

Nuovi sistemi per la sicurezza di un territorio

DI GIOVANNI MANCO
E DI LUIGI BATTAGLIA E MATTIA SICILIANO

*Ingegnere - Coordinatore
Commissione Telecomunicazioni
Ordine Ingegneri Napoli*

*Ingegneri - Componenti
Commissione Telecomunicazioni
Ordine Ingegneri Napoli*

Nel mondo globalizzato lo sviluppo di un territorio appare sempre più legato alla capacità di garantire alle persone e alle strutture che su di esso risiedono un sufficiente livello di sicurezza rispetto agli atti criminali, compresi gli attacchi terroristici, gli incidenti e gli eventi naturali avversi. In una società complessa come quella in cui viviamo, ciò può essere ottenuto solo affiancando alle politiche di prevenzione e coesione sociale avanzati strumenti di protezione basati sull'impiego di moderni sistemi ICT per la sicurezza.

1. Introduzione

In generale la problematica della sicurezza abbraccia aspetti e contesti molto differenti tra loro. Si parla di sicurezza in tutti i campi: nel mondo dei trasporti, delle costruzioni, del lavoro, ecc. Nel presente articolo la sicurezza viene affrontata con riferimento alle minacce (rischi) a cui sono esposte le persone e i beni di un territorio: criminalità organizzata, microcriminalità urbana, terrorismo internazionale, frane, manovre/avarie che danneggiano infrastrutture critiche (reti telefoniche, elettriche,...). Pertanto la sicurezza è strettamente legata non solo a fenomeni di natura sociale, culturale, economica e politica, ma anche a calamità naturali e ad avarie che possono ledere il corretto funzionamento dei complessi sistemi/infrastrutture da cui dipende sempre più la nostra vita. Il compito di come garantire un sufficiente livello di sicurezza attraverso adeguate misure di prevenzione e protezione è certamente complesso, perché si tratta di tener conto di una moltitudine di eventi e di attori estremamente eterogenei. Inoltre, sono vari gli scenari e gli obiettivi che di volta in volta si è costretti a considerare: National Protection, City Protection, Peace-keeping, ecc. Va anche notato che ormai sono molte le situazioni in cui la garanzia di sicurezza si estende oltre i limiti nazionali: si pensi, ad esempio, al ruolo che svolge l'Unità di Crisi del Ministero degli Esteri per le persone ed i beni italiani all'estero.

Un approccio efficace per assolvere un tale compito è quello di adottare metodologie sistemiche, che consentono di implementare nuovi modelli di sicurezza attraverso l'integrazione di più competenze professionali e tecnologie. Un tale metodo porta di fatto, oltre allo sviluppo di nuove politiche per la coesione sociale e la sicurezza territoriale, alla realizzazione di un'infrastruttura tecnica definita come Systems-of-Systems (SdS - Sistema dei Sistemi) - vedi fig. 1 - basata soprattutto sulle moderne tecnologie dell'Informazione e della Comunicazione (ICT - Information & Communication Technology). Capace, appunto, di integrare più sistemi e sorgenti di informazioni eterogenee tra di loro, al fine di supportare in tempo reale l'operato dei diversi enti preposti nei processi di protezione: Polizia Urbana, Polizia di Stato, Guardia di Finanza, Difesa, Protezione Civile, Pubblica Amministrazione, Giustizia, gestori di infrastrutture, comunità per la sicurezza sociale, ecc.

In pratica l'obiettivo del SdS per la sicurezza è quello di creare, con metodi nuovi, un sistema-rete in grado non solo di gestire la complessità dei fenomeni, ma anche di far superare le lacune e la "farraginosità" degli attuali sistemi e procedure, che non offrono una visione completa dello scenario operativo, e che risentono anche della sovrapposizione o mancanza di coordinamento dei compiti dei vari enti coinvolti. Il tutto ormai nella consapevolezza generale che la si-

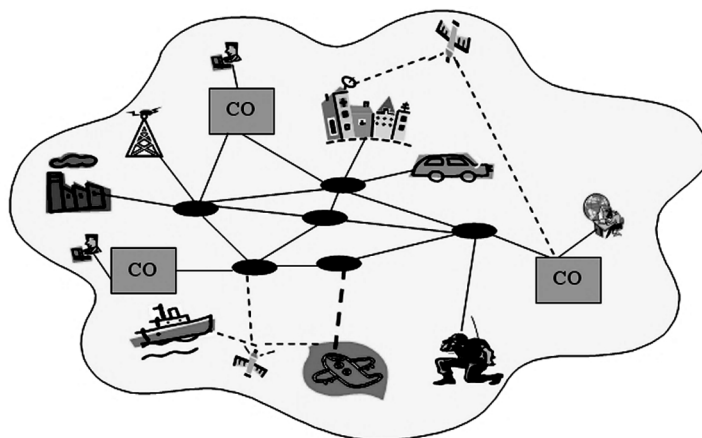
curezza di un territorio, anche se solo percepita, è un valore fondamentale per lo sviluppo socio-economico dello stesso. Proprio per questo essa va assunta come elemento strategico della governance territoriale, a cui dedicare particolare attenzione nella definizione di nuovi modelli operativi e nell'allocazione di adeguate risorse umane, finanziarie e strumentali.

2. Architettura generale dei nuovi sistemi di sicurezza

L'impiego di sistemi ICT per la Sicurezza (o Protection) risale già ad alcuni decenni fa. Sinora il campo applicativo ha riguardato prevalentemente la protezione delle informazioni (dati) trattate dai sistemi informatici e telematici, e quella delle persone/beni mediante sistemi basati su una serie di dispositivi periferici, quali: videocamere, varchi di accesso e unità biometriche. Tuttavia grazie ai nuovi progressi del settore ICT nelle aree della potenza di calcolo, della memorizzazione, dei nanosensori e delle reti e servizi di comunicazione (Internet, reti TLC fisse e mobili, reti di satellitari di comunicazione e posizionamento), oggi si parla ormai di SdS basati sulla Network Centric Operation (NCO).

La NCO è una metodologia operativa, adottata in campo civile e militare, che deve il suo sviluppo al Dipartimento della difesa USA, il quale, alla fine degli anni '90 del secolo scorso decise di innovare completamente il proprio sistema di comando e controllo sfruttando al massimo i risultati del mondo ICT nei settori delle reti di telecomunicazioni, del calcolo distribuito (GRID Computing) e dei nuovi sensori. L'obiettivo di tale programma, denominato Joint Vision 2020, era appunto, quello di dar vita ad un nuovo modo di operare della difesa USA, passando da una visione centralizzata (platform-centric) ad una distribuita (network-centric) che puntasse molto anche sul ruolo delle persone in

FIG. 1 - AMBIENTE OPERATIVO DI UN SdS PER LA SICUREZZA



campo. Il tutto con l'intento di affrontare meglio le nuove sfide di sicurezza interna e di governance dei conflitti internazionali dove spesso, come nel caso del terrorismo, esiste una forte asimmetria in termini di forza, tecnologia e metodi di scontro. Il programma confidava in un rivoluzionario contributo dell'ICT nel modo di affrontare il problema della difesa, contributo che doveva essere paragonabile a quello che l'E-Business stava dando al classico modo di fare Business.

Dopo l'attacco alle torri gemelle del 2001, il governo USA emanò per la sicurezza civile l'Homeland Security Act 2002 (per la cui implementazione creò un apposito dipartimento responsabile anche della prevenzione dei disastri naturali), che prevede l'impiego di metodologie di NCO.

L'adozione di un approccio Homeland Security impone l'elaborazione di un innovativo modello di connessione e cooperazione delle forze in campo (persone, infrastrutture di comunicazione/elaborazione e dispositivi operativi/terminali), in grado di far acquisire una posizione di vantaggio nella lotta asimmetrica contro le minacce, riducendo al minimo i danni. Ciò di fatto si traduce nella messa a punto di un paradigma che tenta di raggiungere il vantaggio operativo (Decision & Operation Superiority) partendo da quello informativo (Information Superiority) e dalla distribuzione delle responsabilità delle operazioni fino all'ultimo degli addetti sul campo.

Non sono pochi quelli che ritengono che l'Homeland Defence (area militare) e l'Homeland Security, rappresentino oggi il contesto operativo e tecnologico dual-use da cui sta nascendo buona parte del futuro dell'ICT, della logistica e dei modelli di cooperazione nell'era della Globalizzazione. Molte importanti Università e società del settore ICT sono impegnate in questo grande sforzo di ricerca e sviluppo.

L'idea di usare la metodologia NCO nel settore civile, con la creazione di quello che possiamo chiamare Network Centric Protection System (NCPS), è ormai adottata da molti paesi sviluppati. Anche in Italia il tema è oggetto di iniziative istituzionali e industriali.

Va sottolineato che l'NCPS, che è un SdS, può essere adottato in tutti gli scenari: sicurezza urbana, monitoraggio ambientale, protezione civile, ecc.

Dal punto di vista concettuale un NCPS opera sostanzialmente una transizione da un'architettura fatta da tanti sistemi separati ad un insieme di sistemi che cooperano (v. fig. 2).

Ognuno di questi è dedicato ad una o più missioni: sicurezza urbana, sicurezza regionale, protezione delle infrastrutture critiche, monitoraggio del rischio idrogeologico, ecc. Un sistema a sua volta può essere organizzato in sottosistemi a cui corrispondono dei domini funzionali/territoriali di competenza: per es. nell'ambito della sicurezza di un'area metropolitana ci possono essere più sottosistemi di tele sorveglianza, ognuno facente capo ad un Centro Operativo comunale che interagisce con uno centrale della Polizia di Stato, con il Sistema Informativo del Comune locale, dell'infomobilità cittadina, e così via, vedi fig. 3.

In altri termini ogni sistema o sottosistema, ha delle sue specificità sia per quanto riguarda i dispositivi terminali gestiti che per la rete di connessione e le funzioni applicative implementate. Infatti bisogna immaginare che in ogni scenario operativo esistono sul

campo vari dispositivi/sensori (videocamere, barriere di delimitazione di aree protette, rilevatori di oggetti o sostanze pericolose), alcuni in dotazione ai diversi operatori (palm-top, caschi con visori e connessioni wireless), collegati ad apparati e centri operativi gestiti tipicamente da un solo ente. L'innovazione introdotta con la nuova architettura consiste nel fatto che le informazioni gestite da un tale ente gestore, così come le sue operazioni, vengono integrate, grazie alle tecnologie ICT, con quelle di altri enti in modo da realizzare un'azione di supervisione e coordinamento più efficiente ed efficace. Il tutto con lo scopo di raggiungere quel vantaggio decisionale ed operativo per combattere, e possibilmente annullare, le minacce alla sicurezza delle persone, dei beni e dell'economia di un territorio.

Spesso si suole indicare l'approccio NCPS anche come creazione di un "Ambiente Intelligente" per la sicurezza, cioè di un contesto in cui sono possibili nuove funzioni di prevenzione e protezione dalle minacce grazie alla capacità di monitorare e controllare gli elementi del contesto stesso.

Una tipica organizzazione delle

Fig. 2 - SCHEMA DI RIFERIMENTO DI UN NCPS



funzioni di uno dei sistemi/sottosistemi del NCPS è quella riportata in fig. 4, in cui si vede che ognuno di essi di norma supporta delle funzioni di: comunicazione; servizi di gestione dei componenti della rete/sistema, sicurezza e distribuzione delle informazioni; elaborazione locali tipiche di un ambiente distribuito di apparati/dispositivi/sensori; elaborazioni globali per tutto l'SdS; gestione delle informazioni possedute (incluse le funzioni di "intelligence" attraverso i dati); funzioni applicative specifiche.

Dal punto di vista tecnico la realizzazione di un NCPS pone complessi problemi sia per quanto riguarda i dispositivi sul campo che per l'intera sistemistica. Certamente sono necessari sottosistemi in grado di memoriz-

zare e trattare grosse quantità di informazioni, così com'è necessario l'impiego di infrastrutture di comunicazione a larga banda. Inoltre è indispensabile l'adozione di avanzate soluzioni sistemistiche per la sicurezza delle informazioni trattate e l'affidabilità e disponibilità dell'intero sistema.

3. La sicurezza urbana

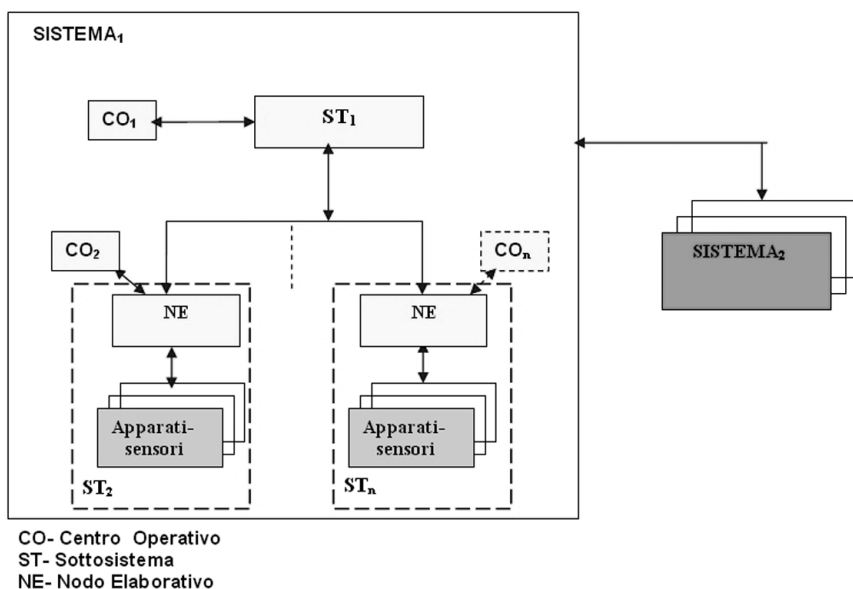
Uno dei temi attualmente più sentiti dall'opinione pubblica italiana è quello

della sicurezza del cittadino nel contesto urbano, con particolare attenzione alla protezione da atti criminali. Come già detto in precedenza, la Sicurezza Urbana necessita di un combinato di azioni che comprendono adeguate politiche sociali, speciali criteri di progettazione architeturale degli ambienti urbani (la cosiddetta Cepted-Crime prevention through environmental design) e la sorveglianza operata dalle forze dell'ordine a ciò preposte. Con riferimento a quest'ultima tipologia di intervento, va detto che sulla spinta della continua sollecitazione a tutelare maggiormente la collettività e a vigilare sulla sicurezza personale del cittadino, in Italia le varie istituzioni centrali e locali stanno delineando alcune direttrici di intervento:

- favorire la stretta collaborazione tra le forze di Polizia (incluso quella Municipale), garantendo interscambio informatico e coordinamento operativo;
- programmare servizi congiunti rivolti in particolare al controllo delle aree critiche o a maggiore rischio;
- rassicurare la comunità, anche con l'impiego dei volontari della sicurezza, nella vigilanza delle aree verdi e dei luoghi a rischio;
- prevenire le forme di microcriminalità, di violenza e delitti di vario genere.

Una serie di progetti sono stati messi in atto e tutti hanno un comune denominatore: l'uso esteso di sistemi integrati di videosorveglianza.

FIG. 3 - ARCHITETTURA GENERALE DEL NCPS



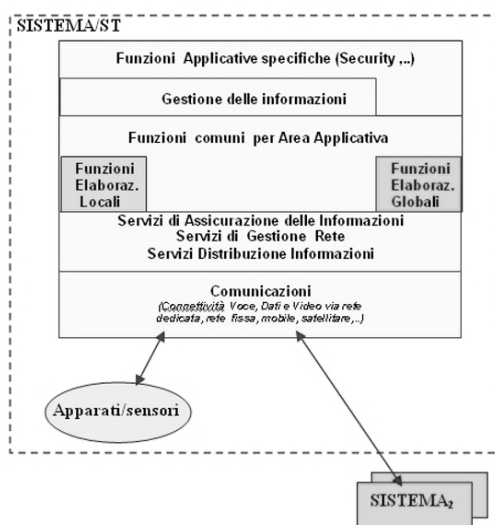
Ad esempio, il Comune di Reggio Emilia è in procinto di realizzare un sistema complesso di videosorveglianza, nell'ambito del Progetto Reggio Sicura. Tale realizzazione avviene con la collaborazione costante ed attiva delle forze dell'ordine (Questura e Carabinieri), che oltre a definire le aree più a rischio (effettuano o forniscono una mappa del rischio), sono anche i titolari del trattamento delle immagini. Complessivamente il sistema di videosorveglianza sarà composto da 217 videocamere sul territorio, collegate attraverso una rete in fibra ottica a 21 video-server (si tratta di un'estensione della rete Lepida), 3 centrali operative presso il Comando Provinciale dei Carabinieri, la sede della Questura e la sede della Polizia Municipale (visione delle sole immagini del monitoraggio del traffico). A tutto ciò sono aggiunte 2 telecamere su 50 autobus Azienda Consorziale Trasporti, un sistema di radio-localizzazione su 43 veicoli della Polizia Municipale ed una Stazione Base presso la Polizia Municipale.

Per verificare l'efficacia di tale sistema è stato inoltre predisposto un sistema di valutazione progressivo sull'evoluzione del senso di sicurezza percepito dai cittadini. Interventi simili sono stati già messi in atto o sono per esserlo in molte aree del paese.

Lo stesso approccio sarà adottato anche nell'area napoletana, secondo le recenti affermazioni del Ministro Amato nell'ambito del "Piano di Sicurezza per Napoli". Anzi, la città di Napoli e la sua provincia dovrebbero diventare la prima area italiana interamente videosorvegliata, estendendo il monitoraggio alle scuole, tratti autostradali, ecc.

Allo stato molti dei sistemi di videosorveglianza in funzione per proteggere infrastrutture, aree riservate e zone urbane, sono basate su sistemi centralizzati. Alcuni di essi prevedono architetture che utilizzano stazioni di videosorveglianza (che integrano una videocamera) con una console di controllo e registrazione. L'accesso ai dati è effettuato mediante applicazioni basate su Web. Ciò consente di rispar-

FIG. 4 - ARCHITETTURA FUNZIONALE DI UN SISTEMA/SOTTOSISTEMA DEL NCPS



miare sulla rete di interconnessione e sull'architettura per l'accesso ai dati, ma è adatta a reti di poche videocamere.

Con lo sviluppo delle Wide Area Network (WAN) e di Internet sono state realizzate anche soluzioni basate su una connessione ad un server, per esempio della rete Internet, permettendo così la realizzazione di un sistema composto da un alto numero di videocamere con un controllo distribuito.

Come indicato al par. 2, i recenti sviluppi nell'ambito dei sensori video stanno rendendo possibile la realizzazione di reti complesse, costituite da un numero elevato di videocamere, in grado di fornire una copertura visuale ottimale di spazi pubblici molto ampi (piazze, aeroporti, stazioni). Tuttavia, al crescere della complessità di queste reti, del numero di sensori, nonché del livello e numerosità delle attività in corso di svolgimento nelle aree pubbliche monitorate, esiste un reale problema di sovraccarico per gli operatori addetti alla sicurezza: è impensabile che un operatore umano sia in grado di controllare mentalmente (o comunque in modo non automatico) un numero così elevato di flussi video, identificare gli eventi rilevanti ai fini della sicurezza e intraprendere azioni di monitoraggio preventive (ad esempio impostare uno zoom su alcune aree di interesse oppure su alcuni soggetti sospetti in modo da acquisire

uno o più immagini sul loro aspetto fisico). Inoltre, è altrettanto impensabile aumentare il numero di persone addette a controllare i flussi video di singole telecamere o gruppi di esse.

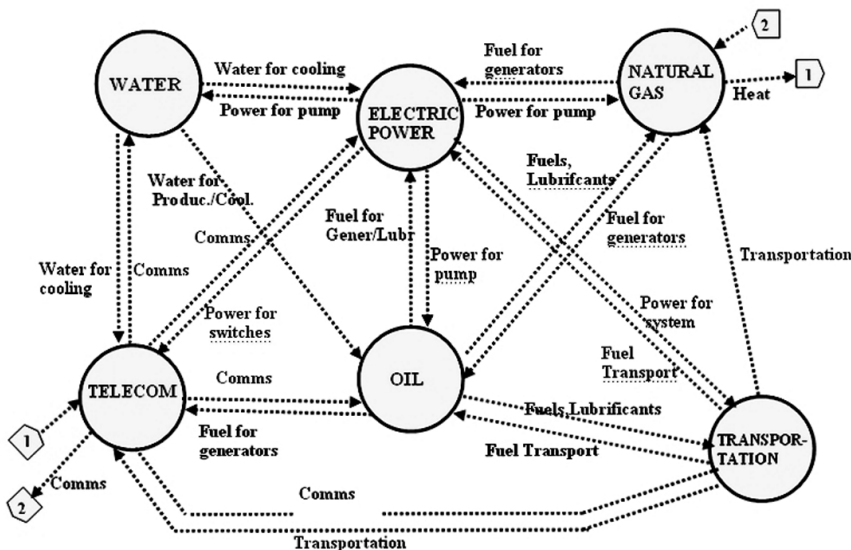
Di conseguenza una sfida tecnologica è quella di progettare e realizzare reti di sensori video capaci di svolgere le proprie attività di monitoraggio e rilevazione di comportamenti anomali in modo autonomo e cooperativo. Tali sistemi dovranno seguire un approccio NCO ed essere in grado di minimizzare l'intervento umano, senza tuttavia escluderlo, come richiesto in molti contesti *mission-critical*. In questa ottica, la telecamera non è vista più come sensore passivo, che ha il compito solo di

acquisire il segnale video per poi trasferirlo ad un'entità intelligente centralizzata, bensì come un nodo intelligente in una rete di sensori intelligente e flessibile, in grado di cooperare con i suoi vicini nel rilevare gli eventi critici e nel decidere cosa fare. Ad esempio una videocamera potrebbe autonomamente rilevare un evento critico e decidere di seguire una persona in un'area affollata.

Sono stati proposti così diversi modelli di reti di telecamere intelligenti. Per esempio si è proposto un modello in cui ogni nodo è a conoscenza dei suoi vicini; le attività di videosorveglianza sono messe in atto da gruppi di uno o più nodi, creati dinamicamente definendo dei parametri per la condivisione delle informazioni e il livello di mutua collaborazione. Il comportamento complessivo della rete dipende dal processo di *decision making* locale, messo in atto da ciascun nodo, e della comunicazione inter-nodo (internodale).

In linea con questi approcci alla videosorveglianza per sistemi di sicurezza urbana, il progetto "Laboratorio di Ambient Intelligence per una Città Amica" (LAICA), svolto nell'ambito del Piano Telematico Regionale della regione Emilia Romagna, si è posto come scopo principale la definizione di modelli e tecniche innovative per l'Ambiente Intelligente. La visione dell'intero progetto si fonda sull'esi-

FIG. 5 - INTERDIPENDENZA DELLE INFRASTRUTTURE CRITICHE



stenza nel contesto cittadino di una rete di grande dimensione (large-scale), costituita da elementi sensoriali intelligenti, ossia dotati di capacità di elaborazione dati, oltre che di acquisizione e trasmissione. I sensori intelligenti sono di diverso grado di complessità e capacità di elaborazione, e di estrazione di conoscenza: dai semplici sensori di rilevazione ambientali, dotati di capacità di integrazione statistica dei dati, a matrici di sensori di prossimità, temperatura e posizione capaci di dare impulsi di pilotaggio ad attuatori o di triggering ad altri sensori, a sistemi di acquisizione di singole immagini (shot), a web-cam e sistemi di videosorveglianza.

Nel prossimo futuro si prevede che questi sistemi ereditano sempre di più le tecnologie, le metodologie, i protocolli tipici delle reti di sensori e dei sistemi distribuiti su larga scala, includendo sempre più diverse categorie di sensori e dispositivi (nanosensori, scanner di nuova generazione, ecc.), non solo limitati ai sistemi di videosorveglianza, ma anche ad altre applicazioni che vanno dall'antiterrorismo all'Home-Care. Tra i problemi delicati da gestire in tutti questi scenari applicativi c'è sicuramente quello della privacy dei cittadini.

4. Le infrastrutture critiche

Lo sviluppo tecnologico, finanziario e sociale dei paesi industrializzati dipende, e dipenderà sempre più, dalla

disponibilità e dal corretto funzionamento di quelle che vengono chiamate infrastrutture critiche 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, e così via. A causa di una serie di fattori di carattere normativo, tecnologico, economico e sociale, queste diverse infrastrutture vanno sempre di più considerate come vitali ed interdipendenti. Dove spesso il collante sono proprie le reti di telecomunicazioni o più in generale il cosiddetto *cyberspace* (vedi fig. 5 - Source CID Rinaldi, Peerenboom, Kelly 2002).

Queste interdipendenze da un lato possono favorire l'amplificazione delle conseguenze di un evento negativo e, dall'altro, le possono rendere più vulnerabili alle minacce criminali e naturali. E' proprio per queste ragioni che in tutti i paesi sviluppati, inclusi l'Italia, è stata posta un'elevata attenzione alla loro protezione.

Un'analisi condotta dal Ministero delle Comunicazioni insieme ad altri gruppi di lavoro a livello nazionale, ha evidenziato che le Infrastrutture Critiche potrebbero rappresentare nei prossimi anni un bersaglio per azioni di natura terroristica, condotte sia con metodi tradizionali tramite il *cyberspace* (cyber-terrorism), sia con azioni combinate (*swarming attacks*), ritenute

dagli analisti le più probabili.

A livello internazionale l'analisi dell'intera problematica riguardante la *Critical Infrastructure Protection (CIP)*, conferma che l'interdipendenza dovuta anche al *cyberspace* impone una particolare attenzione verso quella che è indicata come *Critical Information Infrastructure Protection (CIIP)*.

Gli Stati Uniti furono i primi, nel 1996, a percepire l'importanza della problematica iniziando una serie di analisi e studi che si concretizzarono, nel 1998, nell'emanazione da parte del presidente Clinton delle *Presidential Decision Directive 62 e 63*, il cui obiettivo era lo sviluppo di un programma mirato alla salvaguardia e protezione di queste infrastrutture per far sì che "qualunque interruzione o malfunzionamento di tali infrastrutture sia breve, infrequente e geograficamente circoscritto". Gli eventi dell'11 settembre del 2001 hanno poi accelerato l'impegno come dimostra la creazione del *Department of Homeland Security*.

Anche organismi internazionali quale il G8, la NATO e, l'ONU (con la 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) 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. Nella quasi totalità delle nazioni industrializzate sono state intraprese analoghe iniziative mirate alla comprensione del problema, alla sua contestualizzazione nelle realtà specifiche, all'individuazione di strategie per ridurre la vulnerabilità del sistema paese e alla predisposizione di piani di intervento in caso di emergenza, con la costante caratterizzazione di una forte cooperazione pubblico - privato. Infatti oltre alle azioni di protezione messe in atto dai singoli gestori delle infrastrutture, servono piani e strumenti di intervento che vedono il coinvolgimento di tutti gli attori in campo.

La situazione in Italia

In Italia si svolge un continuo sforzo per identificare i settori critici, in linea di massima si possono definire i seguenti settori:

- Bancario e Finanziario;
- Sicurezza ed Ordine Pubblico;
- (Tele-) Comunicazioni;
- Servizio Sanitario;
- Energetico e dei Trasporti (aereo, marittimo, terrestre);
- Pubblica Amministrazione;
- Servizio Idrico;

Il governo italiano proseguendo con il suo piano di modernizzazione e informatizzazione della P.A. (vedi i vari piani di azione dell'E-Government elaborati dal 2000 in avanti), ha ribadito l'importanza del CIP e CIIP. In particolare sono state definite delle regole per gli standard e la sicurezza ICT per i servizi della P.A., impegnando sin dall'ottobre del 2003 anche l'ISCOM (Istituto Superiore delle Comunicazioni) per la certificazione della sicurezza ICT su tutto il territorio nazionale. L'ISCOM svolge anche funzioni di gestione dell'OCSI, che ha come compito la definizione degli standard di sicurezza nel campo dell'ICT. In particolare la definizione delle linee guida IT-SEC, della ISO27001 e della ISO/IEC IS15408 (Common Criteria).

Nel Marzo del 2004 presso il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri, fu creato il *Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate*, per redigere un rapporto sulla situazione nazionale. Oggi come oggi esistono una serie di organismi che trattano il CIP e il CIIP, collegati alla Presidenza del Consiglio ed ai ministeri della delle Riforme e delle Innovazioni nella P.A. (ex MIT), delle Comunicazioni e dell'Interno.

Inoltre le sempre maggiori esigenze di sicurezza hanno fatto nascere anche organismi di supporto per la P.A., come il CERT (Computer Emergency Response Team) ed il GovCERT il quale non fa altro che coordinare il CERT stesso. Il CNIPA (Centro Nazionale di Informatica per la Pubblica Amministrazione), invece, che svolge il compito di sovrintendere tutte le problematiche di Information Technology della

Pubblica Amministrazione.

Il Ministero dell'Interno, delega invece alla Polizia Postale e delle Comunicazioni il compito di regolare, studiare nuove strategie di tecniche investigative per il computer crime, e la coordinazione con altri uffici. In particolare il Ministero dell'Interno, istituisce il CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) che ha il compito di salvaguardare le infrastrutture critiche nazionali ed adoperarsi nei casi di necessità. Tale centro infatti, oltre ad operare con le maggiori agenzie internazionali (Interpool, CIA, FBI), svolge anche attività di collaborazione con i maggiori players nazionali. In generale si conferma l'esigenza che tutti questi attori pubblici e privati, rientrino operativamente nella logica dell'NCPS facendo cooperare i loro sistemi e sottosistemi dedicati alla CIP o CIIP. In altre parole, anche per ridurre la complessità del tutto, se da un lato ogni gestore/attore rispondendo a delle normative e a delle guidelines mette su dei mezzi e strumenti di protezione specifici del proprio settore è bene poi che resti connessi ad un unico sistema nazionale. Ciò non solo per una corretta gestione delle emergenze ma anche per una corretta e trasparente azione di prevenzione.

5. Conclusioni

La presenza nella nostra società globalizzata di vari fenomeni che ogni giorno minacciano la sicurezza delle persone, delle cose e dell'economia di un territorio, sta facendo crescere l'esigenza da parte delle istituzioni e delle organizzazioni a ciò preposte di adottare nuove e più efficaci misure di protezione.

In particolare, oltre all'attuazione di adeguate politiche che tendono a ridurre il disagio sociale e ad aumentare il benessere collettivo, appare necessario un impiego ottimale delle moderne tecnologie per la sicurezza, ed in special modo di quelle ICT. In altre parole è indispensabile costruire nuove infrastrutture che realizzino sistemi basati su una metodologia NCO in grado di far cooperare tutte le forze in campo, raggiungendo il massimo dell'efficienza e dell'efficacia operativa. Ovvia-

mente, data la complessità dei problemi da affrontare e la continua evoluzione tecnologica in atto, il compito non è semplice. Notevoli sono gli sforzi di natura tecnologica e sistemistica che il settore della ricerca e delle imprese della sicurezza devono affrontare; così come sono elevati quelli culturali e organizzativi delle istituzioni ed organizzazioni a ciò preposte. Sicuramente un'adeguata diffusione anche in Italia di queste infrastrutture, unitamente alla creazione di una gestione unitaria della sicurezza a livello nazionale, sarebbe di grande beneficio per la tutela del nostro Paese; con tutto ciò che questo significa in termini di benessere delle persone e sviluppo economico dello stesso. Ovviamente si è coscienti del fatto che questi risultati, per l'impegno tecnico, organizzativo ed economico che richiedono, non possono essere ottenuti in un solo colpo. Tuttavia è importante procedere con determinazione nella direzione giusta.

ACRONIMI

- CERT - Computer Emergency Response Team
- CIP - Critical Infrastructure Protection
- CIIP - Critical Information Infrastructure Protection
- CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
- CNIPA - Centro Nazionale per l'Informatizzazione della PA
- CO - Centro Operativo
- Comms - Communications
- GRID Computing - Infrastruttura per il calcolo distribuito
- ICT - Information&Communication Technology
- IEC - International Electrotechnical Commission
- ITSEC - Information Technology Security Evaluation Criteria
- ISO - International Standard Institute
- NCO - Network Centric Operation
- NCPS - Network Centric Protection System
- NE - Nodo Elaborativo
- OCSI - Organismo di Certificazione della Sicurezza Informatica
- SdS - Systems of Systems
- ST - Sottosistema
- WAN - Wide Area Network