Centro Studi "Gino Germani"

LINK UNIVERSITY CAMPUS

Convegno

INFRASTRUTTURE CRITICHE E SICUREZZA NAZIONALE

VULNERABILITÀ E STRATEGIE DI PROTEZIONE DEL SISTEMA-PAESE

Lunedì 26 febbraio 2007

Palazzo Marini – Roma

DOCUMENTO DI IMPOSTAZIONE ***(a cura di Luigi Sergio Germani e Diego Baliani)***

1) Protezione delle infrastrutture critiche e sicurezza nazionale: evoluzione del pensiero strategico statunitense *(di Luigi Sergio Germani)*

A partire dalla metà degli anni ’90 comincia a diffondersi tra le *élite* politiche occidentali la consapevolezza della crescente vulnerabilità dei paesi industrializzati derivante dalla forte interdipendenza e interconnessione fra le infrastrutture socio-tecnologiche su cui si basa il funzionamento delle società moderne.

I sotto-sistemi e le reti infrastrutturali, che rappresentano elementi di vitale importanza per un sistema-paese, vengono denominate “infrastrutture critiche”. Non tutte le infrastrutture sono critiche, e non tutte le infrastrutture critiche hanno lo stesso livello di criticità. Un guasto di natura accidentale in una infrastruttura di criticità molto elevata, oppure un attacco terroristico mirante a distruggere o paralizzare quest’ultima, potrebbe provocare danni economici enormi o innescare un processo di crisi dell’ordine pubblico e della sicurezza interna ed esterna del Paese colpito.

Tra le infrastrutture ritenute critiche dalla maggior parte dei paesi industrializzati vi sono le seguenti :

a) infrastrutture per la trasmissione e distribuzione dell’energia (elettrica, del gas, del petrolio);
b) infrastrutture per il trasporto di merci e persone (automobilistico, ferroviario, aereo, ecc.);
c) telecomunicazioni e infrastrutture informatiche;
d) organismi governativi e pubblica amministrazione;
e) infrastrutture per l’erogazione e lo smaltimento delle acque;
f) sistema bancario e finanziario.

Nelle società moderne le infrastrutture critiche sono sempre più strettamente interconnesse e interdipendenti. Ciò è dovuto anche all'utilizzo sempre più diffuso di tecnologie informatiche e telematiche. La crescita vertiginosa dell'interdipendenza aumenta l'efficienza delle infrastrutture critiche, ma allo stesso tempo determina una crescente vulnerabilità di queste ultime e della società nel suo complesso.

In un contesto di elevata interdipendenza un guasto (causato da un evento naturale o da un azione umana colposa o dolosa) in una infrastruttura critica può facilmente produrre effetti a cascata ed estendersi rapidamente alle altre infrastrutture critiche, amplificando i danni e le disfunzioni fino a provocare una crisi catastrofica dell'intero sistema nazionale. Tale risultato può derivare anche da una serie di guasti che presi singolarmente non sono particolarmente gravi, ma che sommati assieme producono un effetto catastrofico.

La presa di coscienza della problematica della protezione delle infrastrutture critiche (PIC) nel mondo occidentale è da ricollegare all'emergere negli anni '90 di un nuovo tipo di terrorismo, il cosiddetto "neo-terrorismo" (detto anche "terrorismo catastrofico"), che mira deliberatamente a provocare un numero elevato di vittime, anche con l'utilizzo di armi di distruzione di massa. Le aggregazioni di matrice jihadista fautrici del terrorismo catastrofico potrebbero tentare di attaccare le infrastrutture critiche di un paese per paralizzare il suo sistema produttivo, i servizi pubblici essenziali, nonché le sue istituzioni pubbliche e strutture politico-decisionali.

La minaccia viene percepita chiaramente negli Stati Uniti a metà degli anni '90, quando si evidenziano i primi segnali del neo-terrorismo[1] e si diffonde la preoccupazione circa la minaccia di attacchi informatici e di *cyber-warfare* (che possono essere attuati non solo da terroristi ma anche da diversi tipi di attori ostili, statali e non-statali). A partire dal 1997-98 viene sempre più enfatizzata negli USA la problematica della PIC come questione attinente alla sicurezza nazionale. I governi europei prendono coscienza della problematica successivamente, in alcuni casi tra il 1997 e il 2000, in altri dopo gli attacchi dell'11 settembre 2001. Oggi la vulnerabilità delle infrastrutture critiche viene vista in numerosi Paesi dell'area occidentale come un problema di sicurezza nazionale da affrontare a livello politico-strategico.

I rischi connessi alla vulnerabilità delle infrastrutture critiche delle società avanzate sono destinati a crescere in maniera costante nei prossimi anni e decenni. I paradigmi tradizionali della sicurezza nazionale non sono adeguati per fronteggiare questa nuova sfida. L'approntamento di una strategia efficace di PIC richiede l'introduzione di significative innovazioni organizzative e di una nuova cultura della sicurezza, sia nel settore istituzionale, che in quello privato.

L'esperienza degli USA in questo campo rappresenta un punto di riferimento per tutti i Paesi avanzati oggi impegnati nell'approntamento o potenziamento delle proprie strategie di PIC. Essa dovrebbe essere attentamente analizzata per comprenderne aspetti positivi e negativi.

[1] In particolare, l'attentato al World Trade Center (New York, 26 febbraio 1993) e all'Alfred P. Murrah Federal Building (Oklahoma City, 19 aprile 1994).

Gli Stati Uniti furono, infatti, i primi a percepire e analizzare la minaccia, nonché a formulare un disegno strategico per affrontarla. Gli elementi essenziali della strategia americana di PIC sono i seguenti:

a) la costituzione di un sistema nazionale di PIC incaricato di:
   - rilevare e monitorare le criticità e le vulnerabilità del sistema-Paese nel suo complesso;
   - predisporre piani per ridurre la vulnerabilità del sistema;
   - predisporre piani per il rapido ripristino di capacità funzionali minime del sistema-Paese, da attivare nell'eventualità di una crisi sistemica delle infrastrutture critiche.

b) l'accentramento della funzione di direzione strategica delle attività di PIC a livello della leadership politica del Paese;

c) l'introduzione di un nuovo modello di collaborazione e condivisione delle informazioni tra settore pubblico e settore privato nelle attività di PIC;

d) il potenziamento delle capacità di *early warning* per la tempestiva segnalazione di imminenti eventi distruttivi riguardanti le infrastrutture critiche;

e) programmi per la diffusione di una nuova cultura della sicurezza sia nel mondo istituzionale che nel settore privato;

f) il ruolo della comunità intelligence nella PIC, che ha il compito di svolgere attività di ricerca informativa e analisi relativa a potenziali attacchi alle infrastrutture critiche.

La prima importante iniziativa del governo USA in materia di PIC fu l'*Executive Order* 13010, firmato dal Presidente Bill Clinton nel giugno del 1996, che costituì una apposita commissione per analizzare il problema e proporre eventuali contromisure (*President's Commission on Critical Infrastucture Protection,* presieduta da John Marsh).

Nell'ottobre 1997 la commissione pubblica il rapporto intitolato *Critical Foundations: Protecting America's Infrastructure*. Nel rapporto si sottolineò la crescente vulnerabilità degli Stati Uniti derivante dal moltiplicarsi delle interconnessioni tra infrastrutture critiche[2], nonché dalla sempre più diffusa dipendenza di queste ultime dall'infrastruttura informatica. Gli attori terroristi emergenti nel nuovo contesto del dopo-Guerra Fredda – spiegava il rapporto – avevano sia le intenzioni che le capacità tecniche per sfruttare tali vulnerabilità. La Commissione rilevò una situazione di rischio senza precedenti per gli Stati Uniti e consigliò la leadership politica di agire rapidamente per affrontare il problema, assumendo un ruolo di direzione e coordinamento di uno sforzo nazionale teso a proteggere il sistema delle infrastrutture critiche nel suo complesso.

La Commissione ritenne il paradigma tradizionale della sicurezza nazionale sostanzialmente inadeguato per fronteggiare la minaccia. La sicurezza nazionale non poteva più

[2] Il rapporto identifica una serie di infrastrutture di importanza vitale per il funzionamento dell'economia, del sistema governativo e di quello militare.

essere considerata come una funzione di competenza esclusiva delle istituzioni pubbliche. Si rendeva sempre più necessaria la cooptazione del settore privato – i proprietari e gestori delle infrastrutture critiche – nelle attività di tutela della sicurezza nazionale.

In risposta al rapporto *Critical Foundations* il Presidente Clinton, nel maggio 1998, emanò la *Presidential Decision Directive* 63 (PDD-63), che diede l'avvio alla costituzione di un sistema nazionale preposto alle attività di difesa delle infrastrutture critiche, coordinato da un responsabile nazionale (*National Coordinator for Security, Infrastructure Protection, and Counterterrorism*). Quest'ultimo aveva il compito di acquisire una visione complessiva del sistema e di predisporre un piano nazionale di PIC (*National Infrastructure Assurance Plan*: NIAP).

Per ogni settore infrastrutturale posseduto e gestito da privati venne individuata una agenzia del governo federale, alla quale spettava il compito di predisporre un piano settoriale di protezione delle infrastrutture critiche di sua competenza, in stretta collaborazione con gli operatori privati del settore.

Il responsabile nazionale aveva il compito di predisporre il piano nazionale di PIC integrando i vari piani settoriali, nonché i piani predisposti da ogni agenzia del governo federale per la protezione delle proprie infrastrutture critiche.

La dottrina americana in materia di PIC dopo l'11 settembre si ispira alla visione strategica contenuta nel rapporto *Critical Foundations* e nel PDD-63, che viene ulteriormente sviluppata e adattata al nuovo scenario caratterizzato dal neo-terrorismo jihadista. I due documenti di dottrina più significativi sono "*A National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*" (febbraio 2003), e "*A National Strategy to Secure Cyberspace*", che riguarda in particolare la difesa delle infrastrutture critiche da minacce provenienti dal ciberspazio.

In questi documenti viene ampliato il numero di infrastrutture considerate critiche e viene introdotto il concetto di "risorse chiave" (*key resources*), come ad esempio centrali nucleari, dighe, o monumenti e simboli nazionali. Un evento distruttivo che colpisse tali "risorse-chiave" non comporterebbe una crisi dell'intero sistema: esse pertanto non costituiscono infrastrutture critiche. Tuttavia, esso potrebbe produrre effetti analoghi a quelli causati dall'impiego di armi di distruzione di massa: danni catastrofici alla salute della popolazione e/o e perdite umane massicce. Un attacco terroristico contro monumenti o simboli nazionali produrrebbe invece gravi effetti psicologici di demoralizzazione e depressione tra la popolazione, nonché danni al prestigio della nazione. Pertanto, secondo la dottrina statunitense di PIC elaborata dopo l'11 settembre, la difesa delle "risorse chiave" deve essere integrata nella strategia di PIC.

Nel marzo del 2003 viene costituita la *Critical Infrastructure Warning Information Network* (CWIN), una rete altamente protetta di comunicazioni finalizzata alla condivisione di informazioni relative alla PIC e alla tempestiva segnalazione di situazioni di pericolo. La rete è gestita dal *Department of Homeland Security* (DHS) e mantiene la sua funzionalità anche nell'eventualità di una crisi sistemica durante la quale le reti normali di comunicazioni cessano di funzionare. La CWIN collega il DHS con altre agenzie del governo federale, governi locali, operatori privati e organismi internazionali.

Nel dicembre 2003 il Presidente Bush emana la direttiva HSPD-7 (*Homeland Security Presidential Directive-7*) che sostituisce il PDD-7 come documento di base della politica USA di PIC. Secondo questa direttiva, la funzione del sistema nazionale di PIC non è quella di proteggere tutte le infrastrutture critiche e le risorse chiave del paese (un compito impossibile), ma di irrobustire il sistema nel suo complesso, soprattutto tramite l'introduzione di misure strategiche di sicurezza tendenti a rendere più difficile il successo di un eventuale attacco e a mitigarne l'impatto distruttivo.

La direttiva del Presidente Bush affida al *Secretary for Homeland Security* la responsabilità di coordinare l'impegno nazionale teso a rafforzare la protezione delle infrastrutture critiche e delle risorse chiave. Il segretario dirige, integra, e coordina l'attuazione delle attività di PIC svolte da agenzie del governo federale, dalle amministrazioni locali e dal settore privato. Egli elabora il piano nazionale di PIC (*National Plan for Critical Infrastructure and Key Resources Protection* – NPCIKRP). A tale fine egli identifica le criticità del sistema, e stabilisce le priorità per interventi preventivi e protettivi. La priorità, secondo la direttiva, deve essere data alla protezione di infrastrutture critiche e risorse chiave la cui distruzione produrrebbe effetti catastrofici simili a quelli causati dall'impiego di armi di distruzione di massa.

Il *Secretary for Homeland Security*, inoltre, ha il compito di costituire un sistema nazionale di allertamento per la PIC, identificando indicatori di pericolo e potenziando la capacità delle istituzioni e degli operatori privati di percepire e analizzare potenziali attacchi alle infrastrutture critiche o alle risorse-chiave.

Il sistema nazionale di PIC istituito dalla direttiva HSPD-7 prevede una intensa collaborazione e condivisione delle informazioni fra Istituzioni e operatori privati (che possiedono e gestiscono l'85% delle infrastrutture critiche del Paese). Analogamente al sistema istituto dal PDD-63, vengono individuate una serie di agenzie governative (denominate *Sector-Specific Agencies*) incaricate di promuovere il rafforzamento della sicurezza di specifici settori infrastrutturali gestiti da operatori privati, in collaborazione con questi ultimi.

2) L'esperienza dei Paesi europei e dell'UE in tema di protezione delle infrastrutture critiche *(di Diego Baliani)*

Il dibattito e le iniziative statunitensi, in particolare il rapporto *Critical Foundations: Protecting America's Infrastructure* della Commissione Presidenziale sulla Protezione delle Infrastrutture Critiche del 1997, hanno avuto ripercussioni anche nel continente europeo, tanto che tra il 1997 e il 1999 numerosi Paesi europei hanno avviato politiche per la protezione delle infrastrutture critiche, soprattutto informatiche. Un ulteriore impulso è giunto in seguito agli attentati terroristici compiuti tra il 2001 e il 2005 in territorio statunitense ed europeo (New York, 11 settembre 2001; Madrid, 11 marzo 2004; Londra, 7 e 21 luglio 2005). Tuttavia, ciascun Paese europeo ha sviluppato una sua sensibilità e un approccio particolari al tema, con il risultato che attualmente non esistono né una percezione comune delle potenziali minacce che gravano sulle infrastrutture critiche nazionali, né prassi e strutture omogenee in tema di PIC.

Nel Regno Unito, ad esempio, è attualmente presente un sistema avanzato di PIC, basato su una chiara definizione di infrastrutture critiche (che nel contesto britannico sono definite *Critical National Infastructure*, o CNI [3]), e gestito da una serie di organismi pubblici in collaborazione con centri privati specializzati. Tra questi spiccano il *National Security Advice Centre* (NSAC)[4] e il *National Infrastructure Security Centre* (NISCC)[5], che si occupano delle misure di prevenzione e protezione delle infrastrutture critiche gestite da soggetti pubblici e privati, nonché il *Civil Contingencies Secretariat* (CSS), istituito per migliorare le capacità di resilienza del governo britannico[6].

Anche la Francia si è dotata di strutture per la PIC. Il responsabile per l'organizzazione della PIC è il Segretario Generale per la Difesa Nazionale (SGDN), istituito presso l'ufficio del primo ministro francese, il quale si occupa degli affari di sicurezza nazionali e internazionali. L'SGDN assiste il primo ministro nell'adozione delle decisioni e promuove la collaborazione tra i ministeri, anche in materia di PIC.

In Germania, la pubblicazione del rapporto USA del 1997 stimolò l'istituzione da parte del Ministero dell'Interno federale tedesco dell'*AG KRITIS*, un gruppo di lavoro interministeriale sulle infrastrutture critiche che nel 2000 produsse un rapporto in cui descriveva le possibili minacce per la Germania, conduceva un'analisi sulle vulnerabilità delle infrastrutture tedesche, suggeriva contromisure e disegnava sistemi di *early warning*. Nel 2005 il governo tedesco ha adotta due documenti importanti, il "Piano Nazionale per la Protezione delle Infrastrutture Critiche Informatiche" (NPSI), e il "Concetto Protettivo Fondamentale per la Protezione delle Infrastrutture Critiche". Quest'ultimo, sviluppato congiuntamente dal Ministero dell'Interno federale (BMI), dall'Ufficio Federale per la Protezione Civile e la Risposta ai Disastri (BMK), dall'Agenzia Federale della Polizia Criminale (BKA) e dal settore privato, fornisce linee guida per l'analisi di eventi potenzialmente pericolosi (provocati dall'uomo o dalla natura), e raccomanda delle misure protettive.

La Svezia ha adottato nel 2002 la sua prima legge sulla politica svedese di sicurezza e preparazione alle crisi, basata sui risultati della Commissione sulla Vulnerabilità e la Sicurezza. La legge presenta un nuovo sistema di pianificazione per preparare il Paese ad eventuali crisi

[3] Secondo la definizione britannica, la CNI comprende quei beni, servizi e sistemi la cui continuità è di tale importanza che la loro perdita, interruzione nel funzionamento e degradazione del servizio potrebbe causare perdite di vite umane su vasta scala, produrre effetti economici o sociali gravi e significativi per la comunità nazionale, o essere degna di attenzione immediata del governo nazionale. La CNI britannica è costituita da 10 settori (e 39 sottosettori): comunicazioni, servizi di emergenza, energia, finanza, settore alimentare, governo e servizi pubblici, sanità sicurezza pubblica, trasporti e settore idrico.

[4] Il *National Security Advice Centre* (NSAC), istituito presso il Servizio di Sicurezza (MI5-Direttorato Intelligence), svolge attività di prevenzione a tutela dell'integrità delle strutture materiali e del personale della CNI.

[5] Il *National Infrastructure Security Centre* (NISCC), centro interministeriale istituito presso l'*Home Office* nel 1999, si occupa della prevenzione e protezione della CNI dagli attacchi elettronici.

[6] Il *Civil Contingencies Secretariat* (CSS), istituito nel 2001 presso il *Cabinet Office*, lavora in collaborazione con diversi ministeri, amministrazioni locali e soggetti privati con l'obiettivo di aumentare la capacità del Regno Unito di approntamento delle difese civili, di gestione delle crisi e di ripristino delle funzionalità del settore pubblico o privato danneggiate.

sociali future di vaste proporzioni, e per predisporre attività per fronte ad una potenziale minaccia di guerra. Ciascuna struttura pubblica incaricata di gestire un'infrastruttura critica fà formalmente riferimento al proprio ministero di appartenenza, ma è subordinata in realtà solo alle decisioni assunte dal governo in sede collegiale.

Nei Paesi Bassi, fu pubblicato nel 1999 il memorandum "*Digital Delta*" relativo alla protezione delle infrastrutture critiche informatiche e delle comunicazioni, e nel 2002 il governo olandese avviò il progetto "*Bescherming Vitale Infrastuctuur*" (Protezione delle Infrastrutture Critiche olandesi), avvalendosi di un "questionario *Quick-Scan*" diffuso tra i ministeri interessati al fine di ottenere una radiografia dei beni e servizi ritenuti "vitali", nonché i processi e le interdipendenze sottostanti. Di fatto, la responsabilità della PIC risiede in capo a diversi ministeri in base alle relative competenze, e coinvolge il settore pubblico e privato.

Nel contesto generale conseguente agli attentati del 11 settembre 2001, e su impulso particolare degli attentati terroristici compiuti in Europa, anche l'Unione Europea ha adottato iniziative per promuovere a livello europeo il dibattito e politiche relativi alla PIC.

In risposta agli attentati di Madrid dell'11 marzo 2004, l'UE ha adottato la "Dichiarazione sulla lotta al terrorismo" (25 marzo 2004), che urge lo sviluppo di una strategia di lungo periodo per il contrasto del fenomeno. Sulla base del conseguente "Piano d'azione sulla lotta al terrorismo" (18 giugno 2004) della Commissione europea, il Consiglio Europeo ha inserito la PIC tra le priorità della lotta al terrorismo.

In particolare, il Consiglio Europeo del giugno 2004 ha chiesto alla Commissione UE di presentare una strategia europea per la PIC; la Commissione UE ha risposto presentando una comunicazione al Consiglio dei Ministri UE e al Parlamento Europeo intitolata "La Protezione delle Infrastrutture Critiche nella lotta contro il terrorismo" (20 ottobre 2004).

Dopo aver recepito la comunicazione della Commissione, nel dicembre 2004 il Consiglio ha chiesto a quest'ultima di presentare un "Programma Europeo per la protezione delle Infrastrutture Critiche" (*European Programme for Critical Infrastructure Protection* o EPCIP) ed ha concordato l'istituzione presso la Commissione UE di una "Rete Informativa di Allertamento delle Infrastrutture Critiche" (*Critical Infrastructure Warning Information Network* o CIWIN, l'equivalente europeo del CWIN statunitense). Infine, la Commissione ha adottato il "Libro Verde sul programma europeo per la Protezione delle Infrastrutture Critiche" (17 novembre 2005), proponendo agli Stati membri una serie di opzioni per l'istituzione dell'EPCIP e del CIWIN entro il 2006, e chiedendo agli Stati membri di avanzare proposte concrete in tal senso.

Nel valutare le iniziative europee, bisogna tener presente la struttura particolare dell'Unione Europea, la quale, a differenza degli USA, non è uno Stato nazionale, e come tale deve sempre tener presente le divergenze nelle percezioni degli Stati membri, ogni qual volta voglia avviare un progetto comune. Nel caso specifico, si tratta di stabilire cosa s'intende per "infrastruttura critica europea" e come si differenzia dalle infrastrutture critiche nazionali degli Stati membri, e quando e come l'intervento spetta all'Unione Europea e non agli Stati membri.

Anche in Italia sta maturando sempre più la consapevolezza dell'importanza della PIC, stimolata tanto dagli eventi catastrofici avvenuti all'estero (ad esempio gli attentati terroristici negli USA o in Europa, o i disastri naturali che hanno colpito gli USA come l'Uragano Latrina, o ancora la possibilità di interruzione volontaria delle forniture di energia da parte dei Paesi fornitori come la per motivi di politica estera), quanto da eventi avvenuti in territorio italiano (come il black-out del 28 settembre 2003).

Una prima iniziativa italiana di rilievo fu l'istituzione nel 2003 di un "Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate" in seno al Ministero per l'Innovazione e le Tecnologie (MIT), che ha prodotto il rapporto "Protezione delle Infrastrutture Critiche Informatizzate – La realtà Italiana", pubblicato nel marzo 2004.

Attualmente, esiste un consenso per istituire in seno alla Presidenza del Consiglio dei Ministri una struttura con il compito di coordinare le iniziative tese a promuovere la nascita di una comunità integrata italiana responsabile della PIC.