Information Warfare 2013

La protezione cibernetica delle infrastrutture nazionali

a cura di Umberto Gori
e Serena Lisi

FrancoAngeli

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con

La versione completa dell'e-book (a pagamento) è leggibile con Adobe Digital Editions. Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta cliccando qui le nostre F.A.Q.

Collana di Scienza Politica e Relazioni Internazionali, diretta da Umberto Gori

Il progresso delle scienze sociali è strettamente legato alla ricerca interdisciplinare. Tale indirizzo non ostacola però l'applicazione di un approccio e di un metodo rigorosamente unitari. L'approccio è quello dei sistemi, il metodo è quello della scienza politica più avanzata. L'uno e l'altro mirano a conoscere il reale nella sua complessità, a partire da dati e variabili fattuali, con l'ausilio, anche, di discipline diverse, teorie empiriche e quindi previsioni aventi valore probabilistico.
C'è una fortissima domanda, oggi, di strumenti aggiornati atti ad interpretare fenomeni complessi e talora privi di precedenti ed a consentirne la previsione, data l'accelerazione dei tempi storici.
A questa domanda la «Collana di Scienza Politica e Relazioni Internazionali» si propone, ambiziosamente, di rispondere, cercando anche di rimuovere, in misura progressiva, le resistenze, ancora vive nel nostro Paese, dovute al tradizionale convincimento che il campo sociale non sia coltivabile con gli strumenti euristici che hanno determinato lo sviluppo eccezionale delle scienze della natura.
La denominazione della collana si giustifica per due aspetti: primo, perché di solito quando si parla di scienza politica si pensa al quadro interno e qui invece si vuole accreditare la tesi che anche il sistema internazionale è analizzabile in tale prospettiva; secondo, perché anche per l'analisi corretta del sistema interno è ormai impensabile non fare un sistematico riferimento al contesto internazionale (e viceversa).
La collana svilupperà sia una parte di metodologia e di tecniche analitiche, sia una parte teorica e di ricerca sugli aspetti di sostanza del vasto campo preso in considerazione. Contribuiranno all'una e all'altra metodologi e scienziati politici, sociologi della politica e studiosi dell'amministrazione, comparatisti e cultori di relazioni internazionali.
La collana ha essenzialmente un taglio operativo. I suoi naturali destinatari saranno quindi, oltreché gli specialisti, anche tutti coloro che, ai diversi livelli, sono detentori di responsabilità decisionali. Scopo ultimo è infatti la progressiva «modernizzazione» dell'Italia nel campo della valutazione scientifica dei fatti politici, interni ed internazionali, che è premessa insieme di razionalizzazione dei processi decisionali e di un corretto funzionamento delle istituzioni e della vita democratica del Paese.

Information Warfare 2013

La protezione cibernetica delle infrastrutture nazionali

a cura di Umberto Gori
e Serena Lisi

FrancoAngeli

La Conferenza, svoltasi presso l'Aula Magna dell'Università "La Sapienza" di Roma, è stata ideata dal Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali dell'Università degli Studi di Firenze (CSSII), dal Centro di Ricerca di Cyber Intelligence and Information Security (CIS) de "La Sapienza" di Roma e dall'Istituto di Studi di Previsione e le Ricerche Internazionali (ISPRI), d'intesa con Maglan Europe, realtà leader internazionale nell'auditing e consulting per la difesa delle informazioni in ambito civile, militare e governativo.

Indice

Prefazione

di *Luigi Ramponi*[*]

Iniziative come la Conferenza CWC concorrono a sensibilizzare l'opinione pubblica e quindi la società nei confronti della minaccia, che già oggi – e in prospettiva – risulta la più attuale, per mantenere la possibilità di vita, di progresso, di sviluppo del nostro Paese, come del Mondo. Con grande piacere, anch'io impegnato da una parte in questo tentativo di diffondere la consapevolezza presso l'opinione pubblica (che poi finisce per essere l'elemento cogente delle decisioni di soluzione nei confronti del problema) e dall'altra nell'attività politica per cercare di dare una normativa a questo problema, debbo realizzare che, progressivamente, la sensibilizzazione ha finito per avere successo. Sono stato di recente a Cosenza, dove un'associazione di ingegneri ha avviato un convegno di questo tipo, basato soprattutto su ciò che loro si aspettano dall'attuazione del DPCM 24/01/2013 che, finalmente, a seguito di un'iniziativa approvata dal Senato e accettata dal Governo, dà una linea, un orientamento per la definizione di una strategia, dei procedimenti e delle esigenze di protezione, realizzando ciò che il Professor Gori auspica, se attuato, nella conclusione del suo intervento. La situazione italiana è accettabile in confronto con quella dei Paesi con cui amiamo confrontarci, anche se abbiamo qualche piccolo ritardo. Ma tale ritardo è nella capacità di coordinamento, di controllo, di guida, dell'azione di prevenzione e protezione nei confronti della minaccia cibernetica.

Il DPCM che è stato approvato definisce le modalità con cui regolare le modalità di coordinamento delle iniziative. Tutti questi sforzi finiscono per determinare la presenza di una coscienza nazionale che facilita le iniziative: la minaccia cibernetica è la più operante e di maggior sviluppo e possibilità future; non riguarda solo la parte della cyber war (cioè della guerra condotta da uno Stato nei confronti di un altro cercando di bloccarne i gangli vitali, cioè le infrastrutture critiche), ma è molto importante anche per quello che attiene al contrasto alle attività della criminalità organizzata, per le attività

[*] Sen. Gen., Presidente di CESTUDIS (Centro Studi Difesa Sicurezza).

di intelligence (ad esempio, per la cosiddetta Business intelligence e la scoperta/protezione dei brevetti), per il contrasto alle attività di terroristi (che possono inserirsi nei sistemi cibernetici per paralizzare, parzialmente o totalmente, le attività della società). Quanto descritto costituisce il quadro che oggi abbiamo di fronte. Il tema del convegno, ossia la protezione delle infrastrutture, costituisce uno dei pilastri sui quali si deve basare la strategia di difesa nei confronti della minaccia cibernetica, sia essa di intelligence, terroristica, criminale o di cyber war. La sessione che mi è stata affidata parla della protezione delle strutture militari. La protezione di tali strutture si articola in due necessità principali. La prima è la protezione di sistemi e strutture riguardanti le capacità di intelligence: la minaccia cibernetica è infatti diversa da quella nucleare, convenzionale e, in parte, anche da quella terroristica, poiché può venire da chiunque (dal singolo individuo come dallo Stato) e non può essere condizionata da una minaccia di "retaliation" (si vedano i casi di dissuasione in caso di minaccia convenzionale e nucleare). Nel caso cibernetico, può esserci un'azione *pre-emptive*, ma una volta subito l'attacco, non può esserci un contrattacco e, talora, neanche una resilienza. Non solo, l'attacco cibernetico può essere condotto da stati che non hanno nulla da perdere nel caso di un conflitto e, quindi, non sono condizionati da una possibilità di ritorsione. Ecco perché diventa estremamente importante l'intelligence - molto più che nei precedenti confronti - poiché consente di prevenire l'attacco. Se mi chiedessero se le nostre Forze Armate possono rinunciare a una brigata, una fregata o a quattro aerei a favore di un potenziamento dell'intelligence e della preparazione contro un possibile attacco cibernetico, risponderei affermativamente, anche se viviamo già in condizioni di inaccettabile ristrettezza della disponibilità dei sistemi appena citati. Ma questo è l'avvenire e vorrei anche concludere lasciando questa riflessione al Vostro pensiero: non credo che in futuro ci possano più essere guerre tra grandi blocchi del tipo di quelle avute durante il Primo e Secondo Conflitto Mondiale, ma ritengo più probabile che, se dovesse accadere un conflitto su tale scala, si combatterà sul piano cibernetico. In breve sarà molto più appetibile cercare di paralizzare l'avversario attraverso il blocco del funzionamento della sua attività, militare e non. Ecco perché le strutture militari e civili devono garantire la resilienza delle infrastrutture. Ed ecco perché è importante diffondere la consapevolezza di tale problematica presso l'opinione pubblica con un'azione congiunta proveniente dal mondo militare, civile ed accademico.

Riconoscimenti

Adesione del Presidente della Repubblica

Patrocini

Presidenza del Consiglio dei Ministri
Ministero degli Affari Esteri
Ministero della Difesa
Ministero dell'Economia e delle Finanze
Ministero dello Sviluppo Economico
Ministero della Salute

Promotori

Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali dell'Università di Firenze (CSSII)

Centre of Research of Cyber Intelligence and Information Security (CIS)

Istituto per gli Studi di Previsione (ISPRI)

ideata d'intesa con Maglan – Information Defense & Intelligence

con la partecipazione di AICA per l'assegnazione del Premio EUCIP 2013

con il contributo di ELT- Elettronica
con la sponsorship di Finmeccanica, Vitrociset

Medaglia di Rappresentanza, con firma del Presidente della Repubblica Giorgio Napolitano, inviata al Prof. Umberto Gori, direttore scientifico della Conferenza, in segno di apprezzamento per l'iniziativa.

La protezione cibernetica delle infrastrutture nazionali: solo un problema tecnico?

di *Umberto Gori*[*]

Gli argomenti trattati in questa relazione introduttiva potranno sembrare ad alcuni risaputi e scontati, ad altri, invece, non conosciuti. Il mio unico scopo è quello di sottoporre all'attenzione di tutti una comune base iniziale di conoscenza.

Gli attacchi cibernetici, fino ad oggi, sono stati in grande misura sferrati da attori criminali per ottenere profitti illeciti e da competitori economici e politici per attività di spionaggio, ma il vero incubo degli Stati sono i sempre più possibili attacchi alle proprie infrastrutture che possano bloccarne il funzionamento o addirittura distruggerle con conseguenze più o meno catastrofiche.

Il problema che si pone con urgenza sempre maggiore è quindi quello della loro protezione e delle metodologie atte ad assicurarla. Anche l'Italia, finalmente, ha iniziato ad occuparsi dell'architettura istituzionale necessaria all'attività di contrasto alle minacce con il DPCM 24/1/2013, anche se moltissimo resta ancora da fare.

Non sta certo a me illustrare e commentare il suddetto decreto: personalità istituzionali qui presenti, oltre a riferire sulla normativa comunitaria, potranno farlo molto meglio di quanto possa farlo io. Vorrei solo metterne in evidenza alcuni punti-chiave funzionali al tema che sto per svolgere. Il Decreto definisce "l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna com-

[*] Professore Emerito, Università degli Studi di Firenze - Presidente del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII), Direttore, Istituto per gli Studi di Previsione (ISPRI), Direttore Scientifico della Conferenza.

ponente ed i meccanismi e le procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi." Dopo di che, l'Art. 2 fornisce la definizione di sei concetti che verranno successivamente ripresi nel testo. I concetti sono quelli di 'spazio cibernetico', 'sicurezza cibernetica', 'minaccia cibernetica', 'evento cibernetico', 'allarme' e 'situazione di crisi'.

Riporto qui di seguito tali definizioni perché, al di là di altre diverse che vengono formulate in altri Paesi o in dottrina, sono quelle cui dobbiamo attenerci nel nostro ordinamento in attesa di opportune modifiche e/o auspicabili convergenze in sede internazionale.

Spazio cibernetico: "l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi".

Sicurezza cibernetica: "condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi".

Minaccia cibernetica: "complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanzia in particolare nelle azioni di singoli individui o organizzazioni, statuali e non, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi".

Evento cibernetico: "avvenimento significativo, di natura volontaria od accidentale, consistente nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi".

Allarme: "comunicazione di avviso (*sic*) di evento cibernetico da valutarsi ai fini dell'attivazione di misure di risposta pianificate".

Situazione di crisi: "situazione in cui l'evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in

via ordinaria ma con l'assunzione di decisioni coordinate in sede interministeriale".

Mi fermo qui. Noto solo che manca una definizione formale ed esaustiva del concetto di *"protezione cibernetica"* che, anche se indirettamente sopra evocata nel contesto esplicativo del concetto di 'sicurezza cibernetica', merita - come vedremo - una trattazione autonoma per la fondamentale importanza strumentale che essa ha ai fini di assicurare, appunto, la sicurezza.

Né vengono definite - e questo è piuttosto strano, stante le preoccupazioni definitorie che si riscontrano nel testo - le *infrastrutture* e, in particolare, le *infrastrutture critiche* che costituiscono l'oggetto più sensibile del Decreto. Ci torneremo fra un attimo.

Il problema della *cyber security* è che essa deve 'rincorrere' continuamente la costante e velocissima evoluzione dei rischi e delle minacce. La sua natura è dinamica, non statica. La sua realizzazione mal si adatta a rigide codificazioni, a formalismi istituzionali, a strutture gerarchiche. Ecco perché assicurare la sicurezza nell'era cibernetica non è soltanto un problema tecnico, ma un problema di mentalità, richiede una rivoluzione culturale particolarmente difficile da ottenere soprattutto nel contesto statuale dove ogni organo difende strenuamente le proprie specifiche competenze, esige un radicale snellimento delle strutture. La gravità delle minacce richiede un sacrificio delle pur legittime prerogative. Le decisioni devono essere quasi sempre immediate, il che richiede un unico centro sovraordinato legittimato a imporre misure di contrasto. Ecco perché ho aggiunto al titolo di questa relazione introduttiva, coincidente col titolo della Conferenza, l'interrogativo: solo un problema tecnico?

In senso certo non conforme a quanto sopra, invece, come ho già messo più in particolare in evidenza durante la Conferenza del 2011, si muove il decreto legislativo del 7 aprile 2011 in attuazione della Direttiva 2008/114/CE (si noti, 3 anni dopo) sull'individuazione e designazione delle infrastrutture critiche europee (ICE) e la valutazione della necessità di migliorarne la protezione. Detto decreto si preoccupa subito di far salve le competenze di una trentina di Ministeri, enti e commissioni varie e solo successivamente si occupa della questione in oggetto, creando ulteriori organismi (NISP – Nucleo Interministeriale Situazione e Pianificazione, oltre ad altre 'strutture' e commissioni).

E veniamo alle *infrastrutture*. Trovo interessante e condivisibile in grandissima parte la spiegazione del concetto quale si ritrova nel vocabolario della Treccani. Per infrastruttura s'intende una struttura o complesso di elementi che costituiscono la base di sostegno o comunque la parte sotto-

stante di altre strutture… *il complesso degli impianti e delle installazioni occorrenti all'espletamento dei servizi ferroviari, aeroportuali, etc.…. l'insieme di opere pubbliche, cui si dà anche il nome di capitale fisso sociale (strade , acquedotti, fognature, opere igieniche e sanitarie) e anche quelle attività che si traducono in formazione di capitale personale (es., l'istruzione pubblica, soprattutto professionale, o la ricerca scientifica intesa come supporto per le innovazioni tecnologiche).*

Per infrastrutture critiche, come è più che noto, si devono intendere quelle strutture il cui malfunzionamento o collasso determinerebbe pericoli gravissimi, o addirittura catastrofici per i servizi essenziali alla vita della comunità nazionale, per la stabilità socio-politica ed economica del sistema politico e per la sicurezza dello Stato.

Tre, secondo alcuni Autori (L. Tabansky), sono i fattori che definiscono una *infrastruttura critica*: la sua importanza simbolica (es., siti storici, musei, monumenti, archivi, etc.), l'immediata dipendenza dal suo funzionamento, le connessioni e dipendenze complesse che possono dar luogo a veri e propri *'effetti farfalla'* o, quanto meno, a un *effetto domino*. Solo le dipendenze dirette sono conoscibili e valutabili nei loro effetti: quelle indirette, che possono causare conseguenze gravissime, sono al di fuori del campo della conoscenza.

È interessante qui evidenziare che in uno studio dell'Ing. Luisa Franchina, pubblicato su "Gnosis" (n. 3, 2008), viene proposto l'utilizzo della piramide a cinque gradini dei bisogni di Maslow per escludere dalle risorse definibili come critiche quelle che realizzano i bisogni immateriali. I bisogni fisiologici e quelli di sicurezza e protezione sono quindi i soli ad essere inclusi nella categoria della criticità.

Incidentalmente, a proposito degli effetti 'domino' o 'farfalla', faccio osservare che i sistemi complessi hanno comportamenti sempre *controintuitivi.*

Come tutte le strutture, anche le infrastrutture possono essere 'in serie' o 'in parallelo'. Nel primo caso, il venir meno di un singolo elemento può far collassare l'intero sistema; nel secondo caso, quest'ultimo è a rischio solo se tutte le sue componenti critiche che svolgono la stessa funzione vengono meno contemporaneamente. In particolare, le infrastrutture critiche ad alta valenza cibernetica debbono, e in genere hanno, elementi *ridondanti*, anche perché - a differenza del passato quando le dipendenze reciproche erano di natura fisica - oggi, con i metodi computerizzati di comando e controllo automatici, si creano ulteriori relazioni e, conseguentemente, ulteriori vulnerabilità. Il fatto poi che la maggior parte di tali infrastrutture siano di proprietà privata non sempre sensibile a problemi di sicurezza, nonché la ten-

denza sempre più spinta a collegarsi al *cloud computing*, crea nuovi e complicati problemi.

La definizione della Treccani contiene *in nuce* anche il concetto di struttura *immateriale*. Ad esempio, oltre al riferimento all'istruzione pubblica o alla ricerca, sono da considerarsi 'immateriali' quelle strutture puramente informative come i *databases* contenenti dati sensibili. La stessa Internet è una infrastruttura in grandissima parte 'immateriale'.

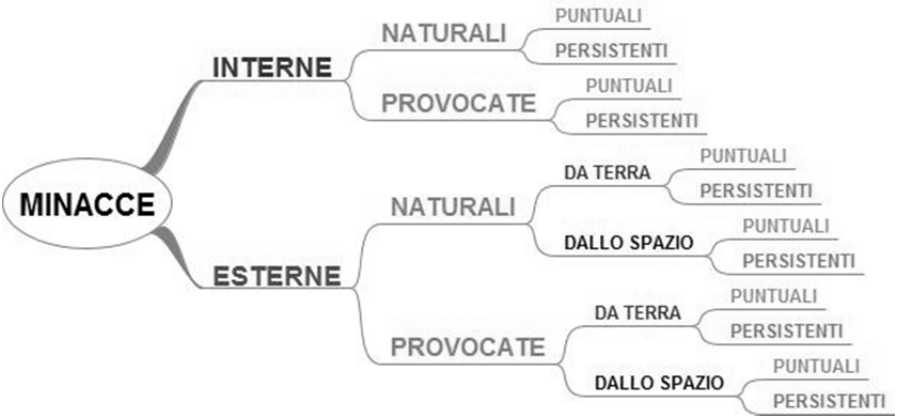
A livello comunitario, l'art. 2, punto a) della direttiva 2008/114/CE, già sopra richiamata, definisce una infrastruttura critica - pur limitatamente ai settori dell'energia e dei trasporti - come "un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini e il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni".

Le *minacce* cui tali infrastrutture devono far fronte possono essere interne od esterne, naturali o provocate artificialmente, da terra o dallo spazio. A prescindere dai fenomeni naturali, i satelliti sono infatti strutture orbitanti, possibili piattaforme d'attacco e, nello stesso tempo, possibili bersagli. Le minacce possono essere puntuali o persistenti (*Advanced Persistent Threats- APT*). Gli strumenti sono quelli più o meno noti (Trojan, Worms, Sniffers, Rootkits, Defacement - modifica o distruzione di dati -, DoS, Stuxnet, etc.).

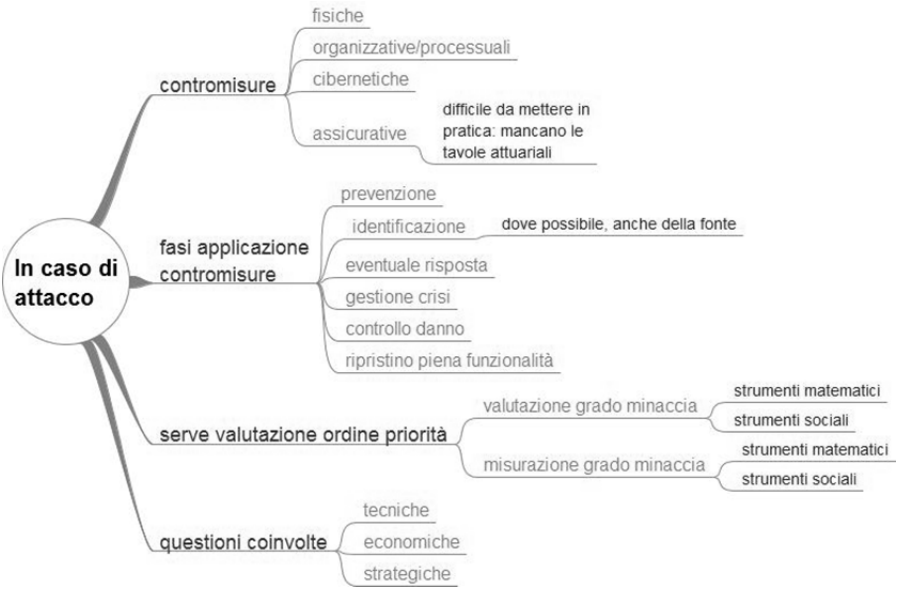
A proposito di *cyber weapons* come lo Stuxnet, i sistemi computerizzati di controllo industriale sono punti di forte vulnerabilità perché la loro protezione non era stata considerata prioritaria.

Le reazioni agli attacchi condotti tramite tali *malware* possono essere di tre tipi: accettazione delle perdite (reazione, questa, tipica di molti Paesi ed aziende); rafforzamento delle infrastrutture con aggravio di spese per ridurre le perdite durante attacchi futuri (è su questo punto che mi soffermerò brevemente); abbandono dell'uso di strumenti cibernetici e ritorno allo *status quo ante.*

Le *vulnerabilità* che devono essere analizzate e corrette sono di quattro tipi: quelle dipendenti dal computer, dalla rete, dal personale e dal contesto, anche fisico. In concreto, nel primo caso si tratta di vulnerabilità dovute all'utilizzo di password troppo semplici e non criptate, o a mancanza o a errori di protezione; nel secondo, di punti di entrata non protetti; nel terzo, di mancanza di addestramento, di atti illeciti di personale scontento, etc.; nel quarto caso, infine, di collocazione di server in zone non protette o di politiche di sicurezza inadeguate.



I metodi per stabilire il *quantum* di vulnerabilità e di resilienza non tengono conto, di solito, del fatto che altre variabili, oltre a quelle tecniche e fisiche, possono avere effetti importanti. Si calcola che l'80% circa dei problemi sia causato da lacune organizzative, fattori sociali e problemi umani. Sarebbe pertanto opportuno accordarci su una definizione interdisciplinare della vulnerabilità.



Veniamo adesso alle *contromisure* che consentono, nella misura del possibile, la protezione delle infrastrutture. Le risposte sono di quattro tipi: fi-

siche, organizzativo-processuali, cibernetiche e assicurative. La quarta misura, se il riferimento è al pagamento di un premio, non è di facile applicazione, data la mancanza, in materia, di tavole attuariali.

Le *fasi* sono la prevenzione, l'identificazione, quando possibile, della fonte dell'attacco, l'eventuale risposta, la gestione della crisi, il controllo del danno e, infine, il ritorno alla piena funzionalità. Occorre però, inizialmente, stabilire un ordine di priorità, valutando e misurando il grado di minaccia ai vari componenti dell'infrastruttura non solo con gli strumenti matematici dell'ingegneria, ma anche con altri metodi che tengano conto degli interessi, degli obiettivi e dei valori sociali. La vulnerabilità dei sistemi cibernetici è infatti una questione tecnica, economica e strategica.

Dato che non è più possibile od opportuno o internazionalmente legittimo rispondere agli attacchi cibernetici con le forme classiche della deterrenza convenzionale o nucleare anche per il noto problema dell'attribuzione di responsabilità (chi è, con certezza, il responsabile?), è necessario rendere *resilienti* le nostre infrastrutture.

Tanto più che sistemi obsoleti e automazione rendono i nostri Paesi troppo vulnerabili alle minacce informatiche. Secondo la McAfee, "la sicurezza deve essere prevista fin dalle fondamenta delle componenti di rete in fase di pianificazione e progettazione", purché - mi permetto di aggiungere – la pianificazione sia 'dinamica', e cioè continuamente 'rivisitata' a fronte dell'estrema fluidità delle minacce.

Sono in particolare le *smart grid*, sempre secondo un Rapporto della McAfee, ad essere particolarmente vulnerabili a causa dell'interconnessione dei sistemi integrati, dell'automazione e dell'obsolescenza della rete energetica, collegata così com'è, ad Internet "senza utilizzare sistemi di cifratura".

Esistono varie metodologie per valutare rischi e minacce e per misurare la resilienza dei sistemi. Alcune fra queste sono *open source*. Qui di seguito una descrizione sintetica delle procedure ci farà entrare nel vivo dei problemi che le istituzioni, le aziende e tutte le infrastrutture sono tenute a risolvere.

Per valutare il rischio che ogni minaccia comporta occorre previamente conoscere alla perfezione il sistema da difendere. Ciò è reso necessario anche perché è solo del proprio sistema che possono essere note tutte le caratteristiche. Difficile, se non impossibile, avere una perfetta conoscenza delle altrui strutture.

Conoscere il proprio sistema significa conoscerne altrettanto bene le vulnerabilità, condizione, insieme alla conoscenza o previsione della mi-

naccia, per misurare il rischio che si corre. Il rischio, infatti, è il risultato del prodotto della minaccia per la vulnerabilità (R=MxV).

Laddove il rischio non fosse misurabile per impossibilità di conoscere il peso della minaccia e/o il grado di vulnerabilità, mi spingo a ritenere che, di fronte all'incertezza, si possa far ricorso al concetto di 'probabilizzazione soggettiva' (De Finetti), e quindi al ricorso all'analisi Bayesiana (Teorema di Bayes).

Ovviamente, la protezione da attuare, per quel che ci concerne in questa sede, è quella cibernetica, e non anche quella fisica. A questo fine, per la sicurezza dei computer, sono fondamentali programmi antivirus aggiornati continuamente, parole di passo complesse, programmi di criptaggio, programmi di protezione (*firewall*) e salvataggio dati (*backup*).

È da qui che inizia l'iter per avere sistemi resilienti.

La *resilienza* è un concetto che solo da poco tempo viene usato qui da noi, soprattutto in certi contesti. Anche se esiste una pluralità di definizioni, intendo qui per *resilienza* la capacità di un sistema di preservare le proprie funzionalità e servizi attraverso procedure e meccanismi di prevenzione, rilevamento, assimilazione e recupero durante e dopo un attacco.

Detta in altri termini, la resilienza è funzione della consapevolezza della situazione presente e prevedibile, della gestione delle vulnerabilità fondamentali di ogni tipo, caratterizzate soprattutto dalla rapidità con la quale esse provocano effetti negativi, e della capacità di adattamento di una struttura, e cioè della capacità di mutare i fattori che definiscono gli stati di equilibrio, quali la strategia, i sistemi di gestione e la struttura decisionale e di comando.

È superfluo osservare che le strategie e le tecniche di resilienza devono adattarsi ai vari settori in cui operano le infrastrutture. Nella letteratura specializzata si arriva a dire che possono darsi tante definizioni di resilienza quanti sono i sistemi infrastrutturali al fine di poter usare modelli quantitativi per misurare nei diversi settori la resilienza a eventi perturbatori, valutando sia l'impatto sulla performance del sistema che il costo del recupero.

La prevenzione può essere *attiva* o *passiva*. Lasciando da parte la prevenzione attiva che consiste nel contrasto alle minacce già note prima che si verifichi l'attacco, la prevenzione passiva si attua attraverso le seguenti fasi: a) identificazione degli assetti e processi critici e della loro rilevanza secondo vari criteri tecnici, economici, sociali, legali, temporali, etc.; b) analisi delle dipendenze delle funzioni critiche dal dominio cibernetico e determinazione della loro priorità, in quanto ogni dipendenza, ad ogni livello della struttura, è una potenziale vulnerabilità; c) analisi delle vulnerabilità. L'identificazione e la valutazione devono avvenire ad ogni livello e per ogni funzione del sistema; d) analisi delle minacce, facendo tesoro degli attacchi passati e analizzando i *trends*. La natura degli attacchi futuri è imprevedibile ed ecco perché è indispensabile la resilienza. Non sono da escludersi eventi tipo '*cigno nero*', caratterizzati da sorpresa e forte impatto. Avverto però che è possibile restringere l'area di incertezza anche con riferimento ad eventi 'inaspettati' tramite determinate strategie euristiche.

A livello internazionale sono stati identificati sette 'meccanismi attenuanti' validi sempre e comunque. Essi sono: 1) creazione della consapevolezza; 2) riduzione delle dipendenze; 3) incremento della ridondanza; 4) sviluppo di soluzioni di *backup* alternative; 5) incremento della flessibilità; 6) trasferimento del rischio; e, 7) condivisione delle informazioni.

Il *rilevamento* consiste nell'analisi critica delle strategie della struttura per gestire gli eventi cibernetici e nella valutazione del tempo intercorrente fra l'attacco e il momento della scoperta.

L'*assimilazione* è la capacità di metabolizzare il mutamento con la creazione di sistemi elastici (assorbenti facilmente il danno) che permettono ol-