad un allarme a un incidente. Tali azioni, a carico dei proprietari degli assets critici del DoD, delle installazioni del DoD, e degli operatori militari, mirano a minimizzare l'impatto operativo derivante dalla perdita o debilitazione di un asset critico, facilitare la risposta all'incidente, e ripristinare rapidamente il servizio danneggiato.

Tra gli obiettivi primari di questa fase, vi è anche quello di minimizzare l'impatto operativo sugli altri assets e infrastrutture critiche non direttamente coinvolti. Le azioni della *Mitigation* sono anche di aiuto e facilitazione per le fasi successive di risposta all'incidente e ricostruzione.

*Phase 5: Incident Response* (dopo l'evento)

Comprende la pianificazione delle attività da intraprendere per eliminare la causa o la fonte dell'evento. Le attività di risposta includono le misure di emergenza messe in atto da terze parti, come forze dell'ordine, soccorso medico, vigili del fuoco, artificieri, agenzie investigative, ecc., nei confronti dell'infrastruttura coinvolta.

*Phase 6: Reconstitution* (dopo l'evento)

Quest'ultima fase riguarda la ricostruzione o il ripristino delle capacità dell'asset critico dopo avere eliminato o contenuto la causa del danno. La responsabilità maggiore per quest'ultima fase, probabilmente la più complicata e meno sviluppata, è dei proprietari dell'asset critico stesso.

È importante evidenziare come nella strategia del DoD la fase più importante dell'intero ciclo è la *Phase 1 Analysis & Assessment*. Infatti, senza una corretta identificazione della criticità dei singoli asset ed una attenta valutazione delle rispettive vulnerabilità, l'implementazione delle altre fasi risulta sostanzialmente di scarso impatto.

Al fine di fornire una linea guida per l'individuazione degli assets critici, l'enclosure 6 del **Manual 3020.45**[81] fornisce, per ognuno dei 10 settori critici per il DoD le funzioni primarie, mentre le agenzie responsabili della protezione dei singoli settori hanno il compito di determinare, per ciascuna funzione, le relative sotto-funzioni essenziali.

A tiolo di esempio, per quel che riguarda il Public Work Sector, le cui funzioni sono Provide and Maintain Utilities, Provide and Maintain Real Property e Provide Emergency Services si considerano, in modo non esclusivo, le seguenti sotto-funzioni:

[81] http://www.dtic.mil/whs/directives/corres/pdf/302045V5p.pdf

| Provide and Maintain Utilities - In support of Defense Critical Infrastructure | |
|---|---|
| **Sub Function** | **Description** |
| Provide Water | **In Support of DCI Assets Include:** Reservoirs, water supply, wells, treatment plants, dams, rivers, desalinization plants, mains, storage tanks, valves/hydrants, back flow prevention, pumping stations, treatment stations |
| Management of Waste Water | **In Support of DCI Assets Include:** Treatment facilities of waste water, sanitary sewer mains, pump stations, force mains, leech fields, storm drains |
| Provide Physical Infrastructure for Communications | **In Support of DCI Assets Include:** Fiber optics, cables, SCADA systems |
| Provide Natural Gas | **In Support of DCI Assets Include:** Distribution systems, storage facilities, SCADA systems |
| HVAC<br><br>(Heating, Ventilating, and Air Conditioning) | **In Support of DCI Assets Include:** Central chiller plants, pumps, cooling towers, evaporators, condensers, distribution systems, regulators, SCADA systems, boilers, furnaces, feed pumps, heat exchangers, heat pumps, heaters, humidifiers/dehumidifiers, compressors, exhaust fans, boiler plants, steam plants, environment control facilities |
| Provide Petroleum | **In Support of DCI Assets Include:** Distribution systems, storage facilities, SCADA systems |
| Provide Electric Power | **In Support of DCI Assets Include:** Electric power generation facilities, SCADA systems, generators, transmission lines, distribution lines, substations, transformers, and switches |
| **Provide and Maintain Real Property - In support of Defense Critical Infrastructures** | |
| **Sub Function** | **Description** |
| Transportation Networks | Maintenance of installation transportation networks (i.e. road, air facilities) within installation boundaries |
| Maintain Buildings that Contain Defense Critical Infrastructures | Maintaining all physical real property infrastructures |
| **Provide Emergency Services - In support of Defense Critical Infrastructures** | |
| **Sub Function** | **Description** |
| Emergency Infrastructure Support | Utilities restoration and emergency building repairs |

Lo stesso **Manual 3020.45**[82] fornisce anche un esempio applicativo (svolto in modo poco dettagliato) relativo al US Northern Command (USNORTHCOM) che ha, fra le altre, la missione di garantire la difesa aerea del Nord America. Per garantire tale missione sono stati identificati i diversi TCA e per ognuno di essi è stato valutato l'effettivo impatto in caso di default (validazione), mentre per quelli effettivamente critici è stata effettuata anche una Sector Interdependency Analysis al fine di evidenziare se e quali ulteriori infrastrutture potrebbero causare la non disponibilità dei relativi TCA. Nello specifico esempio è stato individuato come critico, fra le altre cose, un deposito di carburante considerato l'unico in grado di garantire l'approvvigionamento dei jet, e la successiva analisi di interdipendenza ha evidenziato la presenza di un ponte la cui distruzione avrebbe causato la necessità di un re-routing tale da non consentire più il soddisfacimento degli obiettivi della missione, con la conseguente identificazione di tale ponte come TCA per il DoD.

Una metodologia ampiamente utilizzata dal DoD per la determinazione delle vulnerabilità delle singole infrastrutture è quella del ***Red Teaming***, ossia l'analisi dei potenziali target con una prospettiva di attacco (rispetto ad un'ottica di sola protezione) al fine di evidenziare tanto possibili vulnerabilità del sistema, quanto modalità e tecniche di attacco. Essa si estrinseca in azioni "aggressive" condotte dal Red Team con l'obiettivo di scoprire (e sfruttare) vulnerabilità fisiche, cyber e organizzative al fine di indentificare le stesse prima che ciò possa essere fatto da un potenziale nemico. Questa metodologia, complementare alle analisi condotte con metodi di intelligence tradizionali, consente una diversa, e per certi versi migliore, stima di quelle che potrebbero essere le intenzioni e le potenzialità dell'avversario. Tale Red Team è, alle volte, contrapposto ad un *Bule Team* il cui compito è identificare e neutralizzare in tempo reale le attività perpetrate dal Red Team o, più in generale, si configura come un "penetration" test i cui risultati rappresentano un valido elemento di partenza per la valutazione del livello di robustezza del sistema. C'è da evidenziare che, purtroppo, per molte delle infrastrutture critiche tale tipologia di analisi può essere solo in parte portata a termine sui sistemi in esercizio a causa del rischio di provocare accidentalmente malfunzionamenti e/o guasti, così come a causa del fatto che, essendo la proprietà/gestione in mano a soggetti privati, lo svolgimento di tali azioni deve essere preventivamente concordato con tali soggetti.

[82] http://www.dtic.mil/whs/directives/corres/pdf/302045V5p.pdf

# 11 Altre esperienze internazionali

A differenza degli Stati Uniti, altre nazioni hanno adottato un approccio strategico diverso. Nel riconoscere le problematiche di sicurezza “All Hazard” legate alla protezione delle infrastrutture critiche, più che distribuire responsabilità ad una pluralità di soggetti, è stato scelto di operare una riorganizzazione della macchina statale allo scopo di creare o espandere le competenze di agenzie governative a cui è affidata in maniera quasi esclusiva la problematica della protezione delle infrastrutture critiche.

In ogni caso, quello che emerge è che, in parallelo ad una organizzazione della macchina governativa in grado di confrontarsi in modo coerente con il mutato contesto socio-tecnologico, le diverse nazioni hanno sviluppato documenti di strategy il cui obiettivo è quello di delineare non solo il ruolo e la responsabilità dei singoli attori, ma anche obiettivi di medio e lungo termine per le singole attività.

***Gran Bretagna***

In maniera similare all’impostazione statunitense, in Gran Bretagna il Home Office è l’autorità deputata alla protezione delle infrastrutture critiche nazionali. Nello specifico, il tema della protezione delle infrastrutture critiche è stato incluso fra le competenze dell’**Office for Security and Counter-Terrorism**[83].

[83] http://www.homeoffice.gov.uk/counter-terrorism/OSCT/

Per gestire al meglio le diverse implicazioni connesse con la minaccia dolosa e terroristica verso le infrastrutture critiche inglesi, il governo ha creato il **Centre for the Protection of National Infrastructure (CPNI)**[84].

Tale organismo, nel cui board siedono rappresentanti del Cabinet Office, del Communications Electronics Security Group (CESG), del Government Communications Headquarters (GCHQ), dei Servizi di Sicurezza (MI5), del Ministero della Difesa e della Polizia, è diretto dal Direttore Generale del Security Service (MI5), ha la responsabilità di promuovere la sicurezza, anche evidenziando eventuali problematiche e vulnerabilità, per tutto ciò che riguarda le infrastrutture critiche nazionali.

***Canada***

L'approccio seguito dal governo canadese è stato quello di riconoscere la valenza All-Hazard e, riconoscendo una frammentazione di responsabilità e di competenze nella protezione, essi intrapresero, fino dal 2003, un complesso meccanismo di riorganizzazione della macchina burocratica che ha portato alla costituzione del **Public Safety Canada**[85], una sorta di super-ministero che ha la responsabilità di coordinare e supportare gli sforzi di tutte le agenzie federali con l'obiettivo di garantire la safety e la security del Canada.

Tale ministero nasce acquisendo ed integrando molteplici agenzie, dipartimenti e competenze (come i servizi di intelligence, la guardia costiera, la polizia Montana, ecc.).

***Germania***

In Germania la prima azione ufficiale per quel che concerne le CIIP è del 1997, quando fu attivata presso il Ministero degli Interni (BMI), sulla scia delle attività poste in essere dal governo americano, una commissione interministeriale per coordinare le diverse iniziative. In particolare per quel che concerne gli aspetti connessi con la sicurezza informatica, essi

[84] Il CPNI ha incorporato il precedente National Infrastructure Security Co-ordination Centre (NISCC) http://www.cpni.gov.uk/
[85] http://www.publicsafety.gc.ca/index-eng.aspx

furono affidati al **Federal Office for Information Security (BSI)**[86], mentre gli aspetti connessi con la sicurezza fisica furono demandati al Centre for the Protection of Critical Infrastructure del Federal Office for Civil Protection and Disaster Response (BBK) in cooperazione con il Federal Office of Administration (BVA) per quel che riguarda gli aspetti di protezione civile e prevenzione dei disastri. Il Federal Office of Criminal Police (BKA) ha il compito di perseguire i crimini perpetrati nei confronti delle infrastrutture critiche.

Un ruolo non trascurabile, stante il fatto che oltre il 90% delle infrastrutture critiche tedesche è gestito da soggetti privati, è svolto dal Federal Ministry of Economics and Labour (BMWA) che ha, fra le altre cose, il compito di garantire la sicurezza del sistema energetico e di quello delle comunicazioni.

Nel 2009 il governo Tedesco ha anche rilasciato il **National Strategy for Critical Infrastructure Protection**[87] che definisce gli obiettivi e l'approccio strategico che il governo vuole perseguire per aumentare la sicurezza e la protezione delle proprie infrastrutture critiche.

***Svezia***

L'esperienza accumulata durante il periodo della Guerra Fredda, unitamente ad una situazione climatica complessa, hanno creato condizioni tali da accrescere, in misura maggiore rispetto ad altre nazioni, le preoccupazioni e da porre l'attenzione governativa sulle problematiche connesse con il corretto funzionamento delle diverse infrastrutture tecnologiche nazionali. Infatti già nel 1999 fu costituita *The Commission on Vulnerability and Security* con il compito di redigere un piano per prevenire e limitare le conseguenze di situazioni di emergenza (sia accidentali che fraudolente) che si sarebbero potute verificare sulle varie infrastrutture critiche ed in particolare su quell'informatica.

La Commissione rilevò la necessità di integrare in un approccio "Total Defence" tutti gli aspetti concernenti la protezione e la difesa delle infrastrutture critiche, nei confronti di

[86] https://www.bsi.bund.de/DE/Home/home_node.html
[87] http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

eventi di carattere naturale, accidentale o doloso provocati sia in modo tradizionale che tramite il cyberspace, e ciò indipendentemente dalla loro natura civile o militare (warfare).

L'obiettivo di perseguire tale risultato fu affidato alla Swedish *Emergency Management Agency (SEMA),* istituita nel 2002 dal Ministero della Difesa come istituzione indipendente, con il ruolo di coordinare tutte le iniziative legate all'attuazione della strategia di "Total Defence" e di verificare l'effettiva capacità della nazione di resistere a situazioni di emergenza di qualsiasi origine.

Successivamente le attività e le funzioni del SEMA sono confluite nella **Swedish Civil Contingiencies Agency (MSB)**[88]. É da notare che il MSB non ha una diretta responsabilità nella gestione delle crisi, che è lasciata ai soggetti preposti a gestire, in situazioni di normalità, i diversi aspetti coinvolti nella crisi (principio di prossimità), ma focalizza la propria azione sugli aspetti di prevenzione (a monte) e di studio delle conseguenze (a valle) delle crisi stesse.

[88] Il MSB ha inglobato la Swedish Emergency Management Agency (SEMA) https://www.msb.se/en/

## Organizzazione Nazionale e Prospettive Future

## PROPOSITIVO

# 12 Inquadramento nazionale e ripartizione delle competenze

La tematica della Protezione delle Infrastrutture Critiche in Italia non ha ancora assunto un assetto definito, né si è redatto un documento strategico nazionale su quelli che dovrebbero essere gli obiettivi, gli strumenti ed i mezzi da mettere in campo su questa tematica.

Da un punto di vista storico, nel 2003 fu costituito presso la Presidenza del Consiglio dei Ministri – Dipartimento per l'Innovazione e le Tecnologie – un Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate. Tale gruppo vedeva la partecipazione congiunta di esponenti delle differenti pubbliche amministrazioni coinvolte nella tematica, rappresentanti dei principali operatori di infrastrutture critiche e rappresentanti del mondo della ricerca e della didattica. Al termine dei suoi lavori il Gruppo di Lavoro rilasciò un **documento**[89] contenente una disamina della situazione italiana, con il prospetto di alcune ipotesi organizzative. Nello specifico tale rapporto indicava la necessità di costituire uno specifico organismo (nel documento veniva individuato lo strumento della struttura di missione) che avesse il compito di redigere un piano strategico nazionale per la protezione delle infrastrutture critiche ed identificasse le modalità di attuazione dello stesso con strumenti organizzativi atti a gestire il mutato contesto socio-tecnologico e le interdipendenze che esso induce.

Successivamente la tematica fu incardinata presso il Nucleo Politico Militare, che attribuì alla **Commissione Interministeriale Tecnica della Difesa Civile (CITDC)**[90] il compito di

[89] Presidenza del Consiglio dei Ministri – Dip. Innovazione e Tecnologie "Protezione delle Infrastrutture Critiche Informatizzate: la realtà italiana", 2004 (estratto)
http://www.infrastrutturecritiche.it/aiic/index.php?option=com_docman&task=doc_download&gid=38&Itemid=103
[90] http://www.vigilfuoco.it/aspx/Page.aspx?IdPage=3865

elaborare una normativa con l'obiettivo di definire i criteri ed individuare le infrastrutture critiche nazionali e le relative minacce e vulnerabilità, oltre che specificare le responsabilità e le competenze dei diversi soggetti coinvolti[91].

Per quel che riguarda gli aspetti connessi più prettamente alla Protezione delle Infrastrutture Critiche Informatizzate, il D.L. n. 155 del 31/7/05 (la così detta Legge Pisanu), nell'attribuire la competenza al Ministero dell'Interno, istituiva il **CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche**[92]. Tale centro si pone come organo di polizia per tutte le attività di prevenzione, repressione e contrasto di azioni criminali perpetrate contro le diverse infrastrutture critiche attraverso il cyberspace. Il modello organizzativo adottato dal CNAIPIC è quello di stipulare delle "convenzioni" con i diversi operatori di infrastrutture critiche al fine di regolamentare lo scambio di informazioni con i diversi gestori, sia preventivamente che durante eventi di crisi. Tale aspetto è un elemento cardinale in quanto consente a chi opera nel CNAIPIC di avere, in anticipo rispetto all'insorgere di una situazione di attacco, tutte le informazioni e le conoscenze necessarie per capire in che modo ed in che forma intervenire.

In parallelo a queste attività di valenza nazionale si è innestata, e per certi versi ha funto da traino per le attività nazionali, la necessità di dare corso alla Direttiva Europea **2008/114/CE**[93] relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione del 8 dicembre 2008. Tale direttiva nasceva come uno degli strumenti messi in atto dalla Commissione Europea per innalzare la protezione, la sicurezza e la resilienza delle diverse infrastrutture critiche di valenza europea. Questa necessità emergeva a valle degli attentati di Londra e Madrid, ma anche sulla scorta del black-out italiano del 2003. La Commissione Europea evidenziava, infatti, come a causa dell'aumento delle interdipendenze fra infrastrutture afferenti a diversi Stati Membri, un incidente che fosse occorso in uno stato avrebbe potuto avere ripercussioni anche sugli altri. Tali infrastrutture sono definite, pertanto, come *ECI – European Critical Infrastructure.* Nello specifico, la designazione ad ECI è frutto di un complesso processo tecnico-politico che prende spunto dal potenziale impatto che può essere causato da un guasto/distruzione di un'infrastruttura in termini di valenza settoriale (percentuale dei fruitori del bene o servizio che l'infrastruttura eroga, rispetto alla popolazione

[91] Alla data di pubblicazione le attività non risultano completate.
[92] http://www.poliziadistato.it/articolo/view/18494/
[93] http://www.vigilfuoco.it/allegati/biblioteca/Direttiva.pdf

nazionale o di altro stato membro) e inter-settoriale, tenendo conto degli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture, dove i criteri di valutazione intersettoriali riguardano:

a) le possibili vittime, in termini di numero di morti e di feriti;
b) le possibili conseguenze economiche, in termini di perdite finanziarie, di deterioramento del bene o servizio e di effetti/danni ambientali;
c) le possibili conseguenze per la popolazione, in termini di perdita di fiducia nelle istituzioni, di sofferenze fisiche e di perturbazione della vita quotidiana, considerando anche la perdita di servizi essenziali.

Tutto ciò viene valutato con riferimento sia agli *effetti negativi esterni*, ossia dovuti alla perdita di funzionalità di un'infrastruttura nell'erogazione del relativo bene o servizio, sia agli *effetti negativi intrinseci,* che vengono a prodursi nei confronti dell'infrastruttura stessa e dell'ambiente circostante. Per ciascuna di queste categorie sono definite a livello europeo delle soglie, sia in termini assoluti che relativi (ad esempio per quelli economici si guarda al PIL della nazione), i cui valori sono però dati classificati, a causa della loro sensibilità[94].

L'elemento principale che emerge dalla direttiva è che, in un tale contesto, gli "obblighi" per ciò che concerne la 'sicurezza' dell'infrastruttura a carico del soggetto proprietario e/o gestore devono essere tali da prevenire, o quanto meno limitare, le conseguenze sulle altre nazioni. In altri termini, stante il ruolo pan-europeo svolto da tali grandi infrastrutture, i livelli di sicurezza devono uniformarsi a uno standard qualitativo elevato e, quindi, le regole da adottare non sono dettate solo dallo Stato Membro in cui sussistono, ma in una certa misura imposte a livello Europeo. Nella sua formulazione attuale la direttiva focalizza la sua attenzione esclusivamente su due settori (Energia e Trasporti).

Tale direttiva è stata recepita nel nostro ordinamento con il D.Lgs 11 aprile 2011, n. 61,[95] che attribuisce al Nucleo Interministeriale di Situazione e Pianificazione (NISP), integrato con rappresentanti del Ministero dello Sviluppo Economico per il settore energia, e del Ministero delle Infrastrutture e dei Trasporti ed Enti Vigilati per il settore trasporti, la

[94] Si evidenzia che anche la lista delle Infrastrutture Critiche è un dato assunto come sensibile e per questo classificato.
[95] Attuazione della Direttiva 2008/114/CE riguardante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2011;061

responsabilità di attuazione. Per tali fini il NISP ricorre all'ausilio di una "struttura responsabile", da individuare fra le strutture della Presidenza del Consiglio dei Ministri, cui sono demandate le attività tecniche e scientifiche relative, nonché i rapporti con la Commissione Europea e con le analoghe strutture degli altri Stati Membri.

Il D.Lgs stabilisce, nello specifico, che per gli operatori delle Infrastrutture Critiche Europee corre l'obbligo della nomina di un *funzionario di collegamento in materia di sicurezza* e della redazione (e costante aggiornamento) di un Piano della Sicurezza dell'Operatore (PSO). Tale PSO dovrà contenere, fra le altre cose l'individuazione degli elementi più importanti dell'infrastruttura, l'analisi dei rischi, comprendente sia la valutazione delle minacce che l'individuazione delle vulnerabilità e del potenziale impatto, e la definizione delle misure di sicurezza da adottare, sia su base permanente che ad applicazione graduata, in relazione al livello di minaccia o di rischio esistente in un determinato periodo di tempo, che dovranno essere messe in atto dall'operatore per adeguare il proprio livello di protezione.

In questo contesto, la citata norma, ai sensi dell'art. 11, attribuisce al Mistero della Difesa, in concorso con gli altri dicasteri competenti, la responsabilità della protezione delle Infrastrutture Critiche Europee ubicate sul territorio nazionale.

*Art. 11 Responsabili della protezione*

*Il Ministero dell'interno, il Ministero della difesa, il Dipartimento della protezione civile della Presidenza del Consiglio dei Ministri ed il Ministero dello sviluppo economico, per il settore energia, ed il Ministero delle infrastrutture e dei trasporti, per il settore trasporti, pongono in essere, nell'ambito delle rispettive competenze, tutte le azioni e le misure indispensabili a garantire la protezione delle ICE ubicate in territorio nazionale, avvalendosi dei propri organi centrali o delle articolazioni locali, ove esistenti, e tenendo informato il NISP.*

**[D.Lgs n. 61/2011]**

Ciò nonostante tale aspetto della norma appare di non immediata trasposizione operativa, in assenza di un piano strategico nazionale in grado di fissare obiettivi e strategie e, quindi, di attribuire ai singoli dicasteri i propri ruoli.

Sulla scorta dell'esperienza internazionale si possono, nella sostanza, individuare tre ambiti all'interno dei quali il Ministero della Difesa è chiamato a svolgere un ruolo rilevante.

*Funzionalità del Sistema Difesa*

Il compito primario è quello di assumersi la responsabilità di preservare le funzionalità operative proprie del sistema Difesa. Ciò si deve tradurre nell'identificazione, nella prioritizzazione e nella protezione di tutte quelle infrastrutture essenziali al Ministero della Difesa affinché esso possa garantire le capacità di esecuzione delle proprie funzioni e missioni. Tale attività, sull'esempio di quanto sta portando avanti il DoD, si deve estrinsecare nella determinazione delle funzionalità critiche e, per ognuna di esse, nell'individuazione delle risorse necessarie con riferimento sia a quelle erogate direttamente da strutture interne alla Difesa, sia a quelle erogate da soggetti esterni ad esso, il tutto tenendo in debito conto anche le eventuali interdipendenze esistenti. Tale attività ha quale ulteriore obiettivo quello di effettuare una valutazione dell'impatto negativo

connesso con il mancato/erroneo funzionamento delle diverse infrastrutture e, quindi, di stabilire la priorità degli interventi.

*Interventi in sede di Mitigazione di Eventi*

La Difesa è stata da sempre uno dei soggetti capaci di intervenire nell'immediatezza di eventi disastrosi quali alluvioni o terremoti. Questa perculiarità, sulla scorta anche di quella che è l'indicazione fornita dalla NATO e da altre esperienze internazionali, dovrà essere incrementata per renderla compatibile con l'attuale scenario socio-tecnologico. Questo comporta che, in parallelo alle capacità logistiche di dislocazione di mezzi e personale in territori colpiti da eventi calamitosi, ed alle attività del genio mirate a ri-costruire componenti infrastrutturali fisiche danneggiate o distrutte dall'evento, occorre sviluppare capacità di intervento anche nell'ambito delle dimensioni umana/organizzativa e cyber di effettuare interventi di mitigazione e favorire ripristino dell'operatività nelle diverse infrastrutture critiche. Occorre, infatti, rilevare che una delle problematiche evidenziate come fortemente critiche dai diversi studi sulla pandemia aviaria H5N1, stante la forte specializzazione dei compiti, è la sostituzione delle risorse umane, problema verificatosi anche nel caso del black-out del 2003 a New York[96]. Analogamente, la possibilità di utilizzare le infrastrutture della Difesa per consentire ai sistemi SCADA degli operatori di infrastrutture critiche di poter operare anche in presenza di seri danni alle proprie reti di comunicazione, è un altro ambito di possibile intervento.

Si noti che per poter mettere in atto tali tipologie di interventi è necessario che il Ministero della Difesa acquisisca conoscenze più articolate sul comportamento e le criticità delle diverse infrastrutture critiche, onde poter predisporre gli opportuni piani di intervento. In quest'ottica la previsione fatta dal D.Lgs 61/2011, che all'art. 11 comma 3 prevede la designazione[97], per ciascuna infrastruttura critica europea, di un rappresentante del Ministero della Difesa che funga da punto di contatto, rappresenta un interessante modello, in quanto favorirebbe il necessario interscambio di conoscenze sia nei confronti dell'operatore che degli altri dicasteri coinvolti. È fortemente auspicabile che venga data piena attuazione a questo aspetto del decreto, e che questo approccio venga esteso anche alla normativa relativa alla protezione delle infrastrutture critiche nazionali.

[96] L'accesso all'isola di Manhattan fu interdetto per quasi 72 ore, imponendo forzatamente questo massacrante turno di lavoro a tutti gli operatori siti sull'isola.

[97] Tale facoltà è prevista anche per Ministero dello Sviluppo Economico per il settore energia, il Ministero delle Infrastrutture e dei Trasporti, per il settore trasporti, il Ministero dell'Interno e il Dipartimento della Protezione Civile.

*Gestione degli attacchi sorva-nazionali*

Un altro ambito di intervento del Ministero della Difesa, dai contorni ancora tutti da definire, è quello della competenza in presenza di azioni avverse perpetrate dall'estero. Questa tematica riguarda in prima battuta soprattutto le attività cyber, ma più in generale la quasi totalità delle infrastrutture critiche. Infatti, in presenza di azioni quali quelle sperimentate **dall'Estonia**[98] nel 2007 o dalla **Georgia nel 2008**[99], la risposta non può essere lasciata esclusivamente ai soggetti privati ed alle forze di polizia, ma impone l'adozione di regole di ingaggio tutte da definire e comprendere, nell'ambito delle quali da più parti si evidenzia la necessità e l'importanza di un ruolo non secondario del Ministero della Difesa. Tale considerazione è avvalorata anche dal fatto che le diverse infrastrutture critiche (a partire proprio dal cyber-space), stante la loro globalizzazione, stanno assumendo una valenza sempre più simile alla **Global Commons**[100], la cui protezione e sicurezza travalica i confini dei singoli stati imponendo la definizione di nuovi strumenti non solo operativi, ma anche giuridici e tecnologici.

[98] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[99] http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf
[100] http://www.act.nato.int/multimedia/archive/41-top-headlines/616-mne-7-access-to-the-global-commons

# 13 Il costo della non-sicurezza

La valutazione dei costi connessi con la protezione delle infrastrutture critiche è un tema su cui vi è un ampio, ma sommerso, dibattito. Da un lato vi è la "pretesa", da parte delle autorità pubbliche, che la salvaguardia delle persone e del benessere della nazione debba avere un ruolo preminente rispetto ad altre tipologie di argomentazioni, ma, nel contempo, stante il fatto che la quasi totalità delle infrastrutture è in mano a soggetti privati, il relativo onere deve essere sostenuto da questi e non dalla collettività, e ciò anche in considerazione dell'attuale contesto della finanza pubblica mondiale. Dal parte loro, i diversi operatori di infrastrutture critiche, sono molto riluttanti ad assumersi oneri che ritengono non propri e, soprattutto, in assenza di un quadro normativo definito e sanzionatorio. Questo anche alla luce degli ingenti costi connessi con l'adozione di quelle misure di sicurezza che i diversi stati, USA in primis, stanno imponendo ai diversi operatori.

Lo studio dell'**OECD**[101] sull'impatto economico delle misure di sicurezza adottate nel campo del trasporto marittimo stima, per i soli soggetti operanti negli USA, in 1,3 miliardi di dollari i costi che dovranno sostenere gli operatori del settore, con un aumento annuo dei costi operativi di circa 730 milioni di dollari. Tali costi andrebbero poi espansi di almeno un fattore 10, considerando che quasi l'80% di tutte le merci mondiali è movimentato via mare, per tener conto anche degli oneri a carico dei soggetti operanti al di fuori degli Stati Uniti.

Ovviamente tale cifra va comparata con la stima dei 58 miliardi di dollari relativi all'impatto che comporterebbe un eventuale attacco multiplo alle infrastrutture portuali statunitensi.

[101] OECD - Security in Maritime Transport: Risk Assessment and Economic Impact - http://www.oecd.org/dataoecd/63/13/4375896.pdf

Aumenti analoghi dei costi sono stati stimati anche per altre tipologie di infrastrutture. Ad esempio, i costi che gli operatori dell'industria alimentare hanno sostenuto per adeguarsi alle previsioni imposte dal governo statunitense (includendo in questi sia gli aspetti di sicurezza fisica, che quelli di compliance e di training del personale) ammontano a circa 2,4 miliardi di dollari (con una stima di circa 4,7 miliardi di dollari a livello mondiale) e con un costo operativo annuo del settore superiore al miliardo di dollari.

Le sole industrie chimiche statunitensi[102] dal 2001 hanno effettuato investimenti per circa 3,5 miliardi di dollari per adeguare i propri livelli di sicurezza.

Sul versante dei costi pubblici, sempre riferendosi alla realtà Americana, il budget annuale del DHS, che conta oltre 230.000 dipendenti, ammonta a quasi 55 miliardi di dollari, mentre, complessivamente, il budget di tutte le agenzie governative poi confluite nel DHS stesso prima del 9/11 non superava i 22 miliardi di dollari annui. Solo per le attività di intelligence civile negli USA si spendono 50 miliardi di dollari l'anno (a fronte dei poco più di 30 miliardi di dollari spesi, precedentemente al 9/11) a cui vanno aggiunti gli oltre 30 miliardi di dollari come costi delle agenzie di intelligence militari.

Maggiormente evidente, anche perché sperimentato da ognuno di noi, è l'incremento dei costi per la sicurezza nell'ambito del trasporto aereo. I soli costi per le attività di screening dei passeggeri negli stati Uniti sono stati stimati in oltre 40 miliardi di dollari. A queste cifre vanno aggiunti anche i costi indiretti legati al maggior tempo di attesa (e quindi alla riduzione della capacità lavorativa delle persone) che sono stati stimati in non meno di 8 miliardi di dollari per anno. Tali valori sarebbero più che raddoppiati se, come proposto in conseguenza del fallito attentato del Natale 2009, si imponesse lo screening di massa mediante body scanner (che comporta un tempo di attraversamento più che doppio rispetto agli attuali metal detector). In questo conteggio occorre anche considerare gli impatti sulle abitudini di viaggio dei passeggeri. Uno studio **della Cornell University**[103] evidenzia che gli aumenti nei tempi di imbarco ha prodotto una contrazione di circa il 6% del traffico passeggeri, che si è ridistribuito prevalentemente sul trasporto viario,

[102] La possibilità di un attacco terroristico in grado di provocare un evento catastrofico nell'industria chimica è uno degli scenari considerati fra i più preoccupanti negli USA al punto che ben 4 (6 se si considerano anche gli attacchi alla filiera alimentare) dei 15 scenari di crisi designati dal FEMA prendono in considerazione questa tipologia di evento http://www.fema.gov/pdf/media/factsheets/2009/npd_natl_plan_scenario.pdf

[103] G. Blalock, V. Kadiyali, and D. Simon, "The Impact of Post 9/11 Airport Security Measures on the Demand for Air Travel" - http://dyson.cornell.edu/faculty_sites/gb78/wp/airport_security_022305.pdf

causando, come effetto collaterale, un incremento annuo di oltre 2.300 incidenti stradali i cui costi, materiali e sociali, dovrebbero essere aggiunti a quelli della security.

Ancora una volta, i costi dovrebbero essere comparati con quelli che potrebbero essere gli effetti di un nuovo attacco, similare a quello del 9/11, che ha prodotto, nei soli 15 mesi dopo l'attacco, e limitatamente all'area di New York, perdite per oltre 27 miliardi di dollari.

Un altro aspetto da non trascurare è la ripartizione dei costi fra soggetti pubblici ed operatori privati. Negli anni immediatamente dopo il 9/11 le industrie mondiali hanno accettato, più o meno volontariamente, di farsi carico di una parte non irrisoria degli investimenti in sicurezza, ma non è chiaro fino a quanto e fino a quando esse vorranno/saranno pronte e/o in grado di far fronte a tali oneri. Questo perché la gran parte delle spese in ambito di sicurezza è percepito come un mero costo non in grado di fornire alcun valore aggiunto in termini di efficienza e/o produttività all'azienda. Per altro vi è una limitata incentivazione nelle aziende private ad investire in sicurezza in quanto i maggiori oneri conseguenti ad un attacco terroristico sono in ogni caso a carico del governo. Vi è, inoltre, la forte aspettativa che, qualora tali industrie fossero soggette ad un attacco terroristico, troverebbero nel governo un soggetto pronto a supportarle, anche finanziariamente, nella ricostruzione.

In questo quadro è fondamentale individuare meccanismi e strumenti di incentivazione finanziaria soprattutto in quei settori in cui la gestione dell'infrastruttura (come ad esempio in Italia per l'energia elettrica) è operata da soggetti che non sono direttamente connessi all'erogazione dei diversi servizi, o, nel caso ancora più articolato, (come nel caso della situazione della nostra rete di telecomunicazione) che un soggetto abbia responsabilità della gestione della rete, mentre altri soggetti concorrenti possono utilizzare la medesima risorsa per l'erogazione dei propri servizi.

Tornando al settore aeronautico questo problema è stato, in parte, superato, addebitando i costi della sicurezza direttamente agli utenti finali, che pagano una quota fissa specificatamente destinata a coprire tale maggiorazione dei costi.

La domanda che, però, molti dei passeggeri si pongono è se, ed in che misura, tutti questi investimenti hanno comportato un concreto aumento del livello di sicurezza, e in

particolare se gli interventi sono adeguati, ovvero se gli stessi sono sovra-dimensionati rispetto alle reali minacce.

È ovvio che se un gruppo terroristico fosse in grado di provocare un black-out a livello continentale quale quello occorso negli USA nel 2003, produrrebbe un danno stimabile, calcolando i soli effetti diretti, in oltre 135 miliardi di dollari con conseguente tracollo dell'economia mondiale.

Per cui è indubbio che il costo della non-sicurezza, ossia quella che la nostra società dovrebbe affrontare se non si intraprendessero opportune azioni strategiche, tattiche ed operative, sarebbe non sostenibile.

Quello che però emerge è la necessità di un diverso paradigma relativo alla spesa in sicurezza, al fine di poter dare alla stessa un attributo non di mero costo, ma di investimento. Occorre, per questo, passare da un'impostazione prevalentemente difensiva ad un'impostazione maggiormente proattiva ed in grado di aumentare in primo luogo la resilienza delle diverse infrastrutture, in un'ottica di service-continuity, andando ad aumentare, in tal modo, il valore aggiunto per i diversi attori coinvolti.

Tali considerazioni sono da vedere anche nell'ottica che il non-investire in sicurezza (nell'accezione di garantire la continuità operativa delle diverse infrastrutture critiche) comporterà una crescente emarginazione dello specifico Stato nello scenario mondiale. Infatti, aumentando il divario fra paesi "affidabili" e paesi in cui i rischi sistemici sono maggiori, il flusso degli investimenti internazionali andrà a ridursi in questi ultimi a beneficio dei primi, accentuando in tal modo l'effetto di *divide*. Inoltre quei paesi/soggetti considerati non affidabili avranno maggiore difficoltà (e quindi ad un costo maggiore) ad accedere alle grandi infrastrutture internazionali. Quanto occorso nell'estate del 2011 sui mercati finanziari ne è, purtroppo, un significativo esempio.

# 14 Conclusioni e prospettive future

Il **World Economic Forum**[104] nel 2008 ha stimato che esiste una reale probabilità, compresa fra il 10% e il 20%, che un evento distruttivo catastrofico coinvolga le infrastrutture critiche informatizzate con un impatto sull'economia mondiale valutato in oltre 250 miliardi di dollari di danni.

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 (ovvero ad una determinata concatenazione di eventi banali).

È possibile che i gruppi terroristici siano interessati (nell'accezione di avere capacità, mezzi e motivazioni, sulla scorta dell'esperienza del 9/11) a creare eventi così devastanti da incidere sul benessere globale?

È una domanda che ci si deve porre per definire in maniera opportuna gli scenari con cui potremmo essere costretti a confrontarci nel prossimo futuro.

In questo quadro si vanno ad inserire anche le profonde modifiche che stanno interessando il mondo del terrorismo; infatti, in accordo con quanto riportato dall'Office of the Coordinator for Counterterrorism del US Department of State

> *"a deeper trend is the shift in the nature of terrorism, from an international terrorism of the late twentieth century into a new*

[104] Global Risk 2008 - https://members.weforum.org/pdf/globalrisk/report2008.pdf

*form of non-state warfare that resembles a form of global insurgency"*

**[Country Reports on Terrorism 2006]**

Ciò rende, per molti aspetti, maggiormente difficili le attività di intelligence e di prevenzione, in quanto i terroristi operano in modo sempre meno articolato/gerarchizzato e sempre più su iniziativa autonoma di piccole cellule se non addirittura di singoli individui.

Per tali entità le infrastrutture critiche potrebbero rappresentare obiettivi con una forte attrattiva sia per il loro valore simbolico, sia perché la distruzione/degradazione di tali infrastrutture ha, ed avrà sempre di più nel prossimo futuro, un impatto notevole sulla popolazione e sulla fiducia che essa ripone nella autorità governative.

A questo si deve aggiungere il fatto che è impossibile proteggere in modo completo tutti gli assets di tutte le infrastrutture critiche: essi sono semplicemente troppo numerosi, dispersi su tutto il territorio e, per altro, il più delle volte facilmente identificabili ed accessibili.

Questo impone, come evidenziato dal NATO Assistant Secretary General for Emerging Security Challenges Gábor Iklódyat durante l'incontro del **giugno 2011 NATO-Russia** sulla protezione delle infrastrutture critiche, la necessità di un cambio di paradigma:

*"Rather than focusing on defence and deterrence, increasing emphasis must be laid on prevention and resilience […] i.e. preparing our societies, infrastructure, etc. to receive the blow but then to recover from it quickly".*

**[Gábor Iklódyat, NATO Assistant Secretary General for Emerging Security Challenges]**

ossia abbracciare il paradigma sotteso agli approcci All-Hazard e, quindi, focalizzare in modo prioritario sull''attenuazione delle conseguenze e sulla velocità di ripristino, più che limitarsi ad agire sulle cause.

# BIBLIO-SITO-GRAFIA

(tutti I link sottoelencati: Ultima Visita: 2011 Settembre 26)


DCSINT Handbook No. 1.02, **Critical Infrastructure Threats and Terrorism**, 2006.

DCSINT Handbook No. 1.05, **A Military Primer to Terrorism,** 2006.

E. Brunner and M. Suter, **International CIIP Handbook 2008/2009**, Center for Security Studies (CSS), ETH Zurich, 2008;

Federal Republic of Germany, **National Strategy for Critical Infrastructure Protection**, 2009.

G. Ackerman, P. Abhayaratne, J. Bale, A. Bhattacharjee, C. Blair, L. Hansell, A. Jayne, M. Kosal, S. Lucas, K. Moran, L. Seroki, S. Vadlamudi, "**Assessing Terrorist Motivations for Attacking Critical Infrastructure**", UCRL-TR-227068, 2007.

G. Blalock, V. Kadiyali, and D. Simon, "**The Impact of Post 9/11 Airport Security Measures on the Demand for Air Travel**", 2005.

Governemnt of Canada **Threats to Canada's Critical Infrastructure**, 2003

National Counterterrorism Center, **2010 Report on Terrorism**, 2011.

OECD - **Security in Maritime Transport: Risk Assessment and Economic Impact**, 2003.

Office of the President. **The National Strategy to Secure Cyberspace**, 2003.

P. Fairley, "**The Unruly Power Grid**", IEEE Spectrum, 2004 .

Presidenza del Consiglio dei Ministri, Dipartimento per l'Innovazione e le Tecnologie, **La *Protezione delle Infrastrutture Critiche Informatizzate***, 2004.

R. Setola, "**How to Measure the Degree of Interdependencies among Critical Infrastructures**", Int. J. of System of Systems Engineering, (IJSSE), vol. 2, No. 1, pp. 38 - 59, 2010

R. Setola, S. De Porcellinis, and M. Sforna "**Critical Infrastructure Dependency Assessment Using Input-output Inoperability Model**", Int. J. Critical Infrastructure Protection (IJCIP), pp. 170 - 178, 2009

S. Bologna, and R. Setola, "**The Need to Improve Local Self-Awareness in CIP/CIIP**", Proc. of First IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005), pp. 84-89, November 2005.

S. Rinaldi, J. Peerenboom, e T. Kelly, "**Identify, Understanding, and Analyzing Critical Infrastructure Interdependencies**"', IEEE Control System Magazine, pp. 11–25, 2001.

US Office of the President. **The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets**, 2003.

US Department of Defence **Directive Number 3020.40** DoD Policy and Responsibilities for Critical Infrastructure, 2010

US Department of Defence **Manual 3020.45**, Defense Critical Infrastructure Program (DCIP), 2010.

US Department of Homeland Security **Presidential Directive-7 on Critical Infrastructure Identification, Prioritization, and Protection**, 2003.

US **National Infrastructure Protection Plan**, 2009.

US Patiot Act, **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act** of 2001.

US PDD 63 - **Presidential Decision Directive 63**, 1998.

Walter Reich, ed., Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind, Woodrow Wilson Center Press, 264-265, 1998.

World Economic Forum, **Global Risk 2008**.

## Ce.Mi.S.S.[105]

Il Centro Militare di Studi Strategici (Ce.Mi.S.S.) è l'Organismo che gestisce, nell'ambito e per conto del Ministero della Difesa, la ricerca su temi di carattere strategico.

Costituito nel 1987 con Decreto del Ministro della Difesa, il Ce.Mi.S.S. svolge la propria opera valendosi si esperti civili e militari, italiani ed esteri, in piena libertà di espressione di pensiero.

Quanto contenuto negli studi pubblicati riflette quindi esclusivamente l'opinione del Ricercatore e non quella del Ministero della Difesa.

## Roberto SETOLA[106]

Roberto SETOLA, è professore associato presso l'Università CAMPUS BioMedico di Roma dove ricopre anche il ruolo di Direttore Scientifico del Master di secondo livello in Homeland Security e Direttore del Laboratorio Sistemi Complessi e Sicurezza.

Da oltre un decennio svolge attività di ricerca nel campo della sicurezza delle grandi infrastrutture.

È il segretario della AIIC (Associazione Italiana esperti Infrastrutture Critiche) ed è stato incaricato di vari ruoli a livello nazionale ed internazionale sulla tematica. È autore di 6 libri e di oltre 100 pubblicazioni scientifiche nell'ambito dello studio di sistemi ed infrastrutture complesse e della loro sicurezza e protezione.

[105] http://www.difesa.it/smd/casd/istituti_militari/CeMISS/Pagine/default.aspx
[106] http://www.masterhomelandsecurity.eu/chi-siamo/direttore-scientifico/