L'ATTIVITÀ SVOLTA DAL GRUPPO DI LAVORO SULLA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE INFORMATIZZATE

Vincenzo Merola*, Roberto Setola°, Salvatore Tucci^
* Presidenza del Consiglio dei Ministri, Dip. Innovazione e Tecnologie, via Po 14, 00198 Roma
° Università CAMPUS Biomedico di Roma, Facoltà di Ingegneria, via E. Longoni 83, 00155 Roma
^ Presidenza del Consiglio dei Ministri, Dip. Risorse Strumentali, via Mercede 96, 00186 Roma

r.setola@unicampus.it

SOMMARIO

La necessità di soddisfare i nuovi bisogni che caratterizzano le società moderne in termini di disponibilità, accessibilità ed economicità di un ampio insieme di servizi e beni impone da un lato un utilizzo estensivo delle diverse infrastrutture necessarie per la loro erogazione e dall'altro un ricorso sempre più massiccio alle tecnologie proprie della Società dell'Informazione al fine di garantire il corretto controllo e la corretta gestione dei diversi processi produttivi e distributivi.

Ciò, unito al fatto che l'apertura dei mercati ha aumentato il numero e la specializzazione dei diversi soggetti che operano nei singoli settori, comporta un mutato quadro tecnologico e socio-economico, caratterizzato da un concetto nuovo: interdipendenza.

Infatti ogni singolo operatore gestisce direttamente solo una piccola porzione dell'insieme di attività e risorse necessarie per l'erogazione di un qualunque bene o servizio. Questo comporta, in particolare, un crescendo livello di accoppiamento fra le infrastrutture al punto che un guasto (di natura accidentale o dolosa) può facilmente propagarsi attraverso le diverse infrastrutture amplificando i suoi effetti negativi.

Queste considerazioni, unite al fatto che il benessere e la sicurezza della nazione dipendono sempre di più dal corretto funzionamento di queste infrastrutture, ha portato alla costituzione di un apposito gruppo di Lavoro presso la Presidenza del Consiglio dei Ministri con lo scopo di iniziare una primissima analisi della realtà italiana individuando priorità ed obiettivi, i cui principali risultati sono riportati nel seguito.

2. INTRODUZIONE

L'appellativo "Protezione delle Infrastrutture Critiche informatizzate" si riferisce ad una tematica recente, che in genere si fa risalire al 1996 con l'istituzione della *Presidential Comission on Critical Infrastruction Protection* (PCCIP) ad opera del presidente Clinton. In realtà la problematica trae la sua origine da una serie di ragioni tecnologiche, sociali ed economiche, che hanno comportato una trasformazione dell'assetto infrastrutturale delle singole nazioni passando da una strutturazione infrastrutturale basata su una serie di operatori verticalmente integrati e sostanzialmente autonomi, ad una in cui operano una pluralità di operatori (ognuno dei quali focalizzato su uno specifico core-business), che necessitano per la propria operatività di interagire con una pluralità di soggetti.

Questo aumenta in modo esponenziale le **interdipendenze** esistenti fra le infrastrutture e quindi la vulnerabilità complessiva del sistema in quanto un qualunque guasto (di natura accidentale o dolosa) può facilmente propagarsi attraverso le diverse infrastrutture amplificando le proprie conseguenze fino ad affliggere utenti anche remoti, sia geograficamente che logicamente, rispetto alla causa originale del guasto.

In questo scenario sono le tecnologie dello ICT (Information and Communication Technologies), con la loro capacità di diffusione e penetrazione, la maggiore causa delle interdipendenze, oltre che delle minacce stante la limitata conoscenza che ancora possediamo del così detto *cyberspace*.

Infatti si deve registrare come la necessità di sfruttare al massimo le singole infrastrutture impone l'adozione di sistemi di controllo sempre più sofisticati e complessi (e quindi un maggior utilizzo delle tecnologie dello ICT) al fine di poter operare in regimi molto prossimi a quelli di saturazione delle singole infrastrutture. Questo comporta, oltre ai problemi di accoppiamento precedentemente evidenziati, anche il fatto che un qualunque guasto, se non gestito in modo adeguato, può facilmente trasformarsi in un evento catastrofico ingigantendosi con un effetto valanga, come occorso nel caso del black-out che ha afflitto la costa orientale americana il 14 agosto 2003.

Il rapporto intermedio della commissione congiunta US-Canada, istituita per far luce sulle cause del black-out, ha evidenziato infatti che la causa scatenante va ricercata nel contatto fra un albero ed una linea a 345 kV [1]. 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 informatico 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, resero 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.

Un altro esempio emblematico è quello occorso il 2 gennaio 2004 quando un guasto all'impianto di condizionamento di un importante nodo Telecom di Roma, con il consequenziale allagamento dello stesso, ha provocato non solo la paralisi del traffico telefonico fisso e mobile di un'ampia area di Roma per oltre 6 ore (e che ha coinvolto anche altri gestori di telefonia), ma anche problemi a causa della mancanza di collegamento telematico a circa 5.000 filiali bancarie ed a oltre 3.000 uffici postali oltre che la paralisi del 75% dei banchi di accettazione dell'aeroporto di Fiumicino con le ovvie conseguenze sul trasporto aereo.

C'è, inoltre, da considerare che le infrastrutture tecnologiche, per la loro rilevanza per le Società moderne, possono rappresentare un possibile obiettivo per azioni terroristico, o comunque criminose. Azioni che possono essere perpetrate sia con metodi tradizionali che tramite il cyberspace o con attacchi congiunti (i così detti *swarming attacks*, ritenuti, per altro, dagli analisti i più probabile e pericolosi [2] con i quali si ipotizzano scenari ove 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).

Tutto ciò impone la necessità di definire strategia, metodi, tecnologie in grado di innalzare il livello di robustezza complessiva del "*sistema di sistemi*" composto dalle diverse infrastrutture tecnologiche interdipendenti [3].

L'argomento è talmente complesso che si può affermare che allo stato non disponiamo di strumenti di analisi sufficientemente sofisticati per poter gestire la sua complessità ed in grado di fornire una visione unitaria della realtà [4].

A tal proposito le diverse nazioni hanno attivato appostiti programmi tesi a sensibilizzare i diversi soggetti pubblici e privati coinvolti circa la reale natura e pericolosità della problematica, e tali da favorire un coordinamento fra i molteplici soggetti coinvolti (per una panoramica sulle diverse iniziative si rimanda a [5]). Tali iniziative, inoltre, presentano una particolare attenzione agli aspetti di cooperazione internazionale stante la natura sovra-nazionale di molte infrastrutture, Internet in testa (come evidenziato anche dalla recente risoluzione adottata dall'Assemblea Generale delle Nazioni Unite [6]) e sugli aspetti di ricerca e sviluppo.

In Italia anche se ancora non è stato individuato un soggetto governativo con il compito di gestire i diversi aspetti sottesi alla problematica della Protezione delle Infrastrutture Critiche Informatizzate (CIIP) diversi organismi hanno iniziano ad attivare specifiche azioni. Nel seguito è illustrata l'attività condotta dal Gruppo di Lavoro Protezione delle Infrastrutture Critiche Informatizzate (GdL) istituito presso il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.

3. IL GRUPPO DI LAVORO SULLA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE INFORMATIZZATE

Sebbene nei diversi paesi industrializzati il tema delle CIIP abbia acquistato, soprattutto a valle degli eventi dello 11 settembre 2001, una rilevanza strategica con la costituzione di apposite strutture di coordinamento quali il *Department of Homeland Security* negli USA (che, per altro, ha sostituito ed inglobato il CIAO e NIPC, www.DHS.gov/pcii), il SEMA in Svezia, il *National Infrastructure Security Co-ordination Centre* in Gran Bretagna (NISCC, http://www.niscc.gov.uk/), il *BSI* in Germania (www.bsi.bund.de) o il *Office of Critical Infrastructure Protection and Emergency Preparedness* in Canada (di recente confluito nel *Minister of Public Safety and Emergency Preparedness*, www.ocipep.gc.ca), ecc. in Italia ancora non è maturata una adeguata sensibilità politica sulla tematica.

Per migliorare questa situazione, nel marzo del 2003, è stato costituito presso il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri un apposito Gruppo di Lavoro

(GdL) aperto alla partecipazione dei soggetti interessati al tema ed il cui scopo principale era quello di svolgere un'azione di inquadramento e di sensibilizzazione sulla questione.

Seguendo una prassi inusuale per la P.A., il GdL è andato aggregando strada facendo i soggetti attenti alla problematica presenti nei diversi dicasteri ed enti coinvolti nella problematica. In tal modo al GdL hanno potuto contribuire sia soggetti istituzionali che operatori privati oltre che esponenti del mondo dell'accademia e della ricerca, un cui parziale elenco è riportato nella Tabella 1.

ABI	GRTN	Min. Infrastrutture e Trasporti	Sogin
ASI	Rete Ferroviaria Italiana	Min. Attività Produttive	Univ. Roma Tre
CESI	SNAM Rete Gas	Min. Comunicazioni	Univ. Roma Tor Vergata
Autorità Comunicazioni	Telecom Italia	Min. Giustizia	Univ. CAMPUS Biomedico
ENEA	WIND	Min. Interno - Polizia Postale	Univ. Bologna

Tabella 1: Elenco (parziale) dei soggetti coinvolti nell'attività del GdL.

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.

Infatti 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, stante la natura fortemente interdisciplinare di questa problematica che richiede il coinvolgimento di soggetti operanti in una pluralità di campi.

Il termine **Protezione delle Infrastrutture Critiche Informatizzate** indica 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.

Dove per **Infrastrutture Critiche** si intende il 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

Tale approccio non va a sostituirsi a nessuna delle iniziative attualmente in atto per quel che riguarda la protezione delle singole infrastrutture. Infatti, fermo restando 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.

Il GdL si è posto quali obiettivi:

- Stimolare in Italia un'attenzione sulla problematica (azioni di sensibilizzazione e awarness)
- Favorire la comprensione del problema CIIP partendo dai partecipanti al GdL (azione culturale)
- Evidenziarne la complessità: le singole infrastrutture sono sistemi complessi, il **sistema di sistemi** che considera anche le loro interdipendenze reciproche ha un livello di complessità di ordini di grandezza maggiore
- Far comprendere la necessità di cooperazione: Le CIIP non riguardano direttamente le politiche di gestione delle singole infrastrutture, ma operano sugli elementi di interdipendenza
- Aggregare intorno ad un unico progetto i diversi soggetti interessati alla problematica
- Rappresentare un Forum di confronto per le diverse esigenze, ed un luogo di condivisione delle esperienze e delle best-practices

In questo spirito il GdL si è prodotto per accrescere a tutti i livelli una maggiore attenzione sulla tematica, per incoraggiare e promuovere la ricerca scientifica sull'argomento e ponendosi quale punto di raccordo nei confronti delle iniziative internazioni in atto.

In particolare oltre a rappresentare il punto di contatto nell'ambito del ***International CIIP Directory*** attuato in ambito G8, ha contribuito alla stesura degli 11 principi (riportati in appendice) avvenuta nel marzo del 2003 a Parigi e ratificati nella riunione dei Ministri dell'Interno e della Giustizia del G8 svoltasi nel maggio del 2003. Principi che hanno, per altro, ispirato anche la risoluzione n. 58/199 ***"Creation of a global culture of cybersecurity and the protection of critical information infrastructures***" adottata dalla 58ma Assemblea Generale delle Nazioni Unite svoltasi il 23 dicembre 2003 [6].

3.1 Il Rapporto del GdL – La realtà Italiana

L'attività svolta nel primo anno di lavoro dal GdL è stata sintetizzata nel documento "Protezione delle Infrastrutture Critiche Informatizzate – la realtà italiana" (vedi Figura 1).

Figura 1: Rapporto prodotto dal Gruppo di Lavoro istituito presso il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri

In tale documento, che ha una distribuzione limitata i soli soggetti competenti, oltre ad un'introduzione ed inquadramento della problematica viene esaminata la situazione italiana relativamente ad alcune delle infrastrutture critiche, ed in particolare: l'infrastruttura elettrica, le reti informatiche, le reti di telecomunicazione, l'infrastruttura per il trasporto del gas naturale liquefatto, la rete ferroviaria, la rete viaria, i circuiti bancari e finanziari, i circuiti sanitari, gli impianti nucleari e la navigazione satellitare.

Quello che emerge da questa analisi è che le diverse infrastrutture sono caratterizzate da una crescente complessità intrinseca che impone un sempre maggior utilizzo delle tecnologie informatiche per gestire ed ottimizzare tutte le risorse. Questo, però, comporta un aumento della vulnerabilità indotta sia a causa delle minacce provenienti dal cyberspace, sia a causa dell'aumentata interdipendenza esistente fra le diverse infrastrutture, oltre che dalla presenza di alcuni elementi critici presenti nelle infrastrutture stesse che, a causa delle predette interdipendenze, vengono a configurarsi come vulnerabilità per l'intero sistema.

Il documento passa quindi a prendere in rassegna le diverse realtà costituite nei vari paese ed ad esaminare i diversi soggetti che in Italia si occupano del problema della Protezione delle Infrastrutture Critiche Informatizzate, ed in particolare:

- **Ministero dell'Interno – Polizia Postale e delle Comunicazioni**. Questa specialità della Polizia ha il compito di contrastare il crimine ad alta tecnologia ed è articolato sul'intero territorio nazionale nell'ambito della quale operano 2000 uomini altamente specializzati e formati. Nell'ambito della Protezione delle Infrastrutture Critiche, la Polizia Postale ha attivato specifiche convenzioni con i principali operatori al fine di facilitare lo scambio di informazioni e la tempestività di intervento in presenza di azioni criminose. Inoltre è in fase di allestimento un centro operativo deputato proprio alla protezione delle infrastrutture critiche;
- **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

- **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.

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.

- ❖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.

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 Governo.

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.

4. CIIP E MILLENIUM BUG (Y2K)

Negli anni immediatamente precedenti la fine del millennio, si è assistito ad un gigantesco intervento sul software esistente nel mondo teso a porre rimedio al cosiddetto *millenium bug*, ovvero alla codifica dell'anno fatto con le sole due cifre (indicato, per questo, anche come problema Y2K).

Questa esperienza è stata caratterizzata da una "entusiasmante" azione di cooperazione e sensibilizzazione internazionale che ha portato all'attenzione dell'opinione pubblica una problematica di carattere prettamente tecnica. Ciò ha consentito di rendere disponibili le risorse necessarie per porre rimedio al problema, tanto è vero che nel passaggio al nuovo millennio non è successo in pratica nulla al punto che alcuni commentatori si sono spinti fino a ritenere esagerati ed in parte infondati i timori in precedenza paventati.

A fianco di questo sforzo di tipo organizzativo e propagandistico, c'è da sottolineare che la problematica tecnica in se stessa era sostanzialmente semplice, perfettamente conosciuta e delineata.

Alcuni osservatori [7] hanno formulato di poter affrontare il problema delle CIIP con le medesime strategie utilizzate per il *millenium bug*, "recuperando" strumenti ed organizzazioni messi a punto in occasione di quell'evento.

Purtroppo, sebbene sarebbe auspicabile realizzare un'aggregazione di forze paragonabili a quelle messe in campo per il *millenium bug*, le soluzioni allora adottate risultano non utilizzabili essendo completamente diversa la natura della problematica [8]. Infatti, il problema delle CIIP è soprattutto un problema di tipo tecnologico-culturale, il problema stesso non è chiaro, i sui contorni sono molto sfumati, le cause scatenanti ignote e, soprattutto, sono ignote le soluzioni da utilizzare.

Nella Tabella 2 sono paragonate fra loro alcune caratteristiche dei due problemi. Dall'analisi della tabella si evidenzia, immediatamente, la maggiore complessità del problema CIIP e la natura completamente diversa di questa problematica rispetto al *millenium bug*. In particolare l'ultima riga della tabella rappresenta uno dei fattori di maggiore differenziazione fra i due problemi.

	Y2K	***CIIP***
Aspetto tecnico	Semplice	Complesso
Sorgente del problema	Nota e singola	Ignote, multiple e concorrenti
Collocazione temporale del problema	Un unico evento la cui collocazione temporale era conosciuta in anticipo	Possono verificarsi più eventi, anche concomitanti, la cui successione e collocazione temporale è impredicibile
Natura del problema	Nota con esattezza, di tipo accidentale (non dolosa) e legata esclusivamente al software	Può essere di natura più disparata, sia di tipo accidentale che dolosa, può generarsi in una qualunque componente delle diverse infrastrutture tecnologiche
Strategie d'azione per rimuovere il problema	Definite, semplici e ben note. Il problema era solo di carattere implementativo	Sconosciute
Rapporto con l'innovazione tecnologica	L'adozione di software commerciale dell'ultima generazione rappresentava una valida soluzione per la problematica	Non esiste alcuna tecnologia che garantisca la soluzione del problema

Tabella 2. Confronto fra la problematica del *millenium bug* (Y2K) e quella della Protezione delle Infrastrutture Critiche Informatizzate (CIIP).

Il *millenium bug* era un problema legato all'utilizzo, in genere per ragioni di compatibilità nei confronti di un patrimonio informatico preesistente, di soluzioni nelle quali persisteva il residuo di una scelta

tecnologica effettuata agli albori dell'informatica. Questo ha configurato il *millenium bug* come un problema sostanzialmente di ammodernamento con l'abbandono dell'arcaica specifica. Naturalmente la complessità della problematica era legata alla vastità del software su cui si doveva intervenire caratterizzato, spesso, dalla presenza di diverse stratificazioni operate durante il corso degli anni con tecniche non sempre ortodosse e con una pressoché costante carenza di documentazione tecnica precisa.

Di tutt'altra natura è, invece, il problema delle CIIP. È l'innovazione tecnologica stessa che ha, se non proprio creato, certamente enfatizzato il problema. Come in precedenza evidenziato, fino a qualche decennio fa, le diverse infrastrutture operavano come sistemi autonomi e questo riduceva di molto i problemi connessi con la possibile propagazione di guasti a cascata. La necessità/volontà di una più efficace condivisione delle informazioni, con il conseguente maggior utilizzo delle tecnologie ICT, ha aumentato, invece, esponenzialmente i punti di contatto esistenti fra le diverse infrastrutture amplificando a dismisura i problemi di vulnerabilità legati proprio alla forte interdipendenza reciproca che si è venuta a creare.

5. G8 PRINCIPLES FOR PROTECTING CRITICAL INFORMATION INFRASTRUCTURES

Nel seguito sono riportati gli undici Principi individuati nella riunione degli esperti delle CIIP dei paesi del G8 svoltasi a Parigi nel marzo del 2003 e ratificati dai Ministri della Giustizia e dell'Interno nella riunione del maggio 2003.

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.*

6. BIBLIOGRAFIA

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

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

[3] R. Setola "La Protezione delle Infrastrutture Critiche Informatizzate", *Automazione e Strumentazione*, pp. 27 - 35, luglio 2003; http://www.ilb2b.it/autom_strum/detalle.asp?id=20030708006&ricerca=6.

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

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

[6] UN Resolution n. 58/199 "Creation of a global culture of cybersecurity and the protection of critical information infrastructures", General Assembly 23 dicembre 2003, http://www.un.org/Depts/dhl/resguide/r58.htm

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

[8] V. Merola, R. Setola, "La Protezione delle Infrastrutture Critiche Informatizzate, un nuovo paradigma per la sicurezza informatica", *ICT Security*, pp. 68-75, aprile 2004.