LE INFRASTRUTTURE CRITICHE INFORMATIZZATE

Sandro Bologna
Roberto Setola
Salvatore Tucci

Il mutato contesto socio-economico mondiale impone l'adozione di nuove politiche per la sicurezza dell'insieme di infrastrutture che, usando le tecnologie ICT, erogano beni e servizi essenziali per il benessere delle popolazioni (Protezione delle Infrastrutture Critiche Informatizzate). La corretta definizione di tali strumenti non può prescindere dalla comprensione delle interdipendenze esistenti fra le diverse infrastrutture, fenomeno di per sé nuovo, complesso e fortemente interdisciplinare: ciò richiede lo sviluppo di ambienti e metodologie per l'analisi di tale classe di sistemi.

3.7

1. INTRODUZIONE

Lo sviluppo tecnologico, finanziario e sociale dei paesi industrializzati dipende, e dipenderà sempre più, dalla disponibilità e dal corretto funzionamento di infrastrutture tecnologiche quali: rete di trasmissione e distribuzione dell'energia (elettrica, del gas ecc.), 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 globalmente con il termine di **Infrastrutture Critiche** 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.
Fino a qualche decennio fa, ognuna di queste infrastrutture poteva considerarsi un sistema autonomo, sostanzialmente indipendente e gestito da operatori verticalmente integrati.
Per un insieme di motivi di natura tecnologica, economica e sociale tale struttura si è profondamente modificata. Le varie infrastrutture tendono, infatti, ad essere sempre più strettamente connesse, al punto che esse risultano **interdipendenti.** Ciò comporta che un *guasto* (di natura accidentale o dolosa) in una di loro può facilmente propagarsi con un meccanismo di domino alle altre, amplificando i suoi effetti e provocando disfunzioni e malfunzio-

Infrastrutture Critiche

Per Infrastrutture Critiche si designa quell'insieme di infrastrutture che garantiscono il benessere sociale ed economico di una nazione. Sebbene non esista una classificazione unica, la maggioranza delle nazioni individuano quali Infrastrutture Critiche:

- infrastrutture per la produzione, trasporto e distribuzione di energia (elettrica, gas ecc.);
- infrastrutture di telecomunicazioni;
- circuiti bancari e finanziari;
- sistema sanitario;
- infrastrutture di trasporto (aereo, viario, ferroviario, navale ecc.);
- infrastrutture per la raccolta, distribuzione e trattamento delle acque superficiali;
- servizi di emergenza;
- filiera alimentare.

namenti anche ad utenti remoti, sia dal punto di vista geografico che funzionale, rispetto dove si era originariamente generato il *guasto*.
Negli ultimi anni si sono avuti diversi episodi rappresentativi del livello di interdipendenza esistente fra le diverse infrastrutture tecnologiche. Il più famoso è certamente quello occorso nel 1998 al Galaxy IV. Il Galaxy IV è un satellite per telecomunicazioni in orbita geostazionaria 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 Airline in fase di decollo subirono ritardi di diverse ore a causa della mancata comunicazione del clima in quota, alcune emittenti radiofoniche rimasero oscurate, ma la cosa più sorprendente 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 [1].
Un altro esempio è fornito dal *worm* "*slammer*" che il 25 gennaio 2003 si è rapidamente diffuso su Internet [2]. 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 Huston 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, come ad esempio negli USA, dove a causa della saturazione della banda della dorsale del fornitore del servizio di connettività, il traffico del sistema di tele-controllo di una società di utilities è risultato bloccato [3].
Un episodio più recente si è verificato il 2 gennaio 2004, quando un guasto ad un impianto di servizio di un importante nodo di Telecom Italia a Roma ha provocato la paralisi del traffico telefonico sia fisso che mobile (anche di altri operatori) per diverse ore in una vasta area di Roma. 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 operazioni di check-in).
Accanto a tali episodi vanno, ovviamente, ricordati i *black-out* che si sono succeduti nel 2003 in molte nazioni e che hanno evidenziato che le società industrializzate dipendono in modo quasi totale dalla disponibilità di energia elettrica. Ciononostante gli utenti tendono ad assumere comportamenti che si fondano sulla certezza (cieca) della continua disponibilità e dell'ininterrotta fornitura di questa risorsa, così come, per altro, anche per i servizi erogati dalle altre infrastrutture critiche.
A proposito dei *black-out*, è interessante notare come nel corso degli ultimi 40 anni si è avuta una costante diminuzione nel numero di episodi, a dimostrazione di una maggiore affidabilità del sistema elettrico. Nello stesso tempo, si è registrato un aumento dell'ampiezza del bacino di utenze che soffrono di tali eventi. Questo a riprova della maggiore complessità esistente nel controllare il sistema elettrico e, soprattutto, della maggiore difficoltà nel circoscrivere le conseguenze di quei (rari) eventi catastrofici.
L'analisi condotta dal governo canadese nel marzo 2003 [4], che risulta per altro generalizzabile a molte altre realtà nazionali, evidenzia una crescente capacità di queste infrastrutture nell'assorbire eventi accidentali (guasti, operazioni erronee da parte del personale ecc.) e quindi una riduzione costante dell'incidenza di questa classe di minacce; tuttavia, altre tipologie di minacce andranno acquisendo una maggiore rilevanza nei prossimi anni. Queste sono sia quelle di carattere "naturale", legate alla presenza di fenomeni climatici sempre più estremizzati e violenti, sia connesse con azioni dolose, ovvero terroristiche.
Infatti, la sempre maggiore rilevanza che le

Infrastrutture Critiche andranno ad assumere nei prossimi anni fa ritenere che le stesse potranno rappresentare un bersaglio per azioni di natura terroristica, condotte sia con metodi tradizionali sia tramite il *cyberspace* (cyber-terrorism), sia con azioni combinate (*swarming attacks*, ritenute dagli analisti le più probabili). Quest'ultima classe di eventi ipotizza scenari nei quali l'azione terroristica condotta tramite il *cyberspace* ha l'obiettivo di rallentare e rendere meno efficaci gli interventi di prima emergenza a valle di un'azione tradizionale, amplificando in tal modo le conseguenze di un attacco.

A livello internazionale l'intera problematica riguardante la protezione delle Infrastrutture Critiche è genericamente indicata con il termine (CIP) *Critical Infrastructure Protection*. Nell'ambito della problematica delle CIP, quando si focalizza l'attenzione principalmente sugli aspetti di vulnerabilità ed interdipendenza introdotti dalla presenza 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 quasi come sinonimi. 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*.

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 Directive* 62 e 63, il cui obiettivo era lo sviluppo di un programma mirato alla salvaguardia e protezione di queste infrastrutture per far sì che "*qualunque interruzione o malfunzionamento di tali infrastrutture sia breve, infrequente e geograficamente circoscritto*".

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*. Le linee strategiche per incrementare la loro sicurezza sono esplicitate nei due documenti emanati dalla Casa Bianca nel febbraio del 2003 [5, 6].

Nella quasi totalità delle nazioni industrializzate sono state intraprese analoghe iniziative mirate alla comprensione del problema, alla sua contestualizzazione alle realtà specifiche, all'individuazione di strategie per ridurre la vulnerabilità del sistema paese e alla predisposizione di piani di intervento in caso di emergenza, con la costante caratterizzazione di una forte cooperazione pubblico – privato.

Anche organismi internazionali quale il G8, la NATO e, l'ONU (con la risoluzione ONU n. 58/199 "*Creation of a global culture of cybersecurity and the protection of critical information infrastructures*" adottata dall'Assemblea Generale delle Nazioni Unite il 23 dicembre 2003 [7]) hanno focalizzato la propria attenzione sulla problematica invitando i paesi aderenti a definire strategie e strumenti per aumentare il livello di protezione di tali infrastrutture, favorire le capacità di ripristino dei livelli di servizio a valle di eventi negativi, sviluppare attività di R&S e favorire la cooperazione internazionale.

In Italia è stato costituito, nel marzo del 2003 presso il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri, il ***Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate***, che ha redatto nel marzo del 2004 un rapporto sulla situazione nazionale [8].

Tale rapporto auspica l'adozione di alcune iniziative tese a ridurre tali pericoli. Fra queste, le attività di Ricerca e Sviluppo occupano un ruolo prioritario dato che, come evidenziato anche nel CIIP Handbook [9] , la situazione attuale della ricerca a livello mondiale è ancora in una fase estremamente iniziale ed immatura. Questo impone la necessità di attivare iniziative che possano fungere da catalizzatore nei confronti del mondo accademico e della ricerca.

Uno degli aspetti di ricerca di maggiore interesse ed attualità è lo sviluppo di modelli e strumenti di ausilio allo studio e alla comprensione del comportamento delle diverse infrastrutture critiche in presenza di interdi-

pendenze reciproche. Infatti, la presenza di queste induce una complessità che sembra essere superiore a quella gestibile dagli strumenti metodologici su cui si basano gli attuali paradigmi di modellista e simulazione [10]. Da qui la necessità di analizzare differenti paradigmi come, ad esempio quelli messi a punto nel campo delle scienza biologiche, storicamente caratterizzati dall'operare con sistemi altamente complessi.
A tal proposito il Gruppo di Lavoro[8], anche sulla base dell'esperienza americana del NISAC (*National Infrastructure Simulation and Analysis Centre*), ha avanzato la proposta di costituire un centro di simulazione virtuale in grado di porsi come elemento catalizzatore per coagulare le necessarie risorse per affrontare una problematica di estrema complessità e fortemente multidisciplinare e multisettoriale.
Nel prosieguo sono presentate alcune delle metodologie proposte per lo studio e la simulazione di questa classe di problemi.

2. MODELLISTICA DI INFRASTRUTTURE INTERDIPENDENTI

Sebbene la modellistica e la simulazione di infrastrutture singole sia un filone di ricerca matura e siano disponibili strumenti di analisi in grado di caratterizzarne i comportamenti su diverse scale temporali e con diversi gradi di astrazione, il panorama per quel che riguarda gli strumenti per l'analisi di infrastrutture interdipendenti è largamente immaturo.
Uno dei primi approcci proposti si basa sulla generalizzazione del modello economico di Leontief per lo studio dell'equilibrio dei sistemi economici [11]. Così come il livello di produzioni di "semi lavorati" influenza le dinamiche di produzione dei beni finali, così il guasto di un elemento può influenzare, a causa delle interdipendenze, il livello di servizio in altre infrastrutture.
Per valutare, per esempio, l'impatto 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 incidenza relativa fra le diverse infrastrutture (Tabella 1).

	Rete elettrica	Trasporti	Ospedali	Telco
Rete elettrica	0	0.2	0.2	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 Leontieff

Nel caso della tabella 1, la prima colonna indica che la distruzione totale della rete elettrica (livello di inoperabilità pari ad 1) ha un impatto diretto sul sistema viario rendendone non funzionante il 40%, il 60% del sistema ospedaliero rimane bloccato, mentre il sistema di telecomunicazione è completamente fuori uso.
Oltre a queste conseguenze "dirette", è necessario valutare anche le conseguenze secondarie, per cui l'impatto complessivo di un guasto è rappresentato dalla soluzione di regime della seguente equazione:

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

Dove $\boldsymbol{A}$ è, appunto, la matrice $m \times m$ dei coefficienti di Leontieff (con m pari al numero di infrastrutture prese in esame), $\boldsymbol{c}$ è un vettore colonna di lunghezza m che rappresenta il guasto indotto dall'esterno ed $\boldsymbol{x}$ è il vettore colonna, di lunghezza m, con le probabilità di non-operatività associate a ciascun elemento.
Volendo valutare, per esempio gli effetti provocati sul sistema di un evento che renda non-operativo l'80% della rete elettrica, dalla (1) si ha

$$\bar{x} = (I - \boldsymbol{A})^{-1}\boldsymbol{c} = \left(\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 0.2 & 0 & 0 \\ 0.4 & 0.4 & 0 & 0.1 \\ 0.6 & 0.8 & 0 & 0.2 \\ 0.1 & 0.2 & 0 & 0 \end{bmatrix}\right)^{-1} \begin{bmatrix} 0.8 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad (2)$$

Risolvendo il sistema si trova che l'inoperabilità totale della rete elettrica è pari al 89%, quella del sistema di trasporto è del 46%, quello delle telecomunicazioni è del 98%, mentre il sistema ospedaliero è completamente fuori uso.

L'esempio, pur nella sua estrema semplificazione, evidenzia come la presenza di interdipendenze comporta una amplificazione delle conseguenze dell'evento a causa di effetti di *feedback* dovuti all'accoppiamento (inter-dipendenza) dei sistemi.

Uno degli aspetti più critici nella definizione di questo modello risiede nella determinazione degli elementi che caratterizzano le interdipendenze (i coefficienti della matrice di Leontieff). Ciò è dovuto sia al fatto che molte dipendenze risultano poco percepite e comprese, sia al fatto che le stesse sono caratterizzate da una pluralità di elementi che ne rende difficile, oltre che la formalizzazione, anche molto spesso la semplice comprensione.

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 o indiretti (ciò 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 in [1], le interdipendenze sono analizzate considerando sei diverse "dimensioni" al fine di cogliere i vari elementi che caratterizzano sia il comportamento legato alla presenza dell'interdipendenza, che il suo insorgere.

In particolare essi individuano quali direzioni lungo le quali 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 esercita delle pressioni sull'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. Per 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 in precedenza 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 tale tipo di interdipendenza.

Si noti che, a differenza delle altre cause di interdipendenza, la *Cyber* interdipendenza è una proprietà assoluta e non relativa e ciò a sottolineare che questo tipo di interazione comporta un'estesa interdipendenza con so-

Infrastrutture Critiche Interdipendenti

Il mutato contesto sociale, economico e tecnologico ha indotto un profondo mutamento nelle architetture delle diverse infrastrutture. Infatti se fino alla fine degli anni '90 esse erano costituite da sistemi autonomi verticalmente integrati ed operati da gestori unici (operanti generalmente in regime di monopolio), l'attuale scenario è caratterizzato dalla moltiplicazione del numero di operatori e dall'utilizzo promiscuo delle diverse risorse al fine di erogare servizi innovativi e migliorare la qualità dei servizi, oltre che ridurre i costi. Ciò ha comportato una crescita esponenziale nel numero di punti di contatto fra le diverse infrastrutture e l'insorgere di un grandissimo numero di interdipendenze fra esse.

stanzialmente qualunque altra infrastruttura che utilizza il *cyberspace*.

Stato operativo: Per comprendere appieno le interdipendenze tra le infrastrutture 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 valle di un guasto.

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.
- *Unità*: un insieme di parti funzionalmente correlate (per esempio un generatore di calore).
- *Sottosistema*: una linea di unità (ad esempio un sistema di raffreddamento).
- *Infrastruttura*. un insieme completo di sistemi simili.

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

Altra caratteristica importante è la *scala temporale*. L'orizzonte di interesse può variare da secondi (per le operazioni del sistema energetico per 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. Per 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 alcun tipo di ruolo. Dualmente, queste giocheranno un ruolo primario per comprendere le conseguenze indotte da modifiche nella normativa di riferimento (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 affiancati 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 concretizzano inaspettatamente a seguito di sequenze di operazioni non previste.

Non essendo semplice ricondurre tutti questi aspetti ad un unico modello matematico, in [12] è proposta l'adozione di modellistiche basate su un approccio *Hierarchical Holographic Modelling* (HHM). La metodologia HHM parte dal presupposto che quando si vuole modellare un sistema complesso possono emergere più modelli matematici o concettuali: ognuno dei quali pone l'attenzione su un aspetto specifico e solo prendendo in considerazione un insieme di modelli si può ottenere una rappresentazione accettabilmente aderente alla realtà dell'intero sistema.

Per meglio comprendere il problema delle dipendenze tra i vari elementi di un'infrastruttu-

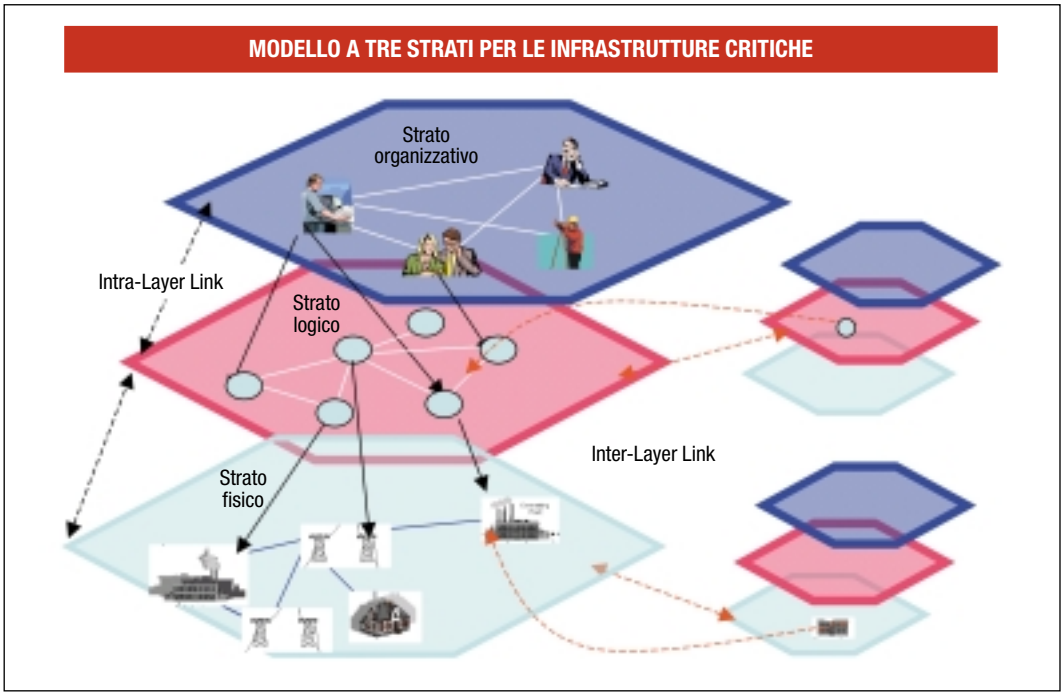

FIGURA 1
Modellazione a strati di una generica Infrastruttura e delle sue interdipendenze

ra e delle interdipendenze tra infrastrutture diverse, è opportuno modellare ogni infrastruttura come un oggetto composto logicamente da tre strati distinti: organizzativo, informatico e fisico [13] (Figura 1). All'interno di ciascuna infrastruttura ogni elemento interagisce, oltre che con gli elementi del suo livello, anche con elementi posti nei livelli contigui (tramite legami funzionali indicati come intra-layer link). Mentre gli omologhi strati delle diverse infrastrutture interagiscono fra loro attraverso legami indicati come inter-layer link.
Questa schematizzazione aiuta ad evidenziare come l'attuale tendenza alla convergenza nelle telecomunicazioni comporti un aumento delle dipendenze fra le diverse infrastrutture.

3. ANALISI SIMULATIVA DI INFRASTRUTTURE INTERDIPENDENTI

Gli approcci descritti nel precedente paragrafo aprono una visuale sul problema e sulla sua complessità. Essi, però non sono in grado di fornire gli elementi quantitativi necessari per poter definire l'impatto dei diversi eventi ne quelle stime che sono indispensabili per poter stabilire un ordine di priorità nelle azioni da intraprendere e sugli investimenti da privilegiare.
In questo contesto, a causa del rapido e profondo mutamento infrastrutturale che caratterizza la totalità delle Infrastrutture Critiche, l'utilizzo di strumenti di predizione basati sull'analisi delle serie storiche si rivela non sempre adeguato soprattutto per quel che concerne la predizione delle conseguenze di eventi catastrofici o terroristici.
Occorre, pertanto, sviluppare modelli e strumenti simulativi in grado di fornire una predizione del comportamento del sistema nei diversi scenari ipotizzabili. La realizzazione di siffatti strumenti si scontra, però, con la complessità che caratterizza questi sistemi e che sembra essere superiore alle capacità di manipolazione degli attuali strumenti metodologici e di calcolo.
Uno degli approcci più promettenti per l'analisi delle interdipendenze tra reti complesse è quello della così detta modellistica ad **agenti** (*Agent-based Modelling*) [14]. L'idea fondamentale che guida questi modelli è che comportamenti complessi possano essere il frutto delle interazioni tra individui elementari autonomi che operano sulla base di regole semplici che, nel loro interagire, fanno emergere quelle caratteristiche comportamentali che caratterizzano il comportamento collettivo del sistema.
In altri termini il comportamento di un insieme di infrastrutture interdipendenti è ana-

Agente

Jennings e Wooldrige in "*Intelligent Agents: Theory and Practice*" definiscono "un agente come un componente informatico situato in un certo ambiente, capace di azioni autonome e flessibili al fine di ottenere i suoi obiettivi di progetto". In altri termini esso agisce senza il diretto intervento dell'uomo, cercando di raggiungere il suo obiettivo massimizzando una qualche funzione valutativa. L'agente è un'entità che opera in modo continuo ed autonomo per conto di altri utenti o agenti, ma anche in maniera indipendente da essi. A tal fine l'agente possiede capacità di comunicazione e di cooperazione con gli altri agenti eventualmente presenti nel sistema. Esso ha, inoltre, la capacità di interagire attivamente con l'ambiente, modificandone cioè le caratteristiche, piuttosto che subirlo passivamente. Un agente deve essere implementato partendo innanzitutto dalle proprietà che deve avere; alcune di esse sono caratteristiche di base, nel senso che si può chiamare "agente" solo un'applicazione che le rispetti. Questi attributi fondamentali sono:

- Autonomia: capacità di essere continuamente attivo senza la necessità di eventi esterni attivatori;
- Socialità: capacità di interagire con altri agenti;
- Reattività: capacità di fornire risposte immediate ai cambiamenti ambientali che vengono percepiti;
- Proattività: capacità di causare eventi non in modo esclusivamente reattivo, ma come se si seguisse un piano autonomo.

lizzabile ricorrendo ad un approccio *bottom-up* che modella l'intero sistema partendo dalla conoscenza del comportamento (locale) dei singoli componenti ed andando a studiare l'evoluzione complessiva del sistema quando questi componenti interagiscono fra loro.

Ciò non è altro che la trasposizione degli approcci comportamentali biologici o sociologici che enfatizzano come l'aggregazione di individui di una determinata specie comporta l'insorgenza di comportamenti "non prevedibili" a partire dallo studio del singolo individuo isolato. L'adozione di strategie quali l'*Agent-based Modelling*, sviluppate soprattutto nel campo della biocomplessità, è legato alla constatazione che le moderne infrastrutture tecnologiche hanno raggiunto una **complessità** paragonabile ai sistemi biologici rendendo necessario per il loro studio approcci propri di questo mondo.

In questo contesto i singoli costituenti sono modellati come entità caratterizzate da *locazione, capacità e memoria*. La locazione dell'entità definisce dove essa si trova in uno spazio fisico. La capacità di un'entità esprime ciò che l'entità è in grado di fare. Un'entità può modificare la sua rappresentazione interna dei dati (capacità di percezione), può modificare il suo ambiente (capacità di comportamento), può adattarsi a cambiamenti dell'ambiente in cui si trova (capacità di reazione intelligente), può inoltre condividere conoscenza, informazioni e strategie comuni con altre entità (capacità di cooperazione), può eseguire azioni senza l'intervento esterno (capacità di autonomia). I dati che rappresentano lo stato di un'entità e la storia delle sue esperienze (per esempio sovraccarico o invecchiamento) costituiscono la memoria dell'entità.

Scienza della Complessità

Negi ultimi anni è avvenuta una naturale convergenza tra svariate aree applicative; interi domini delle scienze, inizialmente distinti e scarsamente comunicanti, hanno iniziato ad integrarsi fortemente, spesso a tal punto da essere assimilabili ad un unico corpo di metodologie, trasversali e multidisciplinari. Questo *trend* è il frutto di un nuovo paradigma, indicato come *Scienza della Complessità*, con il quale gli elementi di similitudini e regolarità che emergono all'interno dei diversi modelli sono percepiti come il segno di un'unitarietà profonda che esula dall'origine dei modelli stessi, emergendo da motivazioni più fondamentali.

Questo comporta che le "vecchie" discipline scientifiche tendono a scomparire per fare posto a nuove ontologie che classificano ambiti storicamente lontani entro nuove classi. Un caso tra tutti è la Biologia che, dopo una breve speciazione in ambiti riduzionistici come la "Biologia Molecolare", la "Genomica e Proteomica", la "Biologia Computazionale", ha riunificato molti di questi ambiti entro la "Biologia Sistemica" all'interno della quale gli oggetti biologici vengono analizzati alla luce della Teoria dei Sistemi Complessi e integrati con strumenti mutuati da altre realtà (l'ingegneria, l'informatica, la matematica e la fisica). Lo studio delle Grandi Reti Tecnologiche e delle Infrastrutture Critiche potrà trarre beneficio dall'applicazione dei risultati prodotti da questa nuova comunità scientifica.

Tale approccio è quello portato avanti dal NISAC (http://www.lanl.gov/orgs/chs/biip/nisac.shtml) e da altri progetti quali quelli sviluppati presso il MIT e gli Argonne Laboratories (http://www.anl.gov/welcome.html).

Una strategia similare è utilizzata in [21] per l'analisi della propagazione di guasti fra infrastrutture eterogenee interdipendenti. In particolare il comportamento di ciascuna infrastruttura è descritta in termini dei suoi macro-componenti che a loro volta sono modellati tramite due dinami-

che interconnesse (Figura 2). Infatti, parallelamente alla dinamica che descrive la capacità operativa del componente, considerate anche le dinamiche proprie dei guasti del componente.
In particolare, al fine di facilitare la gestione in un unico framework di infrastrutture eterogenee, il modello proposto adotta una rappresentazione fortemente astratta in modo di poter descrivere il comportamento input-output di ciascun elemento, a prescindere dalla specifica natura, in termini di un insieme limitato di quantità comuni:

- *Operative Level* (*OL*): la capacità del componente di eseguire il proprio compito. Essa rappresenta un misura potenziale della quantità di servizio o prodotto erogabile dall'elemento, cioè OL = 100% non significa che l'elemento eroga il massimo, ma che potrebbe farlo se richiesto.
- *Requirements* (*R*): cosa occorre al componente per poter garantire OL = 100%.
- *Faults* (*F*): il livello che affligge, per ciascuna tipologia di guasto, l'elemento.

Tali macro componenti interagiscono fra loro in termini di erogazione di servizi (OL) e di richieste di risorse (R). Un guasto in un componente, oltre che ridurne la capacità operativa e quindi i servizi erogabili, può propagarsi anche ad altri elementi. Tale propagazione può avvenire attraverso differenti meccanismi che, riprendendo la schematizzazione proposta in [1] sono descritti mediante tre distinte matrici di incidenza:

- *Physical Fault Propagation,* che descrive la propagazione dei guasti attraverso connessioni fisiche;
- *Geographical Fault Propagation,* che enfatizza la possibilità che guasti si propaghino fra componenti contigui spazialmente;
- *Cyber Fault Propagation,* usata per descrivere la propagazione di guasti di natura informatica (virus, worm ecc.).

Si noti che l'utilizzo di tre distinte matrici di incidenza per modellare la propagazione dei guasti, oltre che per enfatizzare le peculiarità delle diverse tipologie di guasto, consente di semplificare l'analisi delle interdipendenze. Infatti, le interdipendenze fisiche sono in genere ben note ai progettisti delle diverse infrastrutture e facilmente acquisibili dagli schemi di progetto. D'altro canto, quelle di carattere geografico, sebbene non sempre note agli esperti delle diverse infrastrutture, possono evidenziarsi mediante un'analisi comparata delle planimetrie delle diverse infrastrutture. Le interdipendenze *cyber* sono, invece, le meno considerate a livello di *risk analysis* e, per certi aspetti, le più pericolose per quel che concerne la sicurezza [5].
Una diversa strategia consiste nel rendere interoperanti strumenti di simulazione sviluppati per specifiche infrastrutture. Per esempio in [15], per studiare l'interazione fra rete di trasporto dell'energia elettrica e la rete di comunicazione, vengono resi interoperanti alcuni dei simulatori più diffusi nei diversi ambiti specifici.
Il principale vantaggio di questo tipo di approccio risiede nella possibilità di utilizzare codici già ampiamente validati e verificati sperimentalmente. Un altro aspetto importante riguarda la ridotta necessità di condividere informazioni di dettaglio delle singole infrastrutture. Questo aspetto consente di superare con maggiore facilità le resistenze che i vari operatori hanno nel condividere informazioni di dettaglio circa le proprie infrastrutture. Infatti potendo far interoperare fra loro i simulatori "normalmente" utilizzati dai diversi operatori, è possibili limitare le informazioni da scambiare ai soli elementi di interdipendenza.

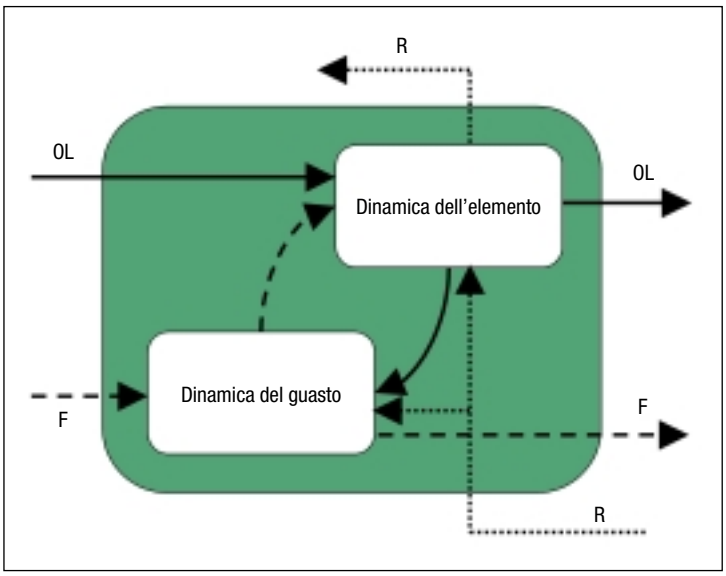

FIGURA 2
Dinamica dei macro-componenti del modello [21]

4. ANALISI TOPOLOGICA

Un altro interessante filone concernente lo studio delle infrastrutture e, più in generale, dei sistemi complessi, riguarda la loro topologia e le implicazioni che questa ha sulle varie proprietà della rete e, specificatamente, sugli aspetti di robustezza.
I lavori pionieristici di Strogatz e Watts [16] verso la fine degli anni novanta e quelli di Barabasi [17] agli inizi del 2000 hanno evidenziato che in molte situazioni la schematizzazione delle reti complesse, quali grafi *random,* non è aderente ai dati empirici.
In particolare i lavori di Barabasi hanno evidenziato che in molte reti il numero dei link per nodo anziché seguire una legge di distribuzione di tipo gaussiano (come è prevedibile in un grafo di tipo *random*) hanno una distribuzione che varia con legge di potenza (Figura 3). Questi grafi, hanno, pertanto una struttura poco "democratica": alcuni nodi, genericamente indicati come *hub*, hanno un numero di connessioni decisamente superiore agli altri e per tale motivo essi rivestono un ruolo fondamentale nella topologia della rete stessa [17].
Per tali sistemi, denominati sistemi *Scale Free*, si può supporre che le caratteristiche topologiche della rete derivino direttamente dalle leggi sottese alla loro evoluzione [18]. Infatti, è possibile dimostrare che una qualunque rete costituita per aggregazione successiva di nuovi nodi con una legge di aggregazione preferenziale (cioè tale che il nuovo nodo ha maggiori probabilità di essere connesso con quei nodi che già risultano molto ben connessi) presenta appunto le proprietà degli *Scale Free*.
Le caratteristiche sottese ai sistemi *Scale-Free* fanno sì che esse risultano particolarmente robuste rispetto a guasti casuali: il numero di nodi che è necessario eliminare prima che (statisticamente) 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 proporzionale al numero di link che è collegato al singolo nodo (grado del nodo), un grafo *scale-free* diviene disconnesso eliminando un numero di nodi inferiore rispetto ad un grafo *random* [19].
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 proliferazione in natura, ma è decisamente più

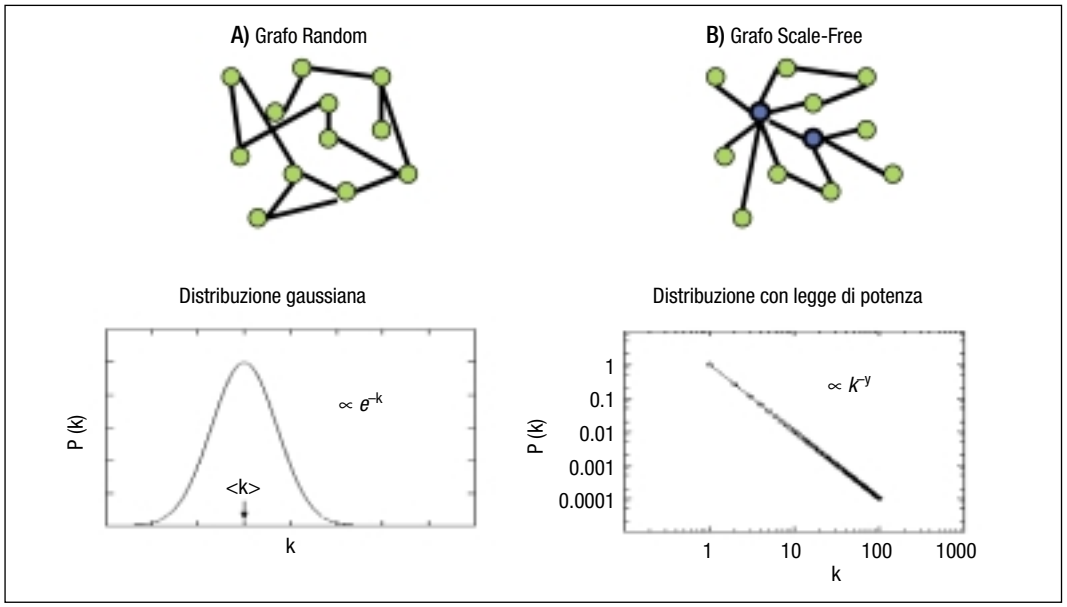

FIGURA 3

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

vulnerabile ad attacchi mirati (potremmo dire terroristici), ovvero ad azioni che coscientemente mirano a ridurre l'efficienza della rete e che pertanto abbiano la capacità/possibilità di colpire nei punti più vulnerabili.
Un altro aspetto riguarda la diffusione delle "epidemie": un sistema *scale-free* non evidenza il classico effetto soglia che contraddistingue i modelli epidemiologici classici. Questo comporta che un'epidemia può diffondersi all'interno della rete anche se il numero degli elementi iniziali infetti è una frazione estremamente limitata rispetto al numero degli elementi che la costituiscono. Al limite anche un sol nodo (come si evidenzia, per esempio, con i virus su Internet) può innescare una rapida diffusione dell'epidemia in quanto gli è sufficiente arrivare ad infettare uno degli *hub*. Ciò impone la necessità di prevedere strategie differenti per contrastare la diffusione di tali "epidemie" [20].
Sebbene siano ancora in gran parte da studiare e comprendere le implicazioni che questi risultati hanno sulle strategie di difesa e di sicurezza, è certamente evidente che strategie adottate sulla base di presupposti che facciano riferimento a modelli topologici *random* potrebbero risultare non efficaci.
In particolare, un aspetto critico riguarda, come evidenziato, l'ipotizzata fragilità di questi sistemi ad azioni mirate tese, cioè, a colpire gli *hub* principali della rete. Infatti considerazioni circa gli effetti che azioni mirate contro tali elementi potrebbero avere sulla popolazione, sia in termini di riduzione di servizi che dal punto di vista mediatico, potrebbero indurre soggetti interessati a creare situazioni destabilizzanti a focalizzare la loro attenzione su questi obiettivi.
Tali considerazioni fanno comprendere come anche l'aspetto della topologia delle singole infrastrutture, nonché la dinamica topologica stessa, sia un elemento da dover considerare con attenzione nel momento in cui si vogliano realizzare sistemi in grado di simulare il comportamento delle infrastrutture critiche.

5. CONCLUSIONI

Migliorare la robustezza delle infrastrutture critiche è un *must* per tutte le nazioni sviluppate. Infatti, da un lato si accresce il ruolo che queste infrastrutture giocano per il benessere delle nazioni, ma dall'altro l'accresciuta interdipendenza e la rapida diffusione delle tecnologie ICT e di Internet anche in settori storicamente non attenti alla sicurezza informatica, costituiscono pericolosi elementi di vulnerabilità. Queste considerazioni, unitamente alla constatazione delle accresciute minacce, sia naturali (dovute soprattutto all'estremizzazione dei fenomeni climatici) che dolose (terrorismo e criminose), impongono l'adozione di opportune strategie per migliorare la *resilience* di queste infrastrutture. Un passo fondamentale in questa direzione è cercare di migliorare la nostra conoscenza sul comportamento mostrato dal sistema di sistemi che viene a costituirsi dall'interconnessione delle diverse infrastrutture critiche. Attualmente gli strumenti metodologici e di analisi di cui disponiamo sembrano non essere adeguati per gestire la complessità che caratterizza questa classe di sistemi. Nell'articolo sono stati illustrati alcuni approcci proposti per affrontare alcuni degli aspetti connessi con la modellistica e la simulazione di tali sistemi. Occorre, in ogni caso, lavorare ancora molto su queste tematiche dato che, citando [9] , non abbiano neanche iniziato a porci le domande corrette per lo studio di questi sistemi.

Bibliografia

[1] Rinaldi S., Peerenboom J., Kelly T.: Identify, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control System Magazine*, dicembre 2001, p. 11-25.

[2] Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness: *Incident Analysis on Microsoft SQL Server 2000 "Slammer" Worm – Impact paper*. Marzo 2003.

[3] North American Electric Reliability Council: *SQL Slammer Worm lessons learned for consideration by the Electricity Sector*. Giugno 2003 http://www.esisac.com/publicdocs/SQL_Slammer_2003.pdf

[4] Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness: *Threats to Canada's Critical Infrastructure*. TA03-001, marzo 2003.

[5] USA White House: *The National Strategy to Secure Cyberspace*. Febbraio 2003; http://www.whitehouse.gov/pcipb

[6] USA White House The: *National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*. Febbraio 2003, http://www.whitehouse.gov/pcipb/physical.html

[7] O.N.U. Risoluzione n. 58/199: *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*. Dicembre 2003, http://www.un.org/Depts/dhl/resguide/r58.htm

[8] Presidenza del Consiglio dei Ministri – Dipartimento per l'Innovazione e le Tecnologie, Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate: *Protezione delle Infrastrutture Critiche Informatizzate – la realtà italiana*. Roma, marzo 2004.

[9] Wenger A., Metzger J., Dunn M., Wigert I. (edited by): *International CIIP Handbook 2004*. ETH, the Swiss Federal Institute of Technology Zurich, 2004. www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf

[10] Amin M.: Modelling and Control of Complex Interactive Networks. *IEEE Control System Magazine*, febbraio 2002, p. 22- 27.

[11] Haimes Y.Y., Jiang P.: Leontief-based model of risk in complex interconnected infrastructures. *Journal of Infrastructure Systems*, Vol. 7, n. 1, 2001, p. 1-12.

[12] Ezell B., Farr J., Wiese I.: Infrastructure Risk Analysis Model. *Journal of Infrastructure Systems*, Vol. 6, n. 3, 2000, p. 114-117.

[13] SAFEGUARD – Intelligent Agents Organisations to Enhance Dependability and Survivability of Large Complex Critical Infrastructure, http://www.ist-safeguard.org

[14] Barton D.C., Eidson E.D., Schoenwald D.A., Stamber K.L., Reinert R.K.: *Aspen-EE: an Agent-Based Model of Infrastructure Interdependency*. Sandia Report SAND2000-2925, Unlimited Release.

[15] Hopkinson K., Giovanini R., Wang X.: *EPCHOS: Integrated Commercial Off-the-Shelf Software for Agent-Based Electric Power and Communication Simulation*. Proc. Winter Simulation Conference, 2003, p. 1158-1166.

[16] Watts D., Strogatz S.: Collective dynamics of "small-world" networks. *Nature*, Vol. 393, giugno 1998, p. 440-424.

[17] Albert R., Barabasi A.: Statistical Mechanics of Complex Networks. *Reviews of Modern Physics*, Vol. 74, 2002, p. 48-97.

[18] Barabasi A., Albert R.: Emergence of scaling in random network. *Science*, Vol. 286, 1999, p. 509-511.

[19] Albert R., Jeong H., Barabasi A.: Error and attack tolerance of complex networks. *Nature*, Vol. 406, 2000, p. 378-382.

[20] Wang X.F., Chen G.: Complex Networks: Small-World, Scale-Free and Beyond. I*EEE Circuit and Systems Magazine*, 2003, p. 6-20.

[21] Panzieri S., Setola R., Ulivi G.: *An Approach to Model Complex Interdependent Infrastructures*. 16th IFAC World Congress 2005, Praga, 4-8 Luglio, 2005.

SANDRO BOLOGNA, laureato in Fisica presso l'Università di Roma la Sapienza nel 1972, lavora in ENEA. Ha circa trenta anni di esperienza come ricercatore, direttore di Unità di ricerca e direttore di Progetti di ricerca nazionali e internazionali. Le sue esperienze afferiscono soprattutto all'analisi e la progettazione di sistemi a calcolatore per applicazioni ad alto rischio. Più recentemente ha svolto attività di ricerca e di divulgazione a livello nazionale e internazionale sul soggetto della modellazione e analisi di vulnerabilità delle reti tecnologiche complesse e sullo sviluppo di tecnologie ad agenti con caratteristiche self-healing per la protezione di infrastrutture critiche.
bologna@casaccia.enea.it

ROBERTO SETOLA è ricercatore presso l'Università CAMPUS Bio-Medico di Roma, è il responsabile della segreteria tecnica del Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate della Presidenza del Consiglio dei Ministri, membro del Gruppo di Lavoro sulle CIIP del Ministero delle Comunicazioni e membro del G8 CIIP Senior Expert Group. È stato, inoltre, designato a rappresentare più volte il governo italiano nelle diverse sedi ove si discuteva delle problematiche connesse con le CIIP. Le sue attività di ricerca riguardano, oltre che le tematiche proprie delle CIIP, la modellistica ed il controllo di sistemi complessi.
r.setola@unicampus.it

SALVATORE TUCCI è Professore Ordinario presso la Facoltà di Ingegneria dell'Università di Roma Tor Vergata. Attualmente è fuori ruolo quale Direttore dell'*Ufficio Informatica e Telematica della Presidenza del Consiglio dei Ministri*, dove ricopre anche il ruolo di responsabile del Sistema informativo dal marzo 1999. È stato Visiting scientist presso l'*IBM Watson Research Center* (USA, 1981) e Visiting researcher presso IRIA (Francia, 1977). Temi di interesse sono i metodi e gli strumenti per l'analisi delle prestazioni e dell'affidabilità dei sistemi informatici, il calcolo parallelo, i sistemi distribuiti e i supercomputer. Più recentemente si è occupato dell'architettura di Internet e della modellistica delle infrastrutture critiche informatizzate. È titolare dei corsi di *Ingegneria del Web*, e di *Metriche e modelli di Internet* presso la Facoltà di Ingegneria dell'Università di Roma Tor Vergata.
s.tucci@governo.it