La protezione delle Infrastrutture Critiche informatizzate

Roberto Setola

Le Infrastrutture Critiche costituiscono la spina dorsale delle economie dei Paesi sviluppati. La convergenza dei media utilizzati, e in particolare l'utilizzo di Internet, sta portando alla creazione di un'infrastruttura globale world-wide. Purtroppo questo fenomeno, contribuendo ad accoppiare le diverse infrastrutture, incrementa la vulnerabilità dell'intero sistema poiché ogni errore o guasto che si verifica in un'infrastruttura può propagarsi ad altre infrastrutture provocando inconvenienti e danni anche a soggetti remoti (sia dal punto di vista geografico che logico) rispetto alla causa del danno.

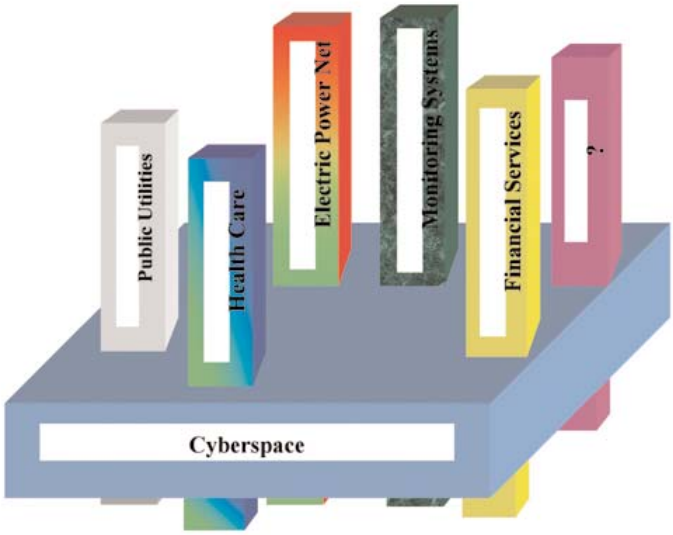


Figura 1 - Il cyberspace sta assumendo il ruolo di Global Information Infrastructure sulla quale si basano ed è condiviso dalla maggior parte delle infrastrutture tecnologiche. A sua volta, l'esistenza del cyberspace è legata al corretto funzionamento di alcune di queste infrastrutture (rete elettrica, reti di telecomunicazioni ecc.) e che rappresentano il basamento su cui esso si poggia.

Il benessere di ampie porzioni della popolazione nei paesi industrializzati dipende e dipenderà sempre di più dalla disponibilità e dal corretto funzionamento di infrastrutture tecnologiche quali: reti di distribuzione dell'energia (elettrica, del gas ecc.), reti di telecomunicazioni, reti di calcolatori, reti di trasporto, sistemi sanitari, circuiti bancari e finanziari ecc. Per la loro rilevanza queste infrastrutture sono generalmente indicate globalmente con il termine di Infrastrutture Critiche [1] poiché un loro non corretto funzionamento, anche per un periodo di tempo limitato, può incidere negativamente sulle attività di singoli o di gruppi comportando perdite economiche se non addirittura mettendo a rischio la sicurezza di cose e persone.

Di per sé ognuna delle infrastrutture critiche è un sistema complesso (complex network) distribuito geograficamente, fortemente non lineare e che interagisce sia con le altre infrastrutture critiche che con diversi operatori: 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. Una caratteristica comune che sta emergendo in questi anni in tutte Infrastrutture Critiche è la sempre maggior diffusione al loro interno delle tecnologie Ict (Information and Communication Technologies) al fine di erogare più efficientemente servizi anche innovativi per andare incontro alle nuove aspettative ed esigenze dell'utenza, al punto che il *cyberspace* è divenuto la vera e propria spina dorsale di tutte le infrastrutture critiche. D'altro canto l'esistenza ed il funzionamento del *cyberspace* dipende dal corretto funzionamento di alcune di queste infrastrutture (come evidenziato nella Figura 1).

La pervasività delle tecnologie Ict introduce ed amplifica, però, l'interdipendenza fra le diverse infrastrutture *critiche* al punto che un *failure* (accidentale o deliberato) di un'infrastruttura può ripercuotersi sulle altre provocando la diffusione ed amplificazione del danno. Disfunzioni e malfunzionamenti possono affliggere anche utenti remoti (sia dal punto di vista geografico che funzionale)

R. Setola, Presidenza del Consiglio dei Ministri, Segretariato Generale, Dipartimento per le risorse strumentali, Ufficio per l'Informatica e la Telematica; Università Campus Biomedico di Roma, Facoltà di Ingegneria

rispetto al punto in cui esso si era verificato. Negli ultimi anni si sono avuti diversi episodi di "guasti" che si sono propagati con un effetto domino attraverso le diverse infrastrutture tecnologiche. Il più famoso ed emblematico di questi è certamente quello accaduto nel 1998 e legato al *failure* occorso al satellite Galaxy IV.
Il Galaxy IV è un satellite per telecomunicazioni in orbita geo-stazionaria sulla costa occidentale degli Stati Uniti. Il suo guasto comportò che circa 40 milioni di pager[1] 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 fu che il *failure* del Galaxy IV comportò anche problemi sulle nanziario (negli Usa circa 13.000 Atm 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).
Questi episodi sono emblematici di quanto sia elevato il livello di interdipendenza esistente fra le varie infrastrutture e di come sia necessario considerare questo fattore per le possibili vulnerabilità che può introdurre al fine di prevenire e limitare i possibili inconvenienti.

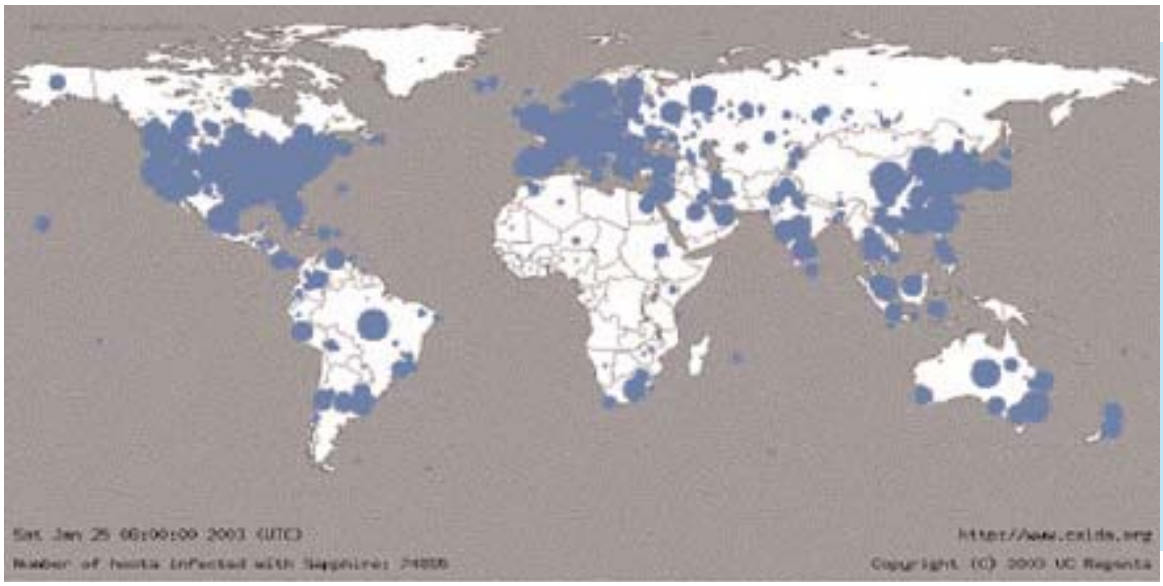


Figura 2 - Area di diffusione del worm slammer 30 minuti dopo il suo rilascio. Il worm in tale lasso di tempo si è propagato dall'estremo oriente, dove si sono registrate le prime rilevazioni, fino a colpire siti in ogni parte del mondo.

high-way: le stazioni di servizio persero la capacità di processare le carte di credito e ciò, anche in considerazione della diffusione di questa tipologia di strumento di pagamento negli Usa, comportò difficoltà nell'effettuare i rifornimenti di carburante. In ultima analisi un guasto ad un satellite di telecomunicazioni comportò l'impossibilità per alcuni automobilisti di completare il loro viaggio [2]. Un altro e più recente esempio è fornito dal *worm "slammer*" che il 25 gennaio 2003 si è rapidamente diffuso su Internet [3].
Questo *worm* sfruttava una nota vulnerabilità nel sistema Sql 2000 server di Microsoft e comportò un anomalo incremento nel traffico IP. Questo ha causato, oltre ai prevedibile problemi di accessibilità a molti siti e ai servizi erogati tramite Internet, anche conseguenze al sistema bancario e fi-

[1] I pager sono dispositivi, molto diffusi negli Usa, che consentono di ricevere messaggi simili ai nostri Sms.

Le interdipendenze fra Infrastrutture Critiche

Le tecnologie Ict hanno contribuito solo ad amplificare le interdipendenze esistenti fra le diverse Infrastrutture Critiche che, per altro, possono essere anche di diversa natura. In [4], ad esempio, gli autori identificano quattro diverse cause di interdipendenza:

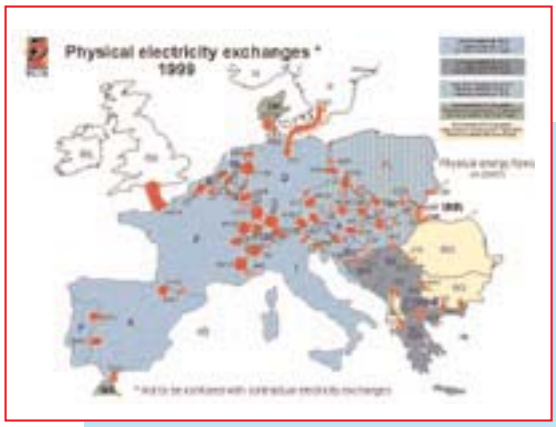
- *Interdipendenza fisica*: due infrastrutture sono fisicamente interdipendenti se lo stato di una è dipendente dall'output materiale (fisico) dell'altra. Ad esempio una centrale elettrica a carbone e la sua rete ferroviaria di adduzione mostrano un'interdipendenza fisica giacché ognuno dei due sistemi dipende dall'output dell'altro: la centrale ha bisogno della rete ferroviaria per la fornitura del combustibile, mentre la rete ferroviaria necessita dell'energia elettrica generata dalla centrale per il proprio funzionamento;

- *Cyber interdipendenza*: un'infrastruttura ha una cyber-interdipendenza se il suo stato dipende dalle informazioni trasmesse attraverso il *cyberspace;*
- *Interdipendenza 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 delittuoso può provocare un *failure* contemporaneo sulle varie infrastrutture (un esempio emblematico di questo si è verificato l'11 settembre quando il crollo delle twin-towers provocò il *failure* di tutte le infrastrutture di comunicazioni, di buona parte della rete elettrica, di quella dell'acqua e del gas che servivano l'area di Manatthan e non solo);
- *Interdipendenza logica*: due infrastrutture sono logicamente interdipendenti se lo stato di ognuna di loro dipende dallo stato dell'altra tramte un meccanismo che non è nessuno di quelli precedentemente esplicitati. Con questo tipo di interdipendenza si può descrivere, ad esempio, la crisi energetica che afflisse la California verso la fine del 2000. La deregulation, varata nel 1996, comportò l'obbligo per le società di utilities di vendere i loro impianti di produzione al fine di favorire la nascita di un mercato aperto dell'energia. Nel medesimo periodo si verificò un considerevole aumento della richiesta accompagnato dalla riduzione degli investimenti nell'ammodernamento degli impianti e delle linee di trasmissione, questi fenomeni, unitamente all'aumento del costo del gas naturale, alle legislazioni varate a tutela dell'ambiente e all'impossibilità da parte delle società di *utility* di scaricare i maggiori costi direttamente sui consumatori finali, comportò una profonda crisi finanziaria di queste. Questo provocò una situazione per cui le società di utilities non furono più in grado di produrre energia in quanto non disponevano di adeguate risorse finanziarie per approvvigionarsi del combustibile e, d'altro canto, i loro problemi finanziari erano connessi all'incapacità di produrre l'energia che pure era fortemente richiesta dal mercato.

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 una estesa interdipendenza con sostanzialmente qualunque altra infrastruttura che utilizza il *cyberspace*.

Attualmente le interdipendenze che più di frequente si evidenziano per i loro effetti negativi sono quelle di carattere geografico allorquando un evento ambientale provoca il contemporaneo *failure* di più infrastrutture (ad esempio quanto un escavatore intercetta e trancia tutte le condutture di servizio che attraversano una determinata strada). Nel futuro prossimo, però, gli accoppiamenti legati alle tecnologie dell'Ict saranno quelli più importanti sia perché a causa dell'incremento nell'uso di queste tecnologie aumenteranno i punti di contatto, sia perché, a differenza degli altri tipi di interdipendenze, essi consentono una rapida propagazione degli effetti anche su aree geograficamente molto lontane rispetto al punto in cui si è prodotta la causa, come evidenziato anche dal *worm slammer* che nel giro di poche decine di minuti provocò problemi su entrambi gli emisferi.

La maggior importanza delle interdipendenze fra le diverse infrastrutture critiche, ed in particolare la *Cyber* interdipendenza, è legata anche all'evoluzione in atto nel contesto socio-economico mondiale ed in particolare è in una certa misura il sottoprodotto della liberalizzazione dei mercati. In presenza di gestori nazionali unici (si pensi, ad esempio ai gestori dei sistemi energetici), ogni operatore aveva sviluppato delle infrastrutture di telecomunicazione proprietarie adibite esclusivamente alle funzioni di monitoraggio e controllo delle proprie infrastrutture distribuite sul territorio. Con l'introduzione della libera concorrenza e la perdita delle posizioni monopolistiche la presenza di tali infrastrutture di servizio è divenuta, di fatto, economicamente e funzionalmente non più sostenibile né significativa. Infatti, da un lato si è andato progressivamente evidenziando la necessità (per fattori economici o normativi) di una maggiore concentrazione dei diversi operatori sul loro specifico core-business, con il progressivo disimpegno e dismissione delle infrastrutture di ser-



(fonte Red Electra)

Figura 3 - Mappa degli scambi di energia elettrica in ambito europeo. Con l'avvento della liberalizzazione del mercato elettrico europeo e la creazione della borsa dell'energia tali scambi subiranno una crescita esponenziale con la necessità di un forte utilizzo del cyberspace per una loro corretta gestione.

vizio, e dall'altro da una parcellizzazione e distribuzione delle competenze su una pluralità di operatori che rendono "inutile" l'esistenza di strutture globali di monitoraggio e controllo.
Queste infrastrutture di supporto hanno trovato generalmente un'immediata e più profittevole riconversione aprendosi a loro volto al mercato offrendo ad una platea più ampia i medesimi servizi di Tlc che precedentemente offrivano in modo dedicato all'unico gestore di riferimento. Questo ha comportato il passaggio da una serie di infrastrutture verticalisitche, nelle quali ogni operatore aveva duplicato le diverse infrastrutture di servizio, ad una situazione in cui le diverse infrastrutture tendono a condividere in modo trasversale i carrier di Tlc e ad operare tramite il *cyberspace* con il conseguente aumento esponenziale dei punti di interconnessione ed interdipendenza fra le diverse infrastrutture. Tale scenario, nell'ambito dell'energia elettrica, diverrà maggiormente reale quando prenderà ad operare la "borsa dell'energia elettrica" dove i vari utilizzatori potranno, istante per istante, scegliere da quale dei diversi soggetti produttori di energia, sia in Italia sia all'estero, acquistare l'energia per i propri scopi e quali tratte di rete di distribuzione "affittare" per veicolare l'energia dalla centrale di produzione all'impianto di utilizzazione. In questo scenario la stessa ipotesi di infrastrutture proprietarie diviene non più perseguibile essendo necessario un enorme scambio di informazione fra una vasta pluralità di operatori/concorrenti in tempo reale.

La protezione delle Infrastrutture Critiche

Tornando al tema dei *failure* che possono affliggere un'Infrastruttura Critica, essi possono distinguersi in due categorie:
- *Failure di natura fisica*: legati alla distruzione fisica di alcune componenti dell'infrastruttura;
- *Failure di natura digitale (cyber):* legati al cattivo funzionamento della parte di controllo e monitoraggio dell'infrastruttura.

A prescindere dalla natura del *failure*, il risultato ultimo di un "guasto" è la riduzione delle prestazioni dei servizi erogati dall'infrastruttura stessa.
Attualmente, come evidenziato in [5], le conseguenze di *failure* di natura digitale sono relativamente modeste, ma si prevede che nel prossimo futuro il cyberspace sarà globalmente la causa principale e il maggior strumento di veicolazione dei *failure*. In questo contesto i sistemi di controllo e monitoraggio costituiscono uno degli elementi di maggiore vulnerabilità. Nel documento *The National Strategy to Secure Cyberspace* [5] i sistemi Dcs (Digital Control System) e Scada (Supervisory Control and Data Acquisition Systems) sono individuati come la seconda delle cause note di vulnerabilità del *cyberspace* subito dopo Internet (per il quale, se non altro, l'adozione del protocollo IPv6 potrebbe rappresenta già una prima possibile soluzione concreta, sebbene non completamente risolutiva, al problema).
Nonostante l'impatto che un *failure* dei sistemi Dcs/Scada potrebbe produrre soprattutto in combinazione con un'azione terroristica tradizionale (swarming attack), la messa in sicurezza di questi sistemi è resa complessa da diversi fattori legati alla natura di tali sistemi. Essi sono generalmente si-

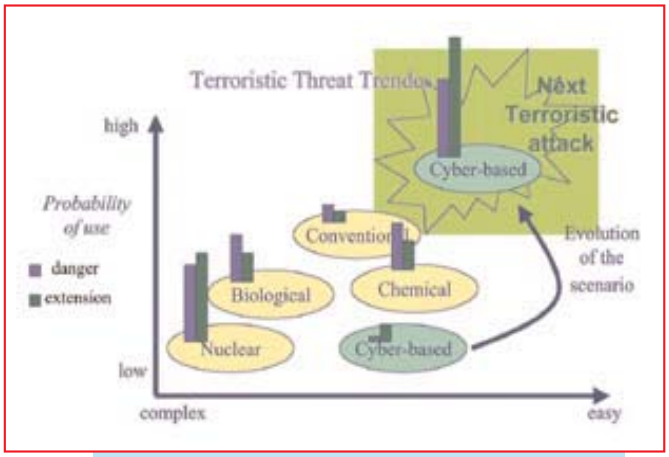


Figura 4 - Nel prossimo futuro il cyberspace sarà uno dei canali privilegiati tramite cui gruppi terroristici porteranno i loro attacchi sia a causa della crescente incidenza che una tale azione potrà avere in termini di potenzialità del danno inferto ed estensione dell'area interessata che per una maggiore facilità di accesso alle tecnologie necessarie per portare a termine tali azioni criminose.

stemi embedded con un lungo life-time e che, nonostante siano relativamente robusti nei confronti di *failure* di natura fisica, sono decisamente meno preparati a gestire *failure* di natura digitale e specialmente quelli connessi con azioni "maliziose". D'altro canto le crescenti necessità di disporre delle informazioni sullo stato degli impianti all'interno della rete informativa aziendale (intranet o internet) comporta la creazione di punti di contatto e quindi l'esposizione di tali sistemi alle conseguenze di eventi o azioni condotte nel *cyberspace*.
Rendere sicuri questi sistemi anche nei confronti di *failure* di natura digitale risulta condizionato da numerosi fattori e vincoli il principale dei quali è la necessità di preservare le caratteristiche di real-time di questi sistemi e ciò si scontra con gli elevati oneri computazionali richiesti per le procedure attualmente impiegate nei sistemi gestionale: sistemi fire-wall, firma digitale ecc. Recenti studi stanno, inoltre, evidenziando che per molte delle infrastrutture critiche il loro stesso modello di svi-

luppo impone un elevato grado di vulnerabilità rispetto ad attacchi terroristici, cioè mirati ad alcuni degli elementi cruciali del sistema. Questi studi sono iniziati verso la fine degli anni novanta, con l'analisi di Internet, ed in particolare della rete costituita dalle connessioni esistenti fra i diversi Dns. Rappresentando tale rete come un grafo e studiando alcuni parametri di riferimento (per maggiori dettagli si veda la scheda allegata) emerse che i dati empirici non rispecchiavano un grafo *random* che, in prima approssimazione, era ritenuto da molti la migliore rappresentazione per le strutture complesse. Altre esplorazioni empiriche, favorite anche dalla disponibilità su Internet di data-base con informazioni su network costituiti da centinaia di migliaia di nodi, rilevarono che le caratteristiche che erano emerse per Internet si ritrovano anche in altri sistemi negli ambiti più disparati: dalla sociologia alla diffusione delle malattie, dalla rete elettrica all'interazione proteica, dalla rete costituita dalle relazioni fra i vari autori di pubblicazioni scientifiche a quella composta dai diversi attori nei film [6]. Una fra le più accreditate teorie che tentano di spiegare le caratteristiche di questi sistemi è lo *scale-free*. Questa teoria, fra le altre cose, evidenzia che una rete è un oggetto "vivo" che, cioè, si evolve nel tempo a partire da un nucleo iniziale e che nella sua crescita, aggiunta di nuovi nodi, questi sono preferenzialmente connessi a nodi che sono già ampiamente connessi.
Questi sistemi presentano valori "ottimali" per tutto un insieme di parametri al punto che diversi studiosi sostengono che tali strutture siano in qualche modo il risultato di una sorta di ottimizzazione ottenuta tramite selezione naturale grazie alla quale sono sopravvissute esclusivamente le strutture più robuste[2]. In particolare esse risultano particolarmente robuste rispetto a guasti casuali (ovvero all'eliminazione causale di un certo numero di nodi). Il risvolto della medaglia risiede, però, nel fatto che esse risultano particolarmente fragili ad alterazioni mirate che vadano a colpire in modo intelligente, cioè premeditato e voluto, alcuni specifici elementi della rete. Non tutti gli studiosi sono concordi nel ritenere valido il modello *scale-free* né, tanto meno, esistono risultati generalizzabili al sistema di sistemi costituito dalle varie infrastrutture critiche interconnesse. Ciononostante quello che emerge da questi studi è che:

1) Un qualunque approccio teso ad analizzare un'infrastruttura complessa non può basasi su ipotesi aprioristiche sulle caratteristiche proprie della rete.
2) Un'infrastruttura è un oggetto complesso che evolve nel tempo e, di conseguenza, la comprensione del suo comportamento non può prescindere dalla conoscenza della sua dinamica evolutiva. In particolare tale evoluzione avviene seguendo regole che tendono ad ottimizzare, sia in ambito locale sia globale, alcuni parametri a discapito di altre caratteristiche della rete e questo impone dei vincoli sul livelli possibili di robustezza ed efficienza della rete stessa.
3) Il profilo di robustezza, inoltre, dipende anche dalla natura delle cause ostili: le attuali infrastrutture si sono evolute "naturalmente" in modo da essere relativamente immuni a guasti accidentali, mentre sembrano essere meno robuste nei confronti di azioni ostili mirate.

Conclusioni

La globalizzazione della società moderna e la pervasività delle tecnologie dello Ict stanno portando alla creazione di un *system of systems* costituito dalle diverse infrastrutture tecnologiche che risultano sempre di più interdipendenti fra di loro. Questo fenomeno, che trova le sue cause prime nella volontà/necessità di rispondere ai nuovi bisogni degli utenti e di adeguarsi ai mutati contesti socio-economici, comporta una maggiore vulnerabilità e criticità dell'intero sistema in quanto un qualunque *failure* (accidentale o deliberato) può amplificarsi e propagarsi attraverso le diverse infrastrutture critiche con la conseguenza di provocare danni anche ad utenti remoti, sia dal punto di vista geografico che logico, rispetto alla causa scatenate del *fault*.
La crucialità di tali infrastrutture e la conseguente necessità di "proteggerle" portarono l'amministrazione americana a sviluppare fin dal 1997 un programma mirato alla salvaguardia e protezione di queste infrastrutture e alla istituzione del "Ciao" (Critical Infrastructure Assurance Office). L'obiettivo principale del progetto era sintetizzato nella prefazione alla direttiva presidenziale n. 63 (Pdd-63) con cui Bill Clinton istituiva il progetto "*Any interruption or manipulation of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the wellfare of the United States*"[3] [9].
Analoghe iniziative sono state intraprese in altre nazioni mirate alla comprensione del problema, alla sua contestualizzazione alle realtà specifiche, all'individuazione di strategie per ridurre la vulnerabilità del sistema paese e la predisposizione di piani di intervento in caso di emergenza, con la costante ca-

[2] In questo contesto l'esempio più emblematico è offerto dal grafo del sistema nervoso del *Caenorhabditis elegans* nel quale si può supporre che l'evoluzione naturale abbia preservato la struttura più robusta rispetto ai mutamenti genetici casuali.
[3] Qualunque interruzione o manipolazione di queste funzioni critiche dovrà essere breve, infrequente, gestibile, geograficamente isolata e tale da arrecare minime conseguenze al welfare degli Stati Uniti.

ratterizzazione di una forte interazione e cooperazione pubblico-privato. L'importanza della problematica è emersa drammaticamente con gli eventi dell'11 settembre al punto che numerosi analisti sono concordi nel ritenere che le infrastrutture critiche saranno fra i bersagli preferenziali di azioni terroristiche o di sabotaggio nel prossimo futuro. Tali eventi hanno comportato un'accelerazione nei progetti relativi alla protezione delle infrastrutture critiche ed una diversa focalizzazione con una maggiore enfasi sul problema degli attacchi terroristici.
In Italia è stato costituito presso il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri un apposito gruppo di lavoro aperto alla partecipazione dei diversi soggetti operanti nel settore al fine di poter formare una visione generale del problema, consentire la condivisione di esperienze e soluzioni e, soprattutto, di favorire, stimolare e coordinare progetti di R&D mirati da un lato ad una maggiore comprensione del problema ed all'individuazione degli elementi di maggiore criticità per l'Italia e, dall'altro lato, allo sviluppo di tecnologie, ma anche di procedure, intrinsecamente meno vulnerabili.
È infatti indubbio che a prescindere dalla tecnologia adottata per garantire soddisfacenti livelli di sicurezza è fondamentale il coinvolgimento attivo dei diversi operatori ed utenti nonché la predisposizione di piani di azione[4] da adottare in caso di *failure* per circoscrivere e limitare i danni e consentire il ripristino dei servizi nel minor tempo possibile. Dal punto di vista della ricerca tecnologica un filone promettente, come evidenziato anche in [7], è quello dello sviluppo di sistemi ad agenti (noti anche come *autonomic system*) costituiti cioè da "individui" in grado di auto-gestirsi ovvero con capacità di adattarsi ed adeguarsi alle mutate condizione al contorno, in grado di diagnosticare la presenza di possibili *fault* sia interni che esterni al sistema (*self-healing*) e di generare autonomamente comportamenti tali da ridurre le possibili conseguenze del *failure* per se stesso e per altri agenti (*self-protection*) realizzando architetture quale quella evidenziata in Figura 5.
Metodologie ad agenti potrebbero trovare impiego anche per migliorare la comprensione del comportamento del *system of systems* costituito dalle diverse infrastrutture interdipendenti. Infatti, come di recente evidenziato in [8], a causa della loro dispersione geografica, dell'alto numero di interdipendenze reciproche e con operatori umani e delle caratteristiche intrinsecamente non lineare e multiscala delle relative dinamiche "*the mathematical methodologies that underpin today's modeling and simulation paradigms are unable to handle the complexity and interconnectedness of these critical infrastructures*". Ciò comporta la necessità di analizzare differenti paradigmi per la comprensione di tali infrastrutture ricorrendo, ad esempio a strumenti di analisi messi a punto nel campo delle scienza biologiche storicamente caratterizzati dall'operare con sistemi complessi e che, come evidenziato anche dagli studi sui sistemi *small-world* e *scale-free*, presentano molte analogie con le attuali infrastrutture tecnologiche. In particolare i sistemi biologici, ove sono presenti comportamenti di self-healing e self-protection oltre a meccanismi che consentono un'efficiente cooperazione fra i diversi individui, potrebbero aiutare ad individuare meccanismi, strategie e strumenti per lo sviluppo di tecnologie intrinsecamente maggiormente robuste.

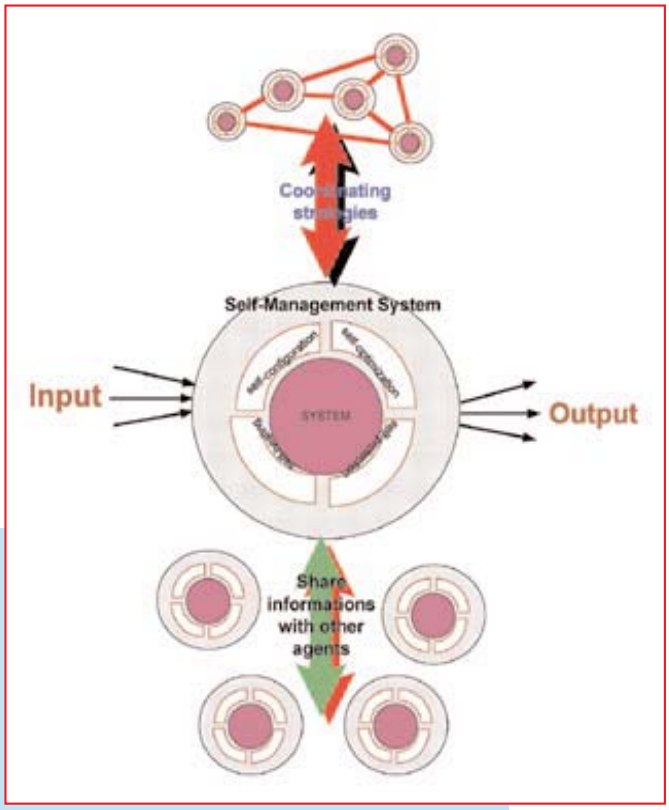


Figura 5 - In un'infrastruttura ad agenti ogni sistema è immerso in uno strato che gli conferisce capacità di self-configuration (adeguamento automatico del sistema in funzione di politiche di alto livello indotte), self-optimization (ricerca continua di opportunità di maggiore efficienza ed efficacia), self-healing (rilevamento automatico di malfunzionamenti), self-protection (difesa automatica da attacchi o azioni ostile e da fallimenti a cascata), in altre parole costituire un self-management system. In particolare ogni agente, oltre che interagire con il campo acquisendo i propri input e generando i relativi output scambia informazioni con gli altri agenti limitrofi al fine di acquisire una visione locale corretta dell'ambiente che lo circonda e concorda/riceve strategie ed obbiettivi globali interagendo con aggregati di agenti (infrastrutture).

[4] Tali piani vanno aggiornati al mutare delle infrastrutture e la loro efficacia, nonché la capacità degli operatori di eseguirli, andrà verificata con opportune esercitazioni periodiche.

Appendice Modelli per Sistemi Complessi

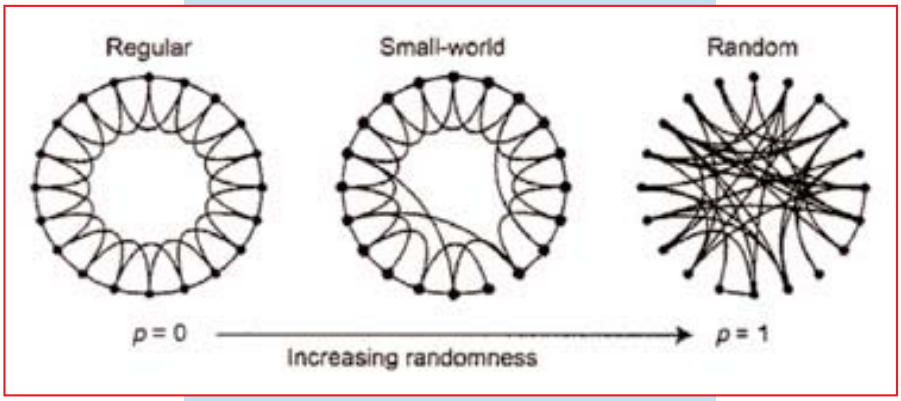


Figura A1 - Variazione del grafo in relazione al variare del livello di soglia p.

Vista la complessità di ognuna delle infrastrutture critiche un approccio intuitivo per il loro studio sembrerebbe quello di considerarli come dei grafi *random,* ovvero come un grafo i cui nodi rappresentano i vari elementi attivi della rete (i trasformatori nel caso di una rete elettrica, i Dns nel caso di Internet ecc.) e i cui rami rappresentano i collegamenti esistenti tra i diversi nodi. In fondo cosa può esistere di più "complesso" di una struttura costruita in maniera completamente casuale che può essere immaginata come ottenuta facendo dei punti a caso su un foglio e collegandoli fra loro con delle linee scelte in modo completamente arbitrario?

Alcuni recenti studi hanno, però, messo in dubbio questa affermazione legando in antitesi la complessità non alla natura aleatoria dei fenomeni sottesi bensì al numero dei parametri indipendenti necessari per descrivere compiutamente un sistema. Come affermato in [10] in un sistema puramente stocastico l'evoluzione futura può essere descritta, quanto meno statisticamente, utilizzando un unico parametro. Per cui la sua descrizione è relativamente semplice così come lo è quella di un segnale periodico dove la conoscenza di un sol parametro consente di effettuare una predizione ottimale del comportamento futuro del segnale. Per tutte quelle situazioni intermedie rispetto a questi due estremi si ha una maggiore difficoltà a predire il comportamento futuro ed è quello che si definisce come complessità strutturale del sistema. Partendo da queste considerazioni Watts e Strogatz hanno iniziato a studiare il comportamento di un grafo al variare del livello di *randomness* presente [11].

Si consideri un grafo regolare (ad esempio un reticolo 1-lattice quale quello descritto in Figura A1) e per ogni nodo si applichi un'operazione di re-wiring legata ad una funzione di probabilità: cioè per ogni link presente sul grafo si consideri il valore assunto da una variabile aleatoria uniforme nell'intervallo [0, 1], se il valore di tale variabile è inferiore ad un valore di soglia p, il link in esame è scollegato dalla sua destinazione originaria e collegato ad un altro nodo scelto casualmente. Al variare del livello della soglia p, si avranno caratterizzazioni differenti per il grafo:

- quando $p = 0$ il grafo risulta inalterato e quindi si preserva la struttura regolare di partenza;
- quando $p = 1$ il grafo risulta completamente random;
- Per tutti i valori intermedi, si ha un grafo che è parzialmente regolare e parzialmente random.

Se si considera quale grandezza di interesse la distanza media $L(p)$ fra due nodi espressa in termini del numero di link che bisogna percorrere per collegarli, al variare del parametro p essa descrive una sorta di curva logistica. Nella struttura regolare la distanza media è grande (per passare dal nodo a al nodo b occorre percorrere un gran numero di link), mentre la stessa si riduce notevolmente in presenza di un grafo random dove la presenza di shourtcut riduce drasticamente il numero di link da dover attraversare (Figura A2).

Un'altra grandezza di interesse è il livello di *clustering* che misura quanto siano strettamente connessi i nodi limitrofi, anche in questo caso al variare di p si ha una curva logistica: buona interrelazione fra nodi vicini nel caso di rete regolare, ridotta interrelazione nel caso di rete random. La cosa interessane che si nota immediatamente dalla Figura A2 è che il cut-off delle due curve è sfalsato per cui esistono valori del parametro p per i quali si hanno grafi che presentano contemporaneamente entrambi gli aspetti positivi: una piccola distanza fra i diversi nodi ed un'elevata interrelazione fra i nodi limitrofi.

Watts definì i grafi che godevano di questa proprietà come sistemi *Small World* in quando era la formalizzazione della teoria sociologica degli anni '50 che sosteneva che presi due qualunque individui sul nostro pianeta essi erano connessi da una catena di relazioni composta in media da sei persone (*six degree of separation*). Queste strutture presentano altre proprietà interessanti che li rendono in un certo senso "ottimali" sia su un orizzonte locale (stretta correlazione e sostituibilità dei vari

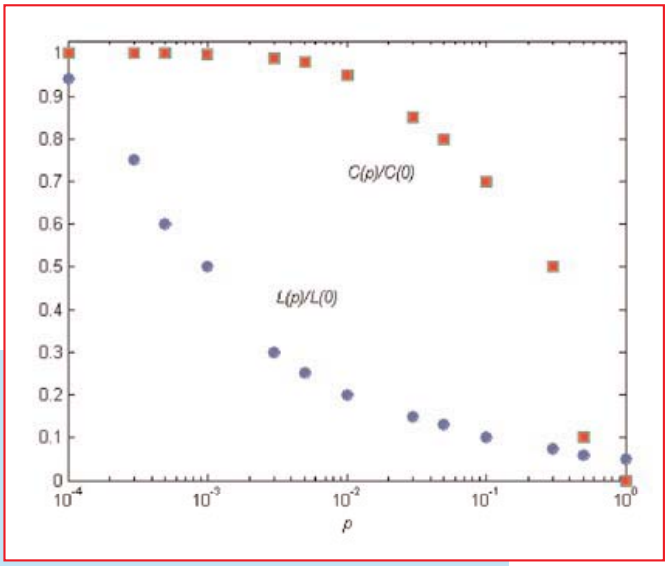


Figura A2 - Andamento del valore della distanza media L(p) e del coefficiente di clustering C(p) al variare del parametro p per il grafo rappresentato nella Figura A1. Il valore di L è definito come il numero di link presenti nel più corto percorso che connette due qualunque nodi, mediato su tutte le coppie di vertici. Il valore del coefficiente di clustering C(p) è definito nel seguente modo: si supponga che un vertice v abbia k_v nodi limitrofi; fra tali nodi limitrofi potranno esistere al più $k_v(k_v-1)/2$ link (questo accade quando ogni nodo appartenente all'insieme dei nodi limitrofi a v è connesso con tutti gli altri nodi dell'insieme). Si definisce C_v la frazione di link realmente esistente e il valore di C è ottenuto mediando su tutti i vertici.

elementi) che su scala globale (rapida trasferibilità delle informazioni fra i diversi punti del rete) [12]. Per alcuni di tali sistemi un'altra interessante caratteristica è legata alla probabilità di distribuzione del numero dei link per singolo nodo. A differenza di quanto accade in un grafo random dove tale distribuzione ha un andamento di tipo gaussiano ($\propto e^{-k}$) quale quello di Figura A3a, quello che emerge è una distribuzione governata da una legge di potenza ($\propto k^{-\gamma}$) simile a quella di Figura A3b.

Questi grafi, cioè, non sono "democratici" alcuni nodi hanno un numero di connessione decisamente superiori agli altri e per tale motivo essi rivestivano un ruolo fondamentale nella topologia della rete stessa [13]. Tali sistemi sono stati indicati con il termine di sistemi *Scale Free* ed è stato evidenziato che le caratteristiche della rete derivano direttamente dalle leggi sottese alla loro evoluzione ed in particolare che sono il frutto di una crescita a partire da un nucleo minimo per aggregazione successiva di nodi che, preferenzialmente, si sono andati a connettere con nodi già ben connessi [14].

Tali sistemi presentano una elevata robustezza intrinseca rispetto a *failure* di natura accidentale, ovvero a rimozioni random di un nodo all'interno della struttura. 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 una 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, un grafo *scale-free* diviene disconnesso eliminando un numero di nodi inferiore rispetto ad un grafo random [15].

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 vulnerabili ad attacchi mirati (potremmo dire terroristici), ovvero ad azioni che coscientemente mirano a ridurre l'efficienza del network 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 l'effetto soglia, per cui una epidemia si diffonde all'interno della rete anche se il numero degli elementi infetti iniziali è una frazione estremamente limitata al limite anche un sol nodo (come si evidenzia, ad esempio, nel caso della diffusione dei virus su Internet) e questo impone la necessità di prevedere strategie differenti per contrastare la dif-

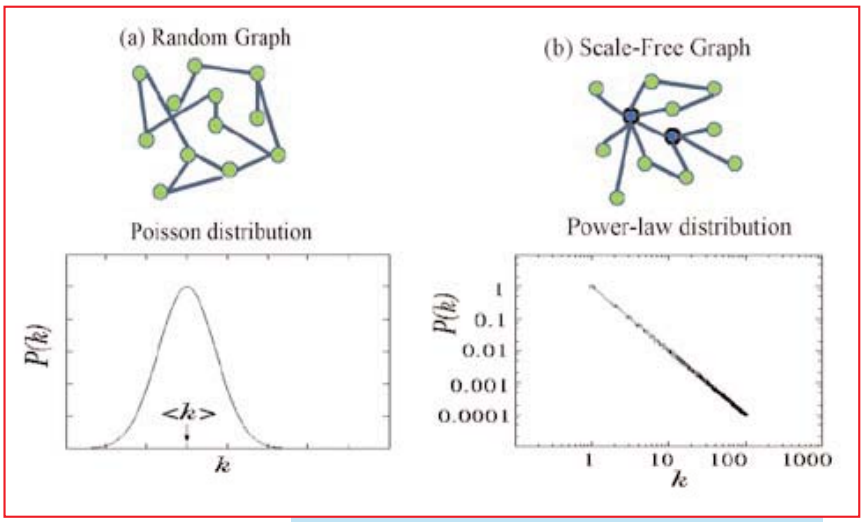


Figura A3 - In un grafo random il numero di link connesso ad ogni nodo ha una distribuzione gaussiana centrata interno al valor medio <k>. In un grafo scale-free vi è una distribuzione del numero di link per nodo meno uniforme: moltissimi nodi hanno pochissimi link e solo alcuni sono connessi con un gran numero di link.

fusione di tali "epidemie" [13]. Gli studi su questo tipo di grafi sono ancora in corso ed in particolare si stanno analizzando i significati e la validità di alcune delle ipotesi alla base del modello *scale-free* in considerazione anche delle discrepanze che emergono fra i dati sperimentale e quelli previsti dal modello.

Bibliografia

[1] Usa President's Commission on Critical Infrastruction Protection, *Critical Foundations: Protecting America'a Infrastructures*, 1997, http://www.ciao.gov.

[2] S. Rosenbush, *Satellite's death puts millions out of touch*, Usa Today, 21 Maggio 1998.

[3] Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, *Incident Analysis on Microsoft Sql Server 2000 "Slammer" Worm – Impact paper*, 12 marzo 2003.

[4] S. Rinaldi, J. Peerenboom, e T. Kelly, *Identify, Understanding, and Analyzing Critical Infrastructure Interdependencies*, Ieee Control System Magazine, pp. 11-25, Dicembre 2001.

[5] Usa, *The National Strategy to Secure Cyberspace*, 2003; http://www.whitehouse.gov/pcipb

[6] D. Cohen, *All the World's a Net*, New Scientist, pp. 24-29, 13 aprile 2002.

[7] S. Bologna, "Salvaguardia di infrastrutture energetiche complesse", *Automazione e Strumentazione*, pp. 129-133, marzo 2002.

[8] M. Amin, *Modelling and Control of Complex Interactive Networks*, Ieee Control System Magazine, pp. 22-27, Febbraio 2002.

[9] Usa, *Presidential Decision Directive 63*, 1998, http://www.ciao.gov.

[10] D. Watts, *Small Worlds*, Princeton University Press, Princeton, 1999.

[11] D. Watts e S. Strogatz, *Collective dynamics of small-world networks*, Nature, vol. 393, pp. 440-424, giugno 1998.

[12] V. Latora, M. Marchiori, *Efficient Behavior of Small-World Networks*, Physical Review Letters, 87, 198701, novembre 2001.

[13] R. Albert, A. Barabasi, *Statistical Mechanics of Complex Networks*, Reviews of Modern Physics, 74, pp. 48-97, 2002.

[14] A. Barabasi, R. Albert, *Emergence of scaling in random network*, Science, 286, pp. 509-511, 1999.

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