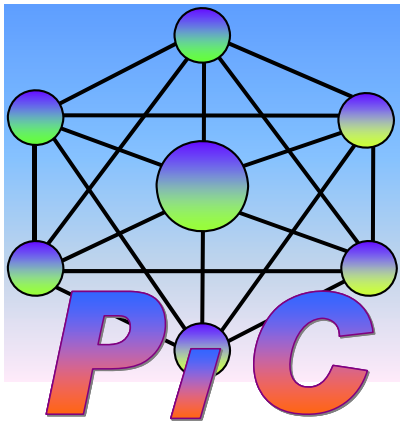
Presidenza del Consiglio dei Ministri

DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE

GRUPPO DI LAVORO SULLA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE INFORMATIZZATE



PROTEZIONE DELLE INFRASTRUTTURE CRITICHE INFORMATIZZATE

La realtà Italiana

10 marzo 2004

Indice

INDICE **2**
PREFAZIONE **4**
PREMESSA **6**
AVVERTENZA **7**
EXECUTIVE SUMMARY **8**
SOMMARIO **10**
INTRODUZIONE **14**
INTERRUZIONI NELLA FORNITURA ELETTRICA NELL'ESTATE DEL 2003 18
17 Luglio 2003 –Interruzione programmata della fornitura elettrica in Italia *19*
14 Agosto 2003 – Costa Nord Est dell'America *19*
28 agosto 2003 - Londra *20*
28 settembre 2003 - Italia *20*
LE INFRASTRUTTURE CRITICHE **23**
ESEMPI DI INFRASTRUTTURE INFORMATIZZATE **24**
L'INFRASTRUTTURA ELETTRICA 24
RETI INFORMATICHE E RETI DI TELECOMUNICAZIONE 25
L'INFRASTRUTTURA PER IL TRASPORTO DEL GAS 25
LA RETE FERROVIARIA 26
LA RETE VIARIA 26
CIRCUITI BANCARI E FINANZIARI 26
L'OSPEDALE E LE SUE CRITICITÀ INFRASTRUTTURALI 27
IMPIANTI NUCLEARI 27
LA NAVIGAZIONE SATELLITARE 27
I SISTEMI DI MONITORAGGIO E CONTROLLO 27
ANALISI DELLA SITUAZIONE MONDIALE **30**
STATI UNITI 31
GRAN BRETAGNA 32
GERMANIA 33
CANADA 33
SVEZIA 34
ISTITUZIONI INTERNAZIONALI 35
LA REALTÀ ITALIANA **40**
LA SITUAZIONE LEGISLATIVA ITALIANA 40
IL RUOLO DEL MINISTERO DELL'INTERNO 41
COMITATO TECNICO NAZIONALE SULLA SICUREZZA INFORMATICA E DELLE TELECOMUNICAZIONI DELLA PUBBLICA AMMINISTRAZIONE 43
OSSERVATORIO PERMANENTE PER LA SICUREZZA DELLE RETI E LA PROTEZIONE DELLE COMUNICAZIONI 44
PROPOSTE **45**

PROPOSTA DI ISTITUZIONE DI UN COMITATO INTERMINISTERIALE PER LE INFRASTRUTTURE CRITICHE INFORMATIZZATE (COM.IN.C.I) 45
Realizzazione di un sito dedicato alla problematica *47*
PROPOSTA DI UNA AGENDA DI RICERCA ITALIANA NEL CAMPO DELLA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE INFORMATIZZATE 48
Proposta per la creazione di un Centro Virtuale di Simulazione e Analisi delle Interdipendenze (SAI) *50*
Supporto alle attività di R&S sulle tecnologie in grado di identificare in modo decentralizzato l'insorgere di stati anomali e di prevenire le conseguenze attraverso opportune politiche locali di gestione *50*
PROPOSTA PER LA CREAZIONE DI UN GRUPPO DI INTERESSE NAZIONALE (GDIN) 51

CONCLUSIONI 54

ELENCO PARTECIPANTI AL GRUPPO DI LAVORO 56

GLOSSARIO 57

RISOLUZIONE N. 58/199 DELLE NAZIONI UNITE 59

BIBLIOGRAFIA 62

DOCUMENTI ISTITUZIONALI 62
DOCUMENTI DI INQUADRAMENTO DELLA PROBLEMATICA 63
PUBBLICAZIONI SCIENTIFICHE 65

Prefazione

Il grande sviluppo registrato dalle tecnologie dell'informatica e delle telecomunicazioni nell'ultimo decennio ha reso possibile l'abbattimento di numerose barriere rendendo facilmente disponibili e fruibili ad una platea pressoché illimitata beni e servizi, prima appannaggio di pochi.

In particolare la diffusione di Internet ha consentito non solo di ridurre i costi connessi con l'erogazione di molti servizi, fra cui quelli propri della P.A., miglioramento l'efficienza dei processi produttivi sottesi, ma, soprattutto, ha contribuito a realizzare una sorta di rivoluzione copernicana grazie alla quale non è più l'utente che deve "fisicamente" recarsi dal fornitore di servizi, ma è il servizio stesso che si rende fruibile nel luogo e nel modo richiesto dall'utente e ciò nei più disparati settori: dalla finanza all'entertainment, dalla sanità alla formazione solo per citarne alcuni.

Questa rivoluzione, auspicata e promossa dal Governo, porta insita, quale risvolto della medaglia, una sempre maggiore dipendenza della nostra società dall'infrastruttura informatica e ciò impone una crescente attenzione da parte di tutti i soggetti preposti su come garantirne la costante fruibilità e il corretto funzionamento a prescindere da eventi sia di carattere naturali sia indotti dall'uomo.

La realizzazione di quest'obiettivo, considerato come prioritario anche nel piano per la e-Europe, si scontra da un lato con la limitata conoscenza che ancora possediamo del cyberspace e delle sue potenzialità e minacce, e dall'altro con il fatto che l'infrastruttura informatica basa il suo funzionamento sull'esistenza e sul corretto funzionamento di altre infrastrutture tecnologiche quali: le reti di distribuzione dell'energia, le reti di telecomunicazione, ecc.

Tutte queste infrastrutture, a loro volta, a causa della loro crescente complessità intrinseca e della necessità di fornire servizi innovativi all'utenza, ricorrono in modo massiccio alle tecnologie dell'ICT (Information & Telecommunication Technologies). Questo si traduce nell'istaurarsi di innumerevoli e complesse interdipendenze fra le diverse infrastrutture rendendo oltremodo difficile, ma nello stesso tempo drammaticamente urgente, il problema della protezione dell'insieme delle infrastrutture tecnologiche sempre più critiche per il benessere della nazione.

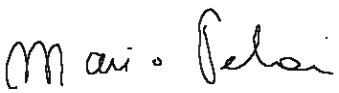
Il Gruppo di Lavoro istituito presso il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri ha avuto l'incarico di iniziare a studiare questa tematica raccogliendo il contributo dei diversi operatori pubblici e privati coinvolti nella gestione e nel controllo delle infrastrutture critiche, cercando di costruire un quadro unitario e quanto più possibile complessivo della problematica.

I risultati del lavoro svolto sono raccolti in questo volume e vogliono rappresentare un punto di partenza per stimolare un ampio dibattito a livello nazionale che possa portare al più presto, come sta accadendo nella gran parte delle nazioni occidentali, alla definizione di una strategia di azione in grado di incrementare il livello di "sicurezza" (intesa come capacità di operare correttamente a prescindere da eventi di qualunque natura) delle infrastrutture tecnologiche nazionali.

Non posso concludere queste mie brevi considerazioni senza ringraziare Vincenzo Merola per la costanza mostrata nel portare avanti le attività del Gruppo di Lavoro e per la sua capacità di sintetizzare e comunicare la vera essenza di una problematica, quale quella della Protezione delle Infrastrutture Critiche Informatizzate, estremamente nuova e complessa.

Mi corre l'obbligo, infine, di ringraziare anche Roberto Setola per l'impegno profuso nel Gruppo di Lavoro. Le sue competenze professionali e la sua specifica preparazione scientifica, hanno consentito di svolgere in pochissimo tempo un'attività seria e concreta che ha trovato importanti riconoscimenti anche a livello internazionale. Di questa collaborazione devo ringraziare l'amico e collega Luigi Fiorentino che, comprendendo l'importanza della problematica per il Paese, ha approvato ed incoraggiato l'impegno dell'ing. Setola in queste attività.

Ing. Mario Pelosi
Capo del Dipartimento per
l'Innovazione e le Tecnologie
Presidenza del Consiglio dei Ministri



Premessa

Seguendo una prassi inusuale per la P.A., il Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate (GdL) è sorto sulla base di una "spinta dal basso" che ha consentito di aggregare, strada facendo, i soggetti attenti alla problematica presenti nei diversi dicasteri ed enti coinvolti nella problematica. Per la sua natura e composizione, il GdL si è attivato prioritariamente su azioni di natura culturali tese, cioè, ad una migliore comprensione del problema, dei suoi confini e delle sue implicazioni nel tentativo di chiarire, inizialmente agli stessi soggetti operanti nel GdL, la reale natura di una problematica estremamente complessa che coinvolge una pluralità di settori e di tematiche.

Da questo lavoro è scaturita la necessità di delineare con maggiore precisione la problematica a livello nazionale indicando, in particolare, la natura ed il ruolo svolto dalle diverse infrastrutture ed evidenziando le interdipendenze fra esse esistenti. Ciò ha portato alla stesura del presente documento, che vuole essere una prima panoramica sulla realtà italiana evidenziandone la natura, la complessità (legata all'interdipendenza di strutture già di per se complesse), le azioni intraprese a livello internazionale ed alcune proposte su come sviluppare opportune politiche di settore.

È doveroso per me ringraziare tutti coloro che hanno contribuito al lavoro del GdL e alla stesura di questo documento, ed in primo luogo tutti i colleghi dei vari dicasteri, autorità ed enti che da subito hanno manifestato un profondo interesse per la problematica, in considerazione dell'importanza che essa rivestire per la nazione.

Un altrettanto doveroso ringraziamento va ai rappresentanti dell'accademia e degli enti di ricerca, la loro sensibilità e l'impostazione alla problematica da loro offerta ha contribuito a mettere in evidenza nel migliore dei modi il soggetto delle attività del GdL.

Non posso non ringraziare calorosamente, poi, tutti quelli che operando come soggetti privati nei diversi settori coinvolti nella tematica hanno offerto la loro disponibilità ed il loro contribuito per il buon esito dell'iniziativa nonostante la stessa si svolgesse su un piano sostanzialmente volontaristico, mostrando grande attenzione verso problematiche del Paese che vanno al di là dei semplici interessi economici legati ai propri business.

Un ringraziamento particolare va al dott. Sandro Bologna dell'ENEA il cui pungolo e la cui competenza sul soggetto è stato uno degli elementi basilari su cui si è fondato il GdL, così come un ringraziamento particolarissimo va al prof. Salvatore Tucci che con il suo appoggio e i suoi contribuiti ha consentito la nascita del GdL e supportato attivamente le sue iniziative.

Questo documento non vuole, però, essere solo il risultato conclusivo di un lavoro avvincente che si è sviluppato nell'arco di alcuni mesi, bensì il punto dal quale partire per sviluppare una politica mirata a garantire un adeguato livello di continuità di servizio e di sicurezza alle diverse infrastrutture critiche interdipendenti.

Avvertenza

Le opinioni e le considerazioni espresse in questo documento, nonché le proposte avanzate, sono da considerarsi come valutazioni personali dei singoli partecipanti al Gruppo di Lavoro e non riflettono necessariamente la posizione del Governo, né quella dei rispettivi Enti e Società.

Executive Summary

This document deals with the Critical Information Infrastructures Protection (CIIP), emphasizing the most relevant aspects and their impacts on our Country.

This problem has gained more and more attention from almost all the developed countries due to the increase relevance that technological infrastructures have on the welfare of large segment of population. Indeed quite every economical and social activities are highly dependent on the existence, correctness and security of infrastructures like: telecommunications, electrical power systems, gas and oil storage and transportation, water supply systems, health care systems, banking and finance circuits, and so on.

Due to their importance, one can refer generally to them as **Critical Infrastructures** since their failure, even for a short time, may produce large negative consequences on national or regional economies, or produce injury to citizens.

Until one decade ago, this problem was not so dramatic. Indeed each infrastructure could be considered as an autonomous system with very few points of contact with respect to the other infrastructures. Due to many reasons, today this scenario has completely changed. The interdependencies among the infrastructures have exponentially increased. One reason for this, but absolutely not the only one, is related to the fact that of the *cyberspace* (i.e. the virtual space obtained by the interconnection of computers, telecommunications systems, software and date), is shared among quite all the infrastructures.

One of the most relevant consequences of the presence of a so large number of interdependencies is that any *failure* (accidental or malicious) in any infrastructure may easily spread across the other with a domino or cascade effect, amplifying its consequences and producing inconveniences also to remote (geographical or logical) users.

This imposes a change in security strategies: no one operator may autonomously guarantee the dependability of its infrastructure. But, due to these large number of interdependencies, he need the cooperation of the other Critical Infrastructures' operators and Government's Agencies.

This document describes some of the critical Italian infrastructures and emphasizes their high level interdependencies. The analysis shows that infrastructures' complexity call for an increased use of ICT tools (Information and Telecommunications Technologies). This allows them to satisfy new users' requirements, but, at the same time, introduces further and unknown vulnerabilities.

In this framework, one can define CIIP as the set of initiatives aimed to increase the robustness of any critical infrastructure that uses for its monitoring, control, or manage any information infrastructure (considering among critical infrastructures, also information infrastructures and Internet specifically).

At international level, the need to improve the protection of the critical infrastructures has gained great attention. In many countries, suited coordination structures have been set up to improve the cooperation among public and private operators. In particular, the US government was the first to focalise the problem with the constitution of a specific commission in 1996 (the *President's Commission on Critical Infrastructure Protection),* and, successively, with the release of the PDD63 from the president Clinton in 1998. Today, many other countries have developed policy on CIIP devoted to:

- Understand vulnerabilities related to national critical infrastructures, emphasizing their criticalities, their interdependencies, and their vulnerabilities;
- Define strategies to mitigate these vulnerabilities;
- Improve infrastructures' robustness with respect to physical and cyber threats;
- Define emergency, contingency and continuity plans;
- Support R&D on CIIP, and specifically devotes to a better understanding of the problem, and to the development of technologies intrinsically robust;
- Support international cooperation.

In Italy, despite the other countries, there is no adequate attention to the problem. To this end, a specific Working Group (WG) has been established at the Dipartimento per l'Innovazione e le Tecnologie (Dept. of Innovation and Technologies) of the Prime Minister' Office. The WG is composed by representatives from ministries, public agencies, private sector operators, academia and research institutions involved with Critical Infrastructures operation, management, and control.

The WG emphasized the need to precisely define the nature and the extension of the problem and to create a common vocabulary among the different infrastructures' stakeholders. Further, it stressed the importance to have an Italian subject able to coordinate, promote and support initiatives on the topic. Indeed this problem has a national-wide dimension with many international connections. It cannot be managed by any particular, public or private, initiative.

Starting from the experiences of G8's Countries, the WG suggests the creation of an Interministerial Committee (**Comitato Interministeriale per le Infrastrutture Critiche Informatizzate – COM.IN.C.I.)**, devoted to**:**

- ❖ Improve the awareness about CIIP and its consequences for the Country;
- ❖ Realize a global vision of the system of systems constituted by the Italian Critical Infrastructures, emphasizing their interdependences;
- ❖ Promote the improvement of critical infrastructures robustness by defining national action plain;
- ❖ Stimulate and support ministries, agencies, and the different, public or private, stakeholders involved with the management and control of critical infrastructures for the development and implementation of suitable strategies and operational plans to reduce their vulnerabilities;
- ❖ Improve the exchange of best-practices about security and information sharing among the different infrastructure's operators, stakeholders ad government;
- ❖ Promote R&D and international cooperation.

Due to the cornerstone role played by the private sector operators, the WG hopes that, on a voluntary base, a **Gruppo di Interesse Nazionale (GdIN)** could be established that aggregates the different critical infrastructures' operators so as to become the principal representative with respect to the Interministeral Committee.

At the same time, it is mandatory to support the R&D by defining a Research's Agenda which covers the different topics involved by CIIP and, specifically, the development of a National Virtual Centre on Simulation and Interdependencies Analysis on CIIP

Sommario

Questo documento ha l'obiettivo di delineare la problematica della Protezione delle Infrastrutture Critiche Informatizzate evidenziando gli aspetti di maggior interesse e criticità per il sistema paese.

L'importanza di considerare questa problematica, e la forte attenzione che su di lei si va concentrando a livello mondiale, è dovuta al fatto che lo sviluppo dei diversi settori della società e di conseguenza il benessere della popolazione nei paesi industrializzati, dipende, e dipenderà sempre di più, dalla disponibilità e dal corretto funzionamento di infrastrutture tecnologiche 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, infrastrutture idriche, 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 ad un decennio fa, ognuna di queste infrastrutture poteva considerarsi come un sistema autonomo sostanzialmente indipendente, gestito da operatori verticalmente integrati. Per una serie di ragioni tale struttura si è profondamente modificata al punto che sempre di più le varie infrastrutture tendono a essere interdipendenti, soprattutto a causa della condivisione del cosiddetto *cyberspace*, ovvero lo spazio virtuale prodotto dall'interconnessione di calcolatori, sistemi di telecomunicazioni, applicazioni e dati. Ciò comporta che un *guasto* (di natura accidentale o dolosa) in una di tali infrastrutture può facilmente propagarsi, con un effetto domino, ad altre infrastrutture 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 è verificato il *guasto* iniziale.

Questo mutato scenario impone un cambiamento di mentalità nell'approccio al problema della protezione delle infrastrutture: il singolo operatore non è più, infatti, in grado di garantire autonomamente il corretto funzionamento e la sicurezza della propria infrastruttura. Se vuole ottenere ciò, egli deve necessariamente interfacciarsi in questo processo anche i diversi soggetti coinvolti nella gestione e nel controllo di tutte quelle infrastrutture da cui la propria dipende o su cui si basa. Tenendo conto che non è sempre facilmente percepibile quali siano le infrastrutture da prendere in esame ed, inoltre, che queste ultime possono a loro volta dipendere, in maniera diretta o indiretta, dalla prima infrastruttura, si comprende come il problema assume un livello di complessità notevole e necessita di opportune azioni di coordinamento.

In questo documento sono esaminate alcune infrastrutture italiane informatizzate. L'analisi ha consentito di evidenziare come la crescente complessità delle diverse infrastrutture impone per la loro gestione un sempre maggior utilizzo delle tecnologie ICT (Information and Communication Technologies). Se ciò da un lato consente di fornire risposte alle mutate esigenze dei mercati e degli utenti finali, dall'altro introduce una maggiore vulnerabilità nel sistema.

Con il termine **Protezione delle Infrastrutture Critiche Informatizzate** si intende, infatti, quell'insieme di azioni connesse con il problema di innalzare il livello di sicurezza, affidabilità e correttezza di tutte quelle infrastrutture critiche che utilizzano, in tutto o in parte, una qualunque infrastruttura informatica per il loro monitoraggio, la loro gestione o il

loro controllo; includendo, naturalmente, nel novero delle infrastrutture critiche anche quelle informatiche e specificatamente Internet.

A livello internazionale la problematica ha assunto una valenza strategica nella gran parte degli stati industrializzati ove sono state costituite opportune strutture di coordinamento fra i diversi soggetti pubblici e privati operanti nel settore delle Infrastrutture Critiche. In particolare, gli Stati Uniti furono i primi a formalizzare azioni a livello governativo sul soggetto con la costituzione della *President's Commission on Critical Infrastructure Protection* nel 1996 e l'emanazione della Presidential Decision Directive n. 63 (PDD63) da parte del presidente Clinton nel 1998. Sulla scorta di quanto fatto dal governo americano anche altre nazioni hanno sviluppato azioni governative tese a:

- Sensibilizzare i diversi operatori circa il problema della protezione delle infrastrutture critiche;
- Comprendere gli elementi di criticità e vulnerabilità delle diverse infrastrutture critiche presenti nel paese, evidenziandone le interdipendenze;
- Definire strategie per mitigare tali vulnerabilità;
- Predisporre piani di emergenza e di contingentamento da attivare in presenza di eventi negativi che interessino più infrastrutture critiche;
- Favorire lo sviluppo di tecnologie intrinsecamente sicure e supportare la cooperazione internazionale.

In Italia, a differenza degli altri paesi, l'attenzione al problema è ancora limitata e per migliorare tale situazione è stato costituito, presso il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri, un Gruppo di Lavoro aperto alla partecipazione dei soggetti interessati al tema ed il cui scopo principale è quello di svolgere un'azione di inquadramento e di sensibilizzazione sulla questione.

La prima necessità emersa è stata quella di definire con esattezza la natura e i confini della problematica oltre che trovare un linguaggio comune fra tutti i soggetti coinvolti. Infatti, se da un lato questa problematica risulta essere fortemente interdisciplinare richiedendo il coinvolgimento di soggetti operanti in una pluralità di campi, dall'altro è importante comprendere che esso non va a sostituirsi a nessuna delle iniziative attualmente in atto per quel che riguarda la protezione delle singole infrastrutture.

Fermo restando, infatti, la competenza sugli aspetti di prevenzione, protezione e sicurezza che ogni operatore deve mettere in atto nel proprio settore sulla base delle indicazioni e direttive che pervengono dalle evoluzioni delle tecnologie e dal quadro normativo esistente, occorre iniziare a prendere in considerazione anche quelle variabili che non sono sotto il diretto controllo di nessun operatore singolarmente ma per le quali occorre sviluppare delle politiche di co-partecipazione alla gestione dei rischi.

L'attività del Gruppo di Lavoro ha evidenziato la necessità di individuare anche in Italia un soggetto in grado di svolgere un ruolo di promozione, sensibilizzazione politica, stimolo, supporto, aggregazione e coordinamento per le iniziative, sia operative che di R&S, sulla tematica. Il problema ha, infatti, una dimensione nazionale con forti collegamenti internazionali e non può essere risolto con iniziative singole sia pubbliche che private.

Prendendo spunto da quanto fatto dalla quasi totalità dei paesi G8, si auspica, pertanto, la costituzione di un **Comitato Interministeriale per le Infrastrutture Critiche Informatizzate (COM.IN.C.I.)** presso la Presidenza del Consiglio dei Ministri, eventualmente promosso dal Comitato dei Ministri per la Società dell'Informazione, quale struttura di coordinamento con il compito di:

- ❖ Favorire la presa di coscienza della problematica e delle sue ripercussioni;
- ❖ Consentire una visione complessiva del *sistema di sistemi* costituito dalle diverse infrastrutture tecnologiche operanti in Italia evidenziandone gli aspetti di maggiore interdipendenza e, quindi, criticità;
- ❖ Promuovere azioni tese a limitare la vulnerabilità delle infrastrutture critiche definendo piani di azione nazionali e individuando le priorità;
- ❖ Stimolare e supportare i dicasteri e i diversi soggetti pubblici e privati coinvolti nel controllo e nella gestione delle diverse infrastrutture nel monitoraggio delle stesse e nell'adozione di opportune strategie ed iniziative tese a ridurre il livello di rischio;
- ❖ Favorire la disseminazione delle best-practices sulla sicurezza ed un fattivo scambio di informazioni fra i diversi soggetti coinvolti nella gestione delle infrastrutture e nella prevenzione e protezione delle stesse;
- ❖ Promuovere la formazione del personale operante nei settori delle Infrastrutture Critiche per quel che riguarda la gestione delle situazioni di emergenza;
- ❖ Promuovere la ricerca e la cooperazione internazionale sul soggetto.

Il ruolo di tale struttura dovrebbe essere, inoltre, quello di coordinare e raccordare le iniziative che andranno ad assumeranno i diversi soggetti competenti, che potranno così operare in un quadro unitario che tenga conto delle molteplici interdipendenze esistenti fra le varie infrastrutture.

Stante le competenze necessarie affinché il Comitato possa avere una visione complessiva del problema, al suo interno dovrebbero essere rappresentati almeno i seguenti dicasteri/enti: Presidenza del Consiglio dei Ministri, Ministero Interno, Ministero Giustizia, Ministero Infrastrutture, Ministero Attività Produttive, Ministero Comunicazioni, Ministero Difesa, Ministero Salute, Ministero Istruzione Università e Ricerca Scientifica, Ministero Ambiente, Ministero Economia e Finanze, Dipartimento per l'Innovazione e le Tecnologie, Dipartimento per la Protezione Civile, Servizi di Informazione, Autorità per le garanzie nelle Comunicazioni, Autorità per l'Energia Elettrica e il Gas.

Il Comitato, inoltre, dovrebbe operare in sinergia con le altre autorità ed enti coinvolti nella gestione e nel controllo delle Infrastrutture Critiche oltre che con gli operatori privati.

In particolare, stante il ruolo cruciale svolto dai diversi operatori nella comprensione della problematica e per l'individuazione delle possibili azioni da intraprendere, sorge la necessità di individuare interlocutori rappresentativi delle diverse istanze ed esigenze. In questo senso il Gruppo di Lavoro auspica la costituzione di un **Gruppo di Interesse Nazionale (GdIN)**, che sulla base di un principio associativo volontario, possa raccogliere i soggetti privati operanti nei diversi ambiti delle Infrastrutture Critiche, assumendo il ruolo di interlocutore privilegiato nei confronti del COM.IN.C.I.

Parallelamente a queste iniziative è fondamentale favorire la ricerca e lo sviluppo sul tema con l'attivazione di un'opportuna **Agenda di Ricerca**, che possa fungere da catalizzatore nei confronti del mondo accademico e della ricerca anche grazie ad opportune forme di finanziamento, compartecipazione e coordinamento.

Nel campo della R&S, azioni di grande importanza sono quelle legate allo sviluppo di tecnologie in grado di identificare in modo decentralizzato l'insorgere di stati anomali e di prevenire le conseguenze attraverso opportune politiche locali di gestione.

Un'altra iniziativa specifica potrebbe essere la costituzione di un centro di simulazione virtuale (**SAI** – Centro Nazionale Virtuale di Simulazione e Analisi delle Interdipendenze) in grado di aiutare a comprendere i diversi scenari di crisi e le modalità con cui potrebbero propagarsi i guasti attraverso le diverse infrastrutture. Questo Centro potrà rappresentare

l’elemento attorno al quale aggregare le diverse esperienze, esistenti o in via di attivazione, in Europa nel campo della R&S su questa tematica, realizzando in tal modo quella massa critica necessaria per poter fornire risposte compiute ai molti e complessi problemi posti dalle Infrastrutture Critiche Informatizzate.

Introduzione

Lo sviluppo tecnologico, finanziario e sociale dei paesi industrializzati dipende, e dipenderà sempre di 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. Infatti, i diversi operatori e gestori, di norma monopolistici, avevano provveduto a creare proprie infrastrutture di telecomunicazione e controllo ed adottato sistemi di gestione proprietari (si veda Figura 1).

Per una serie di ragioni, legate sia all'adozione delle tecnologie ICT nelle procedure di gestione e controllo, sia alla liberalizzazione ed internazionalizzazione dei mercati con conseguente eliminazione dei gestori monopolistici nazionali, sia alla volontà/necessità di soddisfare nuove aspettative ed esigenze degli utenti, tale struttura si è profondamente modificata. Le varie infrastrutture tendono, infatti, ad essere sempre più strettamente connesse e ciò soprattutto a causa della condivisione di quello spazio comune generalmente indicato come il *cyberspace*, ovvero lo spazio virtuale prodotto dall'interconnessione di calcolatori, sistemi di telecomunicazioni, applicazioni e dati. Questo ha comportato che le infrastrutture critiche sono divenute fortemente **interdipendenti,** al punto 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 malfunzionamenti anche ad utenti remoti, sia dal punto di vista geografico che funzionale, rispetto al punto ove si era originariamente generato il *guasto*.

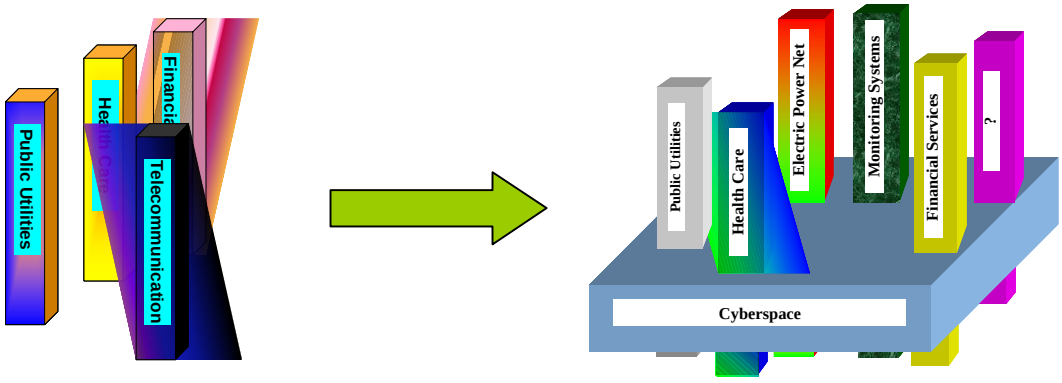


Figura 1: In questi anni si va sempre più evidenziando il passaggio da una serie di infrastrutture autonome e sostanzialmente indipendenti ad una situazione in cui le diverse infrastrutture condividono uno spazio comune, genericamente indicato come *cyberspace*. Ciò comporta una crescita esponenziale del livello di interdipendenza esistente fra le diverse infrastrutture anche in considerazione del fatto che lo stesso *cyberspace* dipende dal corretto funzionamento di alcune delle infrastrutture che su di esso si basano per il loro funzionamento.

In realtà, le tecnologie dell'ICT hanno contribuito solo ad amplificare le interdipendenze esistenti fra le diverse Infrastrutture Critiche che, per altro, possono essere anche di diversa natura. In letteratura sono generalmente individuate 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 ha bisogno 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 doloso può provocare un guasto contemporaneo sulle varie infrastrutture;
- *Interdipendenza 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 consente di modellare quei legami connessi con fenomeni socio-economici, culturali o indotti da vincoli normativi e legislativi.

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 sostanzialmente qualunque altra infrastruttura che utilizza il *cyberspace*, e ciò anche a prescindere dal concetto di prossimità geografica.

Attualmente le interdipendenze che creano più inconvenienti sono quelle di natura geografica. Molti analisti sono, però, convinti che nel futuro gli accoppiamenti legati alle tecnologie dell'ICT saranno quelli più importanti sia a causa dell'incremento nell'uso di queste tecnologie, con il conseguente aumento dei punti di contatto, sia perché, a differenza degli altri tipi di interdipendenze, essi consentono una rapida propagazione degli effetti anche su aree geograficamente remote rispetto al punto in cui si è prodotta la causa. Ciò fa ipotizzare che nel prossimo futuro il *cyberspace* sarà globalmente la causa principale e il maggior strumento di veicolazione dei guasti.

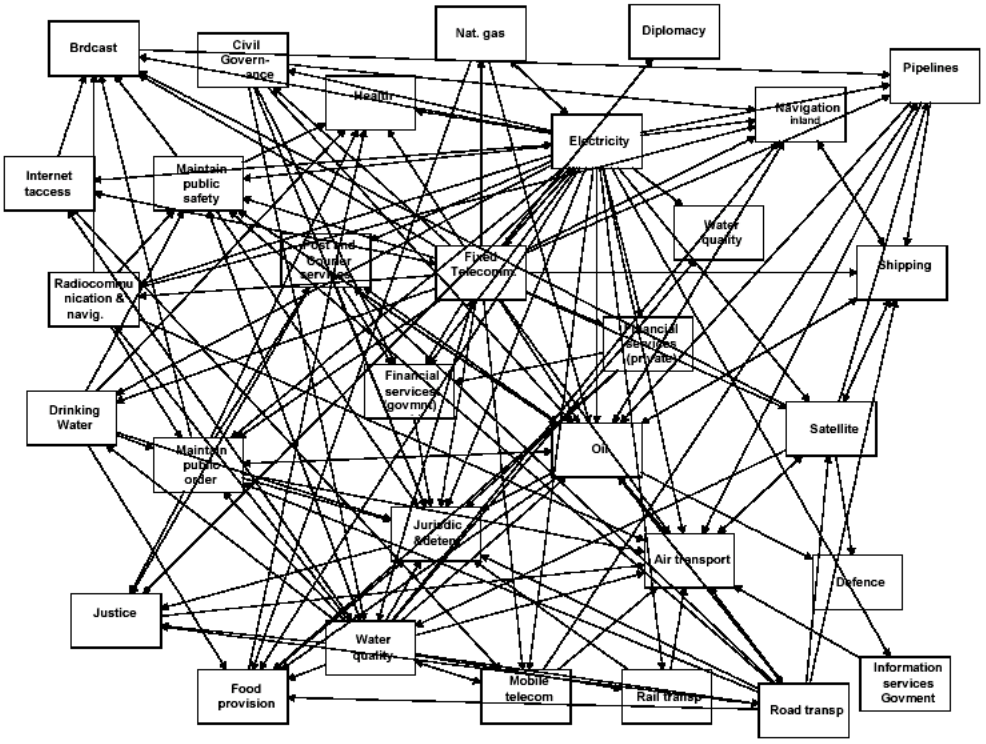


Figura 2: Grafico delle interdipendenze esistenti fra le diverse infrastrutture operanti in Olanda (Fonte TNO). L'incredibile numero di interazioni evidenziate rende di difficile lettura il grafico e ciò sottolinea come sussistono molteplici accoppiamenti fra praticamente tutte le infrastrutture considerate nell'analisi.

In letteratura sono riportati diversi episodi emblematici di come un guasto possa propagasi, amplificandosi, attraverso infrastrutture eterogenee sfruttando la presenza delle interdipendenze reciproche. Alcuni di questi episodi sono riportati nella tabella seguente.

1997	Un teenager fu in grado di disattivare da remoto la centrale telefonica di Worcester (MA-USA) lasciando scoperto un bacino di oltre 600 utenze fra cui la locale stazione dei vigili del fuoco e creando problemi al locale aeroporto.
1998	In conseguenza di un guasto del satellite per telecomunicazioni Galaxy IV, 40 milioni di pagers andarono fuori servizio; 20 voli United Airline in decollo subirono pesanti ritardi a causa della mancata comunicazione delle condizioni atmosferiche in quota; alcune radio persero la capacità di trasmettere; diversi automobilisti non poterono rifornirsi di carburante a causa dell'impossibilità di processare le carte di credito presso le stazioni di servizio lungo le high-way.
2000	A Maroochy Shire (Australia) un ex-dipendente riuscì ad introdursi nel sistema di tele-controllo di un impianto di depurazione provocando, da remoto, il riversamento di circa 1.200.000 litri di liquami non trattati direttamente nell'ambiente.
2001	Un attacco hacker alla Cal-ISO, la principale società per il trasporto dell'energia elettrica in California, fu scoperto solo dopo 17 giorni. Non è stato possibile stabilire che tipo di informazioni siano state carpite durante questo periodo né quali erano i reali obiettivi dell'azione.

	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 di importanti nodi di telecomunicazioni provocò ripercussioni 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 Streat) che indirette (legate al crollo di fiducia degli investitori), e sull'intero comparto del trasporto aereo le cui conseguenze non sono ancora terminate. Un'altra conseguenza indotta sul sistema economico è stata la diversa ripartizione degli investimenti con un aumento generalizzato di quelli per la sicurezza (cresciuti in alcuni comparti anche di un fattore 10). Alcune stime indicano in 83 miliardi di dollari l'impatto economico dell'evento.
2002	La chiusura erronea di una valvola di emergenza su uno dei due metanodotti di Singapore comportò l'interruzione della fornitura del gas naturale a sette centrali elettriche. Questo comportò un taglio del 30% nella produzione di energia elettrica nazionale (ridotto all'8% dopo aver attinto alle risorse di emergenza) con un conseguente black-out di 90 minuti che, fra le altre cose, comportò l'interruzione della produzione in molte imprese chimiche dell'isola per la cui riattivazione furono necessari diversi giorni di lavoro.
2003	Il worm informatico Slammer, con la sua rapida diffusione, ha causato problemi ai circuiti finanziari (quello del sud-est asiatico fu quasi completamente bloccato, in USA 13.000 ATM andarono fuori servizio, in Italia in 11.000 uffici Postali ci furono notevoli problemi), ai trasporti aerei (diversi voli in partenza dall'aeroporto di Huston e di Vancouver subirono pesanti ritardi o furono cancellati) ed ai sistemi di emergenza (il call-center del 911 di Seattle andò fuori servizio). Negli USA il worm è riuscito a penetrare anche all'intero del sistema di controllo di una centrale nucleare in dismissione (senza creare seri problemi grazie alla presenza di circuiti di back-up in analogico) e ad interrompere il traffico dei sistemi di monitoraggio e controllo di due società di distribuzione dell'energia elettrica (in un caso penetrando all'interno del sistema informatico e nell'altro saturando la banda del canale ATM utilizzata per la connessione con le unità periferiche).
2004	Il guasto al sistema di aria condizionata di un importante nodo Telecom a Roma ha provocato la paralisi del traffico telefonico, sia fisso che quello di diversi operatori mobili, per circa 6 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 postale sono rimasti privi di connessione telematica) e sul trasporto aereo (il 70% dei vettori operanti nell'aeroporto di Fiumicino è stato costretto a ricorrere a procedure manuali per le operazioni di check-in) .

Tabella 1: Alcuni degli incidenti riportati nella letteratura mondiale che evidenziano la forte interdipendenza esistente fra le diverse infrastrutture critiche e le conseguenze della propagazione a cascata di un guasto con l'interessamento di utenti remoti, sia dal punto di vista logico che fisico, rispetto alle cause prime del guasto.

La sempre maggiore rilevanza che le Infrastrutture Critiche andranno ad assumere nei prossimi anni fa ritenere che le stesse potrebbero 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 il più probabile). In particolare, si ipotizzano scenari nei quali l'azione terroristica condotta tramite il *cyberspace* ha l'obiettivo di rallentare e rendere meno efficaci le azioni di prima emergenza a valle di un'azione terroristica tradizionale, ovvero amplificando le conseguenze di un attacco tradizionale. Si pensi, ad esempio, all'incremento del potere distruttivo di un ordigno tradizionale qualora il gruppo terroristico riuscisse a penetrare nel sistema di controllo di un oleodotto e fosse in grado di aprire le valvole di emergenza facendo fuoriuscire copiose quantità di liquido infiammabile in concomitanza con la deflagrazione.

La crucialità di tali infrastrutture e la conseguente necessità di "proteggerle" portò l'amministrazione americana a sviluppare fin dal 1996 un programma mirato alla salvaguardia e protezione di queste infrastrutture il cui obiettivo era quello di far sì che "*qualunque interruzione o malfunzionamento di tali infrastrutture sia breve, infrequente e geograficamente circoscritto*".

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 sono state intraprese in molte altre nazioni con la costante caratterizzazione di una forte cooperazione pubblico – privato.

Di recente anche organismi internazionali quale il G8 e la NATO 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, formalizzando, a tal fine, in ambito G8 una serie di principi. Gli stessi principi sono ripresi e ribaditi anche nella recente 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.

A livello internazionale l'intera problematica riguardante la protezione delle Infrastrutture Critiche è genericamente indicata come **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 estremamente labile a causa dello strettissimo accoppiamento esistente 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.

Sintetizzando, il problema della **Protezione delle Infrastrutture Critiche Informatizzate** riguarda, pertanto, la messa in atto di azioni tese ad innalzare il livello di sicurezza, affidabilità e correttezza di tutte quelle infrastrutture critiche che utilizzano, in tutto o in parte, una qualunque infrastruttura informatica per il loro monitoraggio, la loro gestione o il loro controllo; includendo, naturalmente, nel novero delle infrastrutture critiche anche quelle informatiche e specificatamente Internet.

Interruzioni nella fornitura elettrica nell'estate del 2003

L'estate del 2003 è stata caratterizzata da episodi connessi con l'interruzione della fornitura dell'energia elettrica in diversi paesi industrializzati: episodi che hanno evidenziato come tali società dipendano in modo sostanziale dal corretto funzionamento di quest'infrastruttura. Gli episodi che si sono succeduti hanno anche evidenziato l'esistenza di numerosissime interdipendenze fra le diverse infrastrutture e quella elettrica, molte delle quali non sempre percepite in modo esplicito non solo dagli utenti finali, ma anche da

alcuni operatori e, quindi, non prese in considerazione nella definizione, ove esistono, dei piani di emergenza.

17 Luglio 2003 –Interruzione programmata della fornitura elettrica in Italia

Il GRTN per scongiurare il pericolo di un black-out ha attivato il piano di emergenza PESSE (Piano di Emergenza per la Sicurezza del Sistema Elettrico) che prevede l'interruzione dell'erogazione dell'energia elettrica, per periodi prefissati, agli utenti interrompibili e, qualora ciò non fosse sufficiente, anche agli utenti non interrompibili.

L'attivazione di questa procedura, con interruzioni di circa un'ora e mezza a macchia di leopardo su tutto il territorio nazionale, ha evidenziato la forte interdipendenza esistente fra l'infrastruttura elettrica e le altre. Si sono registrati problemi a: trasporti automobilistici (mancato funzionamento dei semafori, gallerie non illuminate, ma anche impossibilità di erogare il carburante da parte delle stazioni di servizio) e ferroviari, ai circuiti finanziari e sanitari, alla pubblica amministrazione, alle telecomunicazioni (sia fissa che mobile) ed all'approvvigionamento idrico e alimentare. Sebbene i disagi patiti dalla popolazione siano stati minimi, grazie alla limitata durata del periodo di sospensione dell'erogazione, l'episodio ha mostrato come un'interruzione nella fornitura dell'energia elettrica provochi ripercussioni immediate su moltissime infrastrutture.

14 Agosto 2003 – Costa Nord Est dell'America

Il black-out verificatasi nel Nord Est degli Stati Uniti e nella provincia canadese dell'Ontario il 14 agosto del 2003 ha causato ingenti danni, il cui ammontare secondo le prime stime conservative sarebbe pari a circa 6 miliardi di dollari per i soli Stati Uniti, di cui circa 1 miliardo solo in beni che sono andati distrutti o resi inutilizzabili a causa del black-out. L'impatto è stato certamente amplificato da numerose concause:

- L'insufficienza dell'infrastruttura di trasporto dell'energia. Nel periodo 1988-98 la crescita dei consumi negli Stati Uniti è stata pari al 30%, mentre la capacità di trasporto è cresciuta solo del 15%;
- Il fatto che il governo della rete sia affidato ad una molteplicità di operatori;
- L'insufficienza dei sistemi di monitoraggio e controllo.

Fra l'altro, l'evento ha posto in luce che i danni causati dall'interruzione della fornitura elettrica sono risultati maggiori di quanto si potesse prevedere a causa della crescente dipendenza di tutti i servizi dalla continuità della fornitura dell'energia elettrica.

Nonostante manchino comunicazioni ufficiali sull'impatto del black-out sulle diverse infrastrutture e servizi, alcune informazioni sono disponibili per quel che riguarda la città di New York che è risultata, per altro, quella che ha risentito maggiormente del black-out. In questa città, la mancanza di energia elettrica ha comportato, fra le altre cose:

- Tre distinte interruzioni, comprese fra i 7 e i 14 minuti ognuna, nel servizio di emergenza 911 con conseguente perdita di centinaia di chiamate di soccorso;
- La necessità di evacuare migliaia di ciclisti intrappolati nei tunnel sottomarini;
- La paralisi delle metropolitane e, più in generale, di tutti i mezzi di trasporto su rotaia;
- La chiusura di tutti e tre gli aeroporti metropolitani;
- La mancata erogazione di acqua potabile ai piani alti degli edifici;
- Un abnorme accumulo di rifiuti solidi urbani dovuti sia al riversamento di ingenti quantità di materiale deteriorato a causa della mancanza di energia, sia alle difficoltà indotte nello stoccaggio dei rifiuti prelevati;
- Il riversamento di un'ingente quantità di acque reflue non trattate direttamente nell'ambiente;

- La necessità di chiudere al traffico automobilistico tutti i ponti e i tunnel cittadini con le ovvie conseguenze sul già caotico traffico cittadino.

Più recentemente Spencer Abraham, Segretario per l'Energia degli Stati Uniti, ha fornito una stima dei danni, diretti ed indiretti, all'economia degli Stati Uniti, dell'ordine di 50 miliardi di dollari, ben superiore a quella citata in precedenza. La grande disparità fra le due stime pone in luce come il tema stesso della quantificazione dell'impatto di una crisi prolungata di un'infrastruttura critica debba essere oggetto di indagini approfondite.

Il rapporto intermedio della commissione congiunta US-Canada, istituita per far luce sulle cause del black-out, ha evidenziato che la causa scatenante va ricercata nel contatto fra un albero ed una linea a 345 kV. Tale evento, per altro relativamente usuale, è stato in una certa misura indotto e, soprattutto, non gestito correttamente a causa di una pluralità di problemi registrati dal sistema SCADA utilizzato per il monitoraggio e il controllo della rete elettrica da parte dell'operatore FirstEnergy. In particolare, si è riscontrato che lo "stimatore" utilizzato per prevedere l'evoluzione della rete rimase non operativo per circa 4 ore riprendendo a funzionare solo pochi minuti prima del black-out (a causa sia di errori umani che di problemi tecnici). Un differente guasto ai server del sistema SCADA, resoro non operativa la gestione degli allarmi (cioè le segnalazioni agli operatori che determinate grandezze assumevano valori anomali), rallentando, inoltre, la funzionalità complessiva dello SCADA (ed in particolare le operazioni di aggiornamento dei valori misurati sul campo), rendendo di fatto "ciechi" gli operatori nella sala di controllo rispetto a quanto stava accadendo alle linee.

È interessante notare che le statistiche sui black-out avvenuti negli ultimi cinquanta anni negli Stati Uniti evidenziano che il numero di episodi sia andato costantemente diminuendo nel corso degli anni a dimostrazione di una maggiore affidabilità del sistema elettrico. Nel contempo, è andata aumentando l'ampiezza del bacino di utenze che hanno sofferto di questi eventi a riprova di una maggiore complessità e della crescente difficoltà di operare e controllare la sicurezza e l'affidabilità dell'intero sistema elettrico.

28 agosto 2003 - Londra

Si è trattato di una sospensione della corrente avvenuta nella zona meridionale della città poco dopo le 18:00 locali, ovvero nell'ora di punta per il traffico. Si sono improvvisamente spenti tutti i lampioni, 270 semafori, ma, soprattutto, il 60% della linea metropolitana è rimasta paralizzata: molte persone sono rimaste intrappolate nelle stazioni di Victoria, London Bridge e Waterloo e nei convogli bloccati in galleria. Sono scattati immediatamente i piani di emergenza e tutti i passeggeri della metropolitana sono stati evacuati.

Questo ha, in una qualche misura, aggravato le conseguenze del black-out. Infatti l'impatto di tutti questi passeggeri sul già caotico traffico del centro ha creato enormi problemi alla circolazione automobilistica che è risultata completamente paralizzata per diverse ore anche dopo la fine del black-out.

I treni della rete ferroviaria al sud della capitale per un raggio di 50 km sono rimasti bloccati, ed anche la City è stata colpita e la Borsa di Londra si è spenta improvvisamente.

28 settembre 2003 - Italia

In Italia, alle ore 3:28 della notte del 28 settembre, si è verificato un black-out che ha interessato l'intera nazione con la sola esclusione della Sardegna. Senza entrare nell'analisi delle cause, per le quali sono state attivate dalle autorità competenti apposite commissioni

di indagine, in questa sede si vuole evidenziare l'impatto che tale evento ha avuto sulle altre infrastrutture tecnologiche a causa delle interdipendenze fra esse esistenti.

Occorre preliminarmente precisare che l'incidente è occorso nella notte fra sabato e domenica, in un momento di quasi totale arresto delle attività produttive, e questo ha consentito di limitarne l'incidenza sulla popolazione e sulle attività economiche. A questo deve aggiungersi la capacità di reazione dimostrata dai diversi soggetti coinvolti nella gestione della crisi che ha consentito di fronteggiare egregiamente la situazione evitando che la stessa degenerasse, ripristinando nell'arco di 6-18 ore l'erogazione dell'energia sulla quasi totalità del territorio nazionale.

L'evento ha afflitto praticamente tutti i settori della vita sociale:

- **Trasporto ferroviario**: è stato completamente paralizzato con la necessità di provvedere al recupero dei 110 convogli che al momento dell'evento viaggiavano sulla rete ferroviaria, soccorrendo gli oltre 30.000 passeggeri e provvedendo a ricoverare i treni nelle stazioni. A Roma, dove era in atto una manifestazione, si è avuta la paralisi della metropolitana con la necessità di soccorrere i passeggeri e provvedere alla loro evacuazione;
- **Trasporti automobilistici:** problemi connessi con l'illuminazione delle gallerie, con le colonnine di emergenze e, nelle città, con il mancato funzionamento dei semafori. L'ora notturna e festiva ha contribuito a contenere i disservizi. Problemi si sono segnalati anche in alcune stazioni di servizio non in grado di erogare il carburante.
- **Trasporti aerei e navali:** l'incidenza diretta sul traffico aereo è stata limitata dal fatto che la maggior parte degli aeroporti durante la notte erano chiusi. Non si è avuto alcun problema circa la sicurezza del traffico aereo (essendo le torri di controllo sempre alimentate), mentre alcuni problemi si sono registrati alle accettazioni e per la gestione dei bagagli. Problemi si sono registrati anche in alcuni porti.
- **Comunicazioni**: per alcuni operatori di telefonia mobile si è verificata l'impossibilità di coprire l'intero territorio nazionale, così come alcuni operatori di telefonia fissa non sono stati in grado di garantire la continuità del servizio di telefonia Alcune stazioni radio e televisive non sono state in grado di trasmettere a causa della mancanza di energia elettrica.
- **Sistema sanitario:** non in tutti gli ospedali i sistemi di emergenza sono entrati immediatamente in servizio e, quasi ovunque, si è dovuto ricorrere ai VV.F. per provvedere al rifornimento di combustibile per i generatori. Si è dovuto, inoltre, provvedere a prestare soccorso ai pazienti domiciliati trasportandoli in ospedale o fornendoli di generatori di emergenza.
- **Filiera agroalimentare**: problemi sopratutto per quelle aree, come la Sicilia, ove l'interruzione dell'erogazione dell'energia elettrica si è protratta per un tempo maggiore. In particolare, si sono registrati problemi con le aziende vitivinicole le cui cantine, in questo periodo dell'anno, sono in piena attività e necessitano di sistemi per la refrigerazione del mosto. Altri problemi si sono registrati per l'apicoltura e la zootecnia, con l'impossibilità di provvedere alla mungitura automatica del bestiame e al successivo stoccaggio del latte. Non si sono registrati problemi rilevanti per la grande distribuzione ove, grazie alla presenza di gruppi elettrogeni ed al limitato periodo di interruzione, non si sono avute interruzioni del ciclo del freddo, cosa che, invece, si è registrata in alcuni

esercizi medi e piccoli soprattutto nelle zone in cui il black-out si è protratto più a lungo.

- **Impianti industriali:** i danni, stante il giorno festivo, sono stati circoscritti alle sole aziende che operano a ciclo continuo ed in special modo alle acciaierie, alle industrie petrolchimiche e a quelle del cemento. Altri problemi si sono registrati al riavvio della produzione il giorno successivo sia a causa di difficoltà nel far ripartire i macchinari sia a causa di problemi indotti: ad esempio un'importante azienda dolciaria non è riuscita a riprendere la produzione il lunedì seguente a causa di un guasto verificatosi presso la società che forniva il servizio di hosting applicativo del sistema informatico di gestione della produzione (sistema di ERP).
- **Circuiti bancari e finanziari:** stante la giornata festiva non si sono avute ripercussioni sui circuiti finanziari. Gli unici servizi bancari colpiti dal black-out sono stati i Bancomat che non hanno potuto procedere all'erogazione del denaro.

È da precisare, in ogni modo, che il verificarsi del black-out in orario notturno ed in una giornata festiva, oltre che limitare i danni diretti, ha semplificato la gestione dell'evento grazie anche all'elevata mobilità di cui hanno potuto godere i mezzi di soccorso. Scenari ben diversi si sarebbero avuti nel caso in cui il black-out si fosse verificato in un giorno lavorativo (si pensi solo all'impatto sul traffico e quindi sulla mobilità dei mezzi di soccorso) o se lo stesso si fosse protratto per maggior tempo.

Le infrastrutture critiche

Individuare quali infrastrutture sono da considerare critiche per il sistema paese è un compito non semplice in considerazione delle diverse e molteplici implicazioni connesse con l'individuazione dei servizi da considerare essenziali e, quindi, le tecnologie e le infrastrutture necessarie per la loro erogazione.

Le diverse nazioni hanno indicato, in relazione al loro contesto ed organizzazione, diversi insiemi di infrastrutture come critiche. A tal proposito la tabella seguente presenta una sintetica rassegna delle determinazioni adottate nei vari stati.

	Australia	Canada	Germania	Norvegia	Olanda	Svezia	Svizzera	USA
Circuiti bancari e finanziari	X	X	X	X	X	X	X	X
Telecomunicazioni	X	X	X	X	X	X	X	X
Energia e utilities	X	X	X	X	X	X		X
Servizi di Informazione	X					X	X	
Circuiti sanitari (health)			X	X	X	X	X	X
Amministrazioni pubbliche	X	X	X		X		X	
Trasporti e distribuzione	X	X	X	X	X	X	X	X
Forniture idriche					X	X	X	X
Servizi di emergenza	X	X		X	X			X
Difesa				X	X		X	
Servizi postali								X
Industrie di base o pericolose					X			X
Educazione e ricerca							X	
Filiera alimentare					X	X	X	X
Servizi di assistenza sociale (welfare)				X	X	X	X	

Tabella 2: Infrastrutture considerate critiche nelle diverse nazioni.

Alcune di esse, come i circuiti bancari e finanziari, le reti di telecomunicazione, i sistemi di trasporto e distribuzione e le infrastrutture energetiche sono ritenute critiche dalla quasi totalità dei paesi industrializzati, mentre altri tipi di infrastrutture godono di una diversa valutazione anche in considerazione delle realtà specifiche del paese e del suo assetto organizzativo.

Le diverse definizioni adottate sono, per altro, mutevoli nel corso degli anni. Ad esempio, negli Stati Uniti l'insieme delle infrastrutture ritenute critiche si è accresciuto nel corso degli anni: nella prima formulazione della Direttiva Clinton (PDD63 – 1998) erano

prese in considerazione esclusivamente quelle infrastrutture che erano vitali per la sicurezza nazionale, nel corso degli anni sono state considerate come critiche anche quelle infrastrutture necessarie per l'economia nazionale, la salute ed il benessere della popolazione ed infine, a valle dell'11 settembre, anche quelle infrastrutture o simboli il cui danneggiamento o distruzione potrebbe avere un impatto deprimente sul morale della nazione.

Esempi di infrastrutture informatizzate

Nei paragrafi seguenti sono descritte alcune infrastrutture informatizzate di rilevante impatto per l'Italia che potrebbero subire malfunzionamenti in considerazione dell'interdipendenze reciproche esistenti. Tale elenco non ha la pretesa di essere esaustivo, né di elencare le infrastrutture critiche per il Paese, ma vuole semplicemente dare una visione della complessità intrinseca di ciascuna delle diverse infrastrutture e delle loro interdipendenze reciproche e, quindi, delle possibili vulnerabilità che mostra il nostro Paese nei confronti di guasti che si propagassero per effetto domino fra le diverse infrastrutture.

Si precisa, infine, che la L. n. 34 del 14/02/2003, con la quale si ratificava la Convenzione internazionale per la repressione degli attentati terroristici mediate utilizzo di esplosivi delle Nazioni Unite del 15 dicembre 1997, nel rifarsi a detta convenzione identifica quali "*Infrastrutture: ogni impianto pubblico o privato che fornisce servizi di utilità pubblica, come la conduzione d'acqua, l'evacuazione delle acque reflue, l'energia, il combustibile o le comunicazioni*".

L'infrastruttura elettrica

La qualità della fornitura di energia elettrica assume un ruolo fondamentale per il Paese. L'energia elettrica presenta, infatti, diverse prerogative quali: la facilità di conversione in altre forme di energia (meccanica, luminosa, termica, ecc.), la facilità e la flessibilità di trasporto, la possibilità di una distribuzione capillare, una generazione economica da sorgenti primarie non altrimenti utilizzabili (idroelettriche, lignite, carboni poveri ecc.). Per contro, uno svantaggio dell'energia elettrica è la sua non immagazzinabilità (se non in quantità molto limitate): questo comporta che, in ogni istante, la domanda di energia deve essere bilanciata da una produzione di energia di pari valore, ovvero che, in ogni istante, deve essere prodotta l'esatta quantità di energia richiesta dai consumatori.

La liberalizzazione del mercato impone l'utilizzo delle tecnologie dello ICT alle nuove esigenze dei sistemi di controllo, automazione e informazione del Sistema Elettrico. La gestione e il governo nazionale di una Rete Elettrica di tipo multi-operatore, connessa a fonti diversificate e distribuite di generazione elettrica, regolata dall'andamento della domanda e dei prezzi del mercato, richiede, infatti, lo sviluppo di applicazioni flessibili, fisicamente distribuite e funzionalmente integrate. La comunicazione tra sistemi di diversi operatori pone requisiti di interoperabilità dei dati, di uniformità dei protocolli di scambio, di sicurezza e affidabilità dei componenti e dei servizi utilizzati.

Il supporto automatico richiesto alle tecnologie ICT dalle nuove esigenze del Sistema Elettrico deve sfruttare le potenzialità offerte dalle tecnologie esistenti, guidandone l'evoluzione e applicando nel contempo tutte le misure necessarie per consentire che la loro integrazione soddisfi i vincoli di disponibilità, integrità e confidenzialità che caratterizzano

le applicazioni critiche del Sistema Elettrico. L'analisi delle interdipendenze del processo elettrico dalle altre infrastrutture critiche del paese, supportata dall'uso di metodologie di valutazione dei rischi associati, dovrebbe guidare la definizione di adeguate politiche di sicurezza e l'identificazione di requisiti di protezione delle infrastrutture ICT, di recupero dalle situazioni di anomalia e di difesa dalle possibilità di attacco.

Reti Informatiche e Reti di Telecomunicazione

Il mondo delle telecomunicazioni si caratterizza per una sempre più stretta integrazione fra trasmissione dati e fonia. Soprattutto a livello di trasporto si osserva una convergenza verso tecnologie (quali SDH) in grado di trasportare (generalmente su fibra ottica) su un unico supporto tutte le tipologie di segnale numerico esistenti (voce, dati ATM o IP, video).

Il mercato delle comunicazioni sta evolvendo da una situazione caratterizzata da un operatore unico (Telecom) verso una situazione caratterizzata dalla presenza di una pluralità di operatori che operano in parte su rete proprietaria ed in parte ricorrendo ad interconnessioni con gli altri operatori. L'importanza commerciale della trasmissione end-to-end sta diminuendo a vantaggio dei servizi VAS (Valued Add Services).

Per quel che riguarda le reti informatiche, si osserva una rapida e generalizzata migrazione verso l'adozione del protocollo TCP/IP. Quando fu progettato questo protocollo non si tennero in conto gli aspetti di sicurezza. Questo fattore, unitamente ad altri fra cui l'esistenza di un numero ridotto di elementi cruciali della rete (quali i punti di peering o i DNS root server) e la presenza di "bachi" nel software, induce un non trascurabile grado di vulnerabilità nell'intero sistema.

Le reti informatiche poggiano il loro funzionamento sulla rete elettrica e sulla rete di telecomunicazioni. Nello stesso tempo, però, sia la rete elettrica che quella di telecomunicazione utilizzano reti informatiche per la loro gestione e controllo. Per una corretta protezione delle reti informatiche è necessario, quindi, limitare l'impatto di queste interdipendenze rendendole, per quanto possibile, nulle o minime.

L'inserimento di gruppi di continuità e gruppi elettrogeni può sicuramente aiutare nel minimizzare l'impatto di malfunzionamenti nella fornitura di energia elettrica, mentre la dipendenza dalle reti di telecomunicazione è invece più stretta ed ineliminabile in particolare per le reti geografiche.

Un altro aspetto di criticità è legato alla presenza dei cosiddetti *malicious codes* e della loro capacità di rapida diffusione su tutto il cyberspace.

Un'attenzione particolare, infine, meritano i sistemi SCADA utilizzati per le operazioni di tele-controllo e tele-monitoraggio degli impianti industriali in genere, ed in particolare delle infrastrutture geograficamente distribuite. Tali sistemi, originariamente progettati per operare in modo autonomo su infrastrutture proprietarie e indipendenti, risultano poco robusti nei confronti di minacce provenienti dal *cyberspace*.

L'infrastruttura per il trasporto del Gas

L'infrastruttura di trasporto e dispacciamento del gas naturale è gestita a livello nazionale da Snam Rete Gas che opera con proprie condotte ed impianti tele-controllati tramite un sistema SCADA.

Essa si compone della Rete Nazionale di Gasdotti costituita da tubazioni di grande diametro che hanno la funzione di trasferire quantità di gas dai punti di ingresso del sistema

ai punti di interconnessione con la Rete di Trasporto Regionale. Questa, formata dalla restante parte dei gasdotti, svolge la funzione di movimentare il gas naturale in ambiti territoriali delimitati per la fornitura del gas ai consumatori industriali e termoelettrici e alle reti di distribuzione urbana del gas.

Lungo le condotte sono collocati gli impianti necessari all'interconnessione delle stesse nonché per il controllo e la gestione dei flussi di gas, e le centrali di comprensione dedicate alla spinta del gas in linea. Tutte le centrali sono dotate di funzionalità operative e di controllo che ne consentono la gestione da remoto.

L'effettuazione del servizio di trasporto, sulla base dei programmi richiesti dagli utenti ed in condizioni di efficienza, affidabilità e sicurezza, è garantita da Snam Rete Gas attraverso l'esercizio del proprio sistema di trasporto.

Il sistema di trasporto del gas è tenuto sotto controllo e continuamente adattato dal Centro Dispacciamento che si avvale dell'ausilio di programmi di previsione, ottimizzazione e simulazione .

Il sistema SCADA impiegato per il monitoraggio e controllo opera su canali trasmessivi proprietari e, stante la criticità del sistema, tutte le sue componenti sono almeno in duplice ridondanza.

La rete Ferroviaria

La rete ferroviaria si caratterizza per l'elevata "fisicità" della stessa con la naturale conseguenza di rappresentare un interessante e potenzialmente agevole obiettivo per chi intenda perseguire azioni destabilizzanti.

Forti investimenti sono stati programmati dal gestore della rete (RFI – Rete Ferroviaria Italiana) per aumentare i livelli di qualità, affidabilità e sicurezza del servizio. In particolare l'adozione di sofisticati sistemi per il controllo centralizzato del traffico (SCC, ACS, ecc.) consentiranno il costante controllo dello stato della sicurezza/integrità/affidabilità dell'infrastruttura. Ciò, se da una parte eleverà esponenzialmente la capacità di controllo della circolazione ed i livelli di sicurezza dell'infrastruttura, rappresenterà, nel contempo, una concentrazione logistica, tecnologica ed informatica critica.

La rete viaria

La rete viaria ha la peculiarità di essere un sistema "aperto" (percorribile, in pratica, da tutti i mezzi che transitano sulla rete, senza particolari limitazioni) che si estende per oltre 20.500 Km ed è caratterizzato dalla presenza di numerosi elementi infrastrutturali (ponti, viadotti e gallerie) che presentano fattori di rischio incidentale nettamente più elevati.

Al fine di migliorare la sicurezza complessiva del sistema viario, l'ANAS ha avviato progetti per la realizzazione di sistemi di controllo, sia basati sull'utilizzo di addetti preposti al monitoraggio dei singoli tronchi viari sia con sistemi completamente automatizzati, in grado di fornire in tempo reale il quadro complessivo della situazione e, quindi, consentire una gestione più efficiente delle situazioni di emergenza.

Circuiti bancari e finanziari

I circuiti bancari e finanziari svolgono un ruolo di fondamentale importanza, il cui funzionamento è assicurato da una serie di operatori che gestiscono le infrastrutture

necessarie per le procedure interbancarie e sono esse a rappresentare l'elemento di maggior rischio per l'intero sistema. L'erogazione dell'energia elettrica e i servizi di telecomunicazione rappresentano un altro elemento di interdipendenza settoriale, così come i fornitori di servizi di ICT. I principali attori del sistema finanziario si stanno già attrezzando con opportuni meccanismi per garantire la continuità dei servizi.

L'ospedale e le sue criticità infrastrutturali

Attualmente l'organizzazione dei servizi sanitari è incentrata su un modello centralizzato che vede negli ospedali il suo elemento cardine. Questo scenario presenta limitate vulnerabilità rispetto alla sussistenza delle altre infrastrutture, sebbene la loro mancanza, ed in particolare la fornitura di energia elettrica, possa degradare notevolmente le capacità operative e la qualità dei servizi offerti.

L'evoluzione in atto tende però verso la nascita di un modello distribuito ove una parte considerevole delle fasi di diagnosi e terapia è attuata in modo distribuito nelle case dei pazienti. In questo mutato scenario si moltiplicano le interdipendenze esistenti fra i circuiti sanitari e le altre infrastrutture.

Impianti Nucleari

Gli impianti nucleari sono sistemi in cui la sicurezza è considerata in dettaglio fin dalle prime fasi progettuali andando ad analizzare tutti i possibili scenari di eventi.

Questo ha comportato che, nonostante le centrali nucleari presentino interdipendenze con molteplici infrastrutture, le stesse risultano adeguatamente protette rispetto ad eventi che possono verificarsi sulle diverse infrastrutture e ciò soprattutto in una realtà, come quella Italiana, dove non esistono impianti in produzione e le attività che si svolgono riguardano esclusivamente il decommissioning delle centrali esistenti.

La Navigazione Satellitare

La navigazione satellitare rappresenta una delle infrastrutture che andrà sempre più assumendo un ruolo di enabling technology sia per gli aspetti di localizzazione che per quelli di sincronismo temporale. In questo scenario l'Europa, ed in particolare l'Italia quale candidata ad ospitare il centro di controllo, è impegnata nel progetto GALILEO che offrirà agli utenti servizi di navigazione e posizionamento con maggiori prestazioni rispetto ai sistemi attuali.

Dato che nei prossimi anni si avrà una sempre maggiore dipendenza dalla navigazione satellitare, si prevede che le interruzioni dei servizi di navigazione potranno avere un sempre maggiore impatto sugli interessi vitali europei. L'infrastruttura GALILEO dovrà, pertanto, essere protetta contro i rischi di qualunque genere, ad un livello equivalente a quello applicabile alle infrastrutture critiche nazionali.

I sistemi di monitoraggio e controllo

In questo contesto un'attenzione particolare meritano i sistemi di monitoraggio e controllo.

Attualmente la gran parte degli impianti ed infrastrutture geograficamente distribuiti sul territorio sono gestiti tramite sistemi di monitoraggio e controllo genericamente indicati come sistemi SCADA (Supervisory Control and Data Acquisition).

Tali sistemi SCADA sono normalmente costituiti da una sala di controllo connessa, tramite dei 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 comandate dal sistema centrale. La distribuzione sul territorio delle RTU assume diverse caratteristiche a seconda del tipo di impianto e può essere a carattere geografico per il monitoraggio, ad esempio, di pipeline o di sistemi di trasporto e distribuzione dell'energia elettrica, più locale, pensando alla gestione del gas di città, fino a dimensioni estremamente contenute per ciò che riguarda i 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 dove le infrastrutture di comunicazione non hanno un buon grado di sviluppo (pipeline), a collegamenti che invece sfruttano le infrastrutture esistenti là dove 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 (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 (Manufactoring Application Protocol), più adatti alla gestione di unità remote relativamente poco intelligenti, spesso connesse tramite collegamenti peer-to-peer. Tali sistemi operavano su network 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.

Ciò implica che le cause che possono "danneggiare" un'azienda, nel senso di renderla incapace di erogare servizi, cominciano a trasferirsi dal piano più tradizionale degli eventi

(attentati) fisici a quello meno palpabile ma certamente ugualmente pericoloso dell'informatica.

Tutte queste considerazioni impongono un profondo ripensamento su quelle che sono le nuove minacce, le quali vanno a sommarsi a quelle più tradizionali, e devono comportare una differente valutazione del rischio a cui sono sottoposte le porzioni critiche di un'azienda, sia per ciò che riguarda danni economici, sia per quanto connesso alla sicurezza dei cittadini.

In questo mutato contesto, diviene fondamentale considerare gli impatti che eventuali *guasti* prodotti nel *cyberspace*, o da esso veicolato, potrebbe produrre sui sistemi SCADA soprattutto nell'ottica che essi possano rappresentare possibili obiettivi di azioni terroristiche.

Per queste ragioni la sicurezza dei sistemi di controllo e monitoraggio costituisce uno degli elementi su cui occorre concentrare maggiormente l'attenzione per quel che riguarda la sicurezza e la protezione delle Infrastrutture Critiche. Non a caso nel documento che delinea la strategia del governo americano per quel che riguarda la sicurezza informatica (*The National Strategy to Secure Cyberspace*), i sistemi DCS e SCADA sono indicati come una delle cause della vulnerabilità del *cyberspace* e la protezione dei sistemi SCADA è divenuta una delle priorità del Department of Homeland Security.

Analisi della situazione mondiale

Alcune agenzie governative hanno iniziato a considerare il problema della protezione delle infrastrutture critiche fin dalla metà degli anni ’90 allor quando si comprese come da un lato la crescente interdipendenza fra le diverse infrastrutture e dall’altro il sempre maggior utilizzo delle tecnologie ICT comportassero un aumento della vulnerabilità delle nazioni nei confronti di questi sistemi.

Gli Stati Uniti furono i primi a formalizzare azioni a livello governativo sul tema con la costituzione della *President’s Commission on Critical Infrastructure Protection* nel 1996 e l’emanazione della Presidential Decision Directive n. 63 (PDD63) ad opera del presidente Clinton nel 1998.

Sulla scorta di quanto fatto dal governo USA anche molti altri paesi industrializzati hanno sviluppato azioni governative tese a:

- Comprendere gli elementi di criticità e vulnerabilità delle diverse infrastrutture critiche presenti nel paese evidenziandone le interdipendenze;
- Definire una strategia per mitigare tali vulnerabilità;
- Sensibilizzare i diversi operatori circa il problema della protezione delle infrastrutture critiche;
- Predisporre piani di emergenza e di contingentamento da attivare in presenza di eventi negativi che interessino una o più infrastrutture critiche;
- Favorire lo sviluppo di tecnologie intrinsecamente sicure e supportare la cooperazione internazionale.

Da un punto di vista organizzativo, fatte salve le specificità e le peculiarità dei diversi paesi, connotazioni uniformi possono rilevarsi in:

- ❖ Costituzione, in una prima fase, di una commissione o gruppo di lavoro con il compito di delineare le strategie più opportune per la realtà del paese, identificando i soggetti e le infrastrutture sulle quali concentrare maggiormente l’attenzione;
- ❖ Costituzione, sulla base del lavoro svolto dalla struttura di cui al punto precedente, di una struttura di coordinamento a livello governativo, generalmente sotto il diretto controllo del responsabile del potere esecutivo, in grado di promuovere le azioni tese a limitare la vulnerabilità delle infrastrutture critiche definendo linee guida, individuando priorità, supportando e stimolando le diverse amministrazioni e fornendo loro strumenti metodologici e risorse finanziarie appropriate;
- ❖ Investire le diverse amministrazioni pubbliche della responsabilità di predisporre piani e strategie per l’attuazione, negli specifici settori di competenza, delle linee guide delineate;
- ❖ Coinvolgimento dei soggetti privati operanti nei diversi settori delle Infrastrutture Critiche nella definizione sia delle linee guida che nei piani di attuazione favorendo, fra le altre cose, la nascita di raggruppamenti di operatori di settore quali interlocutori privilegiati;
- ❖ Interventi normativi e legislativi tesi a favorire lo scambio delle informazioni e migliorare le azioni investigative sia a livello nazionale che internazionale soprattutto per quel che riguarda il *cyberspace*;

- ❖ Predisposizione di strutture di monitoraggio e controllo in grado di intervenire con tempestività e realizzazione di piani di intervento da adottare in situazioni di emergenza;
- ❖ Impulso alle attività di R&S sia per quel che concerne gli strumenti per favorire la comprensione del problema (modellistica) che per lo sviluppo di tecnologie e procedure sicure;
- ❖ Favorire la cooperazione internazionale stante la trans-nazionalità della problematica legata alla natura sovra-nazionale di molte delle infrastrutture critiche.

Nel seguito sono sinteticamente descritte le principali iniziative intraprese in alcuni paesi.

Stati Uniti

Il primo atto ufficiale rivolto al problema della vulnerabilità introdotto dall'uso crescente delle tecnologie informatiche fu la creazione, nel luglio 1996, della **President's Commission on Critical Infrastructure Protection (PCCIP)**. Lo scopo della Commissione era quello di formulare una strategia per difendere le infrastrutture critiche da attacchi fisici e informatici.

Nel maggio 1998 è stata diramata dal presidente Clinton la Presidential Decision Directive n. 63 (**PDD 63)** sulla difesa delle Infrastrutture Critiche il cui obiettivo era quello di intraprendere un insieme di azioni in modo che "*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*"[1]. La PDD63 ha dato vita al:

- **Critical Infrastructure Assurance Office (CIAO)** una struttura interministeriale con il compito di coordinare, stimolare e supportare tutte le azioni mirate alla salvaguardia delle infrastrutture critiche americane.
- **National Infrastructure Protection Center (NIPC)** una struttura creata all'interno del FBI con lo scopo di monitorare le diverse minacce e favorire le azioni investigative circa le azioni delittuose perpetuate contro le Infrastrutture Critiche (www.nipc.gov).
- **National Infrastructure Assurance Council (NIAC)** con lo scopo di favorire l'interazione pubblico/privato ed in particolare favorire la nascita, all'interno delle diverse comunità, di **ISAC (Information Sharing and Analysis Center).**
- **Partnership for Critical Infrastructure Security (PCIS)** un forum per favorire l'incontro degli operatori dei diversi settori e il dialogo pubblico privato al fine di aumentare la sicurezza delle Infrastrutture Critiche (www.pcis.org).
- **The Institute for Information Infrastructure Protection (I3P)** un'organizzazione per coordinare lo sviluppo di una Agenda di ricerca nazionale sul soggetto della protezione delle infrastrutture critiche basata sulla collaborazione e la condivisione della conoscenza tra mondo accademico, industria e agenzie governative (www.thei3p.org).

Gli eventi dell'11 settembre hanno portato ad un'accelerazione delle azioni tese a prevenire e rendere sicure le infrastrutture statunitensi con l'istituzione del ***President's***

[1] Qualunque interruzione o malfunzionamento di queste infrastrutture critiche deve essere breve, infrequente, gestibile, geograficamente circoscritto e comportare il minimo deterioramento del welfare degli Stati Uniti.

Critical Infrastructure Protection Board (Executive Order 13231 dell'ottobre 2001) nel quale sedevano tutti i responsabili delle diverse agenzie che operano nel settore e che riferiva direttamente al Presidente.

Attualmente il **Department of Homeland Security** (DHS www.dhs.gov/dhspublic/) ha assunto il ruolo di coordinare tutte le iniziative che riguardano la Protezione delle Infrastrutture Critiche incorporando molte delle strutture ed agenzie che operavano in questo settore, compresi il CIAO e il NIPC. Parallelamente a questa ristrutturazione, il cui scopo è quello di unificare le responsabilità e limitare le aree di sovrapposizione, si è registrato un forte aumentato dei fondi stanziati per le CIP: al solo DHS sono stati assegnati per il 2004 fondi per $ 829 milioni (di cui circa $ 500 milioni per lo studio delle criticità delle diverse infrastrutture e lo sviluppo delle prime azioni per ridurne la vulnerabilità e circa $ 300 milioni per la realizzazione di sistemi di warning advisor). Nel febbraio del 2004 il DHS ha attivato il *Protected Critical Infrastructure Information Program* con lo scopo di favorire lo scambio di informazioni sulle Infrastrutture Critiche fra gli operatori privati e il governo federale, su base volontaria ed in un contesto di assoluta riservatezza (www.DHS.gov/pcii).

Nel febbraio del 2003 la Casa Bianca ha rilasciato due documenti sulla strategia nazionale in tema di sicurezza delle Infrastrutture Critiche:

- *National Strategy to Secure Cyberspace* che fornisce un primo quadro di riferimento e le priorità da seguire nel settore della protezione del *cyberspace* e delle infrastrutture critiche da minacce di tipo informatico;
- *National Strategy for Physical Protection of Critical Infrastructures and Key Assets* che è una pubblicazione complementare alla precedente che considera più direttamente le conseguenze di azioni terroristiche tradizionali sulle infrastrutture critiche.

È stato, inoltre costituito nel 2001 il **National Infrastructure Simulation and Analysis Center** (NISAC) fondato con lo scopo di promuovere lo sviluppo di attività di ricerca sulla tematica dai Los Alamos National Laboratory e dai Sandia National Laboratories ed a cui collaborano anche altre importanti istituzioni di ricerca quali il Massachusetts Institute of Technology, la Purdue University, la Cornell University, la Lucent Technologies e gli Argonne National Laboratory.

Gran Bretagna

La politica della Gran Bretagna per quel che concerne le CIIP è incentrato su due elementi. Il **National Infrastructure Security Co-ordination Centre (NISCC),** creato nel 1999 alle dipendenze del Ministero degli Interni, con lo scopo di coordinare tutte le iniziative governative messe in atto per la protezione delle infrastrutture nazionali nei confronti di attacchi informatici (http://www.niscc.gov.uk/), e il forum indipendente **Information Assurance Advisory Council (IAAC)**, istituto marzo del 2000, all'interno del quale i diversi attori pubblici e privati sviluppano le politiche necessarie a garantire la sicurezza e la fruibilità delle infrastrutture informatiche.

Il NISCC, 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, ha sviluppato un Programma di Protezione **Critical National Infrastructure (CNI)** che definisce una politica di mutua cooperazione tra i gestori di quei servizi che devono essere

garantiti da attacchi esterni per la sicurezza nazionale (http://www.niscc.gov.uk/cni/index.htm).

Nel NISCC è anche confluito il **Unified Incident Reporting and Alert Scheme (UNIRAS),** un organo tecnico di raccolta dati e supporto ai problemi della security, istituito nel 1992 (http://www.uniras.gov.uk/) e che gestisce anche il UK Government CERT.

Nel maggio del 2003 il NISCC ha organizzato una conferenza degli utilizzatori e produttori di sistemi SCADA operanti in Gran Bretagna al fine di far prendere coscienza circa le vulnerabilità indotte sugli SCADA dal *cyberspace*, favorendo in tal modo la nascita di un forum dedicato ai sistemi SCADA ove utilizzatori e produttori possano definire congiuntamente strategie per migliorare il loro livello di sicurezza.

Germania

Per quel che concerne le CIIP, la prima azione ufficiale è del 1997 quando fu attivata presso il Ministero degli Interni (BMI), sulla scia dell'emanazione della PDD63 da parte del governo americano, una commissione interministeriale per coordinare le diverse iniziative. In particolare per quel che concerne gli aspetti connessi con la sicurezza informatica, essi furono affidati al Federal Office for Information Security, **Bundesamt fur Sicherheit in der Informationstechnik (BSI** www.bsi.bund.de), mentre gli aspetti connessi con la sicurezza fisica furono demandati al 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 perpetuati 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.

Più recentemente è stato istituito, presso il BSI un ufficio dedicato al problema delle CIIP, il **Schutz Kritischer Infrastrukturen in Deutschland** (http://www.bsi.bund.de/fachthem/kritis/index.htm), al fine di promuovere una politica di cooperazione fra il governo e i soggetti privati coinvolti nella gestione delle diverse infrastrutture. Tale ufficio, fra le altre cose, ha avviato la mappatura di tutte le infrastrutture critiche tedesche al fine di evidenziarne le vulnerabilità e per la conseguente definizione di politiche di protezione.

È stato istituito, inoltre, una gruppo di lavoro sulla protezione delle infrastrutture critiche denominato **Arbeit-Kreis Schutz von Infra-Strukturen (AKSIS**) http://www.aksis.de/ il cui scopo è l'analisi delle connessioni esistenti fra le diverse infrastrutture e della loro dipendenza dall'infrastruttura informatica al fine di evidenziare possibili strategie per ridurne la vulnerabilità.

Canada

L'approccio seguito dal governo Canadese è stato quello di incorporare tutti gli aspetti legati alla sicurezza in un quadro di "Total Defence". Questo portò, nel 2001, all'istituzione del **Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP),** afferente al Department of National Defence**,** nel quale confluirono le

responsabilità proprie della protezione civile con quelle connesse con la protezione e la salvaguardia delle infrastrutture critiche. Tale struttura aveva il compito di definire le strategie nazionali per proteggere le infrastrutture critiche sia per quel che concerne gli aspetti di sicurezza fisica che quella cyber, a prescindere da quale possa essere l'origine e la causa della minaccia. Il OCIPEP aveva il compito di sviluppare, coordinare ed implementare le relative politiche attuative, fungere da organismo di coordinamento a livello governativo e porsi quale agenzia incaricata della gestione degli eventi di crisi www.ocipep.gc.ca.

Nel dicembre del 2003 il OCIPEP è stato integrato nel **Minister of Public Safety and Emergency Preparedness** (PSEPC), sotto la diretta responsabilità del vice primo ministro. Nel PSEPC sono confluite anche altre strutture coinvolte nella protezione delle infrastrutture critiche fra cui parte delle agenzie di intelligence e il *National Crime Prevention Center* e ciò al fine di riportare la responsabilità dell'analisi e della gestione delle situazioni di emergenza in capo ad un'unica struttura per massimizzare la capacità di risposta e il coordinamento con le strutture provinciali e locali.

Nel marzo del 2004 il PSEPC ha attivato un programma di ricerca, con un budget di 3 milioni di dollari canadesi nell'area delle interdipendenze fra infrastrutture critiche.

Svezia

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 verificarsi 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 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).

La **Swedish Emergency Management Agency (SEMA)** è stata istituita nel 2002 dal Ministero della Difesa come istituzione indipendente, ed ha 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. L'obiettivo che si pone il SEMA è la riduzione delle vulnerabilità e il miglioramento delle capacità di gestione degli eventi di crisi (www.krisberedskapsmyndigheten.se). Il SEMA, con un budget annuale di circa 200 milioni di Euro, finanzia i progetti elaborati dalle diverse istituzioni pubbliche per migliorare il rispettivo livello di sicurezza effettuando una verifica sulla bontà dei progetti presentati e sulle priorità dei diversi interventi rispetto al sistema paese. Il SEMA, inoltre, stimola e finanzia attività di R&S tese a migliorare la conoscenza sulle minacce, rischi e vulnerabilità delle diverse infrastrutture e sulle tecnologie atte a migliorarne la robustezza (il budget allocato per R&S nel 2003 è stato di circa 6 milioni di Euro), oltre che analizzare tutti quegli aspetti di interdipendenza che travalicano le responsabilità dei singoli operatori.

Il SEMA non ha una diretta responsabilità nella gestione delle crisi, la cui responsabilità 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.

Il SEMA ha al suo interno una direzione dedicata al problema della sicurezza informatica che ha il compito di promuovere gli aspetti di prevenzione, formazione e

scambio di informazioni fra i diversi operatori coinvolti e con i gestori delle infrastrutture critiche.

A livello di difesa nazionale è stato istituito il **National Office of Information Operations/Critical Infrastructure Protection (IO/CIP)** con il compito di costituire una segreteria tecnica per il governo dedicata al problema della protezione e della difesa delle infrastrutture critiche e di promuovere attività di ricerca.

Nel 2001 è stata creata un'istituzione privata, **The International Institute for Critical National Infrastructures (CRIS)** che raccoglie l'adesione di diversi esperti ed istituzioni di ricerca con l'obiettivo di mettere a fattor comune esperienze e conoscenze sul tema (http://www.cris-inst.com).

Istituzioni internazionali

Il problema della protezione delle infrastrutture critiche, vista la sua natura transnazionale, è stato di recente posto anche all'attenzione di diversi organismi internazionali.

Nel marzo del 2003 si è svolta a Parigi la prima riunione degli esperti dei paesi del **G8** sul problema delle CIIP nell'ambito della quale sono stati delineati undici principi, ratificati durante la riunione dei Ministri della Giustizia e dell'Interno del maggio 2003, che dovrebbero ispirare le politiche dei diversi paesi al fine di accrescere il livello di protezione delle diverse infrastrutture e riportati nella tabella 4.

Le infrastrutture dell'informazione costituiscono una parte essenziale delle infrastrutture critiche. Allo scopo di proteggere efficacemente queste ultime i Paesi devono proteggere le infrastrutture informative critiche da eventuali danni e attacchi. Una protezione efficace comprende l'individuazione delle minacce nei confronti di dette infrastrutture, la riduzione delle vulnerabilità, in modo tale da limitare i danni e minimizzare i tempi di recupero nel caso di attacco portato a termine, e l'identificazione della causa o dell'origine del danno o dell'attacco, affinché sia sottoposta all'analisi degli esperti o all'indagine degli investigatori. Un'adeguata protezione richiede comunicazione, coordinamento e collaborazione a livello nazionale ed internazionale tra tutte le entità a rischio (industria, mondo accademico, settore privato, organi governativi tra cui le forze di polizia). Tali impegni dovrebbero essere condotti con il giusto riguardo nei confronti della sicurezza delle informazioni e delle leggi applicabili in materia di mutua assistenza legale e tutela della privacy. Per perseguire questi obiettivi abbiamo adottato i seguenti PRINCIPI ed invitiamo i Paesi a tenerli in considerazione nello sviluppare una strategia atta a ridurre i rischi per le infrastrutture informative critiche:

I. I Paesi dovrebbero avere reti per la segnalazione delle emergenze riguardanti vulnerabilità, minacce e incidenti nel cyberspace.

II. I Paesi dovrebbero innalzare la soglia di consapevolezza per agevolare la comprensione, da parte delle entità a rischio, della natura e della portata delle loro infrastrutture informative critiche e del ruolo che ognuno deve svolgere per proteggerle.

III. I Paesi dovrebbero esaminare le proprie infrastrutture e individuare le interdipendenze tra loro, aumentando in tal modo il livello di protezione.

IV. I Paesi dovrebbero incoraggiare la collaborazione tra le entità a rischio, sia pubbliche che private, al fine di condividere e analizzare informazioni idonee a prevenire, investigare e rispondere ad attacchi

	o danneggiamenti in pregiudizio delle proprie infrastrutture critiche.
V.	*I Paesi dovrebbero costituire e mantenere reti di comunicazioni per le situazioni di crisi e verificarne l'efficienza e la stabilità nei casi di emergenza.*
VI.	*I Paesi dovrebbero garantire che le linee di condotta riguardanti la disponibilità dei dati prendano in considerazione la necessità di proteggere le infrastrutture informative critiche.*
VII.	*I Paesi dovrebbero favorire il tracciamento degli attacchi contro le infrastrutture informative critiche e, qualora sia opportuno, la comunicazione ad altri Paesi delle informazioni riguardanti i tracciamenti.*
VIII.	*I Paesi dovrebbero condurre attività di formazione e addestramento allo scopo di migliorare le capacità di risposta agli attacchi e testare i piani di continuità e contingenza nel caso di attacco, nonché incoraggiare le entità a rischio ad intraprendere attività similari.*
IX.	*I Paesi dovrebbero garantire di avere adeguate leggi sostanziali e processuali, come quelle descritte nella Convenzione sul Cybercrime del 23 novembre 2001, e di personale specializzato in grado di investigare e perseguire a norma di legge gli attacchi alle infrastrutture informatiche critiche e coordinare le indagini in collaborazione con altri Paesi secondo le evenienze.*
X.	*I Paesi dovrebbero avviare attività di cooperazione internazionale, quando ciò sia opportuno, per salvaguardare l'integrità delle infrastrutture informative critiche, attraverso lo sviluppo ed il coordinamento dei sistemi di segnalazione delle emergenze, lo scambio e l'analisi delle informazioni inerenti vulnerabilità, minacce ed incidenti, ed il coordinamento delle attività d'indagine nel rispetto delle leggi nazionali.*
XI.	*I Paesi dovrebbero promuovere attività di ricerca e sviluppo, in ambito nazionale ed internazionale, ed incoraggiare l'applicazione di tecnologie per la sicurezza certificate secondo standard internazionali.*

Tabella 4: Principi elaborati dagli esperti CIIP dei paesi del G8 nel marzo del 2003 e ratificati dai Ministri degli Interni e della Giustizia nella riunione del maggio 2003.

Il **G8** al fine di favorire la cooperazione internazionale, anche a vantaggio dei paesi non membri, ha predisposto un **International CIIP Directory** con l'indicazione delle strutture e dei punti di contatto esistenti in ognuno dei paesi membri del G8 sulle diverse tematiche[2] proprie delle CIIP.

La **NATO** fin dal 1997 ha analizzato il problema della Protezione delle Infrastrutture Critiche nell'ambito del *Information Operation (IO)*. Dal 2001, sia in ambito **EPAC** (Euro-Atlantic Partnership Council) che in ambito **PfP** (Partnership for Peace), ha preso ad analizzare il soggetto anche in connessione con le problematiche di Protezione Civile da un

[2] Le categorie prese in considerazione nel *International CIIP Directory* sono: Alerts & Warnings, Threat Analysis, Vulnerabilities, Working with Critical Industry, Central Government policy issues, CIIP Research & Development, Information Sharing, Cyber Crime investigation

lato e del terrorismo dall'altro. Ha attivato una road-map il cui scopo è quello di favorire una migliore comprensione del problema e l'attivazione di adeguate iniziative soprattutto per quel che riguarda la formazione, la cooperazione internazionale e le attività di R&S.

La **Commissione Europea** non ha definito una politica per la protezione delle infrastrutture critiche, che è dominio principale di competenza degli Stati Membri. In ogni caso, a seguito degli attacchi tipo "distributed denial of service" e/o virus che si sono avuti nel 2000, la Commissione ha lanciato una serie di iniziative nel campo della sicurezza dell'informazione e delle reti di comunicazione ed informatiche.

Nonostante la mancanza di una politica comunitaria integrata, la Commissione ha cominciato ad occuparsi delle problematiche attinenti alla protezione delle infrastrutture critiche all'interno del suo programma di ricerca sulle Tecnologie dell'Informazione (Programma IT). Nel dicembre del 1997, il Programma IT lanciò un'attività di consultazione con l'obiettivo di definire un'agenda Europea della ricerca sulla "dependability" nella Società dell'Informazione. Due furono le aree tematiche individuate come prioritarie: i) i sistemi e le infrastrutture informatiche in grande scala (large-scale); ii) i sistemi aperti composti da un insieme molto numeroso (centinaia di migliaia/milioni) ed eterogeneo di sistemi "embedded".

Il risultato di quest'attività è stata la **European Dependability Initiative** (**DEPPY** - http://deppy.jrc.it/default/) gestita dalla Direzione Generale Società dell'Informazione all'interno del programma di ricerca e sviluppo *"Tecnologie per la Società dell'Informazion"* (programma IST) del Quinto Programma Quadro. Nel periodo 1998-2002, DEPPY ha lanciato una serie di progetti di ricerca e sviluppo nel campo della dependability dei sistemi e servizi per la Società dell'Informazione e, più recentemente, sull'analisi di rischio e vulnerabilità delle infrastrutture di comunicazione ed informazione nonché le loro interdipendenze con altre infrastrutture critiche (http://www.cordis.lu/ist/cpt/dependability.htm). DEPPY ha anche promosso la cooperazione internazionale e nel 1998 ha istituito la **EU-US Joint Task Force on R&D on CIP,** sotto gli auspici del **Joint Consultative Group** dell'Accordo EU-US sulla Scienza e la Tecnologia del 1997. In fine, vale la pena di ricordare le iniziative di road-map e di policy nei tre progetti denominati DDSI (www.ddsi.org), ACIP (http://www.iabg.de/acip/index.html) ed AMSD (www.am-sd.org) che hanno contribuito a definire le priorità della ricerca nel VI programma quadro (2002-2006) sulla sicurezza e la dependability delle grandi infrastrutture informatiche e di tutte le infrastrutture a loro connesse o da loro dipendenti.

A livello politico e regolamentare, la Commissione ha cominciato, a partire dal 2001, a definire un approccio Europeo alla sicurezza delle reti e dell'informazione che, partendo dalla Comunicazione COM(2001) 298, ha portato alla costituzione nel novembre 2003 della **European Network & Information Security Agency (ENISA**). Elemento principale dell'approccio Europeo è la consapevolezza di dover responsabilizzare e coinvolgere tutti gli attori - dagli utilizzatori agli ISP, dai fornitori di servizi agli operatori telecom, dalla pubblica amministrazione a tutti i settori economici ed industriali - nell'adottare tecnologie, standard e buone pratiche di sicurezza. A tal fine, si sono individuate una serie di azioni mirante a prevenire i problemi di sicurezza (come intrusioni, virus, ecc.) e a fornire una difesa da incidenti o vulnerabilità, tramite il miglioramento della sicurezza e dell'integrità dei sistemi degli utilizzatori (cittadino o impresa) e delle reti informatiche globali. È importante sottolineare come questo approccio Europeo alla sicurezza delle reti e

dell'informazione è centrato su obiettivi ed interessi tipici del *primo pilastro* (mercato interno, protezione del consumatore, protezione della privacy, ecc.).

Le sole misure di prevenzione e difesa non sono sufficienti ad assicurare la sicurezza e la protezione delle reti ed infrastrutture informatiche. Le attività criminali commesse contro queste infrastrutture sia con strumenti tradizionali che con strumenti informatici richiedono adeguate misure di protezione e lotta che sono tipiche del *terzo pilastro* (giustizia, forze di polizia, ecc.). In questo contesto, la Commissione ha, nel 2002, proposto una Decisione Quadro sugli attacchi severi a sistemi informativi. Questa Decisione Quadro, tenendo conto dei principi della Convenzione sul crimine informatico del Consiglio d'Europa, cerca di armonizzare, a livello Europeo, la definizione di crimine informatico, le sanzioni previste per i crimini informatici, nonché di migliorare gli strumenti di cooperazione in Europa tra organi investigativi giudiziari.

A livello operativo, la Commissione ha promosso, tramite il Piano di Azione eEurope 2002, delle iniziative di sensibilizzazione sui problemi di sicurezza delle reti al fine di coinvolgere i settori pubblico e privato in una discussione atta a condividere le esperienze e le conoscenze necessarie per affrontare il problema della dependability delle infrastrutture informatiche (http://www.cordis.lu/ist/ka2/dependability.html):

- Il progetto **Dependability Development Support Initiative (DDSI)** il cui obiettivo era triplice: i) studiare il quadro legale e le iniziative Europee ed internazionali di potenziale interesse per la protezione delle infrastrutture critiche di informazione; ii) facilitare la discussione tra pubblico e privato sulla protezione delle infrastrutture di informazione; iii) formulare proposte per iniziative politiche (inclusa la ricerca e sviluppo) a livello Europeo e/o nazionale in questo settore (http://www.ddsi.org/).
- **European Warning and Information System Forum (EWIS)** rivolto a rafforzare il coordinamento tra i CERTs/CSIRTs in Europea al fine di aumentare la capacità di anticipare e combattere attacchi informatici in Europa (http://ewis.jrc.it).
- **European Working Group on Interdependencies and Vulnerabilities in Information Infrastructures** (**I3V** - http://deppy.jrc.it/default/show.gx?Object.object_id=KM------00000000000004F4) il cui compito era quello di stimolare, a livello Europeo, rappresentanti di diversi settori economici e tecnologici a discutere e condividere esperienze sulle interdipendenze tra infrastruttura di informazione ed altre infrastrutture convenzionali.

Le **Nazioni Unite** (**ONU**) hanno più volte sottolineato l'importanza di attuare politiche tese a migliorare la sicurezza delle infrastrutture informatiche.

Nel 1998 l'Assemblea Generale ha adottato la risoluzione n. 53/70 "*Development in the field of information and telecommunications in the context of international security*" sulla sicurezza dei sistemi globali di informazione e telecomunicazione che esortava gli stati membri a sviluppare principi che favoriscano la protezione delle infrastrutture e che limitino le minacce, esistenti e potenziali. A questa risoluzione seguirono altre sullo stesso argomento: la 54/49 del 1999, la 55/28 del 2000, la 56/19 del 2001 e la 57/53 del 2002.

Nel 2000 fu adottata la risoluzione n. 55/63 che stabiliva le basi giuridiche per contrastare il crimine informatico, poi ripresa nella risoluzione n. 56/121 del 2001.

Nel 2002 fu adottata la risoluzione n. 57/239 sulla creazione di una cultura globale per la *cybersecurity*.

Il tema specifico della protezione delle infrastrutture critiche è stato, invece, trattato dalla 78ma Assemblea Generale che il 23 dicembre 2003 ha adottato la risoluzione n. 58/199 ***Creation of a global culture of cybersecurity and the protection of critical information infrastructures*** (riportata in appendice). Questa risoluzione, nel riconosce che le infrastrutture critiche sono sempre più interdipendenti anche a causa del crescente ricorso alle infrastrutture informatiche, evidenzia come ciò si traduca in una maggiore vulnerabilità dell'intero sistema e, quindi, nella necessità di mettere in atto azioni tese a ridurre le vulnerabilità e le minacce, a minimizzare i possibili danni e a favorire le azioni di ripristino anche intervenendo sulla formazione e preparazione del personale. In particolare, la risoluzione invita gli stati membri a tenere in conto, nella definizione delle proprie strategie, degli "*Elements for protecting critical information infrastructures*" riportati in allegato alla risoluzione stessa e che ricalcano, nella sostanza, i principi elaborati nel marzo del 2003 dal G8.

La realtà italiana

La situazione legislativa Italiana

In Italia, la protezione delle infrastrutture critiche informatizzate, e più in generale la protezione delle infrastrutture critiche, è normata da una serie di atti:

a) **D.L. 29/12/1992, n. 518,** modificato con **L. 18/8/2000, n. 248**, volto a reprimere i comportamenti illeciti di pirateria informatica.

b) **L. 23/12/1993 n. 547**, testo organico in tema di delitti informatici.

c) **D.M. Interni 31/3/1998**, che, nell'ambito del Decreto del Ministero dell'Interno del 22/1/1992, ha sancito che le attività investigative delle forze di polizia sulla criminalità informatica ed attività illecite nel settore dell'elettronica sono di competenza della Polizia di Stato, istituendo presso il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno, il **Servizio di Polizia Postale e delle Comunicazioni** che è stato definito, con D.M. del 13/1/1999, "organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle comunicazioni".

d) **Decreto Interministeriale tra Ministeri dell'Interno, Comunicazioni e Giustizia del 2/3/1998,** aggiornato con analogo decreto del 21/9/1999 e successive modifiche, che ha istituito l'Osservatorio permanente per garantire la sicurezza delle reti e la tutela delle comunicazioni.

e) **D.Lgs. 16 marzo 1999 n. 79,** che recepisce la direttiva 96/92/CE sul mercato interno dell'energia elettrica e **decreto del Ministero dell'Industria e del Commercio 17 luglio 2000** che assegna al GRTN (Gestore della rete di trasmissione nazionale S.p.a.) le attività di trasmissione e dispacciamento dell'energia elettrica nel territorio nazionale.

f) **D.Lgs. 23 maggio 2000 n. 164** che recepisce la direttiva n. 98/30/CE sul mercato interno del gas naturale.

g) **D.L. 374/2001,** trasformato in **L. 438/2001**, volto a introdurre strumenti più adeguati di indagine e di repressione del terrorismo.

h) Direttiva del Presidente del Consiglio dei Ministri del 16 gennaio 2002 (G.U. n. 69 del 22/3/2002) su **"Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali"**

i) **Decreto Interministeriale tra Ministero delle Comunicazioni e Ministero per l'Innovazione e le Tecnologie del 24/7/2002**, che ha istituito il Comitato Tecnico Nazionale sulla sicurezza informatica e delle telecomunicazioni nella Pubblica Amministrazione.

j) **L. del 14/2/2003 n. 34** che ratifica la Convenzione internazionale per la repressione degli attentati terroristici mediate utilizzo di esplosivi delle Nazioni Unite del 15 dicembre 1997.

k) **D.Lgs 9 aprile 2003, n. 70** che recepisce la direttiva 2000/31/CE su taluni aspetti giuridici della società dell'informazione, ed in particolare il commercio elettronico indicando, fra l'altro, le responsabilità dei Provider di servizi Internet.

l) **D.Lgs 30 giugno 2003, n. 196 - Codice in materia protezione dei dati personali** (noto come Testo Unico sulla Privacy), in vigore dal 01/01/2004 e che sostituisce la **L. 31/12/1996, n. 675**, sulla protezione dei dati personali.

Questi atti normativi si sono aggiunti o sono stati integrati in una serie di norme preesistenti che hanno arricchito e potenziato il Codice penale e il Codice di procedura penale. Si precisa che l'azione tesa a produrre un danneggiamento è considerata un crimine nel momento in cui essa è messa in atto, a prescindere dal fatto che la stessa produca o meno un danno.

Inoltre, dopo gli eventi dell'11 settembre l'articolo 270-bis del c.p., è stato modificato con D.L. 374/2001 (trasformato in L. 438/2001) in modo che azioni compiute in Italia sono considerate crimini anche se le stesse sono orientate verso uno Stato esterno o contro un organismo internazionale.

Con la L. n. 34 del 14/2/2003, che ratifica la Convenzione internazionale per la repressione degli attentati terroristici mediate utilizzo di esplosivi delle Nazioni Unite del 15 dicembre 1997, viene fornita una prima identificazione legislativa delle infrastrutture critiche che vengono individuate come: "*ogni impianto pubblico o privato che fornisce servizi di utilità pubblica, come la conduzione d'acqua, l'evacuazione delle acque reflue, l'energia, il combustibile o le comunicazioni*".

Dal punto di vista delle responsabilità di garantire la qualità del servizio e la sicurezza delle reti informatiche alcuni vincoli provengono indirettamente dall'attuazione delle disposizioni di legge n. 675 del 31 dicembre 1996 avente per oggetto "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" e quella dei provvedimenti legislativi ad essa collegati (DPR 318 del 28/7/99 - "legge sulla privacy" e il D.Lgs 30/06/2003 n. 196).

Si segnala, infine, che sono in fase di conclusione i lavori preparatori per sottoporre al Parlamento Italiano la ratifica della ***Convenzione su Cybercrime*** del Consiglio d'Europa che è stata sottoscritta il 21 novembre 2001 a Budapest da 23 Paesi, fra cui l'Italia. Lo scopo della convenzione è quello di facilitare la protezione della società nei confronti del cybercrime adottando appropriati atti normativi e migliorando la cooperazione internazionale.

Il ruolo del Ministero dell'Interno

Il Ministero dell'Interno è il Dicastero deputato alla sicurezza del Paese intesa come gestione delle politiche attinenti alla prevenzione e repressione dei reati e di quei comportamenti giudicati idonei a mettere in pericolo la vita e l'integrità fisica dei cittadini e dei loro beni.

Il complesso dei livelli di responsabilità per quanto attiene alla sicurezza nazionale si articola in ambito nazionale, provinciale e locale. Detentori di tali responsabilità sono il Presidente del Consiglio dei Ministri, quale organo istituzionale deputato a promuovere ed indirizzare la politica del Governo, il Ministro dell'Interno, in qualità di Autorità Nazionale di Pubblica Sicurezza, il Prefetto ed il Questore, Autorità Provinciali di Pubblica Sicurezza, competenti territorialmente per quanto attiene alla sicurezza pubblica. Inoltre, sono previsti dalla normativa in materia, la legge 1 aprile 1981, n. 121, il Comitato Nazionale per l'ordine e la Sicurezza Pubblica ed il Comitato Provinciale, ove, rispettivamente a livello nazionale e provinciale, si individuano le criticità in materia di sicurezza pubblica e si elaborano strategie per garantire la difesa da qualunque tipo di minaccia.

Il Ministro dell'Interno, oltre ad essere il vertice istituzionale ed amministrativo del suo Dicastero, è anche Autorità Nazionale di Pubblica Sicurezza, ovvero l'organo che detta a livello nazionale le direttive per la gestione dell'ordine e della sicurezza pubblica. Tali direttive vengono fatte proprie, per poi essere emanate con efficacia provinciale e locale, rispettivamente dalle Autorità provinciali e locali (Prefetto, Questore, dirigente Commissariato, Sindaco).

L'apparato amministrativo che si occupa a livello centrale della gestione dell'ordine e della sicurezza pubblica è il Dipartimento di Pubblica Sicurezza del Ministero dell'Interno.

Il sistema appena descritto si basa su una visione globale della sicurezza, le cui politiche di alta amministrazione sono affidate ad Autorità il cui ruolo le rende trasversali alle tematiche che compongono il nostro tessuto sociale ed economico.

Le nuove potenzialità offerte dall'interconnessione e dalla condivisione delle informazioni hanno in breve tempo contribuito a produrre un aumento nell'offerta di nuovi servizi al cittadino ed, in genere, a tutti gli utenti pubblici e privati. L'espansione delle possibilità offerte dalle nuove tecnologie ha, d'altro canto, comportato un aumento esponenziale delle vulnerabilità dei singoli sistemi. L'interconnessione delle reti ha comportato una maggiore vulnerabilità dell'intero Sistema Paese, tanto da spingere a pensare, riguardo alla sicurezza delle infrastrutture critiche informatizzate, in termini di sicurezza globale. Da qui scaturisce la necessità di stabilire un piano di sicurezza complessivo, articolato in una fase strategica ed una successiva di carattere operativo ove, in particolare, entrano in campo competenze attinenti alle funzioni di polizia di sicurezza e giudiziaria con prevalenza per forze di polizia specializzate nel settore del *cyber-crime*.

Il Ministero dell'Interno ha da oltre un decennio compreso i pericoli e le potenzialità offerte dalle nuove tecnologie nell'ambito della società dell'informazione.

L'attuale assetto organizzativo per il contrasto al crimine ad alta tecnologia è delineato attraverso il D.I. del 31.3.1998 con il quale è stato creato il Servizio Polizia Postale e delle Comunicazioni in seno alla Direzione Centrale per le Specialità, ovvero l'organo di gestione e coordinamento operativo dei 19 Compartimenti regionali e delle 79 Sezioni provinciali che compongono gli uffici territoriali in cui operano i 2000 operatori della Specialità della Polizia Postale e delle Comunicazioni.

Inoltre, il Servizio di Polizia Postale e delle Comunicazioni è stato individuato, con D.I. 13.1.1999, Organo Centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazione e costituisce il punto di contatto operativo *h24x7 (24 hours for seven days)* per l'Italia, con gli uffici di polizia appartenenti ai Paesi aderenti al G8 che si occupano di crimini informatici.

Il continuo contatto con le realtà che agiscono nello specifico campo ha favorito la creazione di un clima di collaborazione e di prossimità tra Polizia e utenti delle reti. Collaborazione che ha creato specifiche sinergie con gli enti e le aziende che gestiscono le infrastrutture critiche del Paese, sino a giungere alla stipula, in alcuni casi, di specifiche convenzioni volte ad attivare piattaforme di comunicazione privilegiate e modalità di intervento più efficaci per la repressione dei crimini informatici.

La collaborazione tra Polizia Postale e delle Comunicazioni e gli altri soggetti che operano a tutti i livelli nel campo delle nuove tecnologie è il passaggio fondamentale per la realizzazione di un sistema di sicurezza integrato, basato sul doveroso e proporzionato contributo di tutti.

Ne consegue che il modello operativo nella repressione del crimine informatico della Polizia Postale e delle Comunicazioni è orientato verso le peculiarità della rete Internet e prevede tre modelli ideali di possibili vittime: utenti privati (navigatori del *cyberspace*), utenti qualificati (soggetti istituzionali non strategici, enti locali ed aziende) e utenti

detentori di risorse critiche, infrastrutturali, informatiche (istituzioni e gestori di servizi essenziali). Ciascuno scenario prevede una specifica modalità di risposta da parte della Polizia Postale e delle Comunicazioni.

Nel caso di azioni in danno di utenti privati l'attività di polizia di sicurezza e di polizia giudiziaria si innescano mediante sia il monitoraggio della Rete alla ricerca di possibili condotte delittuose che minacciano la massa degli utenti, sia attraverso la denuncia della stessa vittima.

Viceversa qualora la vittima fosse un soggetto pubblico oppure un'azienda l'intervento della Polizia Postale e delle Comunicazioni sarebbe avviato di concerto con le unità organizzative delle vittime deputate alla sicurezza ICT.

In questa ottica, la Polizia Postale e delle Comunicazioni con le sue strutture territoriali è ovunque impegnata, a livello informativo ed operativo, in politiche di collaborazione con le istituzioni e con le aziende che operano nell'ICT, al fine di ridurre l'incidenza del *cyber-crime*.

Infine, nel caso di un *computer attack* ad un'infrastruttura critica informatizzata le modalità repressive devono essere, data la criticità della risorsa, standardizzate e preordinate. Pertanto è necessario predisporre una serie di protocolli di intesa con i soggetti detentori delle risorse strategiche per la collettività al fine di prestabilire sia procedure di comunicazione dei dati in tempo reale che procedure operative per la repressione tempestiva ed efficace dell'attività criminale.

Il futuro in materia di contrasto al *computer crime* prevede progettualità orientate verso una presenza tempestiva sul *crime scene investigation* mediante forme di collegamento permanenti tra le strutture suddette ed un centro operativo nazionale, per la gestione delle emergenze informatiche ad alto impatto causate da crimini informatici.

Comitato Tecnico Nazionale sulla Sicurezza Informatica e delle Telecomunicazioni della Pubblica Amministrazione

Istituto nel luglio 2002 con decreto interministeriale del Ministro delle Comunicazioni e Ministro per l'Innovazione e le Tecnologie con funzioni di indirizzo e coordinamento di iniziative in materia di sicurezza nelle tecnologie dell'informazione e delle comunicazioni nella Pubblica Amministrazione.

Il comitato, in particolare, concorre alla definizione del Piano Nazionale della Sicurezza delle tecnologie dell'informazione e comunicazione della pubblica amministrazione e alla predisposizione di un modello organizzativo nazionale di sicurezza ICT per la pubblica amministrazione.

Il comitato sta promovendo la costituzione di un *Computer Emergency Response Team* (CERT) della Pubblica Amministrazione (**CERT-PA**) che fungerà da *Early Warning System* operando 24x7 con personale altamente specializzato.

Il CERT-PA nasce con l'obiettivo di assistere le P.A. nel compito di garantire la continuità del servizio nel caso in cui la stessa possa essere compromessa da attacchi informatici e virus, fornendo tempestivamente informazioni su come evitare o gestire la situazione a fronte di attacchi informatici, e di fornire assistenza agli utenti vittime degli stessi. Tale CERT opererà in collaborazione con le analoghe strutture istituite da Università e Enti di ricerca italiani (CERT-IT, GARR-CERT) e con gli organismi internazionali FIRST, TF-CSIRT, FORUM CERT-PA.

Il comitato, inoltre, sta promovendo l'attuazione di "***Piano di Sensibilizzazione e Formazione alla Sicurezza del Patrimonio Informativo della Pubblica Amministrazione***" rivolto a tutti i dipendenti della P.A. con lo scopo di:

- Creare la necessaria consapevolezza (awareness) sulle minacce, vulnerabilità e rischi che potenzialmente possono gravare sul patrimonio informativo della P.A.;
- Generare la conoscenza di base per comprendere i fabbisogni di sicurezza e i relativi accorgimenti di prevenzione/protezione in termini organizzativi, operativi, tecnologici e giuridico-normativi;
- Promuovere l'utilizzo di adeguate metodologie e strumenti relativamente alla gestione dei processi fondamentali della sicurezza.

Tale piano di sensibilizzazione nasce dalla constatazione che tutti i dipendenti, ed in particolare i quadri dirigenti, hanno responsabilità non solo per quanto riguarda la loro sicurezza individuale ma anche per quanto attiene alla sicurezza complessiva del *cyberspace* nel quale si trovano ad operare. Per garantire questa responsabilità in modo appropriato, ciascuno deve essere consapevole dei rischi e delle vulnerabilità che contraddistinguono le informazioni che può influenzare e controllare, e deve conoscere gli accorgimenti fondamentali che possono essere attuati per prevenire intrusioni, attacchi o altre minacce al patrimonio informativo della P.A.

Osservatorio Permanente per la Sicurezza delle Reti e la Protezione delle Comunicazioni

Istituito originariamente nel 1998, vi fanno parte membri del Ministero dell'Interno, delle Comunicazioni e della Giustizia.

All'interno dell'Osservatorio opera, fra l'altro, il "sottogruppo Internet" che si occupa degli aspetti legislativi ed investigativi connessi con l'utilizzo di Internet. In particolare, tale sottogruppo definisce i servizi che obbligatoriamente gli ISP devono fornire agli investigatori in presenza delle relative autorizzazioni emesse dalla magistratura.

Il "sottogruppo Linee Guida" sta effettuando un'analisi sulle metodologie e le procedure di risk assesment messe in atto dai diversi operatori di telecomunicazioni.

Proposte

La rilevanza della problematica, come evidenziato anche dai recenti eventi di cronaca, e l'attuale assenza di azioni incisive in Italia fa sorgere l'esigenza di avviare un insieme di azioni che possano consentire di stimolare la necessaria sensibilità al problema e, quindi, colmare il gap tecnologico/culturale che si sta creando su questa tematica fra il nostro Paese e le altre nazioni industrializzate.

In particolare, stante l'intrinseca intersettorialità delle Infrastrutture Critiche Informatizzate, è necessaria la costituzione di organismi in grado di creare una visione unitaria del problema, all'interno della quale far confluirei diversi aspetti, esigenze e problematiche proprie di ciascun settore.

Solo in questo modo potranno individuarsi e concretizzarsi quelle iniziative che sono necessarie per garantire un soddisfacente livello di continuità di servizio e di sicurezza alle diverse infrastrutture necessarie per il benessere del Paese.

In questo spirito il Gruppo di Lavoro ha individuato alcune proposte operative che nel seguito si delineano.

Proposta di istituzione di un Comitato Interministeriale per le Infrastrutture Critiche Informatizzate (COM.IN.C.I)

La complessità e le peculiarità della tematica, che abbraccia responsabilità condivise da più dicasteri e soggetti pubblici e privati impongono di individuare il più appropriato assetto organizzativo per le necessarie azioni governative.

A tal fine, seguendo il percorso procedurale già sperimentato con successo da moltissime nazioni (Stati Uniti, Svezia, ecc.) si propone di istituire un **Comitato Interministeriale per le Infrastrutture Critiche Informatizzate (COM.IN.C.I.)** che abbia quale compito l'inquadramento complessivo della problematica al fine di elaborare **la soluzione italiana** per la protezione delle Infrastrutture Critiche Informatizzate definendone sia gli aspetti metodologici ed operativi che quelli più prettamente organizzativi.

Tale comitato, dovrebbe essere istituito presso la Presidenza del Consiglio dei Ministri, eventualmente promosso dal Comitato dei Ministri per la Società dell'Informazione, quale struttura di coordinamento con il compito di:

- Favorire la presa di coscienza della problematica e delle sue ripercussioni;
- Consentire una visione complessiva del *sistema di sistemi* costituito dalle diverse infrastrutture tecnologiche operanti in Italia evidenziandone gli aspetti di maggiore interdipendenza e, quindi, criticità;
- Promuovere azioni tese a limitare la vulnerabilità delle infrastrutture critiche definendo piani di azione nazionali e individuando le priorità;
- Stimolare e supportare i dicasteri e i diversi soggetti pubblici e privati coinvolti nel controllo e nella gestione delle diverse infrastrutture nel monitoraggio delle stesse e per l'adozione di opportune strategie ed iniziative tese a ridurre il livello di rischio;
- Favorire la disseminazione delle best-practice sulla sicurezza ed un fattivo scambio di informazioni fra i diversi soggetti coinvolti nella gestione delle infrastrutture e nella prevenzione e protezione delle stesse;

- ❖ Promuovere la formazione del personale operante nei settori delle Infrastrutture Critiche per quel che riguarda la gestione delle situazioni di emergenza;
- ❖ Promuovere la ricerca e la cooperazione internazionale sulla tematica.

A tale comitato dovrebbero partecipare, quanto meno, rappresentanti dei seguenti dicasteri:

- Presidenza del Consiglio dei Ministri
- Ministero Interno
- Ministero Giustizia
- Ministero Infrastrutture
- Ministero Attività Produttive
- Ministero Comunicazioni
- Ministero Difesa
- Ministero Salute
- Ministero Istruzione Università e Ricerca Scientifica
- Ministero Ambiente
- Ministero Economia e Finanze
- Dipartimento per l'Innovazione e Tecnologie
- Dipartimento per la Protezione Civile
- Ufficio del Consigliere Militare
- CESIS
- SISMI
- SISDE
- Autorità per le garanzie nelle Comunicazioni
- Autorità per l'Energia Elettrica e il Gas

oltre che prevedere un rapporto organico con gli altri Enti Pubblici operanti nei settori delle Infrastrutture Critiche e con i diversi soggetti privati deputati alla gestione di tali infrastrutture.

Il comitato, lungi dall'invadere le sfere di autonomia e responsabilità dei diversi soggetti preposti, dovrebbe favorire una contrattazione bilaterale o multilaterale in grado di conciliare i livelli di servizio, affidabilità e sicurezza richiesti dagli utilizzatori con le necessità, disponibilità e vincoli propri dei fornitori garantendo prioritariamente e preminentemente quei servizi ed infrastrutture connessi con la sicurezza nazionale e con il benessere della popolazione.

In altri termini, il ruolo del comitato dovrebbe concentrarsi, senza entrare direttamente nelle politiche di sicurezza e gestione delle diverse infrastrutture, esclusivamente su quegli elementi di **interdipendenza** esistenti fra le diverse infrastrutture tecnologiche ed il cui controllo sfugge alla gestione dei singoli operatori.

Le azioni del COM.IN.C.I dovrebbero, pertanto, essere mirate a:

- ▪ L'identificazione, nella realtà italiana, delle Infrastrutture da ritenere Critiche;
- ▪ L'individuazione di tutti i soggetti coinvolti nella loro gestione e deputati al loro controllo;
- ▪ La comprensione delle maggiori interdipendenze esistenti a livello di infrastrutture;
- ▪ L'individuazione delle infrastrutture, delle problematiche e delle interdipendenze sulle quali concentrare le priorità;
- ▪ La definizione di linee strategiche per la nazione.

Il COM.IN.C.I. dovrebbe essere affiancato e supportato, anche in considerazione della complessità e difficoltà di attivare una struttura di coordinamento costituita da una così vasta platea di interlocutori, da una struttura più operativa che abbia il compito di:

- Raccogliere ed elaborare i dati relativi alle diverse realtà italiane al fine di offrire una visione complessiva della situazione nazionale;
- Sviluppare metodologie di analisi del problema che possano essere utilizzate nella realtà italiana per comprendere e caratterizzare la problematica;
- Fornire strumenti metodologici ai diversi operatori affinché questi possano operare costanti azioni di auto-valutazione della propria realtà, dei propri livelli di vulnerabilità e dei propri elementi di criticità;
- Individuare tecniche per la circoscrizione dei guasti e per il recovery in presenza di eventi negativi anche in considerazione della perdita del concetto di prossimità geografica indotta dalla presenza del cyberspace;
- Realizzare azioni di sensibilizzazioni, culturali e di formazione tese a far crescere una maggiore coscienza e conoscenza sulla problematica;
- Analizzare le iniziative in atto a livello internazionale per quel che riguarda la protezione delle Infrastrutture Critiche Informatizzate;
- Costituire di un punto di raccordo con le diverse istituzioni straniere operanti nel settore;
- Contribuire, in concorso con gli altri soggetti preposti, alla definizione dei piani per il contenimento delle emergenze e per favorire il ripristino dei livelli di servizio, e ciò anche con l'ausilio di tecnologie innovative;

Realizzazione di un sito dedicato alla problematica

La necessità di una costante cooperazione pubblico-privato da un lato, e dall'altro l'elevato numero dei soggetti da coinvolgere, fa nascere l'esigenza di disporre di canali di comunicazioni efficaci.

In questo contesto è emersa la necessità di approntare anche in Italia un sito che possa fungere da elemento di disseminazione delle conoscenze per quel che riguarda le CIIP oltre che l'infrastruttura tecnologica abilitante per la costituzione di una comunità virtuale (forum associativo) all'interno della quale i diversi operatori possano iniziare a condividere esperienze, esigenze, necessità e soluzioni.

All'interno di tale sito potrebbero essere raccolte le notizie circa eventi organizzati a livello nazionale ed internazionale, i collegamenti ai siti governativi operanti sulla tematica e alle sezioni dei siti dei diversi dicasteri italiani ove la tematica e attualizzata ai diversi specifici settori, documentazione di inquadramento e tecnica sulla problematica, best-practice e case-history oltre che le esperienze fatte a livello internazionale in occasione di eventi di crisi che abbiano coinvolto una o più infrastrutture critiche.

Una sezione riservata del sito sarebbe impiegata per la costituzione del primo forum virtuale fra i diversi operatori.

Nella Figura 8 è rappresentata una ipotesi di implementazione del sito.

Figura 8: Proposta per la costruzione di un sito dedicato alla problematica delle CIIP.

Proposta di una Agenda di Ricerca italiana nel campo della Protezione delle Infrastrutture Critiche Informatizzate

Il problema della salvaguardia e sicurezza delle Infrastrutture Critiche non può essere ridotto ad un mero problema di gestione della sicurezza (intesa come repressione dei comportamenti criminali). Servono attività di ricerca mirate all'analisi del problema nonché lo sviluppo di tecnologie di difesa e protezione per i diversi domini applicativi. Di conseguenza, si configura l'esigenza di partire con una **iniziativa di R&S a livello nazionale**, con forti collegamenti internazionali per la natura trans-nazionale del soggetto, mirata alla risoluzione di questi nuovi problemi, analogamente a quanto già attuato dal resto dei Paesi occidentali, Stati Uniti in testa.

In questo contesto si ritiene utile proporre una **Agenda di Ricerca** sul soggetto della Protezione delle Infrastrutture Critiche Informatizzate, il cui obiettivo è l'identificazione di aree di ricerca che vanno al di là delle responsabilità dei gestori delle singole infrastrutture e che quindi richiedono un'azione di coordinamento e un approccio multi-settoriale. Le attività di ricerca mirate allo sviluppo di metodi, strumenti e tecnologie di carattere generale, dovranno essere svolte nell'ambito di collaborazioni tra operatori e soggetti di ricerca e dovranno essere complementari alle attività che i diversi operatori già svolgono per loro iniziativa.

Sono identificabili sei aree di ricerca strategica, all'interno delle quali confluiscono un insieme di discipline che vanno dalla matematica alla fisica, dall'ingegneria alla modellistica, dall'informatica alla biologia, dallo studio dei sistemi complessi alla simulazione e all'ingegneria socio-cognitiva. Il tutto deve essere accompagnato da un'opportuna e permanente attività di formazione sul soggetto specifico.

Metodi e strumenti per l'analisi delle vulnerabilità delle infrastrutture complesse informatizzate. Le attività di ricerca in quest'area dovranno essere mirate allo sviluppo di strumenti per l'analisi di vulnerabilità da mettere a fattor comune tra i diversi settori applicativi (elettrico, olio & gas, telecomunicazione, trasporti, ecc.). Anche se apparentemente molto diverse, con l'introduzione crescente delle tecnologie ICT più o meno tutte le infrastrutture critiche hanno il loro tallone di Achille nei sistemi SCADA e DCS, largamente usati per la gestione e il controllo delle stesse.

Metodi e strumenti per l'analisi delle capacità reattive e per il ripristino dello stato normale delle infrastrutture complesse informatizzate. Particolarmente importanti sono lo sviluppo di strumenti e metodologie in grado di correlare in tempo reale le informazioni più disparate per identificare situazioni di pericolo non identificabili dall'analisi separata di diverse fonti di dati. Sempre in quest'area sono particolarmente rilevanti gli aspetti di modellazione dei processi decisionali, lo sviluppo di interfacce evolute per meglio presentare le informazioni e lo sviluppo di strumenti di supporto alle decisioni in grado di aiutare il decisore nelle difficili scelte da compiere in presenza di attacchi.

Metodologie e tecnologie per aumentare la capacità di sopravvivenza delle infrastrutture complesse informatizzate. In quest'area, filoni di ricerca promettenti sembrano essere tutte quelle tecniche architetturali generalmente indicate come *intrusion-tolerant, self-healing, context-aware, self-stabilizing* che hanno l'obiettivo di garantire il corretto funzionamento del sistema e/o dell'infrastruttura anche in situazioni anomale e che hanno dimostrato buoni risultati a livello di sistemi ben delimitati ma che adesso dovrebbero esportarsi a livello di sistema di sistemi. In quest'area, interessanti sono anche i risultati che provengono dal mondo della ricerca interdisciplinare sui sistemi complessi che permettono, fissato un obiettivo, di ottimizzare la topologia della rete

Definizione di modelli e di metriche per l'analisi dei rischi delle infrastrutture critiche informatizzate. Si sente l'esigenza di sviluppare strumenti di tipo analitico che permettano delle analisi di rischio nel senso convenzionale del termine ma scalabili al livello di complessità delle infrastrutture di interesse, analisi economiche di costo/beneficio degli investimenti in sicurezza e in nuove tecnologie.

Definizione di modelli e piattaforme di simulazione per la generazione di scenari e l'analisi delle interdipendenze di infrastrutture critiche informatizzate. In quest'area si colloca il filone di ricerca riguardante la generazione di scenari incidentali e modelli di attacco, particolarmente utile alla prevenzione di disastri attraverso azioni di valutazione preventive.

Sviluppo di modelli e strumenti per l'Ingegneria socio-cognitiva. L'Ingegneria Socio Cognitiva può offrire un insieme di metodi che nell'ambito dei paradigmi sistemici, cognitivi e sociali, con il supporto delle moderne tecnologie software e di intelligenza artificiale permettono di realizzare modellazioni e simulazioni delle conseguenze di certe decisioni sulla dinamica di una situazione di emergenza.

Al di là delle specifiche attività di R&S, serve identificare, inoltre, chi in Italia potrebbe svolgere un ruolo di aggregazione e coordinamento delle varie iniziative di R&S. Il problema ha, infatti, una dimensione nazionale con forti collegamenti internazionali e non può essere risolto con iniziative singole, pubbliche o private.

Allo scopo di stabilire una stretta sinergia tra utenti e ricercatori e allo stesso tempo non favorire un dominio applicativo rispetto ad un altro, sarà auspicabile che le azioni di ricerca vadano definite in sinergia con un **Gruppo di Interesse Nazionale**.

Proposta per la creazione di un Centro Virtuale di Simulazione e Analisi delle Interdipendenze (SAI)

Il blackout americano del 14/08/03 ha messo in evidenza interdipendenze prima difficilmente immaginabili. Per esempio l'interdipendenza fra: sistema elettrico, sistema dei trasporti e sistema di raccolta e smaltimento dei rifiuti. Lo stesso problema delle interdipendenze è stato evidenziato dagli altri black-out occorsi nel 2003, con un impatto crescente al crescere del tempo di disservizio.

Allo stato attuale, l'unico strumento in grado di aiutare a compiere delle valutazioni sulle possibili conseguenze di scenari incidentali che coinvolgano, con un effetto domino, due o più infrastrutture è quello simulativo. Ciò fa nascere l'esigenza di poter disporre di un ambiente di simulazione in grado di integrare modelli provenienti da diversi settori applicativi, quali:

- reti di mobilità ferroviaria, stradale, ecc.
- reti del sistema dei servizi di emergenza.
- reti elettriche, olio e gas, acqua.
- reti di telecomunicazione e di reti informatiche.
- reti dei servizi finanziari

Tale risultato potrebbe ottenersi attraverso la costituzione di un **Centro Virtuale di Simulazione e Analisi delle Interdipendenze** (**SAI**). Il Centro dovrà avere il compito di integrare i diversi modelli settoriali fornendo una visione unitaria del sistema di sistemi composto dalle diverse infrastrutture critiche interdipendenti. Ciò consentirebbe di fornire ai decisori politici e amministrativi indicazioni circa le possibili conseguenze che potrebbero prodursi nei diversi scenari di crisi.

Il Centro, lasciando la responsabilità dello sviluppo dei modelli di settore ai gestori e/o proprietari delle singole infrastrutture, dovrebbe concentrarsi specificatamente sulle attività di analisi delle interdipendenze e di tutti quei fenomeni che travalicano i singolo settori.

La costituzione del SAI potrà rappresentare, inoltre, il primo passo verso la realizzazione di un centro di ricerca Europeo sulle CIIP in grado di aggregare le diverse realtà di ricerca esistenti. Ciò consentirebbe di creare quella massa critica necessaria per affrontare compiutamente le sfide poste dalle CIIP, dalla loro interdisciplinarietà e dalla loro complessità intrinseca. Questo processo di aggregazione è, per altro, già in corso negli USA dove alcuni dei più prestigiosi istituti di ricerca (Los Alamos National Laboratory, Sandia National Laboratories, solo per citare i principali) hanno dato vita al NISAC (*National Infrastructure Simulation and Analysis Center*) con il preciso scopo di favorire la realizzazione di strumenti di analisi adeguati alle problematiche poste dalle CIIP.

Supporto alle attività di R&S sulle tecnologie in grado di identificare in modo decentralizzato l'insorgere di stati anomali e di prevenire le conseguenze attraverso opportune politiche locali di gestione

A causa della natura intrinseca e dei forti investimenti negli attuali sistemi SCADA, non è ipotizzabile a medio termine (10-20 anni) una sostituzione di tali sistemi. Di conseguenza, al fine di aumentarne il livello di sicurezza, occorre pensare a soluzioni di tipo "*add-on*" distribuite che siano in grado d fornire ai diversi componenti dell'infrastruttura strumenti in grado di identificare, sulla base delle informazioni interne e provenienti dal mondo

circostante, l'insorgere di stati anomali e quindi attivare azioni che ne limitino le conseguenze.

Il GdL ritiene, pertanto, fondamentale individuare strumenti, azioni e forme in grado di promuovere lo sviluppo di tecnologie e di sistemi di *Intrusion Management.* Ovvero di sistemi che, a differenza del semplice *Intrusion Detection*, rilevino, sulla base dello scostamento del sistema dal suo stato di funzionamento normale, l'insorgenza di un malfunzionamento e siano in grado di supportare le consequenziali politiche di gestione. Ovviamente il rilevamento e la classificazione di un malfunzionamento non sono generalmente realizzabili tramite l'individuazione di una singola anomalia. È necessario correlare più eventi rispetto ad una scala temporale e/o spaziale, e ciò specialmente per le infrastrutture complesse distribuite su vaste aree geografiche ove avvengono trasmissioni di dati e/o flussi di materia o energia da un punto all'altro, quali sono appunto le infrastrutture di telecomunicazione, di trasporto e distribuzione dell'energia elettrica, dal gas, ecc. Di pari importanza sono poi le correlazioni spazio-temporali su infrastrutture diverse ma interdipendenti; al fine di individuare fenomeni di propagazione del malfunzionamenti da una infrastruttura all'altra.

La tecnologia più promettente in questo campo è la tecnologia *multi-agents*, che consiste nello sviluppare una popolazione di agenti autonomi, comunicanti tra loro attraverso meccanismi di scambio di informazioni (messaggi), ognuno dei quali implementa algoritmi più o meno sofisticati che vanno dai modelli statistici alle reti neurali, al *data mining*, all'uso di basi di conoscenza e di tecniche che si ispirano al comportamento del sistema immunitario per la comprensione delle anomalie, la determinazione dei malfunzionamenti e la conseguente definizione di strategie opportune tese a limitarne l'incidenza ed a favorire il ripristino delle condizioni di funzionamento nominali.

Proposta per la creazione di un Gruppo di Interesse Nazionale (GdIN)

Per poter affrontare in modo fattivo il problema delle CIIP, non è possibile prescindere da un forte coinvolgimento dei diversi operatori pubblici e privati coinvolti nella gestione e controllo delle diverse infrastrutture.

In considerazione dell'elevato numero di soggetti da coinvolgere, in molte nazioni si è favorita la nascita di forum associativi in grado di rappresentare e mediare le esigenze proprie dei diversi settori ed operatori consentendo di individuare efficienti ed efficaci canali di comunicazione pubblico/privato in grado di favorire l'opportuna disseminazione delle informazioni sia dai soggetti pubblici verso quelli privati che viceversa.

Ad esempio questa è la strada perseguita in Gran Bretagna con l'istituzione del **Information Assurance Advisory Council (IAAC)** e negli USA con il **National Infrastructure Assurance Council (NISAC).** In particolare quest'ultima struttura ha l'ulteriore scopo di far nascere, all'interno delle diverse comunità degli **ISAC (Information Sharing and Analysis Center),** ove i diversi operatori coinvolti nella gestione di una singola tipologia di infrastruttura possono condividere esperienze e definire strategie di azione comuni per migliorare i relativi livelli di sicurezza ed affidabilità.

Gli ISAC, inoltre, svolgono anche un ruolo di intermediazione operando come delle *clearing room* consentendo di fornire ai soggetti pubblici le informazioni richieste dalla legislazione americana su eventuali incidenti evitando che le stesse possano divenire elemento di turbativa del mercato.

Questi forum favoriscono, inoltre, una maggiore cooperazione fra i diversi operatori consentendo la condivisione di esperienze e best practice.

Queste considerazioni sono alla base dell'idea di costituire anche in Italia un **Gruppo di Interesse Nazionale (GdIN)**, che sulla base di un principio associativo volontario, possa assumere un ruolo di promozione e di mediazione fra i soggetti pubblici investiti della responsabilità delle CIIP ed i diversi operatori privati coinvolti.

Il GdIN, partendo dall'assunzione che ogni settore economico, industriale e sociale, rilevante per gli aspetti della protezione delle infrastrutture critiche (elettrico, olio & gas, acqua, telecomunicazione, bancario, sanitario,...) abbia sviluppato **strategie di settore** per assicurare la continuità della fornitura dei servizi previsti, anche in caso di emergenze dovute a cause naturali e/o ad attacchi terroristici sia di natura convenzionale che di natura informatica, si pone i seguenti obiettivi:

Identificare le interdipendenze tra le varie infrastrutture nazionali. Il problema delle interdipendenze è un problema che assume ogni giorno una nuova dimensione come conseguenza della globalizzazione dei mercati, dell'introduzione massiccia delle tecnologie ICT e delle evoluzioni in atto nei sistemi SCADA.

Identificare nuove necessità di ricerca e sviluppo comuni. Oggi esistono iniziative di ricerca e sviluppo tradizionali per i diversi settori, (elettrico, olio e gas, telecomunicazioni, acqua, trasporti, ecc.) tra loro non coordinate e spesso in duplicazione. La crescente interconnessione fa nascere l'esigenza di un coordinamento della ricerca nel campo della protezione delle infrastrutture critiche, che partendo da un'attività di *gap analysis* produca una Agenda di ricerca in cui si pongano delle priorità importanti per tutti i soggetti, siano essi operatori e/o proprietari di infrastrutture critiche. Per esempio lo sviluppo di piattaforme comuni di simulazione di scenari incidentali per lo studio dei fenomeni di interdipendenza oppure lo sviluppo di metodi e strumenti per l'analisi di vulnerabilità o per l'analisi del rischio.

Identificare nuove necessità di preparazione e organizzazione del personale. Gli eventi americani 11/09/01 e 14/08/03 hanno dimostrato che la miglior difesa contro le emergenze naturali e gli attacchi terroristici è la preparazione del personale. Tutti sono d'accordo nel dire che le conseguenze del black out del 14/08/03 sono state limitate dal fatto che a valle degli eventi dell'11/09 è stata sviluppata una consapevolezza a livello popolare e sono state sviluppate procedure e best practices, per cui tutti conoscevano meglio che cosa fare. Di conseguenza la necessità di sviluppare procedure e strumenti di supporto all'addestramento e alla cooperazione tra vari settori, varie istituzioni, vari corpi dello stato da attuare durante gli eventi di crisi.

Identificare politiche e procedure comuni per la condivisione delle informazioni. La crescente interdipendenza pone l'esigenza di stabilire delle politiche di condivisione delle informazioni, soprattutto per gli aspetti di sicurezza legati all'utilizzo di quella risorsa comune che è il *cyberspace*. Oggi esistono già associazioni di categoria per la condivisione delle informazioni e l'analisi congiunta delle cause e degli effetti di eventi disastrosi, per esempio il *North American Electric Reliability Council.*

Identificare bisogni di adeguate misure legali e legislative. Oggi esistono sicuramente delle barriere di accesso all'informazione in entrambi le direzioni, da pubblico a privato e da privato a pubblico. Se si vuole sviluppare una politica di protezione nazionale verso attacchi deliberati alle infrastrutture critiche, siano essi fisici che informatici, nasce la necessità di adeguate misure legislative che rendano possibile il *disclosure* dell'informazione senza incorrere a delle sanzioni di tipo punitivo ne che le stesse vadano ad interferire con le dinamiche proprie dei mercati.

Identificare bisogni di integrazione internazionale. Molte infrastrutture critiche hanno una dimensione sopranazionale con interazioni internazionali. Ciò complica notevolmente il problema e crea l'esigenza di creare dei collegamenti istituzionali tra i soggetti operanti nelle diverse nazioni. Il Gruppo di Interesse Nazionale dovrebbe identificare i bisogni comuni in questo campo e riportare queste esigenze nelle sedi istituzionali preposte allo sviluppo di politiche di cooperazione internazionale.

Conclusioni

Gli eventi di cronaca che hanno costellato l'estate del 2003 hanno evidenziato come le diverse infrastrutture tecnologiche, su cui si basano le società industrializzate, dipendono fortemente dal corretto funzionamento dell'infrastruttura elettrica. D'altro canto la crescente complessità di questa impone un massiccio utilizzo delle tecnologie tele-informatiche e quindi, la dipendenza dell'infrastruttura elettrica, sia in modo diretto che indiretto, dal corretto funzionamento di tutto un insieme di infrastrutture tecnologiche.

Un analogo discorso potrebbe ripetersi per qualunque infrastruttura tecnologica. In questo scenario è facile riconoscere la presenza di **interdipendenze** reciproche fra le diverse infrastrutture che rappresentano altrettanti elementi di vulnerabilità per l'intero sistema. In modo speculare rispetto a quanto accaduto nell'estate del 2003, potrebbero aversi, ad esempio, ripercussioni, se non addirittura il blocco, dell'erogazione dell'energia elettrica quale conseguenza di un guasto all'infrastruttura di telecomunicazioni o dell'azione di un virus su quella informatica.

La presenza di questi elementi di vulnerabilità, uniti ai rischi connessi con il fatto che le infrastrutture tecnologiche **potrebbero divenire obiettivi per azioni terroristiche**, spinge verso l'adozione di politiche atte a preservarne il corretto funzionamento, a circoscrivere e limitare l'incidenza di eventuali guasti e ad attivare procedure per garantire un rapido ripristino dei livelli di servizio.

Per la definizione di tali politiche è però necessaria una forte **co-partecipazione** sia da parte dei diversi soggetti pubblici preposti al controllo delle infrastrutture tecnologiche sia da parte degli operatori privati che materialmente gestiscono queste infrastrutture.

A tale scopo, nei vari paesi, sono state istituite strutture di coordinamento interministeriali ed è stata favorita la nascita di aggregazioni di operatori che possano porsi come interlocutori privilegiati nei confronti delle organizzazioni statali.

L'Italia risulta una delle pochissime nazioni industrializzate ove ancora non si è iniziato ad operare unitariamente sul tema della **Protezione delle Infrastrutture Critiche Informatizzate,** cioè sulla difesa e salvaguardia di tutte quelle infrastrutture (incluse quelle informatiche e, specificatamente Internet) che utilizzano, in tutto o in parte, una qualunque infrastruttura informatica per il loro monitoraggio, la loro gestione o il loro controllo.

Prendendo spunto dalle iniziative condotte dalle altre nazioni, il Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate ritiene doveroso suggerire la costituzione, in seno alla Presidenza del Consiglio dei Ministri, di un opportuno **Comitato Interministeriale** con lo scopo di coordinare e stimolare le politiche rivolte alla Protezione delle Infrastrutture Critiche Informatizzate. Nel Comitato, al fine di garantirne una visione complessiva del problema, dovrebbero essere rappresentati tutti i dicasteri e gli enti coinvolti nel controllo delle diverse infrastrutture critiche. Tale Comitato non dovrebbe interferire con le politiche di gestione e sicurezza settoriali attuate dai diversi operatori, per le quali già esistono le opportune strutture governative di controllo, ma focalizzare la propria attenzione sugli elementi di interdipendenza il cui controllo sfugge alla gestione dei singoli operatori e travalica i diversi ambiti di competenza. Il Comitato dovrebbe, inoltre, individuare meccanismi per un fattivo confronto con i diversi operatori privati che materialmente gestiscono le diverse infrastrutture. A tal fine, il Gruppo di Lavoro suggerisce la promozione di un **Gruppo di Interesse Nazionale** che raccolga, su base volontaria, i diversi operatori privati e che possa porsi quale interlocutore privilegiato nei confronti del Comitato.

Andrebbe, inoltre, fortemente **stimolata la R&S** sul soggetto, la **formazione** del personale e la **cooperazione internazionale**.

L'entusiasmo, la disponibilità e le competenze evidenziate all'interno del Gruppo di Lavoro da parte di tutti i soggetti coinvolti, fa ritenere che l'Italia, anche sfruttando le esperienze delle altre nazioni, sia in grado di sviluppare in tempi rapidi un'adeguata politica per la protezione delle Infrastrutture Critiche Informatizzate potendo aspirare a giocare un ruolo non secondario a livello Europeo e mondiale su una tematica che sarà di drammatica attualità nel prossimo futuro.

Elenco partecipanti al Gruppo di Lavoro

Coordinatore:
Dott. Vincenzo Merola (Presidenza del Consiglio dei Ministri - Dip. Innovazione e Tecnologie)

Segreteria Tecnica:
Ing. Roberto Setola (Presidenza del Consiglio dei Ministri – Dip. Risorse Strumentali)

Partecipanti (in ordine alfabetico)

Avv. Antonio Amendola (Autorità Comunicazioni)
Dott. Stefano Amore (Min. Giustizia)
Ing. Gian Nicola Belcastro (GRTN)
Dott. Fulvio Berghella (ABI - Euros)
Dott. Sandro Bologna (ENEA-CAMO)
Ing. Maurizio Bonanni (Min. Comunicazioni)
Prof. Danilo Bruschi (Politecnico Milano)
Dott. Guido Caldarelli (INFM)
Dott. Mario Caporale (ASI)
Ing. Alessandro Caroselli (Min. Comunicazioni)
Dott. Alessandro Corona (CASPUR)
Prof. Michele Crudele (Università CAMPUS Biomedico di Roma – Centro ELIS)
Dott.ssa Giovanna Dondossola (CESI)
Ing. Paolo Donzelli (Pres. Cons. Ministri – Dip. Innovazione e Tecnologie)
Dott.ssa Natascia Falcucci (GRTN)
Dott. Silvio Fantin (GRTN)
Dott.ssa Antonella Fasoli (Min. Infrastrutture)
Ing. Luisa Franchina (Min. Comunicazioni)
Ing. Angelo Ferrante (GRTN)
Dott.ssa Maria Cristina Fiorentino (Rete Ferroviaria Italiana)
Ing. Franco Fiumara (Rete Ferroviaria Italiana)
Prof. Dario Forte (Università di Milano DTI Crema)
Prof. Francesco Garofalo (Università di Napoli)
Ing. Fabio Ghioni (Telecom Italia)
Prof. Giulio Iannello (Università CAMPUS Biomedico di Roma)
Dott. Massimiliano Magi Spinetti (ABI)
Ing. Roberto Marcoccio (WIND)
Ing. Massimo Mencaroni (WIND)
Prof. Stefano Panzieri (Università Roma Tre)
Dott. Tommaso Palumbo (Min. Interno - Polizia Postale)
Ing. Andrea Pompili (Telecom Italia)
Ing. Michele Ricciardi (Snam Rete Gas)
Dott.ssa Lilia Rossi (Min. Attività Produttive)
Ing. Alberto Sanna (Ist. H San Raffaele)
Prof. Gian Piero Siroli (Università di Bologna)
Ing. Alberto Stefanini (CESI)
Ing. Gian Franco Tamborrino (Snam Rete Gas)
Prof. Salvatore Tucci (Pres. Cons. Ministri – Dip. Risorse Strumentali - Università Tor Vergata)
Prof. Giovanni Ulivi (Università Roma Tre)
Ing. Loredana Vajano (Autorità Comunicazioni)
Ing. Salvatore Viviano (ASI)

Si ringrazia per la collaborazione:

Ing. Vittoria Allona, Ing. Antonio Serra.

Glossario

Uno dei principali ostacoli che si incontrano ogni qual volta si affrontano problemi multi-disciplinari è quello di avere un vocabolario comune che consenta un'efficace comunicazione superando quelle barriere di incomprensione legate ai differenti significati ed accezione che i medesimi termini sono andati assumendo nei differenti contesti.

Questo glossario ha, pertanto, lo scopo di tentare di costruire un vocabolario comune ai diversi interlocutori su questa tematica così complessa e variegata.

CYBERSPACE: (il termine, coniato dallo scrittore canadese William Gibson, assume un pluralità di significati, per i fini di questo documento esso è definibile come) spazio virtuale, senza riferimenti a nessuna topologia geografica, prodotto dalla interconnessione di computer, reti di telecomunicazioni, applicazioni e dati;

INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT): strumenti ed infrastrutture di calcolo e telecomunicazione, inclusi software applicativo, processi di elaborazione delle informazioni, dati ed informazioni vere e proprie;

INFRASTRUTTURA CRITICA: 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;

INFRASTRUTTURA CRITICA INFORMATIZZATA: infrastruttura critica che utilizza per il suo controllo, o la sua gestione o il suo esercizio una infrastruttura informatica;

INFRASTRUTTURA INFORMATICA: infrastruttura preposta alla trasmissione, memorizzazione e gestione di dati in formato digitale;

INTERDIPENDENZA: relazione funzionale tra due sistemi o infrastrutture attraverso la quale lo stato di ogni infrastruttura è correlato allo stato dell'altra, influenzandolo ed essendone reciprocamente influenzato;

MINACCIA: possibile causa che può arrecare danni ad un'infrastruttura;

PROTEZIONE DELLE INFRASTRUTTURE CRITICHE (CIP): misure prese per assicurare i sistemi e le risorse la cui distruzione o temporanea indisponibilità potrebbero produrre un impatto debilitante sul benessere sociale, economico e la sicurezza nazionale di un paese;

PROTEZIONE DELLE INFRASTRUTTURE CRITICHE INFORMATIZZATE (CIIP): azioni tese ad innalzare il livello di sicurezza, affidabilità e correttezza di tutte quelle infrastrutture critiche che utilizzano, in tutto o in parte, una qualunque infrastruttura informatica per il loro monitoraggio, la

loro gestione o il loro controllo; includendo, naturalmente, nel novero delle infrastrutture critiche anche quelle informatiche e specificatamente Internet.

RISCHIO: impatto negativo complessivo di un evento, che include sia la probabilità che le conseguenze dell'evento. Nel caso di infrastrutture critiche informatizzate, il rischio sussiste sia a livello fisico che a livello informatico con influenza reciproca dei due settori;

TCP/IP (Transmission Control Protocol/Internet Protocol): protocollo di comunicazione adottato in Internet per la trasmissione di dati e messaggi tra computer in rete;

SCADA (Supervisory Control and Data Acquisition): sono i sistemi utilizzati per il monitoraggio ed il controllo degli impianti industriali e le infrastrutture distribuite geograficamente sul territorio;

VULNERABILITA' DELLE INFRASTRUTTURE CRITICHE: predisposizione del sistema complessivo in oggetto ad essere attaccato e danneggiato in relazione anche alla capacità di mantenere una funzionalità più o meno limitata in situazioni di emergenza. Concetto legato alla interdipendenza tra infrastrutture che può indurre vulnerabilità per effetto domino.

Risoluzione n. 58/199 delle Nazioni Unite

Nel seguito si riporta la risoluzione adottata il 23 dicembre 2003 dalla 78ma assemblea generale delle Nazioni Unite ed avente per oggetto la "creazione di una cultura globale della sicurezza del cyberspace e la protezione delle infrastrutture critiche informatizzate" http://www.un.org/Depts/dhl/resguide/r58.htm

United Nations A/RES/58/199

General Assembly

Resolution adopted by the General Assembly

[*on the report of the Second Committee (A/58/481/Add.2)*]

58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures

The General Assembly,

Recalling its resolutions 57/239 of 20 December 2002 on the creation of a global culture of cybersecurity, 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on establishing the legal basis for combating the criminal misuse of information technologies, and 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002 on developments in the field of information and telecommunications in the context of international security,

Recognizing the growing importance of information technologies for the promotion of socio-economic development and the provision of essential goods and services, the conduct of business and the exchange of information for Governments, businesses, other organizations and individual users,

Noting the increasing links among most countries' critical infrastructures — such as those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health — and the critical information infrastructures that increasingly interconnect and affect their operations,

Recognizing that each country will determine its own critical information infrastructures,

Recognizing also that this growing technological interdependence relies on a complex network of critical information infrastructure components,

Noting that, as a result of increasing interconnectivity, critical information infrastructures are now exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns,

Noting also that effective critical infrastructure protection includes, inter alia, identifying threats to and reducing the vulnerability of critical information infrastructures, minimizing

damage and recovery time in the event of damage or attack, and identifying the cause of damage or the source of attack,

Recognizing that effective protection requires communication and cooperation nationally and internationally among all stakeholders and that national efforts should be supported by effective, substantive international and regional cooperation among stakeholders,

Recognizing also that gaps in access to and the use of information technologies by States can diminish the effectiveness of cooperation in combating the criminal misuse of information technology and in creating a global culture of cybersecurity, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Recognizing further the importance of international cooperation for achieving cybersecurity and the protection of critical information infrastructures through the support of national efforts aimed at the enhancement of human capacity, increased learning and employment opportunities, improved public services and better quality of life by taking advantage of advanced, reliable and secure information and communication technologies and networks and by promoting universal access,

Noting the work of relevant international and regional organizations on enhancing the security of critical information infrastructures,

Recognizing that efforts to protect critical information infrastructures should be undertaken with due regard for applicable national laws concerning privacy protection and other relevant legislation,

1. *Takes note* of the elements set out in the annex to the present resolution for protecting critical information infrastructures;

2. *Invites* all relevant international organizations, including relevant United Nations bodies, to consider, as appropriate, inter alia, these elements for protecting critical information infrastructures in any future work on cybersecurity or critical infrastructure protection;

3. *Invites* Member States to consider, inter alia, these elements in developing their strategies for reducing risks to critical information infrastructures, in accordance with national laws and regulations;

4. *Invites* Member States and all relevant international organizations to take, inter alia, these elements and the need for critical information infrastructure protection into account in their preparations for the second phase of the World Summit on the Information Society, to be held in Tunis from 16 to 18 November 2005;

5. *Encourages* Member States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity;

6. *Stresses* the necessity for enhanced efforts to close the digital divide, to achieve universal access to information and communication technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building, in particular to developing countries, especially the least developed countries, so that all States may

benefit fully from information and communication technologies for their socio-economic development.

Annex

Elements for protecting critical information infrastructures

1. Have emergency warning networks regarding cyber-vulnerabilities, threats and incidents.
2. Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.
3. Examine infrastructures and identify interdependencies among them, thereby enhancing the protection of such infrastructures.
4. Promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures.
5. Create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.
6. Ensure that data availability policies take into account the need to protect critical information infrastructures.
7. Facilitate the tracing of attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other States.
8. Conduct training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack, and encourage stakeholders to engage in similar activities.
9. Have adequate substantive and procedural laws and trained personnel to enable States to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other States, as appropriate.
10. Engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.
11. Promote national and international research and development and encourage the application of security technologies that meet international standards.

Bibliografia

Nel seguito sono riportate alcune pubblicazioni significative sull'argomento delle CIIP. Per facilitare la consultazione, i documenti sono stati suddivisi in tre gruppi comprendenti i documenti elaboratati da soggetti istituzionali, i documenti di inquadramento della problematica e le pubblicazioni di carattere più propriamente scientifico.

I diversi documenti sono ordinati alfabeticamente rispetto al nome dell'istituzione che lo ha prodotto ovvero rispetto al suo primo autore.

Documenti Istituzionali

Canadian National Contingency Planning Group, *Canadian Infrastructures and their Dependencies*, marzo 2002.

Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, *Threats to Canada's Critical Infrastructure*, TA03-001, 12 marzo 2003.

EC Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "*Network and Information Security: Proposal for a European Policy Approach*", COM(2001)298 final, 06.06.2001.

EC *Council Resolution on a common approach and specific actions in the area of network and information security* 2002/C 43/02, 28.01.2002.

EC *Council Resolution on a European approach towards a culture of network and information security* 2003/C 48/01, 18.02.2003.

EC Proposal for a Regulation of the European Parliament and of the Council Establishing the *European Network and Information Security Agency*, COM(2003)63 final 2003/0032(COD), 11.02.2003.

EC Communication from the Commission to the Council, the European Parliament, the European economic and social committee and the committee of the regions "*Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*", COM(2000)890 final, 26.01.2001.

EC Proposal for a *Council Framework Decision on attacks against information system* COM(2002)73 final, 19.04.2002.

CEER, Council of European Energy Regulators, *Quality of Electricity Supply: Initial Benchmarking on Actual Levels, Standards and Regulatory Strategies,* Aprile 2001, www.autorita.energia.it

CEIDS, Consortium for Electric Infrastructure to Support a Digital Society, *The Cost of Power Disturbances to Industrial and Digital Economies Companies*, rapporto EPRI n. 1006274, Exec. Summary http://ceids.epri.com/ceids/Resources/InfoKit.jsp

NATO CCMS, *Vulnerability of the Interconnected Society*, Final Report, ottobre 2002.

NATO/EAPC, *Critical Infrastructure Protection – Concept Paper*, Civil Protection Committee (CPC) in EAPC Format, working paper, 2 luglio 2003.

O.N.U. Risoluzione 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. http://www.un.org/Depts/dhl/resguide/r58.htm

U.S. Critical Infrastructure Assurance Office, *Practices for Securing Critical Information Assets*, gennaio 2000.

U.S. President's Commission on Critical Infrastruction Protection, *Critical Foundations: Protecting America's Infrastructures*, 1997, http://www.ciao.gov.

U.S. *Presidential Decision Directive 63*, 1998, http://www.fedcirc.gov/library/legislation/presDecDirective63.html.

U.S. *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*, febbraio 2003, http://www.whitehouse.gov/pcipb/physical.html

U.S. *The National Strategy to Secure Cyberspace*, febbraio 2003; http://www.whitehouse.gov/pcipb

U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, Report to the Committee on Energy and Commerce, House of Representatives, GAO-03-233, febbraio 2003, www.gao.gov .

U.S. Department of Energy, *Maintaining Reliability in a Competitive U.S. Electricity Industry: Final Report of the Task Force on Electric System Reliability*, settembre 1998, Secretary of Advisor Board, Washington, DC. www.eia.doe.gov/cneaf/electricity/page/pubs.html

U.S. – Canada Power System Outage Task Force, *Interim Report: Causes of August 14th Blackout in the United States and Canada*, novembre 2003.

Documenti di inquadramento della problematica

ACIP (EC Project IST-2001-37257), *Advanced Modelling and Simulation Methods and Tools for Critical Infrastructure Protection*, 14 gennaio 2003

M. Amin, *Modelling and Control of Complex Interactive Networks*, IEEE Control System Magazine, pp. 22-27, febbraio 2002.

Z. Baird, J. Barksdale, P. Zelikow, *Protecting America's Freedom in the Information Age*, A Report of the Markle Foundation Task Force, ottobre 2002.

S. Bologna, *Salvaguardia di infrastrutture energetiche complesse, Rivista Automazione e Strumentazione*, pp. 129-133, marzo 2002.

A. Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection – Defending the U.S. Homeland,* Center for Stragic and International Studies, Washington, 2002.

M. Cogwell (Ed.), Critical Infrastructres, Nova Science Publishers, New York, 2003.

EPRI, *Electricity technology Roadmap: 1999 summary and synthesis*, EPRI, Palo Alto, Ca., Rep C1-112677-V1.

DDSI (Dependability Development Support Initiative EC Project IST-2000-29202), *Summary of DDSI findings*, novembre 2002.

D. Denning, *Information Warfare and Security*, Addison-Wesley, 1998.

B. Ferraris di Celle (Ed.), *Le nuove Frontiere della Sicurezza Informatica, il meglio della rivista ICT Security – Infrastrutture Critiche*, a cura di A. Leggio, Nuovo Studio Tecna, ottobre 2003.

J. Green, *The Myth of Cyberterrorism*, Washington Monthly, novembre 2002.

I3P Institute for Information Infrastructure Protection, *Cyber Security Research and Development Agenda*, gennaio 2003.

E. Luiijf, H. Burger, M. Klaver, *Critical Infrastructure Protection in The Netherlands: A Quick-scan*, EICAR Conference, 2003.

V. Merola, R. Setola, *La Protezione delle Infrastrutture Critiche Informatizzate, un nuovo paradigma per la sicurezza informatica*, ICT Security, febbraio 2004.

V. Merola, R. Setola, S. Tucci, *L'attività svolta dal Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate*, Atti Convegno nazionale Valutazione e Gestione del Rischio, Pisa 19-21 ottobre 2004.

R. Marsh, ed., *Critical Foundations: Protecting America's Infrastructure: The Report of the Presidential Commission on Critical Infrastructure Protection,* Goverment Printing Office, Washington, D.C., 1997.

J. Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, Report for Congress RL30153, The Library of Congress, 4 febbraio 2002.

J. Moteff, C. Copeland, J. Fisher, *Critical Infrastructures: What Makes an Infrastructure Critical ?*, Report for Congress RL31556, The Library of Congress, 21 gennaio 2003.

J. Moteff, G. Stevens, *Critical Infrastructure Information: Disclosure and Homeland Security* Report for Congress RL31547, The Library of Congress, 29 gennaio 2003.

D. Mussington, *Concept for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development*, RAND Science and Technology Policy Institute, 2002.

ÖCB, The Swedish Agency for Civil Emergency Planning, *International CEP Handbook 2002*, Civil Emergency Planning in NATO/EAPC countries, 2002.

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

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

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

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

A. Sanna, *L'Evoluzione delle Tecnologie e dei Servizi per la salute e il benessere del Cittadino*, ICT Security – Marzo 2003.

R. Setola. *La Protezione delle Infrastrutture Critiche Informatizzate*, Automazione e Strumentazione, pp. 27 – 35, luglio 2003.

R. Setola, *La Protezione delle Infrastrutture Critiche Informatizzate: iniziative in atto*, Atti del Convegno Scientifico Nazionale "Sicurezza nei Sistemi Complessi", Bari, 16–17 ottobre 2003.

D. Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism*, The McGraw-Hill, 2003

A. Wenger, J. Metzger, M. Dunn (edited by) *International CIIP Handbook*, ETH, the Swiss Federal Institute of Technology Zurich, 2002.

A. Wenger, J. Metzger, M. Dunn, I. Wigert *International CIIP Handbook 2004*, ETH, the Swiss Federal Institute of Technology Zurich, 2004.

Pubblicazioni Scientifiche

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

M. Amin, *Toward Self-Healing Infrastructure Systems*, IEEE Computer, agosto 2000.

M. Amin, *Toward Self-Healing Energy Infrastructure Systems*, IEEE Computer Applications in Power, gennaio 2001.

P. Anderson, I. Geckil, *Northeast Blackout Likely to Reduce US Earnings by $6.4 Bilion*, Anderson Economic Group, AEG Working Paper 2003-2, 19 agosto 2003.

C. Balducelli, S. Bologna, *Agent Based Architecture to improve survivability of Large Comnplex Critical Infrastructures*, Proceedings of 9th International Emergency Management Society Conference, Waterloo, ON, Canada, 14-17 maggio 2002.

C. Balducelli, *Modelling Attack Scenarios against Software Intensive Critical Infrastructures*, Proceedings of 10th International Emergency Management Society Conference, Sophia-Antipolis, Provence, France, 3-6 giugno 2003.

S. Bologna, F. Lambiase, E. Ratto, *Large Scale Electric Power Distribution and Telecommunication Systems Survivability*, Proceedings of the IEEE Computer Society on Information Survivability Workshop (ISW 2000), Boston, 24-26 ottobre 2000.

S. Bologna, *Modelling and Simulation of Critical Infrastructures and their Interdependencies: Linking Complex Systems and Interacting Agents Approaches*, Workshop EU-US Collaboration on Dependability of Infrastructures & Interdependencies, National Conference Center, Lansdowne, VA, USA, 23-24 settembre 2002.

S. Bologna, C. Balducelli, G. Dipoppa, G. Vicoli, *Dependability and Survivability of Large Complex Critical Infrastructures*, Prooceedings of SAFECOMP2003, Edinburg, England, 22-25 settembre 2003.

S. Bologna, T. Beer: *Integrated Approach to Modelling, Simulation and Analysis of Large Complex Critical Infrastructures*, Workshop "Critical Infrastructure Protection – Status and Perspectives", Frankfurt, 29-30 settembre 2003.

S. Bologna, C. Balducelli, G. Dipoppa, A. M. Gadomski, G. Vicoli, *SAFEGUARD: una piattaforma multi-agente per estendere le capacità di sopravvivenza di infrastrutture critiche sottoposte ad attacco informatico*, Atti del Convegno Scientifico Nazionale "Sicurezza nei Sistemi Complessi", Bari, 16–17 ottobre 2003.

S. Bologna and G. Vicoli, *Interacting Agentes Modelling and Simulation of Large Complex Critical Infrastructures Interdependencies*, Italian Society for Computer Simulation Conference 2003 (ISCS 03), Cefalù (PA), 27-29 novembre 2003.

E. Casalicchio, R. Setola, S. Tucci, *A survey on Modelling and Simulation techniques for Interdependent Critical Infrastructures*, Italian Society for Computer Simulation Conference 2003 (ISCS 03), Cefalù (PA), 27-29 novembre 2003.

R. Carlson, *Sandia SCADA Program High-Security SCADA LDRD Final Report*, Sandia Report SAND2002-0729, aprile 2002.

P. Crucitti, V. Latora and M. Marchiori, *A model for cascading failures in complex networks*, Italian Society for Computer Simulation Conference 2003 (ISCS 03), Cefalù (PA), 27-29 novembre 2003.

G. Dondossola et al., *A methodology for the Evaluation of the Security Risks of Internet-based Remote Control Applications of Utilities*, Workshop "Critical Infrastructure Protection – Status and Perspectives", Frankfurt, 29-30 settembre 2003.

G. Dondossola, S. Donatelli, *Modellazione delle strategie di tolleranza delle anomalie ICT in ambito elettrico*, Italian Society for Computer Simulation Conference 2003 (ISCS 03), Cefalù (PA), 27-29 novembre 2003.

R. Ellison., Fisher D., Linger R., Lipson H, Longstaff T., Mead N. *Survivable Systems: An Emerging Discipline*. CERT – SEI, CMU. Pittsburgh USA, 1999.

G. Iannello, R. Setola, *Evolution Control a Strategy to Mitigate Vulnerability of Interdependent Critical Infrastructures*, Fourth European Dependable Computing Conference (EDCC-4), Toulouse (Francia), ottobre 2002.

V. Merola e R. Setola, *Il ruolo dei sistemi di controllo e monitoraggio nel cotesto della protezione delle Infrastrutture Critiche Informatizzate*, Atti del Convegno Scientifico Nazionale "Sicurezza nei Sistemi Complessi", Bari, 16–17 ottobre 2003.

G. Mauri e G. Dondossola, *Le vulnerabilità informatiche nell'automazione delle rete elettrica*, rivista Energia Elettrica, numero 5/6, volume 78, settembre-ottobre 2001.

North American Electric Reliability Council, *SQL Slammer Worm lessons learned for consideration by the Electricity Sector*, 20 giugno 2003.

P. Oman, E. Schweitzer, & J. Roberts, *Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions,* Paper #1, Western Power Delivery Automation Conference, 10-12 aprile, Spokane, (WA), 2001.

S. Panzieri, I. Scarano, R. Setola, *Vulnerabilità informatica dei sistemi SCADA connessi alle reti pubbliche,* Atti Convegno nazionale Valutazione e Gestione del Rischio, Pisa 19-21 ottobre 2004.

S. Panzieri, R. Setola, *Vulnerabilità indotte dal Cyberspace nei sistemi di monitoraggio e controllo,* Atti Convegno nazionale ENERSIS 2004, 1-2 aprile 2004.

A. Reka, A. Barabasi, *Statistical Mechanics of Complex Networks*, Review of Modern Physics, 74, 47, 2002.

D. Reinrmann, J. Weber, *Analysis of Critical Infrastructures: The ACIS methodology*, Critical Infrastructure Protection (CIP) Workshop, Frankfurt, 29-30 settembre, 2003.

A. Sanna, *Vulnerabilities of Communication Infrastructures for Healthcare*, Facing Vulnerabilities of Interdependent Infrastructures, a European Conference on partnership in research and development – CESI, Milan (Italy), November 21, 2001.

R. Setola, G. Ulivi, *Modelling Interdependent Critical Infrastructure*, Recent Advances in Intelligent Systems and Signal Processing, in Electrical and Computer Eng. Series, Mastorakis, N. E., et al. editors, WSEAS press, ISBN 960-8052-87-4, pp. 366 – 372, 2003.

R. Setola, G. Ulivi, *A Fuzzy Modelling for Interdependent Infrastructures*, Italian Society for Computer Simulation Conference 2003 (ISCS 03), Cefalù (PA), 27-29 novembre 2003.

S. Strgatz, *Exploring complex networks*, Nature, vol. 410, pp. 268-276, 8 marzo 2001.

G.P. Siroli, *Computer a prova di Hacker*, Le Scienze, pp. 68-73, aprile 2003.

A. Stefanini ed E. Ciapessoni *La vulnerabilità del sistema elettrico come infrastruttura interdipendente*, Rivista dell'AEI, Assoc. Elettrotecnica ed Elettronica Italiana, vol. 88, Novembre 2001.

Y. Tu, *How robust is the Internet ?,* Nature, vol. 46, pp. 353-354, 27 luglio 2000.

Tutti i link presenti in questo documento sono stati verificata al 8 marzo 2004.