On. Gen. Luigi RAMPONI

Con il Patrocinio ed il contributo della
FINMECCANICA SpA

NUOVO TERRORISMO
LA CAPACITÀ DI DIFESA DEL SISTEMA PAESE

Atti del convegno promosso dal
Centro Studi Difesa e Sicurezza
a Roma il 20 aprile 2004

A cura di
Giuseppe CORDOVA
Salvatore SCURO

Edizione Ce.Stu.Di.S.
Palazzo Valdina - Piazza in Campo Marzio, 42 - 00186 Roma
Ten. 06 67604328/5712 fax 06 67604025 E-mail cestudis@inwind.it

SALUTO ED APERTURA DEL CONVEGNO

Ringrazio tutti coloro che hanno accettato il mio invito. Come vedete ho dato un taglio diverso allo svolgimento di questo convegno: le altre volte il discorso si snodava attraverso interventi successivi; questa volta, invece, ho ottenuto la collaborazione di tre bravissimi e gentilissimi giornalisti, i quali terranno le fila dei tre dibattiti, riferiti ai settori dell'Energia, dei Trasporti e delle Telecomunicazioni nel tentativo di variarne e di renderne ancora più interessante lo svolgimento.

Questo secondo convegno, organizzato sulla strategia degli interventi da adottare nei riguardi del nuovo terrorismo, nasce dalle considerazioni fatte la volta scorsa. In quell'occasione il convegno entrava nel merito dell'impegno delle strutture del settore pubblico nei confronti della minaccia terroristica: tuttavia ci accorgemmo tutti che il settore pubblico non poteva assumersi da solo questo onere data la macroscopicità della minaccia. Questa constatazione chiama in causa il settore privato che deve essere sensibilizzato a predisporre operazioni di prevenzione e di attenuazione degli effetti di possibili attacchi. In questo convegno, allora, analizzeremo in quali termini il privato può gestire il problema, naturalmente tenendo bene a mente quali siano le caratteristiche della minaccia e quale sia la strategia da adottare. Questi concetti li esponemmo dettagliatamente la volta scorsa, ma credo sia opportuno ricordarli.

On. Luigi RAMPONI
Presidente del Centro Studi Difesa e Sicurezza

On. Luigi Ramponi
Presidente IV Commissione Difesa Camera dei Deputati
Presidente del Centro Studi Difesa e Sicurezza

STRATEGIA INTERVENTO PREVENTIVO

La minaccia portata alla società civile, alla struttura statale, dal nuovo terrorismo è minaccia globale. Globale in termini di origine etica, spirituale, ideologica, politica; globale in termini di origine geografica, globale in termini di possibilità di manifestazione attuativa nei confronti di qualsiasi settore della vita pubblica.

Tale aspetto di globalità richiede una azione di contrasto, ispirata e sostenuta da una **strategia globale**. Per definire tale strategia è indispensabile conoscere bene le caratteristiche di tale minaccia.

- È una minaccia **DIFFUSA** nel senso che può **ORIGINARSI** e **MANIFESTARSI** in ogni parte del mondo, là dove avvengano tensioni di varia origine, che possono diffondersi ed espandersi in qualsiasi altra area e colpire direttamente ed indirettamente interessi nazionali umani ed economici.
- È una minaccia che può **colpire pressoché dovunque** considerato il fatto che la moderna società è società libera, aperta, con strutture tecnologicamente avanzate che hanno consentito e sempre più vanno consentendo una elevata qualità della vita, ma che, nel contempo, rendono tutta la struttura sociale enormemente più vulnerabile.
- È una minaccia **VOLATILE**, difficile da determinare e da inquadrare perché:
    1. non richiede grandi e pesanti strutture;
    2. non richiede grandi, potenti, sistemi d'arma;
    3. non richiede una pesante organizzazione.
- È una minaccia nei cui confronti **non vale la ritorsione**, perché una volta subito l'atto terroristico le possibilità di rifarsi sono insignificanti. Una volta portato l'attacco il terrorista ha raggiunto il suo scopo, il suo effetto, il suo successo.
- È una minaccia **Asimmetrica** perché ottiene molto con poco e può colpire con mezzi limitati ed ottenere effetti devastanti materiali e psicologici.

- È una minaccia **ETEROGENEA** che può oggi avvalersi dei mezzi più disparati (N.B.C., tradizionali, cibernetici) e colpire qualsiasi parte o componente della organizzazione sociale.
- È minaccia che per essere portata a termine richiede risorse limitate: costa poco ed ha un enorme rapporto costo-efficacia.
- È una minaccia molto spesso fortemente **ISPIRATA** in termini etici, razziali, religiosi, culturali. Tali motivazioni, possono raggiungere il sovrumano e assicurano una forza, una carica, agli adepti che mette in crisi qualsiasi azione di contrasto basata sul senso di conservazione dell'essere umano.

Di fronte ad una minaccia di tale portata e di tale globalità, di fronte ad una vulnerabilità pressoché estesa a tutta la struttura del funzionamento della moderna società, di fronte al possibile effetto domino che può derivare anche da un solo attacco ad un punto nevralgico del sistema di guida e controllo dell'erogazione di uno qualsiasi dei servizi fondamentali per la società (energia, trasporti, sanità, comunicazioni, ecc...), di fronte al possibile coinvolgimento a catena di percentuali enormi di popolazione, con ulteriori effetti derivati di portata disastrosa, di fronte a questo reale e possibile scenario, debbono essere assunte decisioni e predisposizioni adeguate con carattere di globalità ed essere, per vastità di respiro, pari alla vastità ed entità della minaccia.

In un precedente convegno abbiamo individuato la strategia che deve ispirare l'azione di difesa e di contrasto. Tale strategia, abbiamo detto, deve assolutamente essere preventiva, per poter avere obiettive possibilità di successo.

Abbiamo poi preso in esame gli sviluppi attuativi di tale strategia nell'ambito delle strutture di difesa e controllo dello Stato, sia in termini di provvedimenti di difesa e prevenzione sia in termini di iniziative di repressione.

Vi prego di consentirmi un paio di osservazioni che desidero fare a margine dell'odierno convegno, riferite appunto a quello precedente.

In quell'occasione ebbi a dire: «l'azione di contrasto deve interessare tutto l'arco dell'organizzazione societaria e vista la caratteristica di impossibilità di efficace azione di ritorsione deve essere PREVENTIVA. Sì, una strategia preventiva che deve "anticipare" la possibilità di condurre e subire attacchi terroristici. Tale strategia non deve essere applicata solo all'azione militare come si tende, sbagliando, a credere. L'opzione militare rimane l'estrema importantissima carta da giocare contro il terrorismo, ma è l'ultima risorsa. Prima di lei la strategia preventiva deve ispirare: la politica nazionale e internazionale, l'azione diplomatica, l'attività di intelligence, la sicurezza interna, l'attività economica/finanziaria, la sicurezza ambientale, la sicurezza cibernetica.

Naturalmente, proprio per questo, l'adozione attiva e reale di intervento militare, prevista da tale strategia, deve avvenire quando si rivelasse opportuna, necessaria e nel momento dovuto, senza attese o tentennamenti controproducenti e rischiosissimi, **ma sempre a seguito di decisione del Consiglio di Sicurezza delle NU**».

Ebbene: in una riunione informale dei suoi ministri degli Esteri svoltasi a Bruxelles all'inizio del mese, la Nato ha potenziato la propria strategia antiterrorismo. L'Alleanza atlantica ha ribadito che continuerà a combattere il fenomeno in tutto il mondo con mezzi «politici, diplomatici, economici» e, solo «se necessario, militari», (sempre comunque nel rispetto della Carta delle Nazioni Unite).

Seconda considerazione. Agli inizi del mese una operazione programmata dal Ministero degli Interni e condotta da Carabinieri, Polizia e Servizi Intelligence, ha portato all'individuazione/controllo di 161 individui, sospettati di connessione con l'area del fondamentalismo islamico.

Tale operazione è stata definita **Operazione preventiva**.

Siamo nel pieno di quella Strategia Preventiva, illustrata nel convegno al quale ho fatto riferimento, e alla conferma che tale strategia deve essere adottata e riguardare come dissi allora tutte le componenti istituzionali dello Stato. Nel caso citato il discorso ha riguardato strutture di Intelligence e strutture di Sicurezza e interesserà anche la Magistratura.

Ma la tipologia e la magnitudo della minaccia non può essere fronteggiata solo dalle istituzioni dello Stato, che pur debbono fare la loro parte che rimane fondamentale.

Il settore pubblico non può da solo assumere l'onere della prevenzione-protezione nei confronti della minaccia che è globale per il dove e per il come e per il quando. La difesa nei confronti del neoterrorismo deve vedere impegnato e coinvolto anche il settore privato. Solo una sinergia che veda un impegno integrato del pubblico e del privato può avere possibilità di successo.

E non basta. Oltre alla necessità di prevenire gli attacchi e di difendere i possibili obiettivi, la eterogeneità della minaccia, la vulnerabilità delle strutture di funzionamento della vita della società e il pericolo incombente del-

l'effetto domino impongono anche la necessità di predisporre misure di emergenza per circoscrivere, attenuare, ovviare ad effetti di portata macroscopica nei confronti della società, conseguenti ad un attacco riuscito da parte del terrorismo.

I tempi di un convegno e le obiettive capacità di pazienza e di disponibilità all'ascolto dell'uditorio sono tali da non consentire un esame esauriente di una così vasta problematica.

Si può tuttavia prendere in esame alcuni dei settori più significativi e di maggiore importanza della rete di funzionamento dei servizi generali per la vita della società al fine di analizzare e mettere in evidenza in quali termini, in sede di partecipazione alla lotta contro la minaccia del neoterrorismo, sono state assunte iniziative e predisposizioni.

In tale contesto verranno esaminati di seguito i settori dell'Energia, dei Trasporti, delle Telecomunicazioni.

Sono questi certamente settori fondamentali, ma, come ho detto dianzi, molti altri sono egualmente importanti quali quello della sanità, dell'ambiente, del credito, dell'informazione e altri che non vengono presi in esame dal convegno solo per ragioni obiettive di tempo.

L'illustrazione di un quadro di situazione, che dia una visione generale con carattere di completezza, anche per avere una idea esauriente della funzione di coordinamento e integrazione delle iniziative dei diversi settori, può e deve essere affidata al Capo del Dipartimento della Protezione Civile, istituzione che costituisce certamente il luogo dei punti sul quale convergono le varie urgenze ed esigenze di protezione e soccorso e il centro di snodo, impulso e coordinamento delle iniziative di difesa e di ristabilimento della situazione in termini di vivibilità. Sarà quindi il dottor Bertolaso ad aprire il discorso con un intervento: successivamente entreremo nel merito delle sessioni che prevedono l'approfondimento, condotto come dicevo dai giornalisti, che ancora ringrazio, nei tre settori dell'Energia, dei Trasporti e delle Telecomunicazioni. Ringrazio ancora una volta i presenti ed invito il dottor Bertolaso ad iniziare.

Dottor Guido Bertolaso
Capo Dipartimento della Protezione Civile

IL DIPARTIMENTO DELLA PROTEZIONE CIVILE

Grazie, Onorevole Presidente, per il Suo invito e per avermi affidato l'onore, e anche l'onere, di parlare oggi del tema del nuovo terrorismo e della capacità di difesa del nostro Paese, nel quale il coordinamento è soprattutto un termine da dizionario, di difficile applicazione nella realtà.

La ringrazio anche per aver coinvolto settori vitali per il funzionamento del Paese quali le Comunicazioni, l'Energia, i Trasporti, che, in genere, vengono trascurati nell'analisi e nella gestione di questa materia.

Aprirò il mio intervento con un riferimento alle attività, come le ha definite il Presidente, preventive, in merito alle quali non ritengo di disporre di competenze specifiche, se non di quelle derivanti dal partecipare e dal fornire il mio contributo ad una serie di Comitati e Gruppi di Lavoro, da tempo istituiti, che si occupano appunto del coordinamento della fase preventiva dove, peraltro, come abbiamo sentito, credo siano indiscusse la responsabilità e la competenza del Ministero dell'Interno e del suo Ministro, in particolare per quanto riguarda le forze di «intelligence» e di contrasto che possono essere messe in campo per evitare che accada qualcosa di grave al nostro Paese.

Purtroppo, le vicende quotidiane, che viviamo tutti con grande angoscia, non possono escludere l'ipotesi che anche l'Italia in un futuro, che speriamo non venga mai, sia coinvolta in qualche fenomeno di tipo terroristico. Giustamente, ricordo, il Capo della Polizia, Gianni De Gennaro, e gli altri che intervennero al precedente Convegno dissero in maniera chiara che riuscire a evitare un attentato terroristico è praticamente impossibile, vista la complessità, la dinamica, la terribile forza di impatto di questo tipo di offensiva. E il caso dell'11 marzo scorso tragicamente conferma questa analisi. Quindi, bisogna fare tutto il possibile nel campo della previsione e della prevenzione, che considererei come aspetti separati, e poi cercare di preparare al meglio la macchina per la gestione delle conseguenze, come ha detto il Presidente.

Noi infatti, a differenza di altri, ci concentriamo, anche su questa tematica, su di un «prima» e su di un «dopo»: il prima è il settore della previsione

e della prevenzione, con tutte le conseguenze e le responsabilità di guida, e il dopo, che, ripeto, speriamo non si verifichi mai, riguarda la gestione delle conseguenze di un atto, di un avvenimento. Vorrei riferirmi in modo un po' provocatorio ad un comunicato stampa dei primi di aprile:

«La decisione di chiedere ai comuni di stilare un piano unificato per affrontare le situazioni di emergenza gravi era scattato in seguito all'inchiesta sulla risposta agli attacchi terroristici dell'11 settembre 2001, che dimostravano deficienze ed imperfezioni delle comunicazioni e del coordinamento fra le operazioni delle diverse forze coinvolte. Le conseguenze di atti terroristici, esplosioni, incendi, crolli strutturali, fumi tossici, sostanze pericolose, devono essere neutralizzate per proteggere non solo le popolazioni, ma anche i soccorritori, poliziotti, pompieri, personale medico.

Ma secondo alcune fonti, il progetto per predisporre un piano di emergenza è ancora in alto mare, a causa di ritardi burocratici e di disaccordi, tra una serie di strutture competenti, su chi deve avere aver il controllo delle risposte ad un attacco terroristico: "Un ente vuole sempre avere il comando di tutto", ha detto il vice responsabile di un settore. "Pretendono che noi stiamo in secondo piano", ha aggiunto, "ma questo non è accettabile, soprattutto perché ci sono degli egoismi di mezzo"».

Ho deliberatamente evitato di nominare le organizzazioni e i personaggi cui questo comunicato stampa si riferisce, che invece li nomina espressamente e che riguarda un articolo comparso in prima pagina sul New York Times del 4 aprile scorso, relativo alla predisposizione dei piani di emergenza di New York. E questo è lo stato dell'arte in una città che l'11 settembre 2001 ha vissuto la tragedia che conosciamo e che ci consente di fare considerazioni del tipo «tutto il mondo è paese». Anche altri Paesi europei non sono affatto sicuri di essere riusciti a mettere in piedi corrette misure di emergenza. Non vedo per quale ragione noi dovremmo essere già assolutamente preparati e in grado di fronteggiare qualsiasi tipo di situazione: certamente possiamo affermare che molte cose sono state fatte; siamo riusciti a realizzare grossi passi avanti, forse anche più di altri Paesi, che, dal punto di vista tecnologico e organizzativo, ritengono di essere più avanti di noi.

Nel campo del «prima» o, comunque, della prevenzione, da tempo sono state messe in piedi azioni di contrasto e di «intelligence», delle quali ovviamente non è mio compito occuparmi. Vorrei, però, ricordare che esiste nel nostro Paese un meccanismo organizzativo che funziona, e al cui vertice è

posto il cosiddetto Nucleo Politico Militare, da tempo istituito presso la Presidenza del Consiglio dei Ministri e presieduto dal qui presente Generale Dino Tricarico, Consigliere Militare del Presidente del Consiglio. Attorno al tavolo del Nucleo Politico Militare siedono tutte le Amministrazioni responsabili di attività che siano in qualche modo connesse con la prevenzione di queste problematiche.

Esiste un «Manuale per la gestione delle crisi», che risale al 1994 e che è giustamente in fase di ridefinizione, alla luce delle vicende che hanno interessato non solo l'Italia, ma tutto il mondo nel corso di questi ultimi anni. C'è poi una serie di Comitati e di strutture tecnico-scientifiche di coordinamento che in qualche modo discendono dal Nucleo Politico Militare: innanzi tutto la Commissione Interministeriale Tecnica per la Difesa Civile, costituita nell'ambito del Ministero dell'Interno, nella quale sono rappresentate tutte le Amministrazioni che debbono elaborare i piani di organizzazione di Difesa Civile per gli specifici settori di competenza; presso il Ministero delle Infrastrutture sono insediate le Commissioni Interministeriali per la Sicurezza del Trasporto Aereo, del Trasporto Navale e altre che consentono alle diverse Amministrazioni di predisporre propri piani e di dare indirizzi alle strutture che gestiscono i servizi, compresi quelli dei quali oggi si parlerà in questo Convegno, e che poi riferiscono direttamente al Nucleo Politico Militare. Questo, a seconda delle situazioni, si riunisce una volta al mese oppure una volta alla settimana per analizzare in dettaglio le problematiche e definire le iniziative che debbono essere adottate. Diciamo quindi che, da un punto di vista organizzativo, esiste nel nostro Paese un meccanismo che riesce a superare nella fase preventiva il non facile problema del coordinamento e che consente che la discussione e la definizione degli eventuali rischi nonché l'identificazione delle possibili soluzioni vengano appropriatamente affrontate nelle varie sedi.

Il Nucleo Politico Militare rappresenta un punto cardine, uno snodo fondamentale, soprattutto per le esercitazioni che si svolgono, come ricordava il Presidente Ramponi, in ambito Nato; infatti, con cadenza quasi mensile, vengono realizzate esercitazioni di diverso tipo che hanno attinenza con la problematica terroristica. Recentemente ne è stata organizzata una che riguardava un'ipotesi terroristica portata dall'aria; nel corso del prossimo mese ne verrà organizzata un'altra che riguarderà i sistemi marittimi e i sistemi di comunicazione navale. Sono molte le attività in fase di realizzazione e di svi-

luppo e credo che il Generale Tricarico possa confermare l'efficacia di questa forma di coordinamento. Ovviamente, nessuno può illudersi che sia sufficiente fare prevenzione su base nazionale, quando si affrontano argomenti di questo genere: si deve passare necessariamente al livello internazionale, coinvolgendo le strutture multilaterali che hanno competenze specifiche, in particolare nell'ambito Nato, dove, posso dire, il nostro ruolo si sta sempre più affermando, anche con specifico riferimento a questo settore.

Più complessa, anche se non dovrebbe essere così, è la questione della fase successiva, ovvero della eventuale gestione delle conseguenze. In effetti, fino a quando si parla di attività di prevenzione, tutti possono ritenersi in grado di realizzare iniziative, pur sapendo bene, come ho detto all'inizio, che l'attentato terroristico verrebbe attuato con quella capacità, con quella fantasia, con quella organizzazione, che, purtroppo, è stata dimostrata sia a New York che a Madrid, e che è difficile per chiunque prevenire.

I bersagli sono troppi, e troppe sono le variabili: occorrerebbe disporre di forze di dimensioni impressionanti e neanche in quel caso si riuscirebbe ad evitare con certezza qualsiasi attacco. Insomma, non esiste un vaccino sicuro al cento per cento. Tutto quello che si può fare, per quel poco che so e per quel poco che mi riguarda, è stato sicuramente messo in piedi, anche e soprattutto dal nostro Paese. Ma, ripeto, cosa accade se un attentato viene effettivamente organizzato e realizzato in Italia? Nella distinzione tra il prima e il dopo non mi sembra che si rinvengano motivi di discussione, come esporrò rapidamente ed evitando di fare commenti, perché ritengo che quello che serve oggi al nostro Paese siano unità di intenti e possibilità di dare certezze e tranquillità ai nostri concittadini, non certo di alimentare conflitti di competenze: si tratta semplicemente di riuscire ad applicare le normative vigenti.

Il «dopo» si inserisce nella realtà della Protezione Civile del nostro Paese, che è molto particolare e diversa da quella degli altri Paesi, non fosse altro che per i tipi di rischi che interessano l'Italia: essi sono, sia dal punto di vista naturale che da quello antropico, molto superiori a quelli degli altri Paesi europei: mi riferisco al rischio vulcanico, al sismico, all'idrogeologico, agli incendi boschivi, oltre che ai rischi indotti dall'uomo.

Il Dipartimento, come sapete, si può considerare il quartier generale del Servizio Nazionale della Protezione Civile, istituito con la legge 225 del 1992.

Il Dipartimento, che peraltro esiste sin dal 1980 a seguito del terremoto dell'Irpinia, si occupa per legge di tutta una serie di attività soprattutto basate su previsione, prevenzione e soccorso e, quindi, sul superamento dell'emergenza. Questo nell'ambito delle esigenze tradizionali di protezione civile. È evidente che il discorso di previsione e prevenzione non si applica alle attività strettamente connesse alla sicurezza del Paese.

L'originalità del nostro sistema di Protezione Civile rispetto a quello degli altri Paesi sta nel fatto che sono strutture operative del Servizio Nazionale della Protezione Civile tutte le istituzioni e tutti i rappresentanti della società civile. Nessun ente dello Stato centrale, né dello Stato periferico, né dei rappresentanti della società civile è escluso dall'essere componente operativa del Servizio Nazionale di Protezione Civile, come il Corpo Nazionale dei Vigili del Fuoco, che, come la legge ricorda, è la struttura fondamentale del sistema; le Forze Armate; le Forze dell'Ordine; il Corpo Forestale; la Guardia Costiera; i Gruppi scientifici che fanno ricerca applicata; il Servizio Sanitario Nazionale; le Organizzazioni di volontariato e la Croce Rossa Italiana; le Società che erogano servizi, soprattutto primari.

Oggi, il Presidente del Consiglio è il responsabile politico della Protezione Civile. È la prima volta, da quando quest'ultima esiste, che il Presidente del Consiglio si avvale del Dipartimento della Protezione Civile per coordinare dodici Ministeri dell'Esecutivo, le Regioni, le Province e i Comuni, l'Istituto Nazionale per la Geofisica e la Vulcanologia, l'ENEA, l'APAT, il Corpo Forestale e le Forze Armate. Il coordinamento, a livello territoriale, avviene attraverso i Prefetti, che, voglio ricordare, sono rappresentanti del Governo e non di un solo Ministero. Come vedete, non viene esclusa nessuna componente: questa è la vera Unità di Crisi del Paese, pronta ad affrontare qualsiasi situazione di emergenza che possa avere conseguenze sulla salute dei nostri concittadini. In aggiunta a questa struttura permanente, di volta in volta, sulla base delle caratteristiche delle specifiche emergenze, entrano automaticamente a far parte del Comitato Operativo di Protezione Civile altre componenti che possono avere un ruolo specifico nella gestione di determinate situazioni: dal Registro Italiano Dighe alle strutture che si occupano della gestione dei trasporti stradali, dei trasporti ferroviari, del trasporto aereo, ai Servizi di Informazione, alle strutture responsabili delle comunicazioni e dell'erogazione dell'energia elettrica. Dunque, come si vede, una realtà operativa ben oleata: ogni Amministrazione ha un proprio

rappresentante permanente in questa Unità di Crisi, che di volta in volta viene convocata o per prepararsi ad affrontare eventuali emergenze o, soprattutto, per gestire le emergenze che dovessero accadere.

La normativa di riferimento è la legge 225, approvata nel 1992, a seguito di un percorso un po' tribolato: il Presidente della Repubblica dell'epoca, Cossiga, la rinviò infatti alle Camere a causa di resistenze da parte di alcune Amministrazioni che temevano di essere esautorate nelle proprie competenze. Di cosa si occupa la Protezione Civile? Degli eventi naturali e di quelli connessi con l'attività dell'uomo. Questo è il punto fondamentale: la normativa non opera una differenza netta tra le emergenze conseguenti ad un'eruzione vulcanica o ad un terremoto o ad un'alluvione, e quelle derivanti da atti commessi dall'uomo, sia involontari che volontari. Su questo mi pare che non ci siano dubbi. Nel 2001 (legge 401 del 2001), il Governo ha modificato parzialmente l'impianto organizzativo della Protezione Civile. Come sapete, era stata immaginata la costituzione di un'Agenzia indipendente, ma l'ipotesi fu accantonata e il Governo ritenne opportuno ricondurre nell'ambito della Presidenza del Consiglio la responsabilità sia politica che tecnica della Protezione Civile. Nessuna Agenzia, la meglio organizzata, la più efficace, sarebbe infatti mai riuscita a coordinare Ministeri come quello dell'Interno, della Difesa, delle Infrastrutture, e le altre Amministrazioni che, come sappiamo bene, non hanno alcuna intenzione di essere coordinate da una Agenzia indipendente, ancorché sotto la vigilanza di uno dei Ministri componenti del Governo. L'unica struttura che riesce a garantire in Italia, e non sempre, il dialogo e la collaborazione fra tutte le Amministrazioni, è la Presidenza del Consiglio dei Ministri; su questa evidenza si è basata la decisione del Governo nel settembre 2001; successivamente è anche stata immaginata (legge 286 del 2002) la possibilità che, in caso di eccezionali situazioni di emergenza, il Presidente del Consiglio possa predisporre che il Capo della Protezione Civile diventi in automatico il Commissario di Governo che provvede al coordinamento di tutti gli interventi ancor prima della dichiarazione dello stato di emergenza che deve essere adottata dal Consiglio dei Ministri. Quindi, se accade qualcosa in questo momento ed è necessario intervenire nel giro di un minuto, grazie a questa disposizione del Presidente del Consiglio, il Capo della Protezione Civile può adottare i necessari interventi e disporre direttamente di tutte le strutture operative e delle componenti del Servizio Nazionale.

Per quanto riguarda l'Unità di Crisi, essa è stata istituita con il decreto legge 83 del 2002 nell'ambito del Ministero dell'Interno, per gestire i diversi aspetti della sicurezza. L'articolo che la riguarda recita:

«L'Unità di Crisi tiene costantemente informato il Ministro, che riferisce con immediatezza al Presidente del Consiglio dei Ministri per l'eventuale conseguente attività di coordinamento».

Ecco quello che la Presidenza del Consiglio dei Ministri deve fare: il coordinamento, che non sottende affatto il concetto di comando o di imposizione; in periodo di pace, coordinamento significa dialogo, confronto e analisi; in periodo di «guerra», coordinamento significa dare direttive chiare e tempestive, che possano consentire a tutto il Paese di rispondere come i nostri concittadini chiedono.

Desidero ricordare che quando il Governo prese in esame questo articolo del decreto legge, il testo diceva che, in occasione di emergenze che coinvolgessero i diversi aspetti della sicurezza pubblica, del soccorso pubblico e della difesa civile, il Ministro dell'Interno avrebbe convocato l'Unità di Crisi. Il testo dell'articolo fu emendato con la soppressione dei termini soccorso pubblico e difesa civile: a mio modesto avviso, ciò significa che l'Esecutivo e, poi, il Parlamento, che ha ratificato questa norma, hanno stabilito che esistono momenti distinti, tra i quali non deve essere creata confusione. Ricordo che la Presidenza del Consiglio coordina questo genere di attività in piena collaborazione con tutte le Amministrazioni pubbliche competenti.

Mi sembra che la linea sia chiara: abbiamo esaminato ben quattro leggi emanate nel corso di questi ultimi 12 anni e si è profilato con chiarezza quale sia il ruolo della Protezione Civile, quale la linea di comando, quale l'impianto organizzativo della preparazione e della risposta alle emergenze. In aggiunta alle varie leggi, l'anno scorso a seguito di quanto avveniva a livello internazionale il Presidente del Consiglio ha adottato una dichiarazione particolare di stato di emergenza mirata a fronteggiare possibili attentati di natura terroristica non convenzionale, chiarendo che sono fatti salvi i poteri del Ministro dell'Interno per le attività di propria competenza e sottolineando l'esigenza di coordinare tutte le Amministrazioni dello Stato e gli Enti che hanno ruolo in questa materia per individuare una risposta e una gestione delle conseguenze, che siano le più efficaci possibile. Questa ordinanza prevede una serie di compiti che, in gran parte, siamo riusciti ad attua-

re, con particolare riguardo al settore sanitario che, come sottolineava il Presidente Ramponi, è uno dei più coinvolti da questa problematica.

Sono stati quindi elaborati piani operativi condivisi con le strutture sanitarie che, come sappiamo, nel nostro Paese sono regionalizzate. In tal senso abbiamo concordato con gli Assessori alla Sanità di tutte le Regioni italiane e delle Province autonome i piani di intervento sanitario in caso di attentati terroristici, perpetrati con armi biologiche, chimiche, o radiologico/nucleari; abbiamo inventato, di fatto, dei nuovi mezzi, che sembrano ambulanze, ma sono unità per il trasporto di pazienti altamente infettivi a causa, ad esempio, della contaminazione con il virus del vaiolo o dell'antrace. Sono stati distribuiti kit di DPI per il personale del 118, perché la cosa bizzarra è che solamente alcune componenti del sistema di Protezione Civile erano dotate di materiali di protezione individuale, senza prendere in considerazione gli operatori che, assieme ai Vigili del Fuoco, alle Forze dell'Ordine ed eventualmente alle Forze Armate, sono i primi ad essere coinvolti nelle conseguenze: come appunto il personale sanitario del 118, che potrebbe essere il primo a morire nel momento in cui arriva sul luogo di un eventuale attentato privo di qualsiasi forma di protezione individuale. Sono già state distribuite venticinque stazioni di decontaminazione campale per il soccorso dei cittadini che si dovessero trovare nelle zone eventualmente interessate da un attentato, dotate di carrelli di trasporto appositamente studiati per consentire l'immediata entrata in funzione della stazione. Sono stati inoltre acquistati antidoti: sappiamo tutti della brillante esercitazione condotta alcune settimane or sono dai Vigili del Fuoco che simulava un attentato terroristico con diffusione di Sarin nell'ambito della Stazione Termini. Il trattamento dell'intossicazione da Sarin si fronteggia con un antidoto, composto da atropina e pralidossima. Se però l'antidoto non è disponibile nei primi 30 minuti dall'attentato terroristico, i morti invece di essere, immaginiamo, 10 potrebbero essere 250. Ecco l'esigenza di avere antidoti e farmaci immediatamente utilizzabili dal personale che deve garantire il soccorso, in modo da poter intervenire con assoluta tempestività laddove fosse necessario. A monte di tutto sono stati organizzati corsi di formazione, avviati con la collaborazione delle Forze Armate, e in particolare con la Scuola Interforze NBC di Rieti, dove abbiamo cominciato a formare il personale che si deve occupare del soccorso sanitario a livello territoriale. Un anticipo di problematiche connesse a possibili rischi, soprattutto di tipo biologico, l'abbiamo avuto con la vicenda della SARS, che ha interessato marginalmente il nostro Paese l'anno scorso. Sono state messe in piedi una serie di operazioni, soprattutto a livello aeroportuale, che è il principale canale di accesso per un eventuale rischio SARS; il lavoro eccellente che è stato svolto oggi viene preso come punto di riferimento dagli altri Paesi europei per sviluppare analoghe iniziative a casa loro; Paesi che, possiamo dire, per le capacità organizzative si trovano tutti nella stessa situazione.

Vi ho letto prima il giudizio del New York Times sull'organizzazione di New York: sappiamo che anche gli Inglesi, come i Francesi e gli Spagnoli, non sono affatto convinti di essere riusciti a mettere in piedi un sistema per la prevenzione, e soprattutto la gestione delle conseguenze, valido ed efficace. Ciò dimostra la complessità di questa materia, una materia della quale ci occupiamo da poco tempo, e nessuno può pretendere che in tempi brevi si possa sviluppare una capacità di risposta eccezionale. Credo però che siamo sulla buona strada e il *black out* che è avvenuto il 28 settembre dell'anno scorso ha costituito un'ottima esercitazione, sia per come si è sviluppato sia per il periodo di tempo interessato, ovvero la notte tra sabato e domenica. Chi poteva dire, alle ore 3.30 di quella notte se il *black out* fosse causato da un attentato terroristico oppure da un albero caduto in Svizzera che aveva tranciato i fili della luce. Per conoscere la causa dell'evento sono state necessarie diverse ore, e poi alcuni giorni per chiarire tutti i dettagli. Qualcuno ha avuto dubbi su quale struttura dovesse gestire questo black out che ha interessato tutto il Paese? Non c'è stato un attimo di dubbio, ho già raccontato come si è sviluppata quella vicenda, i problemi che abbiamo vissuto a livello nazionale sono noti, ma credo di poter dire che è stata un'eccellente prova di buon funzionamento della macchina della Protezione Civile, quando l'obiettivo è lavorare assieme, mettere da parte eventuali individualismi, voler funzionare come una squadra, come deve essere. La sala operativa della Protezione Civile si è immediatamente attivata appena avvenuto il *black out*; il Comitato Operativo, del quale ho parlato prima, si è riunito a poco più di un'ora dall'inizio dell'emergenza; il Capo Dipartimento, ai sensi dell'articolo di legge che ho ricordato, è diventato in automatico Commissario straordinario del Governo; nell'arco di ventiquattro ore si è così gestita tutta la vicenda e non vi sono state né vittime, né polemiche.

Altro momento di verifica è stato offerto dalla famosa «emergenza neve» con quello che ha provocato sia sulle strade, che nel settore delle ferrovie, che

nel campo dell'approvvigionamento dell'energia elettrica. Anche in questo caso i problemi che si sono verificati potevano essere stati causati dal crollo di un ponte a causa di un attentato terroristico o dalla caduta di tralicci o ancora dall'esplosione di una linea ferroviaria, sempre per attentati. Le conseguenze di questi diversi fenomeni sono sempre le stesse ed è quindi evidente che la gestione degli eventi deve essere coordinata dalle strutture che ne hanno le competenze e le capacità; noi abbiamo proposto, proprio per risolvere il problema delle comunicazioni e della viabilità stradale e ferroviaria, la creazione di un coordinamento a livello regionale che riferisca ad un coordinamento di livello nazionale, in modo che si sappia quello che è accaduto e come deve essere gestito. Le conseguenze della nevicata di Modena si sono riflettute, come sappiamo, sulla Toscana, sulla Lombardia, sul Trentino Alto Adige, sul Veneto e sulla Liguria; quindi è stato coinvolto il sistema Paese ed è stato necessario fornire una risposta unitaria, coordinata dalla struttura che a livello centrale ha la responsabilità di garantire il funzionamento e la gestione di tutti i servizi. Questa è la verità; questo è lo stato dell'arte; poi ci possono essere differenti opinioni su quello che è l'impianto organizzativo e quella che è la linea di comando.

Concludo nello stesso modo con cui ho iniziato, ricordando che il coordinamento è un'attività complessa, equiparabile al ruolo della direzione di un'orchestra: chi dirige, deve saper far suonare tutta l'orchestra nel miglior modo possibile, senza privilegiare né penalizzare alcun componente.

Il nostro Paese non ha bisogno di polemiche o di conflitti di competenza, bensì di chiarezza, di sinergie e occasioni per riflettere insieme e per individuare percorsi condivisi ed efficaci.

Nel ringraziare di nuovo il Presidente Ramponi per l'opportunità che mi ha voluto offrire, desidero ricordare che io sono soltanto un servitore dello Stato, pronto ad operare in qualunque funzione possa rendersi necessaria. Auguro a tutti una serena e proficua continuazione dei lavori.

PRIMA SESSIONE

INTERVENTI

Dott. Lamberto Sposini

Dott. Domenico Di Petrillo

Dott. Alberto Accardi

Dott. Massimiliano Salvi

Dott. Alessandro Ortis

LA CAPACITÀ DI DIFESA DEL SISTEMA PAESE NEL SETTORE DELL'ENERGIA

Introduzione del moderatore dott. Lamberto Sposini condirettore del Tg5

I componenti della prima sessione sono l'ing. Alessandro Ortis, Presidente dell'Autorità per L'Energia ed il Gas, il dott. Domenico Di Petrillo e il dott. Alberto Accardi, responsabili, rispettivamente, della sicurezza dell'Enel e dell'Eni e il dott. Massimiliano Salvi, Presidente dell'Acea Distribuzione.

Una piccola premessa: dopo l'11 settembre 2001 con il suo devastate impatto, anche mediatico, noi ci siamo accorti che è praticamente cambiato tutto; ad esempio, in occasione di tutti i dirottamenti aerei, che ci sono stati dopo l'11 settembre (fortunatamente ce ne sono stati pochi, perché proprio l'11 settembre ha fatto alzare la guardia dell'azione di contrasto), ci siamo chiesti, almeno noi giornalisti che siamo un po' cinici, ma credo che se lo siano chiesto un po' tutti: «È un dirottamento normale, oppure è un dirottamento dell'altro genere?». Dopo l'11 marzo di Madrid ci siamo chiesti, nelle ore immediatamente seguenti: «È stata l'ETA oppure è stato l'altro terrorismo?».

Questo per dire che in qualche modo i terroristi, anche se non dovessero più colpire, come ci auguriamo tutti, sono riusciti a cambiare oggettivamente, pur se di poco, le nostre abitudini ed anche le nostre opinioni. Ormai abbiamo capito che il terrorismo ci può colpire in qualsiasi luogo e in qualsiasi ora del giorno. Una volta il terrorismo colpiva obbiettivi più mirati; oggi si colpisce la gente che va a lavorare, che prende la metropolitana, che prende il treno; la gente può essere colpita addirittura in ufficio, nel proprio ufficio. Vi ricordate quando, dopo l'11 settembre, quel piccolo aereo si andò a schiantare sul Pirellone (Pirellone che è stata reinaugurato due giorni fa): anche in quell'occasione ci si è chiesto se si trattasse di un atto terroristico oppure di qualcos'altro. E abbiamo tirato tutti un sospiro di sollievo quando abbiamo saputo che non era stato un atto terroristico.

Siamo quindi entrati in questa logica: che ci piaccia o no, è con questa situazione che dobbiamo fare i conti. Questo per dire che ormai l'azione contro il terrorismo riguarda tutti, riguarda tutta la società, nessuno è escluso, dato che nessuno è più al riparo da nulla. Perciò bene ha fatto il nostro amico

Presidente Ramponi a coinvolgere in questa chiacchierata non solo la Protezione Civile, che istituzionalmente è tenuta a tenere il coordinamento nel caso di rilevanti emergenze, ma anche, ed è la prima volta, almeno per quanto riguarda la mia esperienza, i rappresentanti delle aziende che si occupano di Energia, Trasporti e Telecomunicazioni.

Noi abbiamo sentito spesso parlare delle predisposizioni varate nei riguardi del terrorismo dalla Protezione Civile, dalle Forze dell'Ordine o dalle Forze Armate. Mai, però, abbiamo sentito parlare di quanto hanno avviato l'Enel, l'Eni o l'Acea in questo settore per contrastare azioni di terrorismo o, eventualmente, per intervenire dopo che sia accaduto qualcosa.

Da questo punto di vista, ha ragione il dottor Bertolaso quando dice che il black out dell'anno scorso ha davvero costituito un banco di prova, meglio di una qualsiasi esercitazione.

Dunque chiediamo subito ai rappresentati della sicurezza dell'Eni e dell'Enel cosa hanno predisposto le loro società nel caso venisse portato un attacco terroristico ad uno dei loro impianti, ad esempio ad un oleodotto o una raffineria. Chiediamolo per primo al dottor Di Petrillo dell'Eni.

Dottor Domenico Di Petrillo
ENI Group Security Manager

IL SISTEMA DI SICUREZZA DELL'ENI

Ringrazio per l'invito e per l'opportunità che mi è stata offerta. L'Eni ha un suo sistema di sicurezza che fa delle analisi dei rischi e della gestione delle eventuali emergenze un sistema molto calibrato e diffuso sia in tutte le funzioni che nella funzione specialistica della sicurezza, da me diretta.

Per quanto riguarda la sua specifica domanda, relativamente alle reti di trasporto e alle piattaforme in Adriatico, la rete ha in se ha una sua sicurezza strutturale data la sua forma ad anello: in caso di attacco non verrebbero meno le possibilità di rifornimento tramite dei *by pass* già strutturali. Parliamo dei 30.000 km della rete strategica, di pertinenza dell'Eni, gestita dalla Snam-gas; se, invece, parliamo della rete del gas che arriva all'utenza, abbiamo a che fare con 300.000 km di tubo, gestiti questi dall'Italgas. Le linee di afflusso vengono da tre direzioni principali: la prima dall'Algeria e la Tunisia, attraverso il gasdotto che parte da capo Bon, arriva a Mazara del Vallo e quindi si immette nella rete nazionale; l'altra proviene del Nord Europa e l'altra dalla Russia. Queste sono le tre linee principali che, quando accedono al territorio nazionale, hanno una forma ad anello, con dei *by pass* intermedi: per ipotizzare un problema di interruzione importante, un attentato dovrebbe, quindi, investire più sezioni e più linee di afflusso. Il sistema poi riceve, anche se in maniera minore, idrocarburi dal sistema delle piattaforme della produzione nazionale e, in maniera ancora minore, da impianti di rigassificazione del gas liquido, arrivato con navi metaniere.

Il sistema tubario è protetto da misure di protezione fisica, che fanno riferimento ad un centro di gestione dell'intera rete, che si trova a San Donato Milanese; esiste anche una sala di regia alternativa in caso di interruzione di qualsiasi tipo. Sono strutture in bunker, che hanno un sistema di controllo telematico.

Più in generale, come ho accennato all'inizio, nello specifico settore della sicurezza l'Eni ha una notevole sensibilità, che, seppure non condizionante, è meritevole di attenzione nelle scelte di *business* e nelle relative operazioni.

Da molti anni, infatti, il Gruppo Eni opera in numerosi Paesi, taluni carat-

terizzati da situazioni critiche per motivi sociali, economici, politici, di grande criminalità e di estremismo confessionale.

Come politica generale, da tempo consolidata nel modo di essere Eni, sia in Italia che all'estero, l'Eni predilige il dialogo e l'integrazione con le Autorità e il territorio. In particolare, nei Paesi in via di sviluppo, associa alle attività industriali importanti progetti sociali tendenti a favorire, oltre all'assistenza di emergenza (ambulatori sanitari), autonome capacità imprenditoriali (es. centri di addestramento professionale, fattorie agricole tipo) piuttosto che sterili e diseducativi sussidi.

Tale assunto, peraltro, è molto importante se si considera che l'Eni opera in un *business*, spesso focale per l'economia e il futuro dei Paesi in cui è presente, con progetti di lunghissima durata che trovano motivo di successo anche nell'integrazione citata. Al riguardo le performance dell'Eni, nei Paesi ad alta criticità, sono ottimali se comparate ad altre di analoghe Società che, con un diverso approccio, spesso soffrono perdite ben maggiori di produzione e conflittualità talvolta condizionanti le stesse attività.

Dottor Sposini: Si può dire che l'Eni svolga un ruolo diplomatico!

Dottor Di Petrillo: Certamente. Tale modo di fare, peraltro ben ribadito nei principi sanciti nel *Codice di Comportamento* e nelle politiche di *Corporate Social Responsability*, è alla base di quel consenso e di quella accettazione che l'Eni incontra nei più diversi teatri, consolidando anche nei quadri locali un singolare senso di appartenenza e consensi nelle popolazioni locali

Tuttavia anche l'Eni ha avuto i suoi caduti: l'unico episodio risale alla guerra civile del Biafra (luglio 1969) allorchè a Kwale (Nigeria) vennero uccisi 10 dipendenti Agip/Saipem ed altri catturati e successivamente liberati; ciò, però, fu determinato da un gruppo di militari sbandati del Briafra nelle fasi terminali del conflitto.

Accettazione, integrazione e consenso sono fattori primari per una reale sicurezza.

Dottor Sposini: Scusi dottor Di Petrillo, ci può spiegare come avviene questa opera di prevenzione? In caso contrario rimaniamo un po' nel vago.

Dottor Di Petrillo: È proprio su questa base che l'Eni, nella seconda metà

degli anni '90, ha costituito una *funzione specialistica di security*, a seguito dell'avvio del processo di privatizzazione, nell'ambito della ristrutturazione globale della Società.

La funzione è stata dislocata nella *Corporate* con la missione di organizzare un *Sistema di Security di Gruppo* mirato alla tutela, in ordine di priorità, delle risorse umane, del *know-how* e degli *asset*, sia in Italia sia all'estero.

La *Policy di Security di Gruppo*, in coerenza con i principi primari dettati nel *Codice di comportamento Eni*:

- fa della prevenzione l'elemento caratterizzante;
- individua nel singolo dipendente il soggetto primario di *security*, nel *management* la responsabilità di considerare le problematiche di security come parte integrante delle scelte di business e nella funzione di *security l'advisor interno* sia per la prevenzione dei rischi sia per la gestione delle criticità.

Inoltre, *la funzione security*:

- ha la responsabilità primaria della diffusione in azienda della *cultura di security*, attraverso specifiche iniziative di formazione/informazione sulle tematiche inerenti, finalizzate a sollecitare e mantenere quella sensibilità necessaria a garantire i risultati suddetti;
- procede sistematicamente al monitoraggio delle aree di crisi e all'analisi dei fenomeni che in esse insistono, in raccordo con i responsabili centrali e periferici di *business*;
- partecipa al processo di comunicazione interna e garantisce l'assistenza alle altre funzioni aziendali nelle più diverse materie;
- costituisce punto di riferimento tecnico-operativo sia nella fase preventiva che nella gestione delle crisi, nonché nei contatti con le Istituzioni, sia nazionali che dei Paesi interessati, nel settore in argomento;
- elabora piani di emergenza e metodologie per la sicurezza globale dei dipendenti e dei siti.

Le diverse criticità internazionali vengono costantemente monitorate non solo per adeguare l'organizzazione di *security* del Gruppo, ma anche per considerare, specie nell'attuale momento critico determinato dall'estremismo islamico, i relativi riflessi in altre aree, compresa l'Italia.

In ogni Paese, in cui il Gruppo opera, è costituito un *Comitato di Security*

di Gruppo, presieduto dal responsabile della *branch* più grande e organizzata, il quale, in raccordo con le diverse funzioni aziendali centrali, attua le varie fasi dei Piani di emergenza prestabiliti.

In Italia le Sedi direzionali sono organizzate con *Sistemi Integrati di Security* standardizzati per assicurare le migliori condizioni di sicurezza e operatività.

È stato, quindi, costruito un sistema di sicurezza fisica flessibile ed efficace, idoneo a gestire situazioni di normale disciplina. In coerenza con l'attuale fase critica, che investe anche il territorio nazionale, sono state apportate le necessarie implementazioni.

L'organizzazione della sicurezza dei trasporti mare e dei terminali è in linea con le recenti prescrizioni dell'agenzia ONU - IMO (*International Maritime Organisation*). In proposito l'ENI si è mossa per tempo per adottare strumenti e procedure adeguati, a seguito di specifici episodi quali l'attacco al Cacciatorpediniere «USS Cole» (porto yemenita di Aden 12 ottobre 2000) e alla petroliera francese «Limburg» (coste dello Yemen 6 ottobre 2002).

La complessa e articolata rete ICT di Gruppo, oggetto di continuo assessment e monitoraggio, è dotata anch'essa di misure di sicurezza pianificate e standardizzate, compresi i settori inerenti la *business continuity* e il *disaster recovery*, sia per le attività in Italia sia per le branch estere.

Si tratta, quindi, di un *Sistema di security* che vede nell'analisi, nella capillare circolazione delle informazioni, nel costante monitoraggio delle criticità/vulnerabilità e nell'integrazione tra le varie funzioni, sia di business sia di supporto, la principale chiave metodologica per l'implementazione di un sistema sostenibile e diffuso.

Tale Sistema non prescinde dalle interazioni con le Istituzioni, sia in Italia sia all'estero, anche per implementare cognizioni e supporto altrimenti non raggiungibili.

In Italia l'interazione è sistematica e costante e investe tutti i settori. Tra questi, considerato l'argomento odierno, quelli di maggior rilievo sono:

- l'*Unità di crisi del MAE*: ha con l'Eni una strettissima collaborazione da tempo consolidata e sperimentata non solo in occasione di moltissime crisi ma anche nel continuo scambio di informazioni. Al riguardo l'Eni ha costituito e costituisce spesso punto di riferimento, anche per le Ambasciate, in occasione di crisi che comportano l'evacuazione di cittadini italiani; spesso, infatti, vi ha provveduto con la sua organizzazione;

- gli *Apparati di Sicurezza e FF.PP.*: attraverso un reciproco scambio di informazioni finalizzato proprio a prevenire i rischi, specie quelli derivanti dall'attuale situazione internazionale;
- le *Prefetture e FF.PP. locali*: per la protezione dei siti e delle *facilities* di trasporto, specie nell'attuale esposizione del Paese alla minaccia dell'estremismo islamico e di alcuni settori del terrorismo/antagonismo interni;
- le *Capitanerie di Porto*: per le misure di *security* previste dalla citata normativa IMO per la sicurezza dei trasporti mare, dei porti e dei terminali. Al riguardo, stante le dimensioni e la molteplicità delle esigenze, l'Eni costituisce un utile punto di riferimento metodologico (Unità di crisi HSE Eni) ed ha allacciato con il Comando Generale delle Capitanerie contatti, finalizzati anche alla migliore gestione delle fasi di emergenza ambientale connesse ad eventi determinati da atti terroristici e non.

L'Eni, inoltre, aderendo a richieste istituzionali nell'ambito della creazione del sistema Paese, partecipa ai corsi del Centro Alti Studi Difesa, inviando ogni anno un dirigente che segue il corso della Sezione Speciale dello stesso Centro. In tale ambito vengono consolidate le diverse esperienze e vengono favorite le possibili interrelazioni tra pubblico e privato su basi più consapevoli.

L'interazione tra pubblico e privato, però, è ancora limitata e lontana dai livelli ottimali. Essa, infatti, soffre di deficienze strutturali essendo legata spesso più ad iniziative personali che, come ad esempio avviene in altri Paesi europei, ad una sistematica e completa collaborazione/supporto in un contesto di reale Sistema Paese.

Credo di essere riuscito a dare un quadro d'insieme sintetico di quello che l'Eni fa per la sicurezza.

Dottor Sposini: Poi le chiederò qualcosa di più concreto, ma adesso passiamo al dottor Accardi dell'Enel. Questo Ente ha avuto, appunto, quel banco di prova dell'anno scorso: vediamo come questo è servito a mettere a punto opere di prevenzione per non dire, di contrasto. Sotto questo aspetto, per la verità, l'Enel presenta una variabile in più, l'ecoterrorismo, del quale abbiamo avuto una manifestazione pochi giorni fa. Mi rendo conto che non è possibile presidiare ogni traliccio d'Italia, perché immagino che non sia quella la strada. Ci dica, tuttavia, quello che si sta facendo contro l'ecoterrorismo, oltre quello che si sta facendo contro i black out dovuti alle azioni terroristiche.

Dottor Alberto Accardi
Capo Sicurezza Holding Enel S.p.a.

IL SISTEMA DI SICUREZZA DELL'ENEL

Ringrazio il Presidente Ramponi per l'invito e rispondo subito alla domanda. Effettivamente noi abbiamo avuto questa «opportunità» del 28 settembre scorso, che ci ha consentito, per lo meno, di fare autocritica e di fare il punto di quella che era la situazione dei nostri standard di sicurezza. Vi assicuro che abbiamo avuto l'occasione di renderci conto di dover ripartire dall'inizio e rivedere situazioni al nostro interno.

Intanto, abbiamo puntato moltissimo su quella che è l'informazione interna: siamo una azienda che è capillarizzata sul territorio nazionale, abbiamo molteplici siti, dico siti in termini generali, perché abbiamo uffici, ma anche stazioni, tutta la rete di trasporto dell'energia, centrali, dighe. L'informazione perviene al centro dalla periferia: essa inizia, cioè, dall'anello più piccolo, dal singolo dipendente, che deve accorgersi di un evento e che, se non in tempo reale, almeno nel più breve tempo possibile, deve far pervenire l'informazione stessa fino la vertice dell'azienda.

Per fare questo abbiamo dato molto risalto alla sensibilizzazione del personale stesso, che deve riconoscere il cosiddetto «segnale debole» e comprendere se quel segnale deve costituire avviso di un pericolo e anche di un pericolo importante. A tal fine abbiamo creato molta sensibilizzazione, ma soprattutto irrigidito e rielaborato le procedure.

Quando parlo della rielaborazione delle procedure, intendo riferirmi a quello che noi chiamiamo il *crisis management*, ossia a tutto quell'insieme di organizzazione interna che consente all'azienda di reagire, nel tempo più breve possibile, all'evento. Dopo il *black out*, insomma, abbiamo messo a punto questa strategia. Abbiamo ipotizzato che l'informazione arrivi dal singolo dipendente, che si trova in un punto qualsiasi del Paese, ed attivi immediatamente con una comunicazione, in genere telefonica, anche se abbiamo visto che alcune linee telefoniche durante il *black out* sono crollate. A tale proposito abbiamo previsto dei sistemi elementari di comunicazione, abbiamo previsto delle linee di *backup*, abbiamo incrementato anche l'uso di sistemi satellitari, proprio prevedendo che le linee di uno o più gestori, come di è verificato, possano venire meno.

Come detto, il singolo dipendente comunica ad un sistema centralizzato, che abbiamo chiamato «batteria», come la più nota «batteria» del Ministero dell'Interno, che fa diretto riferimento a me; ed io faccio diretto riferimento al vertice dell'azienda, con immediate valutazioni sul tipo di evento, per poi attivare tutta una serie di procedure che riguardano i vari settori dell'azienda, se si tratta di un evento che la coinvolge per intero. Sono poi state previste delle emergenze locali, che coinvolgono solo alcune società o divisioni dell'azienda stessa, e abbiamo anche che previsto che l'evento possa avere un riflesso soltanto su alcune aree del Paese.

Quanto detto descrive brevemente come ci siamo attivati in vista di un emergenza come quella del 28 settembre scorso: cerchiamo, quindi, di avere una informazione nei tempi più rapidi possibili dalla periferia verso il vertice, abbiamo sensibilizzato il personale e messo a punto predisposizioni immediate.

Importantissimo è il raccordo con la Protezione Civile, con la sala EMERCOM, se l'evento ha rilevanza nazionale, oppure con le sale crisi delle Prefetture, se l'evento ha riflessi locali che interessino una o più provincie o, addirittura, una o più regioni.

Questo raccordo è essenziale e noi abbiamo costituito a tale scopo quella che noi chiamiamo «unità di raccordo», con una turnazione continua di tecnici e dirigenti, che sono sempre gli stessi. Abbiamo cioè costituito un gruppo di cinque dirigenti, più altri cinque di riserva, in modo tale che siano sempre le stesse persone, che si conoscano, che, abbiamo detto, vadano anche a mangiare la pizza assieme, in modo tale che sappiano benissimo, l'uno rispetto all'altro, come reagiscono in certe circostanze. Sono questi i dirigenti che possano operare in sala EMERCOM con la Protezione Civile o nelle Prefetture. Questo è stato fatto proprio per creare una simbiosi con la parte che si occupa di sicurezza nazionale.

Dottor Sposini: Evidentemente è colpa mia: non riesco a farvi dire qualcosa di più concreto. Non so se dovete essere riservati e se non potete dire più di tanto. Io, sinceramente, da cittadino, se devo esprimere una opinione in questa sede, non mi sento così al riparo sentendo le vostre relazioni. Per carità, non vuole essere una critica. Non so in sala, ma io non ho capito cosa succede se c'è un attacco terroristico nei riguardi del sistema dell'energia elettrica o nei riguardi dell'approvvigionamento di carburante.

Vediamo se siamo più fortunati con l'acqua: cosa succede se dei terroristi inquinano un acquedotto? Cosa fa l'Acea? Vediamo di partire da cose molto basic.

Dottor Massimiliano Salvi
Presidente Acea Distribuzione S.p.a.

IL SISTEMA DI SICUREZZA DELL'ACEA

Buon Giorno. A parte il fatto che io rappresento la distribuzione e quindi il settore dell'Acea che si occupa dell'energia elettrica, posso però dire che le procedure sono assolutamente simili e ripetibili. Prima si è detto che la minaccia, soprattutto in questo ultimo periodo, può essere imprevedibile nei tempi e nei modi. Di conseguenza, poiché l'Acea opera a Roma e quindi in una città particolarmente a rischio come simbolo della cristianità e centro di numerose istituzione, noi abbiamo sviluppato, al di la degli aspetti di prevenzione, che devono vedere anche impegnate le Istituzioni, un sistema integrato di gestione dell'emergenza. Questo sistema integrato di gestione dell'emergenza si sviluppa su due binari. Ci sono degli investimenti dedicati, che abbiamo rafforzato in questi ultimi tempi anche alla luce dell'esperienza del *black out* e dei distacchi programmati che sono avvenuti nel mese di giugno del 2003, e delle procedure che hanno due dimensioni di operatività: una interna aziendale e una verso le Istituzioni. Se vogliamo andare sul concreto in termini di investimenti, noi abbiamo attivato in misura maggiore rispetto al passato dei sistemi di videosorveglianza e di controllo accessi degli impianti sensibili, fermo restando che il presidio militare deve essere di competenza delle Istituzioni; abbiamo tutta la rete di alta tensione, quella di media tensione, le linee primarie e le cabine secondarie in telecontrollo e quindi gestibili in presa diretta tramite controllo remoto dalla sala operativa, che opera 24 ore su 24 con personale di turno continuo; abbiamo delle forme di *backup* e di ridondanza in quanto i sistemi elettrici, analogamente ai sistemi citati dal collega dell'Enel, sono progettati e costruiti ad anello e quindi c'è la possibilità di fare quasi sempre delle manovre a rovescio.

Dottor Sposini: Mi spiega meglio cosa vuol dire che sono fatti ad anello?

Dottor Salvi: Formano un cerchio e quindi se si verifica un guasto da una parte, sezionando opportunamente il guasto si può procedere alla rialimentazione a rovescio. Questo avviene nella quasi totalità dei casi. Abbiamo acqui-

stato in maniera molto più rilevate rispetto al passato dei gruppi elettrogeni, che non erano risultati sufficienti nella situazione locale e nazionale in occasione del black out, ci siamo di dotati di sistemi di telecomunicazione satellitare, analogamente a quello che ha fatto l'Enel, e abbiamo studiato delle procedure per la rialimentabilità delle centrali di produzione della città di Roma, quindi di Montemartini e Tor di Valle, anche in assenza di alimentazione dalla rete di trasmissione nazionale. Questo è un elemento molto importante per noi stessi, per la cittadinanza e per la sicurezza, in quanto consentirebbe, anche in presenza di una mancanza di energia elettrica diffusa, di alimentare tutta una serie di utenze sensibili, sia istituzionali che di ospedali e di trasporti, pari a circa il 20% della potenza impegnata. Questo dal punto di vista degli investimenti. Ovviamente si potrebbe anche fare di più in una città come Roma, dove ci sono circa 70 utenze particolarmente rilevanti e che sono servite, come ho detto prima, da sistemi ridondanti. Ovviamente si potrebbe creare anche una ridondanza tripla o quadrupla, ma c'è anche un tema di costo e di sostenibilità da parte di aziende che hanno anche dei vincoli di redditività.

Per quanto riguarda le procedure, e quindi mi sposto sul secondo binario di risposta all'emergenza, abbiamo delle procedure aziendali molto strette, c'è un comitato di crisi, a seconda della tipologia di eventi, che può essere un disastro, un disservizio grave, un disservizio importante (c'è tutta una casistica e una classificazione); sappiamo chi deve fare cosa, chi deve comunicare il disservizio, come deve essere sezionato il guasto, quali sistemi di *back up* debbono essere attivati, abbiamo un elenco puntuale di tutte le utenze prioritarie alle quali dobbiamo garantire il servizio, a partire dai disabili fino agli ospedali e alle istituzioni, ovviamente compatibilmente con la potenza che dovesse venire a mancare a seguito di un attacco terroristico. Abbiamo, a seconda della tipologia del disservizio, l'indicazione di quelli che sono più o meno i tempi di rialimentabilità. Ovviamente questo deve essere fatto in maniera molto integrata con le Istituzioni, sia a livello locale, quindi comunale, sotto la guida del prefetto e dell'ufficio territoriale del Governo, sia a livello nazionale con la Protezione Civile.

Come è stato citato in precedenza noi siamo parte, assieme alle altre aziende di pubblici servizi, dei Comitati di coordinamento e quindi attiviamo sia una sala di crisi interna che replica la sala di crisi che viene attivata all'interno delle Istituzioni, della quale siamo partecipi assieme ad altre aziende ed

anche al GRTN. Abbiamo avuto, appunto, la lezione del *black out* e dei distacchi programmati che ci ha consentito di affinare le procedure operative, non che prima non esistessero, ma così le abbiamo affinate e provate sul campo. Abbiamo avuto una lezione importante anche di reazione da parte della cittadinanza che è stata molto composta e positiva in quanto il *black out* si è verificato, almeno per la città di Roma, in concomitanza con un altro evento importante che era la «notte bianca», che aveva portato centinaia di migliaia di persone in strada: non ci sono state scene di panico, non ci sono stati feriti, né eventi più gravi e progressivamente prima di 24 ore tutte le utenze sono state rialimentate. Quello che non possiamo dare è la certezza, ma adesso siamo consapevoli di aver migliorato e in una situazione di emergenza, quale quella di un attacco terroristico, riteniamo di poter dare delle risposte, anche più immediate rispetto al passato. Molto rilevante, ci ritorno sopra, è il tema della possibilità, a questo punto, di rialimentare attraverso linee dedicate le centrali di produzione in assenza di energia dalla rete di trasmissione nazionale. Certamente Roma ha un territorio molto vasto: ha circa 1.400 km quadrati di superficie, essendo il comune più ampio di Europa. Giusto per dare delle dimensioni in termini di elementi di impianto, che bisognerebbe monotorizzare e proteggere, si parla di circa 130 km di rete ad alta tensione, circa 9000 km di rete di media tensione, circa 20.000 km di rete di bassa tensione, 12.000 cabine secondarie e 70 cabine primarie, che sono quelle che poi convertono la tensione da alta a media. Di conseguenza il presidio di tutti questi impianti non è ovviamente possibile, non è neppure funzionale. Bisogna scegliere, assieme alle Istituzioni, quali di questi sono realmente prioritari per la continuità del servizio e vedere di telecontrollarli il più possibile, in modo di consentire delle manovre in remoto dalla sala operativa, senza dispiegare sul territorio le squadre. Per quanto riguarda la presenza sul territorio, come ho detto prima, la distribuzione opera con una sala operativa elettrica che è presente 24 ore su 24; ci sono delle squadre dislocate in alcuni punti cardinali di Roma, anch'esse a turno continuo. Tale organizzazione è simile a quella dell'acqua: quindi abbiamo il Comitato di crisi per quanto riguarda l'acqua che è trasversale, abbiamo le stesse casistiche di disastro o di disservizio. Per quanto riguarda gli agenti di inquinamento, che sono quelli che citava prima il dottor Sposini, ci sono dei sistemi, magari più artigianali, di rivelazione della presenza di agenti tossici nell'acqua che sono le trote: noi in certi punti strategici di alimentazione degli acquedotti romani abbiamo...

Dottor Sposini: Finalmente qualcosa di concreto!

Dottor Salvi: Me lo sono riservato alla fine. Le trote sono animali che rilevano immediatamente la presenza di agenti tossici: abbiamo predisposto in alcuni punti strategici di alimentazione della città di Roma alcune vasche, dove sono presenti questi pesci, vasche videosorvegliate anch'esse 24 ore al giorno. Se si presenta un comportamento anomalo delle trote o una moria delle stesse, riusciamo immediatamente a prelevare dei campioni di acqua, a fare subito delle analisi su quelli che riteniamo gli agenti patogeni più significativi.

Dottor Sposini: Mi scusi, quanto tempo passa dalla constatazione che la trota non sta benissimo al prendere provvedimenti concreti?

Dottor Salvi: Per i provvedimenti sicuramente si parla di minuti, perché abbiamo delle possibilità di rilevazione attraverso i nostri laboratori, praticamente immediate. Certo lo è sugli agenti principali, altrimenti per fare una analisi completa ci vorrebbero delle ore.

Dottor Sposini: Bene! Presidente Ortis, dal quadro che abbiamo sentito lei, da dirigente oppure da cittadino, si sente tranquillo oppure ha qualche preoccupazione?

Ing. Alessandro Ortis
Presidente Autorità per l'Energia e il Gas

VALUTAZIONI SULLE MISURE DI SICUREZZA ADOTTATE NEL SETTORE DELL'ENERGIA

Dal quadro che è stato fatto, anche a seguito dall'intervento dell'amico Bertolaso, posso dire che distinguerei nell'incontro di questa mattina due momenti in relazione al tema che stiamo affrontando. Trattiamo subito l'argomento della gestione dell'emergenza e del recovery, dopo l'evento, e su questo fronte, per esser molto concreto, mi posso rifare all'esperienza di settembre. Ogni Paese ha il suo settembre: l'11 settembre al di là dell'Atlantico, qualche settembre anche nel Regno Unito (*black out* londinese), qualche settembre in Germania, il severo settembre del *black out* nel nostro Paese.

Devo dire che sotto questo aspetto la macchina ha funzionato: mi riferisco alla gestione dell'emergenza e alla fase di *recovery* del sistema elettrico, che è un sistema a rete, come si ricordava. In ogni problema, tuttavia, c'è anche l'aspetto positivo, lo ricordava Bertolaso: è stata secondo me, una esercitazione formidabile e, in quanto a gestione emergenza e a *recovery*, il nostro Paese ha dato veramente un esempio molto positivo. Entro le 10 di sera il sistema Italia era completamente rialimentato fino alla Sicilia, ancorché l'inizio della rialimentazione fosse avvenuto presto nel nord del Paese. Diverso è il problema che ci sta di fronte rispetto a questa relativa serenità: dico relativa, perché in termini di gestione dell'emergenza e del recovery tanto e di più si può sempre fare, si può sempre migliorare.

Parlando di energia non si deve, infatti, dimenticare che al di là dell'elettricità c'è anche la catena dell'*oil* e la catena del gas. Il Paese è dotato, anche per accordi internazionali, di scorte strategiche, *target* definito, controllato e, se non rispettato, oggetto di seri rimproveri: per il petrolio si tratta di scorte sufficienti per 90 giorni; per le scorte strategiche di gas noi disponiamo di 5.1 miliardi di metri cubi, calcolati secondo l'ipotesi che il metanodotto più significativo, la linea di importazione più significativa del Paese, che in questo momento sono i 28 miliardi di metri cubi dall'Algeria, possa essere sostituita per almeno 60 giorni con scorte interne.

Dottor Sposini: Mi scusi Presidente una piccola interruzione. È cambia-

to qualcosa in questi valori dopo il nostro 28 settembre 2003, oppure è rimasto tutto come era prima.

Dottor Ortis: Queste misurazioni, queste valutazioni sono riferite al nostro fabbisogno interno. Quello che, secondo me, dobbiamo tenere presente nel dopo 11 settembre è proprio l'altro argomento che vorrei trattare: è quello della pregestione dell'emergenza e del recovery e cioè la prevenzione; per seguire lo stimolo del Presidente Ramponi, esaminare come poter alzare la guardia. Sotto questo aspetto credo che il nostro Paese abbia spazi e possibilità per sviluppare e ottimizzare questo alzare la guardia di fronte al terrorismo, al terrorismo a carattere politico o a quello di altro tipo, anche a quello ecologico, e, più in generale, di fronte agli atti criminosi e alle minacce.

Affronterei il tema sotto due o tre aspetti: il primo è il livello di interrelazione fra i vari attori e bene si è fatto ad immaginare di avere qui presenti non solo le Istituzioni, ma anche gli operatori del settore energia. E quando dico interrelazioni tra Istituzioni e operatori, noi dobbiamo assolutamente alzare lo sguardo al di là dei confini domestici. Perché questo problema riguarda ormai il livello internazionale. Mi riferisco anche a livello comunitario europeo, dell'Unione Europea, che pure è un livello continentale e anche politicamente dotato di una certa coesione.

In questo senso noi dobbiamo immaginare che il sistema energetico italiano ha dimensioni e interrelazioni globali. Lo dice anche tutto il processo del protocollo di Kyoto per quanto attiene la protezione ambientale. In questo senso noi dobbiamo stare attenti a valorizzare tutti i nostri rapporti, per esempio, a livello dell'Agenzia Internazionale dell'Energia, una struttura dell'OCSE, che si occupa di tutta la filiera energetica, *oil*, gas ed elettricità, e che ha al suo interno un complesso di Paesi con i quali si può e si deve condividere le attività di *intelligence* e immaginare soluzioni. Parlo del Nord America, Giappone, Oceania, l'Australia per intenderci, e di tutti i Paesi dell'OCSE, quindi di quelli comunitari.

Dobbiamo quindi alzare lo sguardo al di fuori del nostro territorio e cercare di capire se sono sufficienti tre livelli rispetto a queste interrelazioni: comunicazione, cooperazione e collaborazione. Sotto questo aspetto, il quadro che noi abbiamo di fronte, e cerco di rispondere alla sua domanda specifica, è un quadro dinamico e noi dobbiamo immaginare di proporci rispetto a

questa situazione in modo dinamico, sia come Istituzioni che come operatori. Lo stesso quadro delle minacce è dinamico, come ricordava stamattina Bertolaso; anche il manuale del Nucleo Politico Militare è in revisione, proprio perché il sistema delle minacce è dinamico. Questo è un elemento importante per gli operatori, perché bisogna pure rapportarsi ad un quadro di riferimento che non è più quello di una volta, ma è dinamico e sfidante la dinamicità stessa. L'assetto del settore è pure esso stesso dinamico. Lo ricordava un relatore poco fa: noi con le liberalizzazioni, benvenute, importanti, positive e vantaggiose per la economicità e la sicurezza del sistema energetico, abbiamo avuto la nascita di nuovi attori.

Abbiamo sentito poco fa che gruppi tipo l'Enel, come vuole la Commissione Europea, si sono organizzati su diverse strutture, alcune deputate alla gestione, alcune deputate alla distribuzione, altre a gestire centrali e via dicendo. Quindi siamo in una situazione dinamica per quanto riguarda gli attori che designano nuove strategie energetiche. Un esempio per tutti: nel nostro Paese il Ministero delle Attività Produttive ha autorizzato dei nuovi gassificatori per l'alimentazione della rete nazionale del gas. Gassificatori significa importazione di gas liquido attraverso metaniere e certamente queste nuove opportunità, anche tecnologiche, individuano una dinamicità nei confronti dei *target* da monitorare, da tenere in osservazione per quanto riguarda la sicurezza. Abbiamo poi uno sviluppo del livello tecnologico sia a livello *hardware* che *software*: quando dico *software*, non intendo solo i sistemi informatici, ma l'organizzazione.

Qualche esempio è venuto fuori oggi: benvenuto l'impegno dei gruppi e degli operatori del settore energetico, quando individuano anche delle unità operative con dei *security* management e dei security manager, perché questo aiuta certamente. Poi ci sono le fasi di attività all'interno di tutta la filiera: qui andiamo dall'inizio, dall'*intelligence* e dal porto di partenza fino alla parte gestione dell'emergenza e recovery. Su questo non mi trattengo in quanto ne ha parlato diffusamente l'amico Bertolaso e credo che, ricordando l'evento del 28 settembre scorso o tanti altri eventi, possiamo trattenerci sullo sfondo. Ma per quanto riguarda l'*intelligence*, il ruolo del Nucleo Politico Militare presso la Presidenza del Consiglio, dei Comitati e delle Commissioni annesse, vale la pena toccare alcuni argomenti. Rispetto ai target, e parlo solo del settore energetico e della fornitura dei servizi, cosa tenere presente per garantire al Paese la sicurezza degli approvvigionamenti? Noi abbiamo un ventaglio vasto per-

ché dobbiamo considerare i punti di approvvigionamento, con la metaniera che parte da una unità di liquefazione del gas, e già questo può essere un target sensibile, come può essere un target sensibile il porto di partenza, l'approdo ai porti su territorio nazionale; e questo per citare un solo sistema di trasporto. Poi abbiamo i gasdotti, gli oleodotti, le centrali di pompaggio, le centrali di spinta e via dicendo e tutti gli altri trasporti. Consideriamo pure che nel settore energetico c'è anche la partita nucleare, per la quale, devo dire, il conforto è anche dato da una progressiva attenzione dedicata dal Governo a questo settore della sicurezza, fino all'esito della nomina di un Commissario e all'affidamento, tramite legge, di responsabilità specifiche per la gestione del *decomission* delle scorie nucleari: c'è anche una componente tariffaria nella bolletta elettrica che consegna mezzi e abbiamo quindi abbiamo una struttura dotata di mezzi per questo settore. Poi abbiamo le reti e noi abbiamo un sistema energetico a rete molto magliato, l'elettricità, le linee elettriche, i gasdotti e qualche tratto di trasporto via oleodotto. Abbiamo le unità di *upstream* nell'Adriatico; abbiamo molte piattaforme di estrazione, sia di olio che di gas, che sono certamente dei *target* che offrono una certa sensibilità. Poi abbiamo gli stoccaggi delle scorte, quindi depositi di *oil*, depositi di gas. Ci sono anche le unità di trasformazione, per cui si va dalle centrali elettriche, che trasformano energia, alle raffinerie. C'è una lista che è arcinota, arciprecisata, sempre aggiornata sia nei *file* del Ministero dell'Interno sia negli altri *file* competenti; quindi il quadro è sotto controllo sotto questo aspetto. Allora noi dovremmo fare una analisi rispetto a quello che può essere una ottimizzazione dello sviluppo del sistema Italia preemergenza e *prerecovery*; sotto questo aspetto direi che c'è spazio per avanzare rispetto alle attuali relazioni. Faccio tre o quattro esempi delle fasi di attività. Abbiamo detto aggiornamento del quadro delle minacce; questa è una attività di *intelligence*, di definizione delle minacce, che fa necessariamente capo alle Istituzioni; però anche gli operatori possono collaborare, hanno un sistema di gangli informativi; penso anche alla nostra rete diplomatica, all'Unità di Crisi, ecc. In questa area forse c'è molto da fare e può essere utile cooptare fin da subito questi *security manager*, naturalmente con criteri di riservatezza; come fase immediatamente successiva, sulla base di questa dinamicità delle minacce, si possono individuare le vulnerabilità: queste possono essere individuate attraverso una cooperazione tra chi conosce queste minacce e chi conosce le proprie installazioni, i propri impianti in modo da individuare rispetto alla minaccia X quello che può

esser il punto più debole di intervento; in questo senso ecco l'altro passo: si può cooperare e lavorare meglio assieme rispetto alla definizione di quelle che sono le azioni da attuare per l'attenuazione delle vulnerabilità. Allora lì ci sono delle azioni a breve sia di investimenti e che di attività, ma ci sono anche quelle a lungo termine. Con riferimento a queste ultime, io mi sono permesso di sollevare la questione a livello dell'Agenzia Internazionale dell'Energia, perché forse è bene che anche i criteri di progettazione delle installazione delle reti si rifacciano ad una visione più aggiornata alle tipologie di minacce. Esempio per tutti, le centrali nucleari sono progettate, essendo una tecnologia più recente, per resistere all'impatto di un aeroplano che ci cada sopra . Ci si può domandare se già in fase di progettazione delle strutture ed infrastrutture, dai porti alle centrali, dalle reti ai gasdotti ecc. si possano portare degli elementi innovativi che nascono da una *intelligence*, da una migliore e aggiornata definizione delle minacce. Questo è possibile e su questo si innescano la progettazione e la ricerca delle tecnologie. Se noi pensiamo ai sistemi di telecomunicazione ed informatica aggregati a sistemi energetici, è enorme lo spazio per individuare delle soluzioni che attenuino la vulnerabilità. Sotto questo aspetto credo che possiamo fare un buon lavoro per alzare la guardia al sistema Italia, fasi assai importanti che precedono allo specifico della difesa e del contrasto. Sotto questo aspetto credo che ci sia una sensibilità assai diffusa nel Paese, come anche a livello comunitario e a livello internazionale: ho citato l'Agenzia Internazionale dell'Energia come esempio per poter attivare, su iniziativa evidentemente dei Governi, un attività che consenta di sviluppare, non solo di più la comunicazione e il coordinamento, ma anche la cooperazione in questo senso. Perciò credo che questa potrebbe essere una proposta operativa interessante per passare da una conferenza assai importante, come questa, ad una fase di *work shop* per addetti ai lavori nel senso operativo del termine. Sarà questa fase, coordinata dal Governo con gli strumenti e le soluzioni più acconce (credo infatti che tutto ciò debba essere assolutamente lasciato all'iniziativa politica e amministrativa), che porterà ad un avanzamento teso a far alzare la guardia.

Presidente Ramponi: Due o tre cose fondamentali. Sono contentissimo di aver cambiato il sistema della riunione, facendo venire dei giornalisti a fare da interlocutori, perché, e ringrazio ancora una volta Lamberto Sposini, ha dato un tono di vivacità al discorso; altre volte ci siamo trovati davanti ad

una certa monotonia; gli sono gratissimo, perché questo è il modo di condurre le cose.

Debbo dire che nel complesso questa prima sessione ha visto espressa da parte del dottor Petrillo e del dottor Accardi l'idea della necessità di avere prima di tutto un organo di controllo, la tempestività delle telecomunicazioni con relativo raddoppio e inoltre la sensibilizzazione del personale. Giustamente Sposini ha detto: «Sì, va bene, ma diteci qualche cosa di concreto». Era necessaria questa prima parte, così come successivamente, giustamente sollecitato, Salvi è entrato nel merito di qualche esempio specifico con il discorso delle ridondanze, con il discorso della difesa manovrata e della inopportunità invece di pensare ad una difesa statica su tutte le strutture; infine, lasciatemi dire, Ortis ha concluso da par suo. La cosa che mi lusinga è questa: la visione strategica, che ha dato Ortis, dell'idea complessiva della macroscopicità del problema; la dimostrazione che è vero quando noi diciamo che il privato è coinvolto tanto come il pubblico è la terminologia che lui ha usato, una terminologia molto familiare all'ambiente militare: cioè l'individuazione della minaccia, la deduzione delle vulnerabilità, l'inizio delle predisposizioni. Caro Presidente mi hai fatto la struttura di un piano operativo di attacco vero e proprio, come viene insegnato normalmente nelle nostre scuole. Quindi non c'è dubbio: sono molto soddisfatto di come si è sviluppata questa prima parte e invito i colleghi che seguiranno nella seconda e terza sessione di considerare disponibili una quarantina di minuti. Prego adesso Andrea Pancani di sostituire Sposini, che ha dato un tono di vivacità che ho apprezzato molto. Chiamo ugualmente Luca Rossetto, Salvatore Cirafici, Sergio Cellini e Giuliano Tavaroli a prendere il posto dei precedenti relatori.

SECONDA SESSIONE

INTERVENTI

Dott. Andrea Pancani

Dott. Luca Rossetto

Dott. Salvatore Cirafici

Dott. Sergio Cellini

Dott. Giuliano Tavaroli

LA CAPACITÀ DI DIFESA DEL SISTEMA PAESE NEL SETTORE DELLE TELECOMUNICAZIONI

Introduzione del moderatore dott. Andrea Pancani caporedattore Tg La7

Rinnovo a tutti voi il buon giorno: saluto il Presidente Ramponi e tutti i presenti; speriamo con il nostro team di essere all'altezza di quello precedente; ho sentito che il Presidente ha dato i voti, noi speriamo di difenderci. Già assistendo all'inizio dei lavori, ho imparato diverse cose; mi ha fatto piacere l'esposizione del dottor Bertolaso, che è stata molto utile anche per chi fa informazione quotidianamente e, in particolare, per noi che la facciamo in televisione. Sono contento anche di smistare il traffico in un *parterre* così importante, sia quello per che riguarda l'intera giornata di convegno, ovviamente, sia specialmente per quello, per partigianeria, della mia sessione.

Prima di iniziare con i relatori del mio gruppo, ruberò solo un minuto sperando di rispettare i tempi. Tutti conoscete l'importanza e il ruolo fondamentale che ricoprono le telecomunicazioni: da una parte i telefonini e dall'altra internet hanno cambiato il nostro modo di vivere, come stanno naturalmente cambiando l'informazione. Questi strumenti sono però dei *target* straordinari per i terroristi, che hanno già saputo utilizzarli in maniera egregia del loro punto di vista.

Bisogna tenere presente che il campo delle telecomunicazioni è molto sensibile. Noi abbiamo relatori molto diversi che quindi potranno entrare nel merito del mondo sia dei gestori della telefonia fissa e mobile che di quello dei *provider*, di quello legato ad internet. Peraltro è proprio tramite internet che circolano e si diffondono messaggi e segnali tra addetti a gruppi terroristici, come abbiamo scoperto

Volevo ricordare solo due episodi a proposito dell'importanza delle telecomunicazioni che transitano attraverso i telefonini. È stato più volte tirato in ballo il *black out* italiano del settembre scorso. Ebbene io, mentre nel cuore della notte mi trovavo a Termini, ho ricevuto un sms che mi segnalava da Milano un'interruzione dell'energia elettrica. Questo messaggio, un messaggio generico, chiedeva, inoltre: «Lì da voi, cosa sta succedendo?». Ho scoperto solo dopo alcuni giorni che il messaggio proveniva da un collega giornalista, che in situazioni particolari o di allarme usa mandare questi sms. Gli

sms di risposta gli danno un po' il polso della situazione. È stato molto utile anche per me, perché solo allora io ho scoperto cosa fosse successo.

L'importanza dei telefonini si è rivelata anche per molti viaggiatori dei maledetti e sfortunati treni dell'11 marzo di Madrid: questi viaggiatori hanno telefonato e rassicurato così i propri familiari dicendo che, sì, da loro c'era il finimondo, ma che essi erano vivi. Nel frattempo, infatti, le televisioni si erano naturalmente allertate con quella notizie e quelle immagini, a cui purtroppo ci stiamo terribilmente abituando. Altri telefonini avevano innescato gli zainetti esplosivi. Si tratta di oggetti legati alla nostra vita, che servono a cose molto utili, ma anche a cose molto tragiche.

Detto questo direi di dare l'avvio alla nostra seconda sessione: presento i nostri relatori che sono il dottor Luca Rossetto, Direttore Generale di Vodafone, il dottor Salvatore Cirafici, Direttore *Asset Governance* di Wind, il dottor Sergio Cellini, Direttore Generale di Tiscali, e il dottor Giuliano, *Corporate Security Manager* di Telecom Italia. Quest'ultimo gioca quasi in casa visto che io, come giornalista della rete LA7, gli sono imparentato. Diamo avvio alle nostre considerazioni: vogliamo sapere quale é lo stato dell'arte delle aziende che sono qui rappresentate, alla luce di quanto finora detto. Partirei con il dottor Rossetto.

Dottor Luca Rossetto
Direttore Generale Vodafone

LE PREDISPOSIZIONI DI SICUREZZA DELLA VODAFONE

Buon giorno a tutti e grazie di aver voluto la nostra azienda qui presente oggi: una azienda che ormai, come le altre aziende di telecomunicazione sia fisse che mobili, fa parte di una infrastruttura nazionale che nei momenti di crisi perde il suo connotato di azienda strettamente di business e diventa un elemento di integrazione nella gestione degli stati di crisi. Alcuni esempi li abbiamo sentiti nel corso della precedente sessione. Devo dire che azioni di crisi che riguardano le nostra azienda e le nostre infrastrutture, magari di non rilevanza catastrofica, anche se non sono all'ordine del giorno, lo sono certamente all'ordine della settimana. Cito alcuni esempi concreti: il tranciamento di un cavo a fibra ottica, attraverso il quale passano molte delle nostra comunicazioni; questo è un fatto che non accade infrequentemente. L'infrastrutturazione del Paese richiede scavi e lavori e qualche volta ci si sbaglia, si trancia un cavo; di questo non se ne accorge nessuno e questo perché le strade sulle quali facciamo passare le comunicazioni in fonia e in dati sono ridondanti e sono quindi in grado di sopportare difetti problemi e interruzioni di notevole entità. E questo riguarda sia l'infrastruttura di trasporto, quella che va sottoterra e trasporta attraverso strutture di Telecom e di altre aziende l'insieme dei dati da una parte all'altra della Penisola, sia riguarda le infrastrutture di ricetrasmissione, le antenne radio base e le unità che le controllano. Le antenne radio base sono generalmente i tralicci con gli apparati di ricetrasmissione verticali, che qualche volta non piacciono agli ecoterroristi e qualche volta vengono deliberatamente danneggiati. Anche questi episodi non sono fortunatamente parte della quotidianità, ma in alcune zone vengono ripetuti, fortunatamente con danni alle cose e non alle persone. La ridondanza è un elemento base per essere attrezzati ai disastri o alle calamità sia di natura dolosa, come gli atti di terrorismo, sia natura di meteorologica, sia di natura involontaria. Ogni singolo elemento della nostra infrastruttura (e parliamo di 10.000 elementi fisici sul territorio: antenne, calcolatori, switch) è monitorato 7 giorni su 7,24 ore al giorno. Noi avevamo, e mi rifaccio all'episodio del nostro settembre, un visibilità perfetta di dove mancava

l'alimentazione in Italia, ora dopo ora, perché vedevamo ogni singola stazione ricetrasmittente, se era in batteria, oppure era alimentata. E questo noi lo visualizziamo, ovviamente da remoto, da quattro centri nazionali, da quattro centri regionali e da un centro nazionale, che controlla lo status di tutti gli elementi della nostra struttura di telecomunicazione. Quindi una rete di sensori particolarmente utile e obiettiva. In secondo luogo siamo dotati di infrastrutture mobili che consentono in caso di caduta totale di parte della copertura del nostro sistema di telecomunicazioni di ripristinare *in situ* le condizioni di coperture e di comunicazione voce e dati.

Dottor Pancani: Mi scusi Rossetto. Sono dei *camper*?

Dottor Rossetto: Esattamente sono degli *shelter*; in linguaggio militare è molto noto cosa è uno *shelter*; noi abbiamo dislocato in 6 punti fisici del territorio nazionale, in modo di essere ad una distanza di viaggio compatibile con la gestione di emergenze anche importanti, delle unità su *shelter*, che sono in grado di ripristinare qualsiasi elemento della nostra rete di telecomunicazioni: non basta infatti mettere l'antenna; bisogna anche mettere gli *switch* di commutazione del traffico, altrimenti non si riesce e ripristinare la comunicazione. Un momento probante di questa nostra capacità di risposta è stato il terremoto del Molise che ha riguardato una zona del territorio limitata, ma con danni importanti. Da Roma sono partite le nostre risorse e in due ore e mezza erano in loco a disposizione delle autorità per ripristinare le telecomunicazioni mobili, che, come è stato citato, nei momenti di emergenza assumono assoluto rilievo nella gestione dell'emotività della popolazione, che naturalmente aumenta. Noi disponiamo anche di generatori mobili, pure questi in *shelter*, in grado di muoversi dovunque, malgrado strade interrotte, come può accadere in casi di disastri o di calamità. Questi generatori mobili sono in grado di sopperire e di rialimentare apparecchi ricetrasmittenti che abbiano esaurito la loro vita di batteria. Parliamo del 28 settembre: nessuno è stato in grado di affrontare un *black out* di durata così lunga. Nel nord Italia, dove il ripristino è iniziato alle 7 del mattino, i nostri servizi erano completamente funzionanti perché la durata delle batterie degli elementi ricetrasmissivi va dalle 4 alle 6 ore, a seconda del traffico di carico, ossia di quanto consuma la struttura, o a seconda di quante batterie stanno nello *shelter*. Non sempre c'è spazio per mettere tutte

le batterie che si vogliono. Questo è un esempio. Tutti gli elementi di rete e alcune antenne sono autoalimentate: quindi hanno generatori che mantengono la continuità per periodi prolungati; sono autoalimentati tutti i nostri centri di smistamento e tutti i nostri *switch* principali, ma non tutte le nostre antenne; questo perché nel territorio una azienda grande come Vodafone ha diverse migliaia di antenne e noi non abbiamo diverse migliaia di generatori. La nostra autonomia sull'ultimo elemento, il più remoto, il più semplice, si misura quindi sulla durata delle batterie che è quella che ho spiegato. Abbiamo però unità mobili che sono in grado di attaccarsi alle antenne, ricaricarne le batterie e andare da qualche altra parte, cosa che è successa effettivamente il 28 settembre al sud.

Si è parlato degli *sms*. Noi ci stiamo attrezzando su stimolo e in collaborazione con le autorità: in caso di emergenza locale o nazionale (l'esempio che è stato portato dal nostro moderatore è particolarmente efficace e stiamo lavorando per istituzionalizzarlo) potremmo mettere in grado l'autorità, che gestiste l'emergenza, di inviare a ogni telefonino dei messaggi *ad hoc*, predisposti dalle stesse autorità per intere fasce della popolazione. Questo è un processo che richiede un po' di tempo e sostanziosi investimenti, perché in caso di calamità nazionale, immaginate quanti sono gli *sms* da inviare.

Dottor Pancani: Riguardo agli *sms*, questo sistema che state predisponendo ha avuto maggior vigore dopo quanto è successo o era stato già pensato in precedenza da Vodafone? Gli ultimi episodi di terrorismo hanno incrementato questo sistema?

Dottor Rossetto: Non sono stati tanto gli atti di terrorismo quanto le emergenze energetiche del 28 settembre a spronarci ad accelerare questo processo; è uno strumento facile e fruibile da tutti e di comunicazione particolarmente tempestiva, ma inviare 20, 30 o 40 milioni di sms con grande tempestività richiede risorse tecnologiche molto grandi per le quali comunque ci stiamo approntando. Non ci sono, infatti, risorse tecniche sufficienti e ben gestite, se non vi sono strutture organizzative, modalità e processi. E questa è le seconda gamba delle modalità con cui Vodafone in Italia si equipaggia a sostenere una emergenza terroristica o di altro tipo. Noi aggiorniamo ogni anno il nostro piano integrato di gestione delle emergenze: con i miei colleghi, molti dei quali sono in sala, e con quelli della squadra che

gestisce queste tematiche, ho rivisto in prima persona pochi giorni fa un tomo alto così, che è il libro delle cose da fare. Vi si trovano tutti gli elementi per quello che io ho chiamato un piano di guerra per affrontare un emergenza: quindi le procedure di *escalation* e le risorse tecniche, che 24 ore al giorno, 7 su 7, sono *ready on call*, pronte per intervenire in caso di emergenze commerciali o in caso di emergenze più importanti e critiche, che sono quelle delle infrastrutture. Quali sono le priorità? Immediatamente entro la prima ora valutare i danni alle persone dipendenti e non e provvedere alla loro salvaguardia; nella seconda ora ci si può preoccupare dei danni alle strutture fisiche e agli *asset* e poi, non voglio farla lunga, di tutta una serie attività che vanno svolte, inclusa quella dei contatti e di messa a disposizione degli enti esterni sia delle nostre risorse organizzative che di quelle tecnologiche. Cito ad esempio un fatto: noi abbiamo presso i nostri 6 punti decentrati sul territorio 800 *sim* con apparecchi telefonici, che vengono messi a disposizione delle autorità preposte, segnatamente la Protezione Civile: queste sim hanno priorità in caso di congestione di traffico, perché in caso di emergenza si concentra una quantità di traffico grandissimo, sia pubblico che privato, proveniente da gente che dice di star bene o che ha dei problemi; e a volte la rete collassa. Sono casi rari, ma può capitare proprio nei casi di emergenza, come è successo a Madrid: io ho parlato con i miei colleghi spagnoli, che mi hanno raccontato come hanno affrontato la crisi; questo è quello che accade: un gran numero di chiamate simultanee da uno stesso punto fisico è in grado di far collassare il sistema.

Dottor Pancani: Non c'è un sistema per fronteggiare anche questo tipo di emergenze?

Dottor Rossetto: Puntualmente no. Esiste la necessità di un tempo di reazione che serve a dirottare *in loco* risorse ricetrasmissive addizionali; questo tempo noi lo stimiamo fra 30 minuti, nel caso la calamità avvenga vicino a dove noi abbiamo le risorse mobili, fino a 4 ore, che è il tempo più lungo che noi stimiamo necessario.

Dottor Pancani: Un'ultima domanda. Gli investimenti di Vodafone per fronteggiare queste sfide sono sufficienti? Capisco che è una nota un po' dolente, ma è importante.

Dottor Rossetto: Vodafone Italia investe nel nostro Paese oltre un miliardo di euro all'anno in investimenti fissi, che sono largamente destinati alle infrastrutture di telecomunicazione, alla loro ridondanza sia per ragioni commerciali che per ragioni di gestione delle emergenze. Noi vogliamo in caso di evento grave mantenere la possibilità, sia per gli operatori pubblici, quindi per le autorità, che hanno anche altri mezzi, sia per ciascuno dei nostri utenti, di comunicare come in un giorno normale. Il tema investimenti è oneroso, ma ci trova consapevolmente presenti in Italia.

Dottor Pancani: Grazie al Direttore Generale di Vodafone. Siamo a Wind, a Salvatore Cirafici, Direttore *Asset Governance* di Wind. Anche a lui chiedo quale é lo stato dell'arte: prima, nell'altra sessione, a proposito di possibili attacchi terroristi, mi pare di aver capito batteriologici o comunque di inquinamento delle acque, si ricorre alle trote: appena le trote stanno male, si riesce a capire che in quell'acqua c'è qualche elemento pericoloso; non so se questo è trasportabile anche alle telecomunicazioni. C'è un sistema, lo chiedo a Cirafici, che in qualche modo può dare una mano, oltre naturalmente alla tecnologia sempre più sofisticata, che può permettere di monitorare apparecchiature e installazioni?

Dottor Salvatore Cirafici
Direttore Asset Governance Wind

LE PREDISPOSIZIONI DI SICUREZZA DELLA WIND

Innanzi tutto saluto i convenuti. La ringrazio per la domanda, perché mi dà la possibilità di fare una piccola dissertazione: è una mia personale opinione, ma questa dissertazione vuole essere un messaggio rassicurante. Lei mi ha chiesto se era possibile trasporre quello di cui si era detto nella precedente sessione anche nel campo delle telecomunicazioni. Io, per via del monitoraggio che la mia Direzione, deputata alla sicurezza e tutela aziendale della Wind, fa sul territorio, devo dire che non vi è al momento un pericolo o un allarme terrorismo per quanto riguarda le cosiddette strutture fisse, fisiche, del territorio. Questo perché, con un approccio molto laico e parliamo appunto di terrorismo, parliamo di poche persone che vogliono destabilizzare, ovviamente con risorse scarse, e che utilizzano, e questo è un termine tecnico, militare, ciò che trovano sul terreno. Posso pure capire un attacco a ciò che fa parte del potenziale bellico nazionale, quindi l'energia, il gas, il metanodotto, l'acqua, e in tal caso si tratterebbe di un atto vile, spregevole, che provoca sicuramente un grande allarme, una grande tensione; ma delle comunicazioni gli stessi terroristi, gli stessi agenti del terrore, se ne servono e il rappresentante dell'Eni ne ha autorevolmente parlato poco fa; i terroristi non hanno una radio base, un posto di comando e controllo, non si portano uno *shelter* quando fanno una azione terroristica: devono sfruttare ciò che hanno sul terreno. Quindi, per quanto mi riguarda, il mio messaggio rassicurante è proprio questo: la mia azienda non vede, e peraltro i dati che abbiamo in nostro possesso ci danno contezza, non vede questo pericolo, almeno per quanto riguarda i nostri apparati di telecomunicazioni. Infatti devo dire che gli atti cosiddetti vandalici, che noi subiamo, come pure le altre società dello stesso campo, non sono imputabili a frange terroristiche, ma ad intolleranze dovute ad un impatto mediatico poco chiaro per quello che riguarda l'emissione volt/metro di alcuni nostri impianti. Ma al di là di questo ribadisco il concetto: non c'è, per quanto ci riguarda e secondo le nostre analisi, un allarme o una previsione: questo non vuol dire che non ci prepariamo all'emergenza. Senza ripetere quello a cui autorevolmente il Direttore Generale ha

poco fa accennato circa il *mix* tecnologico, anche perché tedierei l'uditorio, parlerei della struttura. La Wind fin dal la sua nascita si è dotata di una struttura organizzativa che ha voluto fare proprio il salto di qualità dalla tutela aziendale, dalla tutela degli *asset*, al *governement* della stessa azienda, cioè al governo della complessità; governo delle complessità, perché la sicurezza è un asset fondamentale, intrinseco, agli interni di una azienda e diventa quindi strategico all'atto di una emergenza. Per quanto mi riguarda e per quanto riguarda la mia struttura è importantissimo il fattore umano, la cultura della sicurezza, la formazione che avviene prima, posto che, come ho detto, non vediamo assolutamente in questo momento un problema di allarme terroristico nei confronti della telecomunicazione mobile.

Dottor Pancani: Però lo potete immaginare?

Dottor Cirafici: Senz'altro; il nostro impegno fino a questo momento è stato di grande supporto delle Istituzioni ed è proprio questo che dobbiamo sempre incrementare.

Dottor Pancani: Istituzioni, in che senso?

Dottor Cirafici: Stavo per citare le rivendicazioni dell'omicidio Biagi e D'Antona, che sono state rintracciate tramite un accertamento fatto proprio dalla nostra azienda: per tali rivendicazioni avevano utilizzato, appunto, delle nostre sim.

Dottor Pancani: Ossia tramite tabulati...?

Dottor Cirafici: Certo: ogni azienda, nell'ambito della sua sicurezza, ha una struttura che è preposta a delle prestazioni obbligatorie...

Dottor Pancani: Su ordine del magistrato, naturalmente?

Dottor Cirafici: su ordine del magistrato, ci mancherebbe altro, ma anche a richiesta delle Forze di Polizia per le anagrafiche: per queste non c'è bisogno dell'ordine suddetto, perché l'identificazione è un compito delle Forze di Polizia e la loro semplice richiesta è bastevole. Noi abbiamo incrementato

con risorse, con investimenti da parte del nostro Amministratore Delegato, il «sistema magistratura», come noi lo chiamiamo in azienda, che è quello che dà supporto alle Forze di Polizia e alla Magistratura. Per quanto riguarda, invece, il supporto alle calamità e alle emergenze, perché anche queste si attagliano ad una emergenza terroristica, noi utilizziamo un'altra procedura e, a prescindere dalle procedure, utilizziamo un *mix* di tecnologie che, senza voler incensare la mia azienda, in quanto essendo semplicemente tra gli ultimi arrivati nel settore abbiamo usufruito delle tecnologia più recenti, possono contare su apparati di continuità all'ultimo grido e quindi di durata maggiore al momento del *black out*. Ma a prescindere da questo, per quanto riguarda il fattore umano, noi utilizziamo un altro sistema: noi informiamo le autorità civili e militari nell'ambito del supporto durante un'emergenza delle *sim*; inoltre forniamo assistenza alla Pubblica Amministrazione, a richiesta e ovviamente secondo certe procedure concordate, per consentire loro la costanza e l'efficienza delle comunicazioni loro offerte; in relazione a tale attività sono predisposte delle cosiddette *short list* dei soggetti da tenere in contatto; tali liste devono essere *short*, se no, come diceva prima il Direttore di Vodafone, c'è un momento di collasso, di confluenza abnorme di contatti nel sito che serve quell'area.

Dottor Pancani: Dottor Cirafici un'ultima domanda. Il Direttore di Vodafone accennava al fatto che dopo Madrid si è messo in contatto con i colleghi spagnoli per capire cosa fosse successo in occasione di una così grande emergenza. Voi avete scambi anche con altri gestori, naturalmente europei, visto che il terrorismo è globalizzato: immagino, quindi, che anche le strategie e le misure da mettere in atto debbano essere il più possibile globalizzate. Avete contatti, vi consultate, vi sentite, scambiate informazioni?

Dottor Cirafici: La ringrazio per questa domanda. Siamo italiani e io sono orgoglioso di esserlo, anche perché prima di espletare questo lavoro sono stato per circa 24 anni un militare; pertanto io per approccio non sono laico, ma principalmente etico: cerco di trovare le soluzioni all'interno del mio Paese. Devo dire che la famiglia delle telecomunicazioni, e non potrebbe essere diversamente, è un continuo, nel senso che sia in Wind che in Tim e Vodafone ci sono manager che hanno attraversato tutte e tre le strutture; c'è quindi una continua osmosi tra i colleghi. Ovviamente ne ho contezza per la

mia struttura, ma devo dire lo stesso anche nel campo commerciale. Quindi nel campo della sicurezza devo costatare e devo affermare che c'è una sinergia e anche una continua osmosi con Vodafone, con Tim, con Telecom. Tra l'altro posso dire che conosco personalmente i miei omologhi e ho continui rapporti con loro per trovare appunto delle procedure, delle sinergie e delle soluzioni. Abbiamo anche ovviamente dei contatti all'estero, non ultimo con una azienda giapponese, che non nomino perché non voglio fare qui pubblicità, che è entrata con noi in *partenership*, e abbiamo contatti anche con altri. Però ribadisco il concetto: io privilegio le soluzioni all'interno.

Dottor Pancani: Grazie al dottor Cirafici per il suo intervento. Sollecito adesso l'intervento del dottor Cellini, Direttore Generale di Tiscali: con lui puntiamo i nostri riflettori più sull'aspetto legato ad internet, alla rete, anche perché Tiscali è il maggior internet *service provider* presente in Europa; parlo come numero di Paesi in cui è presente in Europa. Insomma ha una bella esperienza: peraltro durante il già più volte citato *black out* la Sardegna è stata una delle poche «isole felici»: mi sembra che la corrente elettrica non sia mai mancata in Sardegna.

Dottor Sergio Cellini
Direttore Generale Tiscali

LA SICUREZZA GLOBALE UN IMPEGNO INSITO NEL DNA DI TISCALI

La Sardegna ha alcuni svantaggi dovuti al fatto di essere un'isola, ma anche dei vantaggi: il black out è stato un evento casuale, ma anche «fortunato», durante il quale Tiscali ha potuto continuare ad erogare il proprio servizio. In Sardegna è presente uno dei più grossi data center europei: certo anche i dati viaggiano con l'energia elettrica, ma dove questa energia elettrica era fornita da gruppi autonomi noi abbiamo continuato ad erogare il servizio e praticamente solo con alcuni problemi, soprattutto nelle prime ore dopo il *black out*, siamo stati tra i primi e tra i meno colpiti il 28 settembre.

Tiscali ha la caratteristica di essere un internet *server provider*, ossia una società che dà soprattutto accesso alla rete internet dislocata in 14 Paesi europei e questo forse è uno dei vantaggi principali, perché permette sia di scambiare informazioni, sapendo in tempi molto brevi quali possano essere le novità e le soluzioni migliori per questo tipo di emergenze, sia di attuare su più territori una serie di azioni sia preventive che di soluzione che sarebbero più difficilmente implementabili in un unico Paese.

Per questo che noi siamo dotati di una struttura operativa che si chiama *Tiger*, che vuole dire *Tiscali International Global Emergency Response*. È un piccolo nucleo formato dai responsabili della sicurezza e dei NOC (*Network Operation Center*) dei principali Paesi Europei. Questi signori sono in contatto permanente, 24 ore su 24 per tutto l'anno, sia tramite internet normalmente, sia, in caso ci fosse una emergenza in questi Paesi, attraverso telefonia fissa o mobile. Di questi tre canali a disposizione, almeno uno, anche nei casi peggiori, dovrebbe essere in grado di funzionare. Si tengono quindi costantemente aggiornati e monitorano il territorio da quelli che possono essere attacchi di vario tipo. Sul fronte internet si assiste soprattutto a quello che potemmo definire un microterrorismo, dovuto ai famosi *hacker*, persone che per motivi vari, talora anche personali, in quanto vogliono dimostrare di essere bravi a penetrare i *firewall*, i sistemi di sicurezza più

importanti, fanno un danno alle aziende e soprattutto alla collettività. Nel solo 2003 sono stati sviluppati 1700 nuovi virus a livello mondiale. Questi virus hanno un impatto economico notevolissimo, che va quantificato non solo per la sostituzione di software o hardware danneggiato, non solo per i data base perduti, che devono essere ricostituiti, non solo per quelli che si chiamano i sistemi di inoculazione, necessari alla «cura» dei virus, ma anche per la produttività persa dalle persone colpite da questi eventi: si stima che nel 2003 l'impatto a livello di danno complessivo di questi virus sia stato di 100 miliardi di dollari. Quando ho visto la presentazione che mi hanno preparato pensavo ci fosse stato un refuso e che fossero 100 milioni: sono invece proprio 100 miliardi; il solo virus *mydum*, che è stato il più devastante dell'anno scorso, ha fatto danni per 22 miliardi di dollari, se consideriamo tutto, compreso appunto il valore della produttività persa. Questo è il danno che fanno al sistema i signori *hacker* e i virus messi in rete.

Le società internet cercano soprattutto di prevenire questa diffusione del virus o questi tipi di attacchi alle reti informatiche con i danni che ne derivano. Come diceva prima il dottor Bertolaso, c'è un sistema di gestione delle conseguenze, che ovviamente è ugualmente importante, anzi in alcuni casi ancora più importante perché si tratta di preservare, difendere e ricostituire soprattutto i *data base*, che sono la ricchezza più grande di tutte le società di telecomunicazioni. Come Tiscali, in particolare, noi abbiamo replicato questi *data base* in almeno tre o quattro località in Europa, nei nostri *data center*. Dal nostro punto di vista, come da quello della grandissima parte delle società «nostre colleghe», è necessario procedere sempre alla replica di questi *data base* in punti difficilmente accessibili: per l'utenza non si creano così gravi problemi. Ma certo l'impatto che questi virus possono avere è sicuramente molto importante.

Recentemente Tiscali è stata chiamata assieme ad altri importanti internet service provider a fare parte del GIAIS (*Global Infrastracture Alliance For Internet Safety*): è una alleanza per la sicurezza su internet, promossa e fortunatamente finanziata soprattutto da Microsoft, che di risorse ne ha parecchie. Questa alleanza serve a coordinare una serie di internet *service provider* a livello internazionale, di condividere alcune tecnologie e metodologie di prevenzione e di condividere, poi, le soluzioni agli eventuali attacchi di *hacker* o di diffusione di virus o di quanti altri danni possono essere apportati alla rete.

Dottor Pancani: E questo sistema è già in atto?

Dottor Cellini: Il sistema è già in atto: ciascuno dei partecipanti contribuisce con quello che è il suo *expertise*, oltre alla parte di presenza internazionale. Nel caso specifico di Tiscali ci stiamo focalizzando soprattutto sulla identificazione e tracciamento dei virus. Come è noto il virus parte da un posto X e poi si dirama il più rapidamente possibile attraverso le reti. Di recente abbiamo identificato un virus che era partito dalla Norvegia, man mano aveva camminato e si era distribuito in Gran Bretagna, per passare poi in Francia: da qui si sarebbe sparso su tutta l'Europa continentale. Bene! Grazie a questo *Tiger*, grazie a questa unità di crisi, grazie alla collaborazione con gli altri internet *service provider*, il virus è stato intercettato in Francia e i danni sono stati limitati. Ovviamente non sempre questo è possibile: ci sono altri casi di microterrorismo informatico dovuti a signori che mettono in batteria un grande serie di *server* che poi scaricano richieste di informazione su un internet *service provider*, su un sito particolare ecc.; normalmente sono attacchi coordinati e fatti partire da Paesi lontani, spesso dalla Cina, dall'India, da Taiwan, dall'Indonesia. È più difficile, così, rintracciare l'origine di questi attacchi, che spesso causano a tutti gli internet *service provider* dei danni di rallentamento del servizio, di sua non accessibilità, talora di distruzione della posta elettronica. Anche in questo c'è un coordinamento: a livello di Tiscali, al suo interno, tra le società che compongono il gruppo; a livello internazionale, paneuropeo, ci sono contatti permanenti, che permettono di ridurre l'impatto di questi attacchi.

Potrei terminare dicendo che ovviamente la rete è lo strumento di propagazione più rapido di tutto questo tipo di problematiche. I terroristi, nello specifico, utilizzano i siti internet e la posta elettronica, come anche gli *sms*, da strumento di comunicazione.

Dottor Pancani: Mi pare che anche dietro qualche file musicale c'era una corrispondenza tra adepti al terrorismo, naturalmente con dei codici da decrittare. Insomma hanno usato anche questo!

Dottor Cellini: Sì! C'è però una stretta collaborazione con tutte le autorità competenti: ognuno degli internet *service provider* collabora con l'autorità giudiziaria. La sola Tiscali ha risposto nel 2003 a 10.000 richieste, parlia-

mo dell'Italia, da parte dell'autorità giudiziaria di accertamenti relativi a tracciati o ad e-mail, ad esempio su pedofilia o cose simili. E Tiscali è relativamente piccola rispetto a quelli che sono altri *player* sul mercato. Quindi immaginiamoci che grandissima mole di informazioni va conservata e gestita per averne un rapidissimo accesso, in caso di emergenza. Proprio per questo ogni contributo finanziario da parte dei Governi o delle autorità è qualcosa che io stesso e tutti i miei colleghi vedrebbero con grandissimo interesse.

Dottor Pancani: La cifra che ha fatto è sconcertante per quello che riguarda i presunti reati, ma ha detto, invece, qualcosa di confortante per quello che riguarda la collaborazione esistente. Lei lo ha evidenziato, come lo ha fatto anche il Direttore di Wind; prima, durante una pausa, ne parlavo anche con il Direttore di Vodafone: quindi grande collaborazione tra le nostre aziende e in questo caso l'autorità giudiziaria. Ciò è di buon auspicio, anche perché sono all'ordine del giorno questo tipo di collaborazioni. Ringrazio anche il dottor Cellini, Direttore Generale di Tiscali per il suo intervento. E vengo all'ultimo intervento, al dottor Giuliano Tavaroli, *Corporate Security Manager* di Telecom Italia. Decrittiamo; cosa possiamo dire: il Capo della sicurezza?

Dottor Giuliano Tavaroli
Corporate Security Manager Telecom Italia

IL SISTEMA DI SICUREZZA DELLA TELECOM

Innanzi tutto grazie dell'invito. Sono il responsabile della sicurezza del Gruppo Telecom.

Dottor Pancani: Il Presidente Ramponi si è raccomandato perché io non la tratti meglio degli altri visto che facciamo parte dello stesso Gruppo: allora le do' subito una mazzata. Ieri sul sito di Repubblica, ma lo riportavano anche altri giornali, c'era scritto: «Hacker nel sito Telecom 187; a rischio la privacy degli utenti». Allora è vero, non è vero, cosa abbiamo rischiato, cosa è successo?

Dottor Tavaroli: Questo è uno di quei casi che non rende merito alla serietà del tema che trattiamo oggi. Telecom Italia ha subìto un *assesment* di sicurezza non richiesto e non sollecitato. È stata evidenziata una vulnerabilità sul sistema website in discussione. È stata segnalata a noi, e poi alla stampa, una falla che era già stata sistemata: è stata una buona occasione per farsi un po' di pubblicità a spese di Telecom Italia. Quello che posso dire si allinea con quanto esposto precedentemente da tutti i colleghi, che hanno presentato il tema della sicurezza. Non vorrei, quindi, ripetere le cose che i miei colleghi hanno esposto in maniera eccellente, perché credo che si sia compreso che esiste un modello di sicurezza nelle telecomunicazioni molto ben conosciuto, stabilito e consolidato, fondato sostanzialmente su architetture ridondanti e su sistemi operativi di gestione delle emergenze estremamente efficienti. Siamo stati testati dal *black out* energetico che oggi, mi è sembrato di capire, è assurto di fatto a simulazione di crisi nazionali, che altri Paesi dopo l'11 settembre hanno fatto trasversalmente su tutte le infrastrutture critiche.

Noi non siamo stati chiamati a confrontarci in maniera verticale, ma questo è il modello di sicurezza: ridondanza, sistemi di intervento rapido, sistemi di alimentazione eccedenti le normali valutazioni del rischio. Questo ha consentito che tutti noi, in una situazione di emergenza come quella del *black out* energetico, appunto, potessimo comunicare nonostante la criticità del

momento. Da questo punto di vista il modello di sicurezza delle telecomunicazioni è efficiente, regge, è importante. Nel modello di sicurezza degli operatori di telecomunicazione, forniamo all'autorità giudiziaria i nostri dati sui clienti solo su richiesta.

Qualcuno, precisamente il dottor Rossetto, ha chiamato questo sistema NOC, mentre noi li chiamiamo SOC (Security Service Operation Center). Il sistema delle telecomunicazioni non solo ha ridondanze, ma ha anche centri di controllo e di governo, esattamente come le reti di energia, dai quali si monitora lo stato delle reti minuto per minuto: si conosce il numero degli accessi ,i carichi, si sa dove si generano le situazioni di crisi. Anche noi di Telecom Italia siamo degli internet provider, il che vale sia per la parte che si occupa specificamente di internet, sia per quella che si occupa di telefonia mobile, ma vale anche per la sicurezza: per questo abbiamo creato il Security Service Operation Center, che monitora tutti i temi della sicurezza. Oltre quanto investito nelle reti del *business*, quest'anno il Gruppo Telecom Italia investe per reti di sicurezza, quindi non in quelle *inbedded* nelle infrastrutture, ma in quelle dirette a migliorare la performance di sicurezza del Gruppo, circa 150 milioni di euro.

Si è detto, e lo confermo, siamo un Paese in cui le infrastrutture critiche si sono assunte la responsabilità della sicurezza. Tuttavia, ci chiediamo: questo patrimonio di competenze tecniche, di sapere e di informazioni quanto può essere utile al sistema Paese? Negli Stati Uniti, per esempio, hanno simulato la gestione di tutte le possibili emergenze, e del rischio verticale (la somma di incidenti contemporanei su tutte le *utilities*: telecomunicazioni, energia, acqua, trasporti, sanità ecc.).

Tornando all'Italia, viene da chiedersi: cosa sarebbe successo durante il *black out* elettrico se non avessero funzionato le telecomunicazioni e se si fossero verificati contemporaneamente attacchi multipli alla rete di internet, alle telecomunicazioni, all'energia? Nella prevenzione e nell'analisi del rischio possiamo fare molto di più. Soprattutto sul piano della condivisione delle informazioni. Le grandi aziende hanno al loro interno delle eccellenze tecnologiche, vivono le questioni della sicurezza tutti i giorni, generano informazioni e profili di rischio. Ma di solito le informazioni vengono scambiate tra di noi, mentre raramente ci viene chiesto di fornirle ad organismi pubblici, che invece dovrebbero fare una sintesi verticale di tutti gli indicatori di rischio. Questo è il contributo, e anche l'auspicio, che volevo portare

in questa sede. Recentemente l'FBI americana ha cambiato il motto dei propri corsi in «Think the unthinkable» (pensa, prevedi l'impensabile): insomma, dopo l'11 settembre è cambiato l'approccio. In questo quadro, credo che il livello di cooperazione tra pubblico e privato sulla sicurezza delle infrastrutture non solo apra grandi ambiti di collaborazione, ma possa e debba migliorare. Concedetemi una considerazione: sono orgoglioso di dire che queste aziende, compresa Telecom Italia, possiedono al loro interno competenze, capacità, e che operano nel campo della sicurezza con grande responsabilità, spendendo energie, anche economiche, e soprattutto la passione costante di tante persone.

Dottor Pancani: Un'ultima battuta soltanto: volevo rivolgerti una domanda su quello che riguarda la privacy, che è l'altro aspetto di tutto quello che ci siamo detti finora. Vorrei una tua opinione su questo aspetto.

Dottor Tavaroli: A questo proposito, credo che tutti noi siamo allineati. La privacy per noi è un valore, perché il cliente è un valore per l'azienda e i dati di chi utilizza i nostri servizi costituiscono un valore. La fidelizzazione del cliente passa attraverso una corretta gestione dei dati della privacy. Voi sapete che è stato emesso un nuovo regolamento della privacy, frutto di un processo legislativo molto lungo, al quale ci siamo rapidamente adeguati. Questa novità cambia alcune cose che si riferiscono ai dati di telefonia: il traffico di telefonia è disponibile all'autorità giudiziaria per 24 mesi, più ulteriori 24 in funzione della tipologia dei reati (terrorismo e criminalità organizzata). Per quanto riguarda, invece, i dati internet, la faccio breve, forse c'è stata una distrazione del legislatore, non è più possibile per l'autorità giudiziaria ricevere o richiedere i dati sulle transazioni da internet dopo i 6 mesi dalla fatturazione. Mentre se si tratta di accessi gratuiti, gli ISP, sono tenuti alla immediata cancellazione dei log delle transazioni. Credo che questa sia una vulnerabilità grave dal punto di vista della sicurezza del Paese, che dovrebbe essere sanata. Non tanto per il gestore di telecomunicazioni, che si è adeguato immediatamente al dettato legislativo, ma piuttosto per una valutazione politica dell'integrità e della sicurezza del Paese.

Dottor Pancani: Grazie, anche per questa finale, utile, sottolineatura, al dottor Tavaroli. Come è andata la squadra Presidente?

Gen. Ramponi: Pancani dice che do' i voti; non do' i voti, ma siete testimoni che anche questa seconda tornata è stata di una utilità pari a quella che ci aspettavamo. Grazie infinite; credo che mi sarà difficile non coinvolgere ancora i giornalisti in questi convegni, perché danno una vivacità, godono di una libertà e di una disinvoltura che molto spesso non è familiare a chi non svolge questa attività e danno un tono di interesse notevolissimo a tutto il discorso.

Voglio solo dire che io ho fissato due o tre idee fondamentali: Rossetto mi ha regalato il discorso della utilizzazione delle risorse esterne nel momento in cui vi è un picco, una concentrazione, dovuta ad una emergenza in un luogo. Ho imparato questa capacità di riindirizzare, utilizzando risorse esterne; Cirafici mi ha fatto fare una riflessione: in fondo è vero le comunicazioni non sono un obiettivo prioritario, perché sono anche un elemento di utilizzazione da parte di coloro che svolgono l'attacco. Cellini: è verissimo il discorso degli hacker, dei virus, che mi era familiare, ma è anche vero che in fondo questa sensibilizzazione, e anch'io devo citare il mio amico Rapetto che già 5 anni fa cominciò a sensibilizzarmi su questo fatto e di come gli Americani erano attenti, forse ha fatto si la presenza degli hacker che in fondo noi si fosse già preparati a prendere in considerazione la minaccia del cibernetico da parte del terrorismo perché prima per fini diversi abbiamo subito e subiamo dei danni infiniti, che lei ha quantificato in cifre spaventose. E infine è consolante il discorso, e me ne vado anche con quest'altra idea, che vi da parte di tutti voi, sotto il coordinamento di Microsoft, questa iniziativa che costituisce il luogo dei punti di tutte le capacità e le eccellenze per essere pronti ad operare e a reagire. Così pure la raccomandazione di Tavaroli, che in fondo si innesta in quella proposta di workshop che ha fatto prima Ortis, di creare un luogo dei punti nell'ambito del quale anche la Pubblica Amministrazione possa valersi della preziosissima risorsa e complesso di conoscenze che voi avete nel contesto della problematica che riguarda le telecomunicazioni. Io faccio del mio meglio nel fare questo. Il convegno precedente ha avuto degli ottimi derivati: speriamo che l'abbia anche questo. Grazie a tutti e chiamo allora il dottor Marco Zanichelli, il dottor Francesco Forlenza, Direttore Generale delle Ferrovie, che ringrazio per essere venuto di persona, il dottor Franco Pecorini, altrettanta presenza importante, il dottor Igino Lai, a prendere posto ed essere coordinanti dalla dottoressa Maria Teresa Lamberti, che prego di sedersi accanto a me.

TERZA SESSIONE

INTERVENTI

Dott.ssa Maria Teresa Lamberti

Dott. Francesco Forlenza

Dott. Franco Pecorini

Dott. Igino Lai

Ing. Pier Francesco Guarguaglini

LA CAPACITÀ DI DIFESA DEL SISTEMA PAESE NEL SETTORE DEI TRASPORTI

Introduzione del moderatore dott.ssa Maria Teresa Lamberti
inviato speciale - Giornale Radio Rai

Buon giorno. Siamo arrivati alla terza sessione, quella che è dedicata ai trasporti, tema che ci vede sicuramente più partecipi a livello emotivo; più coinvolti, è ovvio, perché la recente ferita della strage di Madrid ci ha fatto sostanzialmente capire, quasi direttamente, quale può essere l'impatto che ha un attacco terroristico sui sistemi di trasporto. Un sistema di trasporto che potremmo considerare sotto due diversi aspetti, ossia il sistema di trasporto come strumento e il sistema di trasporto come bersaglio.

Se torniamo a Madrid dell'11 marzo di quest'anno, «l'11 settembre» degli Europei, ci sono state tredici bombe con dieci esplosioni su tre treni; ci sono stati 201 morti e oltre 1500 feriti. In questo caso, naturalmente, il treno è stato un bersaglio, diversamente da quello che è avvenuto, per esempio, nell'altro «11», l'11 settembre a New York, quando gli aerei sono stati strumento di morte lanciati contro le Twin Towers. Era un bersaglio, parliamo di sistemi di trasporto diversi, la nave Achille Lauro, sono bersagli i treni, sono bersagli le stazioni, i binari e non possiamo non far finta di non temere quando parliamo di tunnel e di viadotti, dei tunnel, specialmente, dei quali possiamo già valutare la vulnerabilità pensando agli incidenti, che non sono legati ad eventi dolosi, ma che ci hanno fatto capire quale può essere il loro livello di vulnerabilità e di pericolosità. Pensiamo ancora ai container, perché essi possono trasportare sostanze esplosive o altamente pericolose, paragonabili ad aggressivi biochimici: il Congresso americano se ne sta occupando con particolare attenzione, perché il 90% dei trasporti cargo nel mondo viene proprio fatto attraverso container e sono quindi pericolosi.

Un ultimo dato per mettere in evidenza, se ancora ce ne fosse bisogno, cosa significa sistema trasporti e cosa significa utilizzare lo stesso come bersaglio, se non come strumento. Una ricerca pubblicata negli Stati Uniti, ma che riguarda tutto il nostro pianeta, ha preso in considerazione gli anni che vanno dal 1997 al 2000 e ha identificato quelli che possono essere i bersagli terrestri. Vi dico solo pochissime cifre: il 41% sono autobus; il 10% sono

stazioni ferroviarie e stazioni della metropolitana, il 22% vagoni della metropolitana e treni. Già solo questi secondi due tipi di bersagli, cioè le stazioni e il materiale rotabile, arrivano assieme ad un valore del 32%: è una cifra elevatissima a livello di rischio. Ci sono poi un 8% di terminal di autobus, l'8% i binari, il 5% i bus turistici, l'1% i tunnel e i porti. Insomma dai fatti di cronaca, ma anche dai dati che possiamo desumere facendo delle brevissime ricerche sui giornali o su internet, sappiamo che i timori non possono che accavallarsi. Chiaramente non possiamo, a questo punto, che chiedere delle risposte, cercare di avere un quadro più dettagliato della situazione, magari anche un quadro più tranquillizzante, come abbiamo cercato di far emergere questa mattina parlando degli altri settori. Questa volta lo facciamo con il dottor Francesco Forlenza, Direttore Generale delle Ferrovie dello Stato, con il dottor Franco Pecorini, Aministratore Delegato della Tirrenia, e con il dottor Igino Lai, Responsabile gestione operativa Autostrade per l'Italia Spa. Manca il rappresentante della nostra compagnia di bandiera, l'Alitalia, che è occupato naturalmente in questioni piuttosto serie, come sapete, ma se avremo modo cercherò io di aggiungere qualche notizia sulla sicurezza dei voli perché tutti noi sostanzialmente ormai non prendiamo un aereo, non ci imbarchiamo su una nave o non saliamo su un treno senza avere dei timori che prima non avevamo. Prima potevamo avere il mal d'aria, ora abbiamo il timore di saltare per aria. È proprio ai nostri interlocutori che vorrei chiedere che cosa si sta attuando sostanzialmente alla luce dei fatti recenti, che cosa si è messo in piedi per garantire la sicurezza ai passeggeri. Se permettete comincerei con il dottor Francesco Forlenza. Che cosa stanno facendo le Ferrovie dello Stato? Per esempio, chi ha avuto occasione di andare recentemente alla stazione Termini ha visto in giro, oltre alla polizia, guardie private; alle volte si sente addirittura un altoparlante con un avviso che chiede di fare attenzione ai bagagli incustoditi. Sono solo dei piccoli segni, ma che cosa veramente sta avvenendo che ci possa garantire la sicurezza sui treni. Parlo di treni e non cito tutto perché il tempo è poco, ma voi sapete benissimo che, per esempio, in Francia ci sono stati degli allarmi legati ai binari: noi parliamo di treni, ma parliamo anche di stazioni e di infrastrutture in generale.

Dottor Francesco Forlenza
Direttore Generale delle Ferrovie dello Stato

LA SICUREZZA NELLE FERROVIE DELLO STATO

Prima di dare una risposta diretta alla domanda che è stata posta e che mi sembra naturalmente centrale, credo che sia importante dare prima un'idea di quanto si è già fatto per la sicurezza nell'ambito delle Ferrovie dello Stato, caratterizzate da dimensioni, distribuzione sul territorio e permeabilità assolutamente diverse da qualsiasi altro sistema.

Ribadisco intanto l'analisi fatta dalla dott.ssa Lamberti: con gli attentati terroristici dell'11 settembre 2001 negli Stati Uniti si è evidenziato che gli obiettivi del terrorismo sono sempre più orientati a *target* civili o in cui vi sia un forte coinvolgimento di civili in aree urbanizzate, dove è facile confondersi nella folla di pendolari, turisti, clienti di centri commerciali, ristoranti.

Questo evidenzia che i settori particolarmente esposti nei Paesi avanzati si stanno rivelando proprio quelli delle Aziende che gestiscono le *pubblic utilities*, i sistemi di trasporto e le sue infrastrutture, i servizi essenziali della comunità e del Paese stesso; cioè tutte quelle attività che nel loro insieme e nella loro funzionalità sono parte integrante della qualità della vita di un Paese moderno.

Questo è stato drammaticamente confermato con gli attentati dell'11 marzo 2004 a Madrid in Spagna, che proprio nel settore ferroviario hanno riproposto una riflessione sul tema della sicurezza.

Per il Gruppo Ferrovie dello Stato l'esigenza sicurezza è sempre stata per legge e di fatto responsabilità della Polizia Ferroviaria che provvede: «alla prevenzione e alla repressione degli illeciti consumati in ambito ferroviario, alla tutela dell'ordine pubblico e all'incolumità dei cittadini nell'ambito dei trasporti effettuati sulle linee ferroviarie, sui treni in sosta o in corsa, negli impianti ferroviari, in ogni loro pertinenza ed in qualunque settore del servizio ferroviario».

L'attività di «Security Aziendale» presso le Ferrovie dello Stato solo negli ultimi anni ha assunto un ruolo e delle finalità proprie, tipiche della «Security Industriale» con problematiche fortemente condizionate, appunto, dalle caratteristiche fisiche del sistema ferroviario.

Sarà opportuno dare un'idea, come ho detto all'inizio, delle sue dimensioni. Oggi le Ferrovie dello Stato sono un Gruppo di 102.000 persone articolato in società, tra le quali, principalmente interessate al tema della *security*, sono Trenitalia Spa, che provvede al trasporto passeggeri e merci, RFI Spa (Rete Ferroviaria Italiana), che gestisce l'infrastruttura ed è responsabile degli impianti e della sicurezza della circolazione dei treni, Grandi Stazioni e Centostazioni, per la gestione della parte commerciale delle principali stazioni italiane.

Per le Ferrovie dello Stato si possono evidenziare le seguenti cifre:

- circolano sulla rete 9.200 treni ogni giorno;
- prendono il treno 475 milioni di viaggiatori (anno 2002);
- vengono trasportate 88 milioni di tonnellate di merci (anno 2002).

Le Ferrovie dispongono di:

- un parco di circa 80.000 rotabili, che si sta rinnovando rapidamente;
- 2700 stazioni distribuite in tutto il Paese;
- una rete di oltre 16.000 Km.

Le Ferrovie effettuano anche un servizio traghetti attraverso lo Stretto di Messina, per la Sicilia.

La nuova organizzazione di trasporto ed i nuovi modelli societari, imposti alle Ferrovie di tutta Europa, hanno richiesto anche una revisione completa delle attività e degli attori della security del settore.

Sui modelli organizzativi ferroviari incide, e non solo sotto il profilo della *security*, un aspetto peculiare e di estrema importanza: il fatto di essere un sistema aperto. Infatti, a differenza delle aziende industriali, che nei propri luoghi di produzione e stoccaggio, oltre a poterli recintare, possono decidere e controllare ciò che vi accede, si tratti di persone o di beni, l'ambiente ferroviario è in maniera intrinseca un sistema che ha necessità di rimanere aperto alla collettività e non solo ai propri clienti.

A questo si aggiunga che gli impianti ferroviari, edificati in origine nelle zone cittadine periferiche, sono oggi inglobati in quelle che sono diventate le aree urbane centrali della città. Le stazioni sono diventate riferimento e «porta ideale» delle città, così da trovarsi inserite in un contesto sociale spesso fortemente deteriorato, la cui riqualificazione passa anche attraverso la l'adozione di misure di sicurezza volte a dare fiducia e tranquillità al cittadino/cliente.

Tutto questo viene esaltato nelle grandi città ove la stazione, oltre che punto di interscambio tra flussi di traffico internazionale, nazionale/regionale e sistema di trasporto metropolitano, con l'apertura di moderni centri commerciali, al suo interno diventerà sempre di più luogo di incontro non solo ferroviario.

La rete, che per la sua capillare ramificazione è forse l'infrastruttura più vasta e distribuita del Paese, ne esalta il sistema aperto con le immaginabili problematiche connesse alla security oltre che al più ampio aspetto della sicurezza d'esercizio.

La revisione delle attività e degli attori della *security* ferroviaria ha messo in luce in questi anni l'esigenza di una politica attiva, che sta facendo emergere la complementarietà delle aziende ferroviarie nei confronti degli organi di sicurezza statali, cui primariamente compete la sicurezza dei cittadini. Le Ferrovie dello Stato, in un ottica di impiego legata ai criteri privatistici delle risorse, hanno cominciato a dotarsi di funzioni di sicurezza industriale volte alla tutela di persone, asset, *know-how*, nonché a svolgere attività di raccordo con le Forze di Polizia.

Come in altri Paesi europei, anche in Italia le forze di polizia ferroviaria e dei trasporti, in un ottica di nuovo approccio ed impegno nel settore ferroviario, spesso connesso a nuove vulnerabilità quali il terrorismo e l'immigrazione clandestina, stanno razionalizzando ed ottimizzando la loro presenza e le modalità di impiego del personale.

Le Ferrovie dello Stato dal canto loro, al fine di apportare il proprio contributo in termini di sicurezza, hanno impostato linee guida di *Security Policy* con la consapevolezza che solo con una visione integrata la *security* diventa parte determinante della qualità del servizio reso al cliente.

A tal fine l'attività di protezione aziendale prevede di:

- rappresentare in via esclusiva il punto di riferimento per il Gruppo in ogni rapporto con il Ministero dell'Interno, Servizio di Polizia Ferroviaria, e con gli Organismi internazionali operanti nel settore *security*;
- redigere i piani sistematici di protezione dell'azienda, individuando le soluzioni organizzative ottimali e monitorando le situazioni di criticità in atto;
- garantire, a livello centrale la gestione di un sistema integrato di security;
- presidiare e coordinare, in ambito nazionale ed internazionale (NATO e UEO), ogni attività inerente all'organizzazione della difesa e della sicu-

rezza, anche in situazioni di crisi e di emergenza, nonché alla protezione civile.

Di rilievo le misure che il Gruppo Ferrovie dello Stato ha già posto in essere al fine di elevare il livello di security nelle stazione e nelle infrastrutture. Negli ultimi quattro anni, preso a modello il progetto di videosorveglianza approntato in occasione del Giubileo 2000 per la stazione Termini di Roma, comprendente 340 telecamere che riportano alla sala operativa gestita dalla Polizia Ferroviaria, sono stati installati o ammodernati impianti di videosorveglianza in 38 stazioni per un investimento di oltre 10.000.000 di euro.

Ulteriori 4.000.000 di euro sono stati stanziati per la tutela, anche con termocamere, degli accessi alle gallerie ferroviarie di maggiore rilevanza per la circolazione e per altri manufatti di prioritario interesse.

Nel quadro di una sempre maggiore integrazione e sinergia con la Polizia Ferroviaria, è di grande importanza il progetto da 22.000.000 di euro attivato tra la Polizia Ferroviaria e il Gruppo Ferrovie dello Stato, per il tramite operativo delle Società Grandi Stazioni e Centostazioni, nell'ambito del Piano Operativo Nazionale (PON) sicurezza Sud, con fondi della Comunità Europea destinati alla sicurezza di aree al alto tasso di criminalità, tra cui il mezzogiorno di Italia.

Dott.ssa Lamberti: Scusi l'interruzione, ma tutti questi soggetti hanno aumentato la presenza di controlli, sia dovuti agli investimenti che all'aumento di personale?

Dottor Forlenza: Hanno aumentato gli investimenti: tanto per fare un esempio e restare in tema con quanto sto illustrando, allo stato attuale, completato l'allestimento delle sale operative, è già in fase di avvio il sistema di videosorveglianza che interessa 18 stazioni del Sud Italia tra cui Napoli, Reggio Calabria, Bari, Catania, Palermo, Cagliari. Sono quindi impianti che sono stati ideati per un problema specifico, quello della garanzia di sicurezza che dobbiamo dare, ma che sono nello stesso tempo idonei anche a gestire la nuova preoccupazione che c'è. Inoltre la vigilanza privata, organizzata dalle stesse Ferrovie, ad esempio nelle aree dove vengono composti i treni, comporta dei grandi costi, ma anche una maggiore sicurezza.

È da evidenziare inoltre, nell'ambito della collaborazione con le Forze

dell'Ordine, la convenzione siglata nel luglio 2003 tra Ferrovie dello Stato e il Dipartimento della Pubblica Sicurezza per la prevenzione dei «crimini informatici sui sistemi di gestione della circolazione ferroviaria», della cui attività si fanno carico congiuntamente il Servizio Polizia delle Comunicazioni e Rete Ferroviaria Italiana.

In uno scenario di rischi in continua evoluzione farsi trovare preparati non è solo un dovere, ma un imperativo. L'impegno del Gruppo Ferrovie dello Stato nella formazione, anche nel settore della *security*, è grande e costante a tutti i livelli.

Fare formazione di sicurezza serve soprattutto a trasmettere una cultura di security che abitui a cogliere quei «segnali deboli» di criticità che possono consentire, se bene utilizzati, di impostare attività preventiva mirata e razionale.

Con la sempre maggiore liberalizzazione in corso, il «modello futuro» vedrà senz'altro le Ferrovie dello Stato sempre più coinvolte e impegnate a supportare le Forze dell'Ordine ed in particolare la Polizia Ferroviaria con attività di *security*.

Sfide sempre più impegnative attendono la sicurezza, oltre che in funzione di prevenzione al terrorismo, anche nei tradizionali settori critici quali il trasporto di tifosi, di merci di valore o pericolose, di tutela degli immobili e stazioni, anche con la partecipazione a progetti di impianti avanzati di telesorveglianza e antintrusione.

Nuovi aspetti di vulnerabilità si presentano fortemente, per una azienda così capillarmente distribuita sul territorio, anche nei settori dell'*information technology* e nelle reti dell'attività di *e-commerce per biglietti e prenotazio*ni.

Altro aspetto rilevante è il contesto, almeno europeo, in cui una grossa azienda di trasporto si deve sentire inserita, anche sotto l'aspetto della sicurezza dei clienti, che richiede una costante presenza nei fori internazionali a ciò preposti. Recentemente abbiamo incrementato questa presenza sia negli ambiti delle Istituzioni che si occupano di trasporto ferroviario, ma anche in altri ambiti dove si incontrano le similari imprese europee. C'è poi un altro ambito dove ci sono tutte le ferrovie del mondo. Questo consente non soltanto lo scambio delle informazioni negli incontri formali, ma anche la costituzione di quella rete di relazioni, di rapporti, che fa poi delle informazioni una rete di *intelligence* significativa: è questa che consente di cogliere i

«segnali deboli» e di trovare le migliori risposte a quelli che possono essere determinati pericoli.

In conclusione l'attività di sicurezza, svolta per oltre un secolo come attività dello Stato con Forze di Polizia specializzate, richiede ora, con l'Azienda Ferroviaria ristrutturata, un approccio completamente nuovo sul piano culturale e normativo.

L'integrazione e la partecipazione nella sicurezza richiedono necessariamente un quadro normativo adeguato e moderno, come già attuato nel settore aereo, che colga l'esigenza di poter sviluppare ulteriori aspetti della sicurezza privata per un reale valore aggiunto alle attività istituzionali.

Se da un lato è necessaria una chiara distinzione fra attività di sicurezza pubblica e di *security* industriale dell'azienda, dall'altro non si può che auspicare, come del resto già avviato, una forte *partnership* fra le stesse al fine di ottenere un calibrato ed integrato sistema di sicurezza.

Dott.ssa Lamberti: La ringrazio; magari torneremo in seguito a parlare di emergenze, perché vorrei sentire anche gli altri ospiti, in particolare il dottor Franco Pecorini, Amministratore Delegato della Tirrenia. Abbiamo parlato di cargo: non è questo il caso, perché nei porti ci sono maggiori controlli sicuramente. Il personale che si occupa dell'imbarco, che sostanzialmente strappa il biglietto quando si sale a bordo, è stato addestrato maggiormente? Che altre misure sono state introdotte alla luce dell'esperienza che purtroppo ci è venuta dall'estero?

Dottor Franco Pecorini
Amministratore Delegato della Tirrenia

IL SISTEMA DI SICUREZZA DELLA TIRRENIA

Intanto io vorrei dire brevemente cosa è la Tirrenia. La Tirrenia, o meglio il Gruppo Tirrenia è uno dei maggiori a livello europeo. Come è noto, svolge servizi di collegamento marittimo a valenza pubblica tra il continente e le isole italiane e trasporta ogni anno circa 13.500.000 passeggeri, 2.100.000 autovetture al seguito e 6.700.000 metri lineari di merci: quindi un grosso Gruppo, una grossa realtà.

Va subito specificato che il Gruppo Tirrenia è in regola con le normative internazionali di sicurezza. Queste normative prevedono che:

- sia nominato un responsabile a livello aziendale della sicurezza: per noi questa figura è il responsabile della gestione flotta e cioè un Comandante con vasta esperienza che risiede presso la Direzione Generale;
- sia nominato un responsabile per ogni nave. Per noi questo responsabile è il 1° Ufficiale di coperta, il più vicino al Comandante, dal quale dipende l'applicazione del piano di sicurezza redatto dall'Azienda ed approvato dall'Amministrazione: il piano di sicurezza è un documento analitico che prevede per ogni situazione di emergenza una serie di contromisure ed è un documento riservato, di cui ogni nave è dotata;
- ci sia un apparato radio che in ogni momento trasmette i dati nave: nome, carico, rotta e velocità ad altri apparati in grado di decifrarne il segnale e quindi di conoscere i dati della nave e la sua posizione. In pratica questo apparato emette e riceve segnali che permettono alle navi e stazioni di terra (Capitanerie di Porto) di conoscere l'identità della nave che trasmette, il carico trasportato, rotta, velocità e luogo di destinazione;
- ci sia un altro apparato radio che, in caso di emergenza, istantaneamente, schiacciando dei bottoni in posizione segreta (uno in plancia, l'altro in zona riservata), trasmette un allarme alla autorità nazionale preposta (l'identità di tale organismo a terra è attualmente riservata);
- siano chiuse le zone sensibili della nave, come plancia di comando, apparato motore, sistemi di controllo antincendio, riserve acqua dolce ecc., in modo da renderle inaccessibili ai malintenzionati.

Questo è quello che abbiamo fatto in linea con le normative internazionali. Oltre a questo il Gruppo Tirrenia ha redatto il Piano di Sicurezza Tirrenia, che sta completando l'iter di approvazione presso il Ministero dei Trasporti.

Inoltre sul piano della componente umana si stanno facendo dei corsi tenuti da esperti di sicurezza ed antiterrorismo, rivolti ai Comandanti ed agli Ufficiali superiori. Successivamente, entro la metà del 2005, questi corsi saranno tenuti per il rimanente personale di bordo. In totale verranno addestrati circa 1500 marittimi su un totale di circa 3000.

Attualmente il personale di bordo è stato opportunamente sensibilizzato da parte dell'apposito Ufficio Sicurezza della Direzione Generale, con specifiche istruzioni sia di carattere generale che di tipo specifico in relazione a fatti e segnalazioni contingenti. Tali istruzioni si sostanziano, in particolare in:

- controllo attento, ben più di prima, dei titoli di viaggio dei passeggeri e del carico pesante: questo si è potuto fare iniziando le attività di imbarco tre ore prima della partenza;
- invito ai passeggeri già imbarcati a non ridiscendere dalla nave;
- verifica delle persone estranee all'equipaggio, ad esempio di quelle addette ai rifornimenti, che intendono salire a bordo: viene fatto il controllo dei documenti personali e vengono rilasciati *badge* identificativi;
- controllo periodico degli specchi acquei circostanti la nave;
- verifica del livello di illuminazione della nave sia all'esterno che all'interno, in particolare nei garage;
- verifica e controllo di eventuali oggetti o bagagli sospetti lasciati incustoditi;
- verifica e controllo dei documenti personali di persone sospette;
- verifica e controllo «a spot» di automobili e autoveicoli pesanti.

Questo è quello che abbiamo realizzato al di là delle normative internazionali.

Dott.ssa Lamberti: Questo è quello che si fa per la normale amministrazione, anche se in un momento di particolare attenzione alla sicurezza: tuttavia il 22 marzo di quest'anno a Civitavecchia c'è stato un allarme bomba relativo ai traghetti. Cosa è successo in quell'occasione?

Dottor Pecorini: Abbiamo frequentemente situazioni di allerta del genere: il caso a cui si riferiva ipotizzava la possibilità di attacchi con barchini esplosivi. Per queste occasioni siamo abbastanza pronti: ne arrivano continuamente, da parte di mitomani, alle Capitanerie di Porto, che subito informano la nave. Sfortunatamente il 99% delle volte questo avviene con la nave in navigazione e si crea un problema.

Dott.ssa Lamberti: Il caso, a cui mi riferivo, ha avuto maggior risonanza perché l'ha data l'ANSA: per fortuna anche quella volta si trattava di un mitomane.

Dottor Pecorini: Ad ogni modo, in questi casi, si attua la seguente procedura:

- alla ricezione di allarme (da parte del Comandante o di altri), viene informata la Capitaneria e la Polizia; come ho detto, naturalmente è più facile che l'allarme giunga proprio da queste autorità che, saputolo, ne danno notizia alla nave;
- iniziano i tempi di reazione necessari per predisporre tutte le misure previste dal Piano al quale abbiamo prima accennato: esse consistono in una serie di contromisure quali l'evacuazione della nave, l'allontanamento dall'ormeggio, ispezione della nave ecc.; tale contromisure sono sostanzialmente immediate in quanto effettuate a mezzo di ricetrasmittenti individuali.

Ovviamente i tempi di ritorno alla normalità sono diversi in funzione di ciò che è stato attuato. Ad esempio, in caso di evacuazione della nave i tempi non potranno essere rapidissimi. Posso però dire su questo argomento che i numerosi allarmi, pervenuti da mitomani o da altre fonti, hanno già determinato situazioni di allerta, costituendo di fatto delle vere e proprie esercitazioni: praticamente, esse hanno finito per interessare quasi tutte le unità della flotta ed una buona parte dei marittimi chiamati ad intervenire. Gli equipaggi hanno sempre risposto con professionalità e senza emotività.

È evidente che in caso di attacchi esterni la nave non ha, né può avere, suoi apparati di difesa. In questi casi la difesa va demandata alle Autorità presenti in porto. Per quanto riguarda la Tirrenia, può affermarsi che tradizionalmente la società ha sempre privilegiato, anche sul piano degli investimenti, la sicurezza della nave, dell'equipaggio, dei passeggeri e del carico. Vorrei

aggiungere a questo riguardo che, come sempre, e soprattutto nel caso che ci occupa, il fattore umano assume un'importanza prevalente e su questo certamente sono stati fatti dei grossi passi in avanti.

Certamente la cosa che più intimorisce è il fatto che chi decide è il terrorista, poiché è lui che può scegliere il momento, il luogo, l'obbiettivo e le modalità dell'attacco; ha quindi una posizione nettamente di vantaggio.

La nave, ovviamente, come tutti i mezzi pubblici di trasporto di massa, può evidentemente costituire un obbiettivo vulnerabile. Questo credo che sia il timore principale anche da parte dell'opinione pubblica in generale, anche se, al momento, non si riscontrano situazioni di flessione del traffico dovute a tale fenomeno. L'unico modo per stare più tranquilli, a mio avviso, è quello di intensificare le misure di sicurezza non solo a bordo, ma direi, soprattutto a terra, nei porti. Non va dimenticato, infatti, che la nave traghetto, per sua natura, ospita oltre che i passeggeri anche autoveicoli. Pertanto, per gli uni e per gli altri, a mio avviso, andrebbero ipotizzate misure analoghe a quelle vigenti negli scali aeroportuali, prima dell'imbarco. Affermo ciò in quanto esistono già apparati in grado di radiografare mezzi pesanti, bagagli, ecc. Per questi ultimi i piani di sicurezza, a cui abbiamo fatto riferimento, prevedono che si possa procedere ad ispezioni, controlli documentali ecc. Anche qui, tuttavia, va detto che il modo più efficace per effettuare tali controlli sui mezzi è quello attraverso apparati specifici in grado di radiografare il carico facendolo transitare in apposite «porte».

Dott.ssa Lamberti: La ringrazio. Spostiamoci adesso ad Autostrade per l'Italia, al dottor Igino Lai, responsabile della gestione operativa. È un po' diversa la situazione per le autostrade: ci si entra e ed esce quando si vuole, non ci si deve imbarcare, ci sono altre strutture e altri sistemi operativi per i controlli. Comunque, dopo i fatti recentissimi in Europa, ci sono stati dei cambiamenti che vi hanno visto coinvolti per garantire una maggiore sicurezza? Ci sono un maggior numero di pattuglie della Polstrada e maggiori controlli, in particolare ai varchi con le telecamere? Che cosa è cambiato?

Dottor Igino Lai
Amministratore Delegato Autostrade per l'Italia Spa

IL SISTEMA DI SICUREZZA DI AUTOSTRADE PER L'ITALIA

Intanto un cordiale saluto. In sostanza è cambiato molto, anche se il numero dei dispositivi non è stato sostanzialmente modificati. D'altra parte per quanto attiene alla viabilità autostradale, si tratta di un sistema in costante allenamento, perché uno dei motivi che creano problemi alla circolazione sono gli incidenti stradali, che generano spesso l'infarto della circolazione stessa. Quindi l'operatività e la reattività del sistema di gestione sono molto collaudate: solo per quanto attiene Autostrade per l'Italia, che gestiste a livello di gruppo 3400 km, pari al 63% della rete autostradale a pagamento, e quindi rappresenta l'1% della viabilità stradale italiana, serviamo il 16% del traffico avendo solo un 3% degli incidenti con conseguenze. Da noi succedono 27.000 incidenti stradali, quindi 70, 80, 100 al giorno, e il sistema di soccorso e di prevenzione, di crisis managemet, non è qualcosa che rimane a livello dei manuali operativi: anche questi indubbiamente servono perché ci consentono di analizzare molto freddamente, soprattutto dopo un evento catastrofico, tutto quello che poteva funzionare meglio o quello che addirittura non ha funzionato e quello che è da modificare; essi vengono così aggiornati di continuo, perché noi abbiamo l'opportunità di misurarci giorno per giorno su queste fattispecie: le emergenze possono venire appunto dagli incidenti, dagli eventi atmosferici, da situazioni di crisi esterne alla circolazione. Tutto questo mette in condizione i gestori delle autostrade a pagamento di avere un particolare allenamento e di consolidare quel binomio forte che esiste tra pubblico e privato. Forse non tutti sanno che da oltre quarant'anni il sistema autostradale a pagamento si avvale di una convenzione con il Ministero degli Interni, Dipartimento della Pubblica Sicurezza, in virtù del quale il Servizio di Polizia Stradale dedica in autostrada una quantità abbastanza consistente di energie in virtù del quale, per esempio, solo sulla rete di Autostrade per l'Italia sono presenti non meno di 300 pattuglie al giorno. Il che significa che ogni km dell'autostrada viene percorso almeno 12 volte al giorno da una pattuglia della Polizia composta da personale particolarmente allenato. A questo monitoraggio visivo svolto dagli agenti si aggiunge quello

tecnico, messo in campo dalla concessionaria, che è composto di tecnologia, ma anche di persone che percorrono la rete autostradale con il compito di eliminare, anzi di prevenire qualsiasi situazione di criticità.

La formidabile rete informatica, di cui sono dotate le concessionarie (siamo stati tra i primi ad inserire in ambito autostradale le fibre ottiche), possiede una capacità trasmissiva talmente elevata da consentire di avere milioni di telecamere, cioè abbiamo in ogni punto della rete telecamere che hanno immagini quasi televisive e che osservano tutto quello che avviene in itinere. Si deve pensare all'autostrada come ad una sorta di città lineare, le cui porte di ingresso sono le stazioni, anch'esse controllate non solo la personale ma anche da sistemi telematici ed informatici, tramite le quali è possibile misurare il flusso e anche calibrare gli accesi; dove ci potessero essere situazioni di emergenza è anche possibile isolare tratti di autostrada ed indirizzare il traffico attraverso diversi corridoi. Tutto questo non solo attraverso azioni operative concertate tra Polizia stradale e concessionaria, ma anche attraverso la diffusione della relativa informazione. Questa avviene attraverso le messaggerie variabili dei cartelloni, i cellulari ed un apposito sistema radio: per quest'ultimo abbiamo una convenzione con la RAI per la frequenza che consente di dare la situazione del traffico minuto per minuto.

Dott.ssa Lamberti: In sostanza è impossibile sfuggire al controllo delle Autostrade perché voi avete un monitoraggio perfetto su tutta la rete autostradale. Volevo chiederle se è possibile risalire alla tracciabilità di chi passa al casello tramite il bigliettino e quindi non riesce a sfuggire più in alcuna maniera. Perché, riguardo ad un viaggio in autostrada, non dobbiamo per forza pensare ad un auto, ma ad un camion che trasporta qualcosa di pericoloso.

Dottor Lai: Esatto. Intanto il sistema è chiuso, ossia controllato. Molti dei nostri viaggiatori preferiscono i sistemi dinamici di pagamento, per cui si affidano al Telepass, il telepedaggio. Noi sotto questo profilo siamo leader mondiali, nel senso che abbiamo circa quattro milioni di apparati in distribuzione e già attualmente più del 50% delle transazioni di pagamento avvengono attraverso questa modalità, ma ci stiamo avviando verso l'80 o il 90%. È chiaro che chi ha un dispositivo che consente un dialogo tra il veicolo e la stazione è di fatto tracciabile, ma per i problemi della privacy, che sono stati

prima trattati, tutti questi elementi non vengono utilizzati se non dove si dovessero verificare un problema: per esempio noi mettiamo a disposizione della Polizia stradale il nostro sistema dove vengono caricate delle liste, ovviamente leggibili solo a loro, attraverso le quali essi possono conoscere le targhe e attraverso le targhe risalire a veicoli sospetti sui quali possa essere esercitato un certo tipo di controllo. Oltre a questo c'è un piano di controlli che il servizio di Polizia stradale mette in atto e che è sistematico, ma ovviamente non può essere puntuale: stiamo parlando di 3.200.000 veicoli, che tutti i giorni percorrono la rete di Autostrade per l'Italia, e di oltre 4.000.000 circolanti sull'intera rete autostradale a pagamento: si tratta di una città lineare con 8.000.000 di abitanti. Quindi è impossibile prevedere ad un controllo sistematico veicolo per veicolo. Tuttavia proprio tutto il modello di controllo e la capacità di reazione sono talmente consolidati e talmente tempestivi che, dal momento in cui avviene l'evento al momento in cui si mettono in essere tutti i provvedimenti utili per gestire l'evento e fare in modo che la criticità dell'evento sia contenuta, trascorre un tempo brevissimo. Vista la diffusione dei cellulari, dopo che avviene un incidente, quando spesso si passa da una situazione di flusso libero ad una di blocco, le nostre centrali operative, che sono accanto a quelle della Polizia Stradale, sono allertate in un solo un minuto dal momento che un utente informa dell'incidente il 112, il 113, il 115 o il nostro *call center*. Questo è uno degli elementi di garanzia del nostro sistema da un lato insicuro, ma dall'altro fortemente sicuro.

Dott.ssa Lamberti: La ringrazio. Lei stava parlando di 112 o di 115 e comunque prima abbiamo messo in evidenza come siano molti i soggetti che possono preposti ad intervenire in caso di emergenza. Era proprio la cosa alla quale volevo tornare con il dott. Forlenza perché volevo chiedere quale è poi il soggetto che è veramente deputato ad intervenire, quale è il livello di coordinamento, quale è il rischio di una serie di doppi controlli: questi potrebbero anche essere i benvenuti, ma potrebbe verificarsi il fatto che, essendoci un doppio grado di controllo, uno dei due soggetti pensa che sia stato l'altro a controllare e sostanzialmente salta una fase.

Dottor Forlenza: No, questo rischio non c'è. Intanto il responsabile dei problemi della sicurezza per quanto riguarda le Ferrovia è la Polizia Ferroviaria, che per legge risponde del problema della sicurezza. Noi dob-

biamo soprattutto mettere il sistema interno in condizioni di favorire l'intervento della Polizia Ferroviaria, ma anche di tutte le altre strutture che è necessario che intervengano e che anch'esse normalmente sono del Ministero degli Interni. Ripeto, l'esperienza fatta in situazioni di emergenza, ad esempio durante il G8, i guai che ci sono stati a Genova, il fatto che ci sia stato un deflusso regolare di tutti i manifestanti da Genova, certo nell'arco di un certo numero di ore, senza avere avuto un problema è sicuramente il risultato di una grande collaborazione in cui ognuno sapeva quello che doveva fare. Noi ci dovevamo preoccupare di gestire i treni e di dare l'informazione relativa, mentre le Forze di Polizia in genere hanno aiutato nell'organizzare questo discorso. Il black out a Roma è stato reso ancora più complesso dal fatto che c'era la «notte bianca»: alla stazione Termini si erano concentrate moltissime persone perché c'era un problema di blocco delle linee ferroviarie. È chiaro che queste sono vicende che non possono essere gestite da risorse interne soltanto, ma che devono esser gestite da un equilibrio di relazioni tra tutte le Forze di Polizia. Da questo punto di vista il nostro è il sistema che per sua abitudine storica è quello più pronto a far lavorare la parte pubblica e la parte privata, considerando noi come soggetti privati, nel modo più efficiente. È ovvio che rimaniamo un sistema aperto e che dobbiamo cogliere gli elementi di rischio o di difficoltà, ma dobbiamo trasformare questa «paura» in timore e in una consapevolezza che ci aiuti a migliorare. Per esempio una delle cose alla quale stiamo pensando è come alzare il livello di attenzione «intelligente» dei nostri 100.000 uomini, che lavorano attorno alle ferrovie. Questi non sono solo oggetti del problema della sicurezza, in quanto ad essi stessi, entro certi nei limiti, trattandosi di persone che non sono state ovviamente né istituzionalizzate né specializzate per questo lavoro, possiamo chiedere una attenzione e una capacità di intervento e di informazione che aiuti le Istituzioni a garantire la sicurezza complessiva. Per esempio, riguardo a questo discorso della collaborazione, ricordo volentieri che un anno fa è stato fatto un accordo tra RFI, che gestisce la struttura, e il settore della Polizia che gestisce le telecomunicazioni per il problema dei crimini informatici che toccano il sistema informativo delle Ferrovie: una buona parte del sistema ferroviario, infatti, si muove ormai con apparati meccanici asserviti a sistemi informatici avanzati. Pensiamo alla centrale, avanzatissima, una delle migliori di Europa, che gestisce il traffico della stazione Termini; lì c'è un altro possibile punto di

attacco ed è ovvio che lì ci debba essere una grande collaborazione tra noi che vi lavoriamo giornalmente e le Istituzioni al fine garantire la sicurezza informatica di questo centro.

Dott.ssa Lamberti: Grazie ancora. Presidente mi sembra che noi si possa stare tranquilli per quello che riguarda i trasporti secondo quanto hanno detto i nostri interlocutori. Fatto sta che una sorta di timore la avvertiamo comunque tutti quanti lo stesso. A me era venuto in mente, non vorrei adesso insistere sull'aspetto delle Ferrovie, ma è evidente che ci sono depositi bagagli in tutte le stazioni, come anche nei porti. Sono stati messi sistemi di controllo ai raggi X dove far passare i bagagli? Non so se sono stati messi ovunque, ma fa impressione pensare che da lì possa esservi una falla nel sistema. Io avrei avuto piacere di sapere dai nostri interlocutori cosa a loro fa paura personalmente.

Dottor Forlenza: Diciamo che noi abbiamo il timore: la paura è un termine negativo, il timore lo vedo come un termine positivo, più portato a farci lavorare per migliorare il nostro sistema. Noi sappiamo che abbiamo di fronte dei rischi e dei pericoli che non sono facilmente governabili in sistemi aperti come il nostro. Lei ha fatto l'esempio di bagagli. È ovvio che noi in certi momenti abbiamo fatto una serie di azioni: per esempio sono stati chiusi i bagagliai automatici, per evitare il deposito di materiali pericolosi. Stiamo facendo, assieme alla Polfer, un lavoro nelle più grandi stazioni per gestire i depositi bagagli con i *metal detector*, che consentono di controllare una serie di cose. Però qui ci potrebbe anche essere un passaggio legislativo utile. Noi, a differenza di quelli che sono gli aeroporti non abbiamo la possibilità di gestire direttamente il controllo dei bagagli. Quindi il controllo dei bagagli nei depositi deve essere gestito dalle autorità di Pubblica Sicurezza. Può darsi che, proprio nell'ottica di ridistribuire meglio ulteriori compiti, questo possa essere un passaggio ulteriore e possibile. Quello che vedo purtroppo difficile, è pensare che tutti i viaggiatori passino, prima di salire sul treno, attraverso il *metal detector*. Quindi credo che non dobbiamo permetterci di vivere tranquilli, dobbiamo invece lavorare con la consapevolezza che ci sono delle cose da fare e che ogni giorno dobbiamo raggiungere un maggior livello di sicurezza anche adeguando i nostri comportamenti a quelle che sono le minacce, che purtroppo sembrano cambiare continuamente.

Dottor Pecorini: Indubbiamente non è che uno ha paura, ma le preoccupazioni sono molte, tanto è vero che stiamo mettendo sotto pressione la struttura nave e quella di terra. Non ci sono nei porti bagagli che vengono lasciati, in quanto vengono trasportati direttamente con l'auto. Io credo che sarebbe importante che nei porti si andassero ad ipotizzare misure analoghe a quelle vigenti negli scali aeroportuali e che sarebbe opportuno, ma qua dovrebbero dire la loro le autorità aeroportuali, che si mettessero in ogni porto quelle porte dove far passare le auto e principalmente i mezzi pesanti, in modo tale da sapere quello che effettivamente si trasporta. Questo è un problema che riguarda le autorità portuali, visto che si stanno facendo porti e banchine da ogni parte: si dovrebbero mettere delle «porte» per il controllo di quello che nel porto entra.

Dottor Lai: Per quanto riguarda il settore autostradale, quello di cui abbiamo bisogno è la fiducia e la serenità da parte dei conducenti, perché sono loro con i loro comportamenti che fanno la differenza: il 92% degli incidenti è provocato proprio da un comportamento di guida non adeguato. Per quanto riguarda invece gli altri elementi siamo noi gestori che, attraverso i nostri sistemi, i nostri modelli e questa forte integrazione tra pubblico e privato, dobbiamo garantire che l'infrastruttura sia percorribile in sicurezza. L'episodio del Monte Bianco, per esempio, ci insegnato molto visto che vi era coinvolto un mezzo che non trasportava delle merci pericolose: ogni giorno ci sono 34.000 veicoli che trasportano merci pericolose, che potrebbero essere definite una sorta di mine vaganti, come ha detto un giornalista, ma sono mine che non scoppiano, perché sono le uniche ad essere condotte da professionisti. Abbiamo una incidentalità minimale, sotto il profilo statistico addirittura irrilevante: abbiamo quindi bisogno di questa grande compartecipazione da parte dei viaggiatori, che devono avvicinarsi al viaggio in autostrada considerando la stessa, quando si va in vacanza, il primo elemento attraverso il quale godere della vacanza.

Presidente Ramponi: Grazie alla brillante conduttrice e grazie ai componenti di questo terzo team, che certamente sono stati all'altezza di quelli che li hanno preceduti.

Ha ragione la conduttrice quando dice che questo è un argomento che ci tocca più direttamente, perché il trasporto indubbiamente ci vede coinvolti e

questo sarà così tanto più si andrà avanti perché la nostra è una società si muove. Ma parlando serenamente, francamente, superiamo il discorso che emerse un mese fa quando il Ministro degli Interni inglese disse: «Un attentato terroristico è inevitabile». Il discorso era stato tradotto male: il Ministro aveva risposto a questa domanda: «È evitabile, avendo adottato tutte le misure di sicurezza, un attentato terroristico?». Lui disse onestamente di no, come hanno detto tutti. Non vi è onestamente la possibilità di affermare che la società è totalmente garantita, se non dicendo delle bugie: non vi è sistema di sicurezza integrato tra pubblico e privato che lo possa garantire; ma detto questo, e dipende appunto da come si pone la domanda, non è affatto vero che sia inevitabile un attentato terroristico. È vero che, come emerge da questa riunione di oggi, vi è una sensibilizzazione anche nel privato di grande livello. È vero che tutti gli interlocutori hanno una risposta che io considero tranquillizzante. È vero che tutti gli interlocutori hanno dimostrato concretamente da una parte la coscienza e dall'altra una conoscenza della delicatezza della funzione che svolgono in termini di sicurezza. Vi sono dei punti che sono fondamentali: a me fa un enorme piacere sentire Forlenza dire che i 100.000 ferrovieri devono diventare protagonisti e sensibili al discorso della sicurezza. Sono tutte cose, dico francamente, che rappresentano un sfida per il privato, perché anni fa o anche qualche anno fa, questo discorso non coinvolgeva direttamente, nei termini di una prevenzione e capacità di controllo e di contrasto ad un attacco terroristico, tutte queste strutture. Quindi io desidero dare atto loro di aver avuto da una parte il coraggio e dall'altra il piacere di venire e di mettersi a disposizione del pubblico per informarlo di quanto, a mio parere in modo confortante, vanno adottando. È anche foriero di soddisfazione il loro impegno, come è emerso in tutti e tre i gruppi, di grande spazio e prospettive per il futuro. E infine recepisco quello che tutti, direttamente o indirettamente, hanno detto circa la necessità di una buona attività di coordinamento e di scambio di idee tra il pubblico e il privato. Grazie ancora a tutti.

È arrivato il momento dell'intervento dell'ing. Guarguaglini, Presidente e Amministratore delegato della Finmeccanica. Prima di dargli la parola, mi piace fare una ulteriore considerazione: durante interventi precedenti si è parlato, tra le altre cose, della necessità di una cultura della sicurezza; abbiamo detto che tale cultura è un elemento, una condizione, essenziale per tutti coloro che fanno parte di una organizzazione, perché consente di entrare nel meri-

to. Quando, ripeto, il Presidente delle Ferrovie parlava dei 100.000 ferrovieri, che dovevano acquisire questo habitat mentale, diceva secondo me una cosa estremamente importante, tanto è vero, per esempio, che nell'ambito di una conversazione tra diverse persone c'è più possibilità di dialogo tra chi ha una cultura analoga, una sensibilità analoga, rispetto a chi, pur essendo della stessa nazione, religione o modo di essere, non è sensibilizzato al contesto dell'argomento che si tratta nella conversazione.

Mi piace dire che sia il Presidente Guarguaglini che diversi altri esponenti di vertice dell'industria della difesa rivelano una sensibilità che, secondo me, è molto importante perché si realizzi quella integrazione tra il problema della sicurezza e coloro che lavorano per la sicurezza. Do' appunto la parola al Presidente Guarguaglini.

Ing. Pier Francesco Guarguaglini
Presidente e Amministratore Delegato Finmeccanica

LA RISPOSTA DELL'INDUSTRIA AL BISOGNO DI SICUREZZA

Tra gli effetti più immediati dell'11 settembre e della diffusione del cosiddetto «iperterrorismo» a livello globale, vi è senza dubbio la sfumatura di quel confine che, negli anni della Guerra Fredda, separava il concetto di Difesa da quello di Sicurezza.

I Governi oggi sono di fronte alla necessità di rispondere a domande quali: da chi dobbiamo difenderci? Come occorre predisporre il nostro nuovo sistema di Sicurezza?

Ciò è tanto più vero per l'Italia. La fine della Guerra Fredda aveva già fatto perdere al nostro Paese alcune rendite strategiche di posizione, in buona parte dettate dalla nostra collocazione geostrategica nel cuore del Mediterraneo.

L'11 settembre, poi, ha accelerato ulteriormente l'urgenza di una rivisitazione dei nostri parametri di sicurezza; oggi, la nostra posizione geografica ci assegna un ruolo parimenti strategico, anche di fronte ad una minaccia che è cambiata. Sta a noi, quindi, prendere coscienza della fine delle nostre rendite storiche, agendo attivamente per ritagliarci un ruolo di baricentro di Sicurezza e attrezzandoci per difenderci dalle nuove minacce.

Ci troviamo al confine di alcune delle aree più instabili al mondo, a cominciare dal Medio Oriente, per finire a tutto il Mediterraneo allargato e, non ultimi, i Balcani.

La strategia politico-diplomatica intrapresa dall'Unione Europea, attraverso l'allargamento progressivo verso est e sud-est e attraverso il partenariato euro-mediterraneo, e la strategia di Barcellona si dimostrano oggi, per quanto rilevanti, insufficienti a contenere minacce, quali quelle del terrorismo, della proliferazione delle armi di distruzione di massa e della proliferazione missilistica, per le quali non esiste un'efficace azione di deterrenza e contro le quali è necessario adottare misure nuove di protezione e di salvaguardia dei nostri interessi vitali.

In questo scenario geopolitico particolarmente fluido, l'industria della Difesa si sta già muovendo per dare il proprio contributo alla Sicurezza del Paese e, più in generale, dell'Europa e del mondo Occidentale.

La tecnologia è un fattore decisivo nella lotta al terrorismo, perché consente di fronteggiare alcune delle sue caratteristiche più subdole e minacciose, ovvero la natura sfuggente, imprevedibile, distribuita e asimmetrica di un nemico che può produrre danni enormi con armi semplici e rudimentali.

Occorre allora un'ulteriore e chiara consapevolezza: le industrie ad alta tecnologia e quelle della difesa in particolare dispongono della gran parte delle tecnologie necessarie a soddisfare i requisiti di Sicurezza. Hanno gli strumenti necessari a presidiare, monitorare, controllare e difendere la totalità delle aree che potrebbero costituire l'obiettivo di un'azione terroristica.

Le tecnologie necessarie a prevenire e fronteggiare la minaccia terroristica, oltre ad essere già in gran parte disponibili presso le più avanzate aziende nazionali, come Finmeccanica, sono concepite per soddisfare al meglio i nuovi requisiti di Sicurezza. Molte di queste tecnologie sono di derivazione strettamente militare, ma ve ne sono numerose di tipo duale ed altre che derivano da applicazioni totalmente civili. L'industria è impegnata affinché tali tecnologie disponibili possano essere utilizzate attraverso un approccio integrato e sistemistico, essendo tale approccio l'unico utile a contrastare efficacemente una minaccia come quella terroristica.

Per sfruttare appieno le potenzialità delle tecnologie disponibili, è necessario che anche le diverse istituzioni coinvolte operino scelte e decisioni in maniera coordinata e «sistemica», integrando la loro azione non solo a livello nazionale, ma anche e soprattutto sul piano internazionale. Alla globalizzazione della minaccia deve corrispondere una risposta globale, a cui la tecnologia può fornire un contributo essenziale.

Rimangono, per l'Italia e per l'Europa, alcuni nodi essenziali ancora irrisolti. Direi che, sin dall'11 settembre e, per noi Europei, a maggior ragione dopo l'11 marzo e gli attentati a Madrid, tali nodi non possono non vederci tutti coinvolti: Istituzioni, Industria, opinione pubblica.

In primo luogo, la tutela della Sicurezza nazionale si presenta indiscutibilmente come una tematica dalle molteplici implicazioni e ad elevato coefficiente di complessità politica e tecnologica. I domini geografici da presidiare, schematicamente riassunti come territorio, acque e zone costiere e spazio aereo, sono molteplici e creare sistemi di Sicurezza ad hoc per ogni sito sarebbe estremamente lungo e costoso. D'altronde, la varietà dei possibili obiettivi della minaccia terroristica, pone anche per l'industria il problema di selezionare adeguatamente tecnologie e sistemi adatti alla missione. Il ventaglio delle soluzioni di Finmeccanica è molto ampio e solo una dialogo costante e approfondito tra i decisori politici ed i rappresentanti industriali può condurre ad una selezione razionale delle risposte più idonee alle esigenze del Paese: ciò, nuovamente, non perdendo mai di vista l'obiettivo strategico della interconnessione e dell'integrazione degli strumenti disponibili. Questo, quindi, il primo nodo da sciogliere.

Il secondo nodo è quello relativo ad una chiara e coerente attribuzione di compiti e responsabilità nel settore della cosiddetta Sicurezza Nazionale, o «Homeland Security».

Una delle prime risposte agli attacchi terroristici dell'11 settembre contro le Torri Gemelle ed il Pentagono è stata la creazione da parte del Presidente Bush di una nuova struttura a tutela della cosiddetta Homeland Security. Il mandato istitutivo del Department for Homeland Security (DHS), creato con decreto presidenziale nell'ottobre 2001, parla di «azioni per individuare, prevenire, fronteggiare, rispondere e favorire il recupero da attacchi terroristici all'interno del territorio degli Stati Uniti». Nella fattispecie, le attività antiterrorismo che competono al Dipartimento possono essere così raggruppate:

- identificare priorità, analisi ed informazioni su possibili minacce terroristiche;
- prevenire attacchi terroristici;
- proteggere le infrastrutture critiche sul territorio degli USA;
- mitigare le possibili conseguenze di un attacco;
- rispondere e favorire il recupero da eventuali attacchi;
- rivedere e suggerire modifiche alla legislazione per rendere più efficace la lotta al terrorismo.

Il DHS accorpa 22 Agenzie autonome o Divisioni ministeriali, impiegando 183.000 persone. Inoltre, il Dipartimento ha il compito di coordinare le attività degli enti federali e di quelli locali, nonché dei possibili soggetti privati coinvolti nella tutela della Homeland Security. L'ufficio lavora in stretto raccordo sia con il National Security Council, per identificare le priorità in termini di intelligence e di protezione delle acque, del territorio e dello spazio aereo USA, sia con il National Economic Council, per favorire una stabilizzazione subitanea dei mercati finanziari in caso di attacco terroristico.

Per quanto riguarda il mandato del Capo del Dipartimento, Tom Ridge, egli è il responsabile del coordinamento della risposta nazionale ad eventuali attacchi terroristici ed il punto di contatto del Presidente in caso di minac-

cia. Inoltre, egli dispone di una limitata autorità finanziaria, nella misura in cui può identificare i progetti di Homeland Security e richiedere un adeguato stanziamento di budget per la copertura degli stessi.

In Italia, e più in generale in Europa, manca un accentramento di compiti e strutture per la Sicurezza nazionale. Sono almeno una decina le Istituzioni e gli Enti che, in vario modo e a vario titolo, si occupano in Italia della «Homeland Security»: la Presidenza del Consiglio, il Dipartimento per la Protezione Civile, l'Autorità Nazionale per la Sicurezza, il Ministero dei Trasporti, quello degli Interni, il Dicastero della Salute, quello della Difesa, il Corpo della Guardia di Finanza che fa capo al Ministero dell'Economia e delle Finanze, per non parlare poi della folta schiera di Enti locali.

Purtroppo, occorre constatare come in questo scenario, le sovrapposizioni e le duplicazioni siano quanto mai pericolose. La frammentazione dei Centri di responsabilità può, infatti, ridurre drammaticamente l'efficacia e la tempestività delle risposte alla minaccia terroristica e al pronto intervento in caso di attacco al nostro Paese. Questa complessità normativa rende confuso il quadro istituzionale nel quale devono oggi maturare le responsabilità di contrasto e di gestione di un eventuale atto terroristico.

Un terzo nodo del quale occorre parlare fa capo alla effettiva disponibilità di risorse finanziarie. La spesa americana per la Sicurezza Nazionale nel 2003 è stata pari a 100 miliardi $, con una previsione di crescita fino a 170 miliardi entro il 2006. Nel solo 2004, il budget per Homeland Security (HS) e Homeland Defence (HD) è di 41,3 miliardi $.

Una quota consistente di questi fondi si riferisce agli investimenti in Ricerca e Sviluppo per applicazioni nell'ambito della Sicurezza.

In Europa, nel 2003, la Commissione ha istituito un Gruppo di Lavoro per avviare un programma di ricerca relativo alla Sicurezza (militare e civile) con un budget di 65 milioni € per il periodo 2004-2006.

Non occorre sottolineare l'entità del gap. Basti dire che il primo rapporto redatto dallo stesso Gruppo di Lavoro prefigura la necessità di un budget annuale pari almeno a 1,8 miliardi € per poter dignitosamente affrontare i progetti di Ricerca e Sviluppo tecnologico legati alla Sicurezza, ma la sensazione che si ha è che, alla fine, i fondi realmente disponibili saranno sensibilmente inferiori.

In più, il problema della frammentazione degli sforzi nazionali, per cui ogni Paese membro stabilisce entità e destinazione delle proprie risorse

finanziarie, è ancora lontano dall'essere risolto; per cui, accanto alla problematica delle sovrapposizioni in ambito nazionale, si pone la drammatica duplicazione tra programmi e progetti dei Governi europei.

Come già evidenziato, la carenza di risorse finanziarie è particolarmente grave nel campo della Ricerca & Sviluppo destinata alle applicazioni per la Sicurezza. Ciò implica importanti considerazioni di carattere economico: da un lato, infatti, la Ricerca può essere considerata come motore di sviluppo economico ed industriale, in un'Europa la cui economia stenta a decollare. Dall'altro, occorre evitare che all'Europa accada ciò che alcuni cosiddetti «Mercati emergenti» hanno vissuto negli scorsi anni: la fuga di capitali stranieri per sfiducia da parte degli investitori sulle condizioni di sicurezza nell'area.

Insomma, tornando alla minaccia terroristica e all'inadeguatezza delle risorse finanziarie, c'è il rischio concreto di creare un gap tra l'impellenza della minaccia ed i tempi necessari a sviluppare nuovi strumenti di Sicurezza e Difesa.

Questi i principali nodi ancora irrisolti e alla cui soluzione l'industria intende fornire il proprio contributo. Per poter fare ciò, l'industria ha bisogno di alcuni chiari punti di riferimento. *In primis*, come già detto, un insieme definito ed omogeneo di soggetti con cui interagire e dialogare, per poter individuare priorità tecnologiche e di prodotto tagliate a misura sulle esigenze di Sicurezza del nostro Paese.

Un'efficace azione di prevenzione e gestione della minaccia terroristica e della nostra Sicurezza Nazionale non può non passare da una razionalizzazione del quadro istituzionale, tenendo nel giusto conto l'esperienza maturata dai diversi Organismi e Amministrazioni.

Va riconosciuto al Governo di aver già approvato alcuni provvedimenti in tal senso. In particolare, alla Protezione Civile è stata attribuita la responsabilità di gestire ogni situazione di emergenza che dovesse verificarsi a seguito di atti terroristici.

Presso la Presidenza del Consiglio dei Ministri è stato istituito il Comitato per la Sicurezza dei Trasporti, dal quale dipendono tre ulteriori Comitati per la Sicurezza dei settori terrestre, marittimo e aereo. Oltre ai piani generali per la Sicurezza che sono già stati predisposti da ciascun Comitato, sono in fase di implementazione piani specifici e dettagliati per la Sicurezza dei singoli siti interessati. In quest'ottica, si è affrontato anche il problema dell'attribu-

zione di responsabilità nel settore marittimo e della messa in sicurezza dei porti italiani, riconoscendo un ruolo di gestione alle Capitanerie di Porto.

È previsto che queste iniziative coinvolgano altri servizi, di particolare rilevanza per la nostra Sicurezza Nazionale.

In conclusione, l'esigenza di dare risposte pronte alla minaccia del terrorismo non può non tradursi nella disponibilità di maggiori risorse finanziarie e nel completamento di quel processo di organizzazione dei ruoli già intrapreso dal Governo italiano. Tutto ciò faciliterà le capacità tecnologiche dell'industria per raggiungere gli obiettivi di Sicurezza nazionale.

In primo luogo, la tecnologia rappresenta uno straordinario «moltiplicatore di forze» contro la minaccia terroristica; essa è, infatti, in grado di coprire tutto lo spettro delle risposte alle possibili minacce e, attraverso gli strumenti di integrazione di sistemi in architetture complesse, può consentire di diminuire notevolmente la soglia di vulnerabilità del nostro Paese.

In secondo luogo, la tecnologia può rappresentare un fattore di convergenza e di aggregazione tra i differenti utilizzatori, contribuendo a superare la frammentazione del panorama istituzionale che abbiamo prima descritto.

Infine, la multifunzionalità e la dualità delle tecnologie necessarie alla lotta al terrorismo fa sì che le industrie aerospaziali e per la difesa dispongano già oggi di capacità e soluzioni allo stato dell'arte. Ciò significa che, pur in assenza di un maggiore impegno finanziario, l'integrazione delle tecnologie esistenti rappresenterebbe un passo in avanti significativo ed efficace.

L'industria italiana è pronta a supportare questo sforzo, consapevole di rivestire un ruolo essenziale per la prosperità e la Sicurezza del Paese.

On. Ramponi: Ringrazio il Presidente Guarguaglini, puntuale come al solito. Emergono alcuni concetti fondamentali: non c'è dubbio che spostandosi dalla Difesa alla Sicurezza il ritardo dell'Europa non fa che confermare una situazione di realtà che c'è e che si ripercuote poi sfavorevolmente nella determinazione e nella concentrazione delle risorse, sia nel campo della ricerca che della produzione. Debbo però dire francamente che le iniziative nazionali riguardanti la Sicurezza in alcuni Paesi già sensibilizzati da esperienze negative precedenti, quali quella che abbiamo fatto noi, per esempio, con le Brigate Rosse, hanno consentito di raggiungere livelli di eccellenza non indifferenti in certe aree di produzione di sistemi di sicurezza. Voi avete, infatti, sentito questa mattina che i responsabili dei diversi settori, Energia,

Trasporti e Telecomunicazioni, non hanno denunciato una mancanza di sistemi: quando le Ferrovie parlano dell'inserimento nelle loro infrastrutture di un controllo automatico della sicurezza non soltanto di carattere meccanico, ma anche di carattere antiterroristico, quando si è parlato della sicurezza degli aerei e delle navi, non c'è dubbio che già oggi l'industria può costituire un validissimo ausilio al contrasto nei confronti di questa minaccia che si sta delineando sempre più pericolosa.

Ultime due considerazioni. Il Presidente Guarguaglini riecheggia, non dico una specie di lamentela, ma di auspicio da parte dei protagonisti: manca ancora un quadro di riferimento generale che assegni in maniera univoca la responsabilità e la capacità di gestione, anche dal punto di vista finanziario delle attività finalizzate a prevenire e fronteggiare la minaccia terroristica. Ora non c'è dubbio che la minaccia terroristica è globale, non c'è dubbio che i settori investiti sono quelli che incidono sul funzionamento e sulla qualità della vita società; però è altrettanto fuori di dubbio che l'elemento di coordinazione principe e generale è la Presidenza del Consiglio, che può anche delegare, per esempio, il discorso della difesa vera e propria al Ministero degli Interni oppure a gruppi che siano il luogo dei punti di convergenza di certe attività particolarmente calettate sul discorso della difesa, della sicurezza, della prevenzione. Quindi non c'è dubbio che deve essere la Presidenza del Consiglio ad assumere quella che si chiama la direzione della manovra: abbiamo sentito oggi citare la struttura che è guidata dal Gen. Tricarico e che rappresenta la prima soluzione; secondo, non c'è dubbio che il Ministero degli Interni ha una competenza generale sulla difesa, così come non c'è dubbio che tante altre componenti debbano contribuire perché questo accada. Tuttavia dal convegno emerge che la sensazione di una soluzione del problema in proposito, anche per la finale che ha caratterizzato l'intervento del Commissario della Protezione Civile ancora non c'è. Quindi in realtà emerge che uno sforzo in ambito nazionale deve essere fatto per identificare esattamente chi è il *deus ex* machina di tutta la situazione.

Il secondo punto, sul quale pone l'accento il Presidente Guarguaglini, è la necessità di un ente dotato di tali capacità che, dice, sarebbe fondamentale come interlocutore per l'industria per l'identificazione e lo sviluppo delle soluzioni tecnologiche necessarie per il supporto in sede internazionale dei prodotti delle industrie italiane. Non c'è dubbio che anche in chiave di sistema Italia, parole che oggi abbiamo sentito tante volte, e anche per un intelli-

gente interpretazione della globalizzazione e della tanta auspicata unità politica europea, non c'è dubbio che poi ogni Stato deve recitare una parte di responsabile protagonista e di responsabile guida delle componenti della Nazione, perché possano presentarsi da una parte tutelate e dall'altra preparate al dialogo europeo. Grazie ancora al Presidente Guarguaglini.

Adesso come al solito la parola è ai politici: vi sono personalità sia della maggioranza che dell'opposizione, in una visione assolutamente bipartizan, perché non vi possono essere differenze di visione partitica nei confronti di problemi di questa delicatezza e sensibilità. Sono così presenti il Ministro delle Comunicazioni, On. Maurizio Gasparri, il Ministro per l'Innovazione e le Tecnologie, dott. Lucio Stanca, l'On. Enrico Letta, della Commissione Attività Produttive, Commercio e Turismo della Camera dei Deputati, il Sen. Erroi, che rappresenta il Ministro delle Infrastrutture e Trasporti. Prego l'onorevole Gasparri di iniziare.

TAVOLA ROTONDA

INTERVENTI

On. Maurizio Gasparri

Dott. Lucio Stanca

On. Enrico Letta

Sen. Bruno Erroi

Intervento dell'On. Maurizio Gasparri
Ministro delle Comunicazioni

Saluto i presenti e ringrazio della possibilità di dare il mio modesto contributo al dibattito.

La connotazione globale, che la minaccia terroristica è andata assumendo, la sua capacità di portare a segno atti di violenza inaudita, con modalità operative a dir poco inquietanti, hanno minato alla base tutti gli ordinari presupposti per la sicurezza, sia di quella percepita dalla popolazione, la quale avverte il pericolo molto prossimo a sé, sia di quella garantita dalle istituzioni preposte.

II processo di revisione, che inevitabilmente già dai fatti dell'11 settembre si è innescato, è stato accompagnato da eventi che non hanno fatto altro che confermare il salto qualitativo della nuova minaccia terroristica, e quindi la necessità di giungere, in tempi brevi, alla formulazione di una risposta efficace, per scongiurare il soccombere del Paese di fronte ad essa.

L'elaborazione di una nuova strategia per la sicurezza ha dovuto constatare la necessità di fornire una risposta globale sia sul fronte della prevenzione e del contrasto di possibili attacchi che su quello della gestione di emergenze derivanti dagli stessi. Tale risposta non può tralasciare alcun aspetto, in quanto rischierebbe solo di fornire facili punti di attacco al sistema: nel portare a termine tale impegno è indispensabile il contributo di tutte le entità del sistema Paese, partendo da quello, scontato, delle forze di pubblica sicurezza e comprendendo tutte le entità pubbliche e private fino a coinvolgere la popolazione stessa.

Dei vari aspetti che una simile complessa materia investe, credo che quello relativo alla problematica delle comunicazioni sia di non poca rilevanza, stante il panorama delle tecnologie che oggi ci viene prospettato e constatato quanto ancora, di questa offerta, il sistema Paese possa e, a questo punto, debba beneficiare, e in difetto delle quali rischieremmo di fornire solo una risposta parziale e quindi di non risolvere il problema.

In tale ottica mi piace considerare le comunicazioni come indispensabile elemento di coesione a quella che giustamente viene prospettata come la cooperazione tra tutte le entità del sistema Paese, e su questo aspetto credo che si possa efficacemente progredire nell'immediato.

La digitalizzazione delle reti è un indispensabile passo verso la fruizione

di servizi oggi indispensabili per il contrasto della criminalità e la loro sicurezza e inattaccabilità, sia da eventi catastrofici sia da terzi, è un altrettanto indispensabile corollario.

La loro globalizzazione, in termini di diffusione capillare e gestione a vari livelli delle stesse, è poi un altro obiettivo da perseguire se vogliamo garantire di non lasciar nessuna porta aperta al terrorismo.

Se con questi obiettivi analizziamo il panorama evolutivo del nostro Paese, scopriamo quanta strada abbiamo ancora davanti prima ancora di poter parlare di sicurezza rinnovata ed adeguata al nuovo contesto.

Dal punto di vista delle entità prime preposte alla tutela della sicurezza, uno sguardo verso le tecnologie oggi a disposizione delle forze dell'ordine registra un buon progresso rispetto al passato almeno sotto l'aspetto delle strutture informatiche di supporto delle investigazioni. In tale ambito la digitalizzazione dell'infrastruttura radiomobile costituirebbe un ideale completamento a tanta raggiunta efficienza, consentendo di estendere capillarmente le capacità di contrasto del crimine anche da parte della singola unità sul territorio, laddove oggi un agente deve avvalersi di reti commerciali, con la loro evidente precarietà in caso di emergenza, per usufruire di servizi a valore aggiunto quali interrogazioni di banche dati, trasmissione di impronte oppure di immagini dalla scena di un crimine o quant'altro.

II panorama tecnologico mette oggi a disposizione l'efficace tecnologia TETRA, di cui auspicabilmente in tempi brevi saranno dotato le nostre polizie, e che contribuirà a sanare questa mancanza.

Se poi estendiamo la visione a tutte le altre entità che efficacemente possono contribuire al progetto di nuova sicurezza, scopriamo una pluralità di situazioni, alcune delle quali necessitano a mio avviso un deciso aggiornamento. Se partiamo dal ruolo attivo che il cittadino può assumere a garanzia della sua stessa sicurezza, scopriamo che la capillarità di diffusione delle reti di telecomunicazione commerciali fornisce un tanto efficace quanto globale mezzo di interazione col sistema sicurezza: in tale ottica la digitalizzazione delle reti radiomobili delle forze dell'ordine va senz'altro nella direzione di un incremento dell'efficacia di questa interazione.

Se buttiamo lo sguardo sulla capacità di reazione del Paese di fronte ad atti terroristici, scopriamo invece una situazione abbastanza frastagliata a livello tecnologico, tale da ridurre l'efficacia di risposta del sistema a livelli insoddisfacenti alle nuove esigenze.

La necessità di un più efficiente coordinamento tra tutte le forze preposte alla gestione di un'emergenza, inteso come capacità sia di prevenire che di far fronte, in maniera efficace e a tutti i livelli, ad un qualsiasi evento a danno della popolazione, deve portare all'integrazione delle capacità d'azione tra più organizzazioni, obiettivo che necessita almeno dell'efficienza e dell'interoperabilità tra le reti di comunicazione: é in questo campo si registrano, a mio avviso, le maggiori mancanze. Ci troviamo di fronte a situazioni ereditate dal passato che, senza sminuire l'utilità che le stesse hanno avuto sino ad oggi, vanno necessariamente adeguate alle necessità presenti a dare, per esempio, un unico sistema integrato di comunicazione che consenta all'occorrenza la gestione da parte delle entità preposte di tutte le organizzazioni in campo. Tali limiti sono talvolta generati da impedimenti normativi generati da provvedimenti obsoleti o da ostacoli burocratici.

La mia Amministrazione sta, tra non poche difficoltà, cercando di rimuovere ogni ostacolo sulla via dell'armonizzazione e della razionale utilizzazione delle comunicazioni a garanzia della sicurezza del paese. Ho provveduto a verificare che ancora oggi esistono reti, ad esempio per l'emergenza sanitaria, incomplete o del tutto inesistenti, basate su tecnologia analogica con limitate possibilità di interoperare, quando invece nella gestione di eventi estremi, come quelli a cui purtroppo stiamo assistendo, deve esistere la massima sincronia ed efficienza tra le organizzazioni preposte, obiettivo questo irraggiungibile in mancanza di uniformità ed interfacciabilità dei mezzi informatici e di comunicazione.

In tal senso vanno lette le innumerevoli pressioni che sono in corso da parte dei miei uffici per la digitalizzazione delle reti, per l'avvio di sperimentazioni, in vista anche della digitalizzazione delle reti di Polizia, dei servizi a valore aggiunto resi disponibili dalle nuove tecnologie. Nella stessa direzione vanno gli sforzi tesi a modificare le normative in modo da favorire una quanto più rapida possibile migrazione verso il digitale.

II campo dell'emergenza sanitaria è emblematico da questo punto di vista: oggi abbiamo zone del Paese dove ancora non esiste una rete di comunicazione per il servizio di emergenza medica e, laddove esiste, essa fornisce servizi basilari, ma limitati rispetto alle potenzialità oggi disponibili, con inoltre territorialità limitate; questo in base a quanto stabilito dall'attuale normativa che tuttavia non tiene conto delle mutate esigenze, di eventi catastrofici che possano richiedere ingenti risorse da coordinare su una vasta area.

Sono convinto che, per dare la risposta globale che cerchiamo, dobbiamo aggiornare i requisiti per questa classe di servizi, ammettendo l'adozione delle nuove tecnologie digitali, oggi di fatto escluse, attraverso una revisione delle attuali regole: attività che sinceramente auspico condivisa da tutte le amministrazioni coinvolte. L'avvio delle sperimentazioni dei nuovi sistemi consentirebbe l'adozione di nuove e più efficienti modalità operative: auspico che ciò avvenga nel più breve tempo possibile.

Nello stesso spirito, ho dato mandato al Segretario Generale di predisporre un tavolo tecnico di studio per un'infrastruttura di rete a supporto delle emergenze, attiva a livello nazionale, attraverso cui coordinare le attività necessarie, dalle comunicazioni con le forze in campo alla gestione dei sistemi informativi verso la popolazione e verso i media affinché veicolino messaggi adeguati, con l'obiettivo di esplorare le possibilità di giungere ad un unico sistema integrato per la sicurezza, in grado di non trascurare alcun aspetto e di garantire a tutte le entità del sistema Paese di operare in maniera efficiente.

Abbiamo oggi, purtroppo, un forte movente che ci spinge a progredire; questo credo avrà il vantaggio di avvicinare le persone e di aumentarne la coesione, come si confà a situazioni estreme tipo quelle che oggi viviamo. Auspico un veloce progresso su questa strada, verso il conseguimento di un'unità nazionale e un senso della Patria che è forse il primo presupposto morale a sostegno della nuova sicurezza.

On. Ramponi: Ringrazio il Ministro Gasparri e prego il Ministro Stanca di prendere la parola.

Intervento del Dottor Lucio Stanca
Ministro per l'Innovazione e le Tecnologie

Ringrazio per l'invito a questo dibattito che tocca un tema molto importante alla luce degli avvenimenti che stiamo vivendo, ma soprattutto alla luce della gravissima minaccia del terrorismo.

Per una società che si avvale sempre di più delle tecnologie digitali e quindi del computer, della rete, domani anche della televisione digitale, dei telefonini, per una cosiddetta «società dell'informazione», la sicurezza è un fatto fondamentale in quanto dipende sempre più dalla disponibilità e dalla continuità delle operazioni di queste tecnologie.

Oggi c'è una vera e propria accelerazione nella definizione dei requisiti di sicurezza a causa della minaccia terroristica. Quindi questa esigenza di fondo, che rimane e che era stata già avvertita, oggi è più forte perché ci confrontiamo con una minaccia come il terrorismo. A dicembre scorso, nel primo summit mondiale sulla «società dell'informazione», organizzato dall'ONU, è stata tratteggiata una magna charta dei principi di questa società, che si avvale sempre più delle tecnologie digitali: in tale ambito la sicurezza è stata richiamata come uno degli aspetti fondamentali per realizzare una società del genere. Non mi addentro ora perché il problema è estremamente complesso, non solo tecnologico, ma anche normativo, organizzativo, di competenze e di metodologie. C'è uno sforzo complessivo che un'impresa o un ente o un sistema Paese deve fare, attivando tutte queste leve, per proteggere queste infrastrutture, e non solo queste infrastrutture fisiche, ma anche il valore più alto, che ancora è dato dalle informazioni che queste infrastrutture assicurano e dai servizi che vengono forniti.

Se questo è lo scenario in cui operiamo, nel mio intervento voglio richiamare alcuni punti essenziali sui quali dobbiamo lavorare come comunità nazionale, ma anche come comunità internazionale. Primo punto: per aumentare la sicurezza bisogna essere sicuri dell'identità personale. Questa sarà assicurata dall'elettronica: non ci sarà più solo la fotografia, il nome e il cognome, l'indirizzo, ma saranno memorizzati su supporti adeguati anche dati biometrici di vario tipo, a seconda delle scelte che saranno fatte. È in corso un dibattito internazionale per la standardizzazione di tali scelte. Il nostro Paese stava già lavorando per l'introduzione della carta di identità elettronica, ma

indubbiamente c'è stata una accelerazione in tale senso. Questo anche a seguito della decisione degli Stati Uniti di introdurre il passaporto elettronico a partire dal 26 ottobre di quest'anno: di conseguenza è stato stabilito che tutti i cittadini dei Paesi che non avranno introdotto anch'essi il passaporto elettronico dovranno richiedere il visto. È stato introdotto di fatto uno standard internazionale. E così anche la Commissione Europea ha avanzato il 18 febbraio scorso una proposta per introdurre il passaporto elettronico europeo. Assumendo come dato di fatto che d'ora in poi l'identità di un persona sarà assicurata da un documento elettronico, in una recente convenzione di Budapest i Paesi partecipanti si sono impegnati ad adeguare il codice penale per introdurre un nuovo reato: il furto dell'identità telematica. Ci sono quindi problemi giuridici e non solo tecnologici connessi all'introduzione di questa identità elettronica. Di più, a livello dei Paesi aderenti al Patto di Shengen, abbiamo ideato un progetto per dare un visto elettronico a chi entra dal di fuori dell'Unione europea e si muove poi liberamente nell'area Shengen, dopo aver, appunto, acquisito il visto da parte di uno dei Paesi aderenti. Abbiamo creato così una «tracciabilità» delle persone con questo archivio, a disposizione di tutti i Paesi Europei, che dà visibilità e controllo dei movimenti di persone, che non sono cittadini europei, ma che sono entrati nell'area Shengen.

Per quanto riguarda il nostro Paese voglio ricordare due iniziative importanti. La prima riguarda l'immigrazione: è in corso di realizzazione la carta di soggiorno elettronica per gli immigrati con l'introduzione di dati biometrici, che condivide, quindi, lo standard della carta d'identità elettronica e della carta nazionale dei servizi. Si tratta cioè di strumenti utili per dare una identità più sicura, una identità in rete: l'aspetto più interessante di tutto questo non è solo tecnologico e normativo, ma la velocità con cui l'identità può essere trasferita in altre zone geografiche, aumentando notevolmente i livelli di sicurezza. Dobbiamo cominciare a pensare in questi termini, perché, anche se siamo ancora in fase di attuazione, di fatto siamo già in un contesto del genere.

Dopo aver esaurito l'argomento riguardante l'identità elettronica, desidero trattarne un secondo anch'esso di grande importanza: esso riguarda l'impegno a cui dobbiamo dedicarci per la protezione delle infrastrutture critiche informatizzate. Questa è una iniziativa che parte a livello internazionale e che ha visto anche il coinvolgimento dell'ONU, pur se è partita in verità dal G8. La considerazione di fondo è che oggi tutte le grandi infrastrutture, dai trasporti

navali ed aerei, dalle ferrovie, all'energia, al gas, all'acqua, ai circuiti bancari, finanziari e sanitari, alla grande distribuzione, alla Pubblica Amministrazione, cioè tutte le grandi infrastrutture materiali, oggi dipendono sostanzialmente da queste infrastrutture immateriali. Si è così sentita l'esigenza, a livello di vari Paesi e anche del nostro, di creare un coordinamento per rispondere a situazioni di emergenza, perché la caduta di una infrastruttura può implicare conseguenze su altre tipologie di infrastrutture: bisogna quindi avere una capacità di prevenzione, di pianificazione, di standardizzazione, di sviluppo delle competenze, di cooperazione, un momento quindi di coordinamento per essere finalmente pronti al momento dell'emergenza a rispondere alla stessa. È quindi una organizzazione che va creata per arrivare ad essere pronti: non si può improvvisare la risposta all'emergenza, se la stessa non è stata pianificata. È un problema molto complesso che riguarda l'intero sistema Paese e che va quindi affrontato con il coinvolgimento di tutte le parti interessate. Noi abbiamo creato presso la Presidenza del Consiglio dei Ministri un gruppo di lavoro per la protezione delle infrastrutture critiche informatizzate: esso ha prodotto anche un ottimo documento, che per ovvie ragioni non ha una libera circolazione; certamente abbiamo fatto tesoro delle esperienze che altri Paesi hanno già acquisito nel realizzare queste strutture di coordinamento. Recentemente ho sollecitato la Presidenza del Consiglio dei Ministri a varare dei provvedimenti per istituire questo organismo di coordinamento, in grado di dare una risposta di sistema ad attacchi terroristici, ma anche alle emergenze dovute alle calamità naturali, a cui nel passato il nostro Paese non ha risposto adeguatamente e non ha saputo coordinare gli interventi alle reti vitali per il funzionamento del sistema Paese. È un intervento assolutamente necessario: non siamo in grave ritardo, ma alcuni Paesi hanno già realizzato queste strutture e noi dobbiamo partecipare a questo network nel cui ambito scambiamo anche esperienze ed informazioni.

La terza area che voglio richiamare nel mio intervento è quella della Pubblica Amministrazione. Devo dire con molta franchezza che non abbiamo un livello adeguato di sicurezza per la protezione delle informazioni vitali per il funzionamento del Paese: sto parlando delle grandi banche dati della Pubblica Amministrazione, che sono essenziali per il funzionamento del nostro Paese, ma anche delle infrastrutture fisiche e di quelle digitali. Lo devo dire, perché all'inizio del 2002 ho emanato una direttiva, con la quale ho chiesto alle Pubbliche Amministrazioni di fare un controllo e di darmi il livello di

sicurezza realizzato nelle loro infrastrutture informatiche, delle tecnologie, delle comunicazioni e dell'informatica. La risposta sicuramente non è stata sufficiente per fare una fotografia adeguata. Anche qui c'è da fare un grossissimo lavoro, in collaborazione con il Ministro Gasparri e il suo Ministero e con quanto si sta facendo a livello europeo. Abbiamo creato un gruppo di lavoro che proprio ieri ha presentato i suoi risultati e che creerà all'interno della Pubblica Amministrazione italiana quello che, a livello internazionale, viene chiamato CERT (*Computer Emergency Responce Team*), un centro di competenza collegato con le altre Pubbliche Amministrazioni europee, coordinato dall'Agenzia europea, per migliorare ed essere centro di propulsione per operare su tutti i campi attinenti alla sicurezza: come ho detto non è un fatto esclusivamente tecnologico, ma è un fatto fondamentalmente organizzativo, di metodologie, di competenze. Questa è un'altra iniziativa che deve andare in porto il più in fretta possibile con la costruzione di questo centro di competenza a livello di Pubblica Amministrazione. Altra area che voglio richiamare, d'interesse per questo dibattito, riguarda il settore privato: anche se capovolgiamo i ruoli, essi rimangano estremamente importanti e complementari. Per quel poco che posso capire di questo settore, nel quale peraltro lavoro da 35 anni, ho la sensazione che da un po' di tempo a questa parte la necessità di sicurezza è aumentata enormemente in priorità di area di investimento da parte delle imprese private. Le imprese tecnologiche, comprendendo anche l'opportunità che si sta creando, stanno muovendo investimenti nella ricerca e nello sviluppo proprio sul tema della sicurezza. Sta a noi, domanda pubblica, sostenere questi sforzi per indirizzarli sui campi, sui prodotti e sulle tecnologie che noi riteniamo più importanti ed essenziali. Dobbiamo comprendere che già nei prossimi anni la tecnologia avrà una accelerazione fortissima su tutto il campo della sicurezza ed è bene che la domanda pubblica non subisca questa accelerazione, ma in qualche modo la determini proprio con la sua forza, come dire, contrattuale e d'interesse per la stessa impresa privata. Probabilmente occorrono anche strumentazioni nuove che, devo dire, la nostra Pubblica Amministrazione non ha ancora del tutto, non nell'acquisire con una gara il prodotto esistente, perché allora si fanno i bandi e si sceglie la soluzione migliore: qui si tratta di ordinare il futuro, di acquisire il futuro e quindi ci vogliono strumenti contrattuali e normative che siano adeguati a questo sforzo che dobbiamo fare per la cooperazione tra privato e pubblico. Faccio solo un esempio: come ha già accennato il Ministro Gasparri, stiamo realizzando,

in termini di progetto oggi e tra qualche mese spero in termini operativi, in tre province italiane un unico numero di emergenza: anziché avere, come capita a tutti noi a casa, la lista, che aumenta sempre di più di tutti i possibili numeri da chiamare in caso di emergenza, e così quando capita l'emergenza trovare il numero giusto diventa un problema, avremo un unico numero di accesso al soccorso; poi l'organizzazione, con le tecnologie, provvederà all'instradamento della richiesta a seconda che l'emergenza sia di un certo tipo o di un altro. È un indicazione che ci viene da alcuni Paesi europei che l'hanno già realizzata: rende più semplice la vita dei cittadini e grazie a questa interoperabilità tecnica possiamo realizzare anche una interoperabilità applicativa. Ripeto che stiamo alla vigilia di test sul campo.

Ultima mia riflessione in questo dibattito schematico è il problema di base: questa nuova società dell'informazione ci sta dando sicuramente delle opportunità, ma sta creando anche dei problemi nuovi. A mio modo di vedere, tra questi problemi quello più difficile da sciogliere è la difesa dell'identità individuale: da una parte in questa società più aperta, più democratica, nella quale ci sono i diritti nuovi di accesso alla rete, di trasparenza, di partecipazione, questa difesa dell'identità individuale è garantita dalla privacy, che è un diritto civile fondamentale in una società che si avvale di queste tecnologie; dall'altra parte vi è l'esigenza della sicurezza, che molto spesso entra in conflitto con i diritti della protezione individuale. Queste tecnologie digitali hanno una lunga memoria, registrano tutto, rimane traccia di tutto, allora qui il problema non va affrontato in termini ideologici o rigidi: bisogna essere pragmatici per trovare quotidianamente o nelle fasi storiche in cui noi viviamo il giusto equilibrio tra privacy, protezione della sfera individuale, e esigenza di sicurezza. Certo se mi si chiede oggi una scelta, che poi dovremmo fare come collettività, di dare a priori delle informazioni che riguardano la mia identità per volare su un aereo che mi porta negli Stati Uniti, e se questo mi garantisce o riduce al massimo il rischio che sul mio stesso aereo non ci sia un terrorista, io personalmente sono disposto a dare quest'informazione perché mi garantisce un maggiore livello di sicurezza; o se volete, più banalmente, io sono più disponibile ad entrare in una banca che ha delle telecamere e che registra il mio ingresso se questo mi dà, come mi dà, maggiore fiducia che nel momento in cui sono in banca non venga un terrorista o un bandito a fare una rapina in cui possa essere coinvolto. Quindi la cosa per certi aspetti mi invoglia, c'è un baratto tra la mia protezione individuale e il fatto che queste informazioni

vengano utilizzate. A mio modo di vedere il problema non è qui; non è sul fatto che si debbano o no registrare queste informazioni: questa è una battaglia di retroguardia e comunque l'esigenza della sicurezza ce lo impone. La vera battaglia è nell'utilizzo della memoria, ossia su chi ha il diritto a poter accedere, in quali circostanze queste informazioni possano essere prese, su chi controlla questo accesso. Visto che un'attività elettronica lascia sempre delle tracce, come la carta di credito che lascia tracce dei nostri acquisiti, il problema vero, di fronte alla minaccia di attacchi terroristici, riguarda solo chi deve intervenire e conoscere questi dati. Lungi da me di dire che la società dell'informazione deve essere la società del «grande fratello»: dobbiamo, tuttavia, essere consapevoli che questa è una scelta difficile, ma che va fatta dato anche il momento in cui ci troviamo, con la presenza della minaccia terroristica. Credo che una maggiore sicurezza, rispetto a una privacy che comunque va difesa nei limiti del possibile, è una scelta necessaria, nel quadro però di una certezza giuridica che deve essere data a noi cittadini. Grazie.

On. Ramponi: Molte grazie al Ministro Stanca; come avete visto man mano che intervengono gli interlocutori noi abbiamo la conferma delle idee base che hanno promosso questo convegno. Nel suo discorso, il Ministro della Innovazione tecnologica non può non fare riferimento a quei protagonisti che abbiamo ascoltato prima, a quei responsabili del sistema dei trasporti, delle ferrovie, della distribuzione dell'energia, a quanto detto poco prima dal Ministro Gasparri. Cioè vi è una integrazione che è nelle parole, ma che deve essere anche nei fatti, perché se il sistema Paese non realizza una sinergia anche nei confronti di questa minaccia, il discorso naturalmente non ha alcun valore nel momento in cui è fatto settore per settore. È chiaro però che a queste responsabilità parziali, oltre alla necessità dell'integrazione sul piano orizzontale, è necessario anche un coordinamento e una guida sul piano verticale, che non può non venire dalla Presidenza del Consiglio e da chi è il protagonista della Sicurezza a livello nazionale. Grazie ancora al Ministro Stanca. Chiedo adesso all'On. Letta che è sempre assiduo e risponde gentilmente alle mie iniziative. Voglio ricordare che l'On. Letta rispose affermativamente ai miei appelli quando era Ministro alle Attività produttive nel precedente Governo e continua a farlo come rappresentante dell'opposizione, caratterizzando sempre con grande stile la bipolarità, il bipartisan, di questi interventi; lo farà ancora una volta. Prego On. Letta.

Intervento dell'On. Enrico Letta
Comm. Attività Produttive, Commercio e Turismo della Camera dei Deputati

Grazie a Luigi Ramponi. Io ritengo molto utile la conversazione di oggi: da parte mia c'è stata soprattutto la curiosità di trarre elementi che siano utili a dare un contributo, anche se un contributo molto limitato, perché è talmente delicata e talmente nuova la sfida che abbiamo di fronte che credo si debba da parte di tutti approcciarla con grande umiltà e con assenza di certezze predefinite. Credo che questo sia l'atteggiamento che sarebbe importante avere da parte di tutti noi che ci muoviamo rispetto a questo tema, ma soprattutto da parte di chi ha responsabilità istituzionali. Ci muoviamo in un tema, un settore, in cui le novità dell'innovazione tecnologica, le novità del sistema rete, della interscambiabilità, delle relazioni, dei movimenti e di ciò che cambia è talmente importante, impressionante, che incide in maniera molto rilevante sulle vicende che hanno a che fare soprattutto con le regole, le leggi, le istituzioni e quindi il modo di fare.

Io mi sono segnato cinque punti. Il primo, quello di partenza, riguarda il nuovo concetto di vulnerabilità che abbiamo appreso in questi anni, se non in questi mesi, ben diverso da quello del passato: vulnerabilità intesa non più in senso tradizionale, dovuta ad atti di guerra veri e propri, quindi il tutto, o vulnerabilità legata ad atti di terrorismo contro singoli: quindi una vulnerabilità che va dal singolo al tutto. Oggi abbiamo di fronte, invece, una variegata, nuova, serie di possibili attacchi alla nostra convivenza, al nostro modo di essere, al nostro modo di vivere, che non sono più riconducibili a questa classica ripartizione, ma che sono talmente variegati che finiscono per mettere in difficoltà anche chi si mette a ragionare di queste cose analiticamente per trovare delle catalogazioni. Da questo punto di vista, la vulnerabilità trova delle difficili catalogazioni e soprattutto delle difficili capacità di dare risposte semplicemente teoriche; vulnerabilità che è a tutto campo, totale e imprevedibile.

Credo che le vicende a cui abbiamo assistito solo alcuni anni primi sarebbero state impensabili nella cinematografia, e invece sono accadute. Credo che questo elemento sia quello nuovo di questi anni: impone, quindi, un salto di qualità nella replica, nella reazione, che ovviamente non può essere più

soltanto legata ad atteggiamenti o approcci classici, ma deve dare prova di fantasia e di capacità per andare su elementi di probabilità. Rispetto al passato, ipotesi che sembravano assolutamente improbabili si sono realizzate e anche la capacità di andare a prevedere l'imprevedibile obbliga a un maggiore dispendio di energie e di risorse.

Rispetto a questo fatto, tratterò un punto particolare, scegliendo uno dei temi che nel convegno sono stati affrontati e che a mio avviso è, in prospettiva, uno dei più importanti: la vulnerabilità nel campo degli approvvigionamenti energetici e nel campo della sicurezza delle relative fonti. Credo che su questo tema sia necessaria una particolare attenzione, soprattutto da parte di un Paese come il nostro, che è particolarmente vulnerabile. Lo abbiamo già visto, perché non c'è bisogno della grande nefandezza dei terroristi per farci piombare nel più grande *black out* che la storia italiana ricordi. È stato semplicemente un albero terrorista svizzero che ha tirato giù l'intera rete nazionale: questo ci porta a dire che in l'Italia c'è la necessità di una attenzione particolare sul tema energetico. Su questo indico tre punti che ritengo essere centrali. Il primo: noi abbiamo una scarsa differenziazione di canali di ingresso nel nostro Paese di alcune delle fonti di energia principali: in particolare, a mio avviso, abbiamo una insufficiente capacità di penetrazione del gas metano attraverso i gasdotti esistenti, che sono sottodimensionati rispetto alla crescita della domanda di gas metano in previsione futura e quindi già oggi rappresentano, in mancanza di sufficienti investimenti, una via di ingresso sicuramente sottodimensionata, ristretta, rispetto alla quale la necessità di investimenti, differenziazione e costruzione di nuove vie di accesso al nostro Paese rappresenta una delle priorità. Anche in questo caso non c'è bisogno di mettere in campo molta fantasia: è chiaro a tutti che questo è un problema, cioè l'ingresso del gas, del metano, nel nostro Paese è strozzato e quindi gli eventuali atti terroristici che avessero a che fare con le poche fonti di ingresso oggi esistenti avrebbero facile gioco per mettere il nostro Paese in ginocchio da questo punto di visto. Siccome non sembra che stia accadendo molto da questo punto di vista, metto questo punto come una delle priorità delle quali sia il quasi monopolista nazionale Eni sia gli altri soggetti pubblici sia il regolatore, che ha la responsabilità delle politiche energetiche del Paese, devono sicuramente farsi carico di questo punto.

C'è un secondo grande tema che ha a che fare con l'ammodernamento della rete elettrica. Come spesso capita nel nostro Paese, e sotto qualunque

colore politico, abbiamo una grande capacità di accalorarci su discussioni che fanno moda: abbiamo avuto almeno un buon trimestre in cui non si è parlato altro che del black out e delle soluzioni da dare a questo problema, abbiamo avuto almeno quattro o cinque «Porta a Porta» che si sono occupati dell'argomento, ne abbiamo parlato in Parlamento, e non è stato dato alcun seguito concreto di tipo legislativo o amministrativo rispetto ai fatti che sono venuti in evidenza rispetto a quella vicenda; e non parlo solo dei fatti del *black out* del 27 settembre, che in fondo ha rappresentato un elemento particolare essendo avvenuto di notte quando la richiesta di energia era inferiore, ma parlo dei distacchi di energia del mese di giugno che avevano portato una differenza tra domanda e offerta chiaramente in corto circuito. Sappiamo tutti che l'avvicinarsi dell'estate ripresenta il problema e affrontiamo l'estate senza aver modificato strutturalmente le cose. Aggiungo: da mesi vanno avanti dei contrasti che stanno bloccando i lavori del CIPE per il finanziamento del completamento di un tratto di elettrodotto, che rappresenterebbe un elemento chiave dell'ammodernamento delle nostre linee di approvvigionamento elettrico, in questo caso dalla Svizzera. E se tali contrasti continueranno ad esistere e a bloccare il CIPE, noi non soltanto questa estate, ma nemmeno in quella prossima o in quella prossima ancora potremo dire di essere tranquilli dal punto di vista dell'approvvigionamento di energia elettrica dall'estero, stante la insufficiente capacità di produzione nazionale, aggravata dalla nota lentezza nella messa in essere di nuove centrali elettriche.

Terzo punto è il rapporto tra il ruolo pubblico e i processi di liberalizzazione. La società che gestisce la rete elettrica, che rappresenta da questo punto di vista un *asset* decisivo per le questioni della sicurezza, sarà privatizzata ed è ovvio che il tema della privatizzazione della rete elettrica rappresenta in termini di questione di sicurezza nazionale uno degli elementi chiave. Quindi io invito ad una attenzione molto particolare. Io ho avuto molti dubbi ed infatti non sono stato d'accordo sulla decisione di andare alla privatizzazione di un asset così fondamentale e così legato alla sicurezza, perché l'idea che possa arrivare un soggetto straniero a comprare la rete elettrica nazionale e gestire l'approvvigionamento e la distribuzione concreta della nostra energia elettrica rappresenta sicuramente un elemento da tenere di conto. Oggi la necessità di mettere in equilibrio questi temi, cioè il ruolo pubblico da una parte e la liberalizzazione dall'altra, e quindi di considerare che

la sicurezza non è un *asset* privatizzabile, ma è un asset rispetto al quale esiste la necessità di un ruolo pubblico fondamentale, lo considero un elemento sicuramente chiave.

Credo che dette queste cose sia possibile da parte mia indicare gli ultimi tre punti che indicano obbiettivi da raggiungere, in termini anche di cultura generale del Paese e della sua classe dirigente. Il terzo punto è quello di comprendere tutti che una maggiore efficienza, forza, efficacia delle azioni dell'Unione Europea, è in questo campo l'unica salvezza possibile; l'idea che si possa fare da soli in un campo come questo la mettiamo da parte perché ci rendiamo conto subito della vulnerabilità stessa; quindi la necessità di avere una fiducia nei confronti delle istituzioni europee, che voglia essere anche un passaggio di poteri, una delega, legando ovviamente questa delega al dare il nostro contributo nazionale, è un elemento fondamentale: non credo che noi possiamo permetterci di essere da una parte dipendenti dalle scelte europee e dall'altra parte avere nei confronti dell'Unione Europea un approccio che non sia profondamente favorevole ad una marcia accelerata dell'integrazione comunitaria. Più integrazione comunitaria vuol dire in questo caso più sicurezza; meno integrazione, più diritti di veto, più voti all'unanimità, vuol dire in questo campo minore sicurezza. A tale riguardo, soprattutto oggi che la discussione sull'Europa riprenderà in tutto il Paese in vista delle elezioni europee, credo che sia molto importante chiarire che esiste un *trade off* tra questi due temi. Non si può immaginare o cercare un'Europa debole a vantaggio del peso e del potere di ogni singolo Stato, sapendo che tale potere nei fatti è evanescente dato che in pratica le frontiere non esistono.

Il quarto e penultimo punto: riprendo una cosa che diceva Lucio Stanca e sulla quale concordo, cioè come sia importante la necessità di trovare il giusto equilibrio tra i diritti della persona, della privacy, e il diritto alla sicurezza. È un tema complicato, perché si possono fare mille esempi per argomentare che bisogna far pendere più su un campo, ossia sul diritto alla sicurezza o far pendere più sull'altro campo; soprattutto è un settore nel quale ho imparato, per le cose che ho sentito, dove non ci sono dinamiche scontate; c'è il famoso esempio delle informazioni che ognuno dà nella sua carta di *frequent flyer* nella quale, tra le tante cose, mette anche il tipo di pasto che uno preferisce avere a bordo; ed è evidente che, quando si indica la cucina *kosher*, qualunque persona che ha accesso a quel tipo di informazione sa che su quel

certo volo esistono una quantità sopra la norma di persone di religione ebraica. Cito questo esempio che è molto particolare, ma che è significativo del fatto che questi temi non hanno un approccio scontato, non hanno una dinamica, per la quale in alcuni casi la privacy è sicurezza e in altri casi la privacy non è sicurezza e rispetto ai quali quindi è necessario che questo equilibrio sia effettivamente ben calibrato.

Ed infine l'ultimo punto con il quale termino. Ritengo che, ed è anche il motivo per il quale il convegno di oggi rappresenta sicuramente un contributo importante, sia fondamentale che il Paese cambi atteggiamento sul rapporto tra questi obbiettivi di sicurezza interna ed esterna e l'uso delle risorse finanziarie: credo che non abbiamo ancora colto fino in fondo il fatto che è finita un epoca nella quale la nostra sicurezza interna ed esterna ce la pagava la guerra fredda ed il nostro posizionamento nella guerra fredda: quell'epoca è finita. La possibilità di spendere per la nostra sicurezza interna ed esterna cifre risibili, perché tanto spendeva il contribuente americano, è un epoca che sta alle nostre spalle: di questo non mi sembra che ci sia ancora la consapevolezza giusta, perché quando si discute su questi temi ogni volta si fa fatica a far capire che le risorse impiegate in questo campo non sono risorse per attività moralmente non giustificate o immorali. È una delle vicende che nella vita parlamentare è più difficile da affrontare, è uno dei tabù che nella dialettica della vita politica e pubblica è una delle questioni chiave. Credo che sia necessario far fare al nostro Paese un salto in avanti nella comprensione che la nostra sicurezza dovremo da oggi in poi pagarcela, nel senso che anche quando sarà fatta a livello comunitario sarà un qualcosa che comunque inciderà sul nostro 740; credo che questa consapevolezza sia forse una delle questioni nelle quali siamo un po' più indietro e sulle quali invece la necessità di far fare un passo avanti definitivo è quanto mai necessario e sulla quale perdere tempo non ha alcun significato. Grazie

On. Ramponi: Ringrazio l'On. Letta. Nessuno meglio di me sa quanto sia faticoso far capire la necessità di dedicare adeguate risorse alla sicurezza, come hai detto, interna ed esterna; ed è vero che ancora oggi nella classe politica italiana questo è un elemento tabù. Speriamo che, se non altro, la minaccia rappresentata dal neoterrorismo possa, tra gli altri elementi negativi, avere l'elemento positivo di aver sensibilizzato finalmente la classe politica italiana tanto da allinearsi quanto meno con quanto fanno i principali componenti

dell'Unione Europea con i quali dobbiamo confrontarci.

Non c'è dubbio che lo squilibrio nelle spese per la sicurezza interna ed esterna tra l'Italia e la Francia, la Germania e l'Inghilterra è addirittura clamoroso. Mi compiaccio anche per la sostanziale convergenza negli altri due punti che hai indicato: cioè il riferimento costante all'Europa, che riecheggia i discorsi fatti dai Ministri Gasparri e Stanca, e la ricerca costante dell'equilibrio tra la privacy e la sicurezza.

Prego adesso il Sen. Erroi di trattare l'argomento dal punto di vista delle Infrastrutture e Trasporti.

Intervento del Sen. Bruno Erroi

Infrastrutture e Trasporti

Grazie Presidente. Affrontare il tema del rischio ***terrorismo*** è un'iniziativa estremamente complessa, come ogni osservazione o riflessione che riguarda una società complessa come la nostra.

La simultaneità degli eventi dovuta alla comunicazione globale ha enormemente aumentato il numero dei soggetti coinvolti dalle determinazioni di decisori anche lontani e distanti. In questa società del mondo, dove la tecnologia ha portato le capacità di offesa in termini impensabili sino a pochi decenni or sono, tutti siamo ormai coinvolti da decisioni assunte a centinaia di migliaia di chilometri di distanza. L'abbattimento delle distanze materiali e immateriali ha comportato come effetto collaterale primario la perdita di protezione a causa delle decisioni di agenti lontani.

Il rischio terrorismo è un effetto paradossale del miglioramento della tecnologia. L'arma atomica, l'offesa genetica, le esplosioni derivanti da micro-ordigni sono fattori di rischio dipendenti evidentemente dalla crescente ricerca tecnologica e dallo sforzo della ricerca di creare e ricreare nuove barriere di protezione alla vita. In questo villaggio globale, dove in poche ore si sorvolano gli oceani, diventa sempre più improbabile realizzare meccanismi di identificazione dei soggetti pericolosi. Le stazioni ferroviarie, gli aeroporti, i luoghi di aggregazione, gli stadi, le piazze che ospitano eventi sociali sono tutti potenziali bersaglio, di un nemico invisibile, che può aggirarsi indisturbato.

In questo quadro drammatico, l'aumento dei margini della conoscenza e della ricerca diviene, anche in questo senso paradossalmente, un fattore di aumento della sicurezza. La società deve recuperare la funzione della «memoria», dell'architettura sociale costruita sul dialogo: programmi razziali o di chiusura indiscriminata porterebbero all'aumento delle rigidità e quindi all'infiltrazione di meccanismi esplosivi di matrice terroristica che si alimentano, paradossalmente, proprio in quella società che non ha consapevolezza del tempo, di un tempo nel quale le barriere sono virtuali e invisibili. Si è riscontrato, infatti, che l'aumento della repressione penale, o il consolidarsi di apparati e di metodiche di controllo di tipo tradizionale non producono né gli effetti sperati di un abbattimento dei livelli di illiceità o di distruzione, né, tantomeno, effetti psicologici di sicurezza nei cittadini.

Invece il primo importante risultato, in termini operativi, sul piano della delimitazione e della progressiva messa in crisi degli apparati criminali o terroristici, può aversi quando il sistema di controllo vada a essere ri-orientato verso l'intelligence strategica e tattica sui gruppi criminali e terroristici, al fine di conoscerne, dall'interno e dall'esterno, il *modus operandi* e le loro dinamiche di evoluzione.

In sostanza, una nuova programmazione degli strumenti, costruita sulla conoscenza e sull'*intelligence*, potrà produrre effetti estremamente positivi, al di là di strategie miranti alla mera distruzione o costruite su un'ipotesi di non legittimazione politica dell'avversario.

La costruzione degli steccati riproduce solo reazioni incontrollabili e l'aumento dei rischi di ri-selezione continua dei bersagli.

Con le società per cui la morte rappresenta l'apoteosi dello spirito, diventa assolutamente implausibile rifarsi a schemi di salvaguardia della vita e di protezione anche degli stessi agenti del terrore.

Su questo, nuovi scenari di dialogo e di integrazione sociale devono aprirsi, essendo insufficienti e inadeguati i mezzi della protezione causalistica mediante uomini e presìdi o le strategie dell'annullamento fisico, mediante distruzione.

L'assetto del sistema della protezione dei trasporti e delle infrastrutture del Paese viene istituzionalizzato nel 2002, nel quadro di riorganizzazione delle difese contro la minaccia terroristica cui gli Stati occidentali sono stati necessariamente chiamati a seguito degli eventi dell'11 settembre 2001.

In particolare, su input della Presidenza del Consiglio, a seguito di indicazioni emerse in ambito G8 e sulla base di richieste formulate in un quadro bilaterale dagli USA, gli organismi preposti alla « gestione delle Crisi» determinarono, a ridosso degli eventi predetti, di predisporre un sistema di coordinamento e controllo in grado di assicurare, in ciascuno dei settori dei trasporti, i più elevati *standard* della sicurezza di esercizio. Di seguito un elenco delle misure prese nei singoli settori.

Sicurezza aeroportuale

- Controllo dei bagagli da stiva
- Rilevazione dei dati biometrici (esiste già qualche esempio)
- Sistemi antintrusione
- Affidabilità del personale aeroportuale

- Recinzione aeroportuali
- Piani di emergenza
- Addestramento da parte di ENAV - ENAC

Sicurezza Portuale

- Piani di *security* della nave
- Ufficiali di bordo addetti alla *security*
- Ufficiali di compagnia addetti alla *security*
- Adeguato equipaggiamento di bordo
- Piani di *security* del porto
- Uffciali addetti alla *security* del porto
- Monitoraggio e controllo degli accessi al porto
- Monitoraggio delle attività di persone e carichi
- Garanzia della disponibilità di opportuni canali di comunicazione per le informazioni relative alla *security*

In aggiunta

- Anticipazione dell'adozione a bordo delle navi del sistema automatico di identificazione
- Predisposizione di un *security alarm* da istallare sulle navi
- Coordinamento per la *security* sui containers
- Sistema di rintracciabilità ed identificazione della nave a lungo raggio
- Introduzione di un sistema su tutte le navi che contenga informazioni sulla proprietà, la bandiera e la gestione della nave, in modo da scoraggiare attività illecite in campo marittimo

Trasporto su strada

Questa modalità di trasporto, caratterizzata da una serie di fattori dimensionali, funzionali, economici e quantitativi, che la differenziano nettamente da quello portuale ed aereo, viene definita come sistema «aperto». A ciò consegue la difficoltà di attuare controlli sistematici.

Criticità

- Sistemi ad accesso libero con eventuali barriere e scopo solo fiscale
- Accessi numerosi distribuiti capillarmente sul territorio
- Bagagli affidati alla cura del passeggero e non del vettore

Misure di sicurezza proposte

- Sensibilizzazione del cittadino sui rischi potenziali
- Applicazione di azioni di deterrenza finalizzate anche a dare evidenza ai passeggeri delle misure di sicurezza
- Utilizzo dei sistemi di sorveglianza automatica a distanza
- Rafforzamento della vigilanza su veicoli e infrastrutture attraverso un maggior coinvolgimento delle istituzioni operanti in ambito locale. Graduazione delle azioni in relazione alla sensibilità degli obiettivi

Trasporto ferroviario

- Sistema aperto all'accesso libero, interconnesso con il sistema stradale
- Accessi numerosi e assenza di barriere lungo la rete
- Bagagli affidati alla cura del passeggero e non al vettore
- Sensibilità dell'utenza a restrizioni che comportino ritardi o limitazioni all'attività di trasporto
- Trasformazione in corso delle stazioni in sistemi commerciali avulsi dalle attività di trasporto

Misure di sicurezza proposte

- Implementazioni sistemi di videocamera a circuito chiuso
- Sistema anti-intrusione e sistema di riconoscimento biometrici
- Sistemi di informatici di monitoraggio rischi
- Cartografie computerizzate
- Sistemi mobili per la sicurezza
- Rilevatori di sostanze nocive
- Apparati di controllo radioscopico
- Protezione delle merci con chiusura di sicurezza e sistemi di radiolocalizzazione
- Deposito automatico bagagli
- Sale di emergenza
- Formazione del personale e collaborazione dello stesso con le Forze di Polizia
- Procedure specifiche del trattamento dei bagagli incustoditi
- Procedura per la protezione dei treni fuori servizio
- Controlli passeggeri a campione o «mirati»

- Controllo merci a campione e controllo della composizione dei treni merci
- Avviso al pubblico
- Servizi di vigilanza privata

Metropolitane e ferrovie locali

Criticità

- Sistema di accesso libero, presenza di eventuali barriere solo a fini fiscali
- Accessi numerosi e distribuiti capillarmente
- Bagagli affidati alla cura del passeggero e non al vettore
- Sensibilità dell'utenza a restrizioni che comportino ritardi o limitazioni all'attività di trasporto

Misura di sicurezza proposte

- Formazione del personale
- Applicazioni di azioni di deterrenza finalizzate anche a dare evidenza ai passeggeri delle misure di sicurezza
- Utilizzo di sistemi di sorveglianza automatica a distanza
- Rafforzamento della vigilanza su veicoli ed infrastrutture
- Controllo a campione di passeggeri e bagagli
- Individuazione e rimozione di bagagli ed oggetti incustoditi
- Sale di emergenza

Interporti e logistica

Criticità

- Bassa per la loro collocazione, di norma, lontana da centri abitati o da zone ad alta densità
- Non si registrano ad oggi azioni o tentativi terroristici
- Possibile introduzione illecita di armi, sostanze tossiche ed altri oggetti nocivi all'interno dell'area

Misure di sicurezza proposte

- Barriere di protezione
- Controllo dei varchi di accesso

- Rete telematica tra tutti i soggetti operanti all'interno dell'interporto
- Previsione di un posto di polizia all'interno di ogni struttura interportuale o assegnazione ai servizi di vigilanza privata di opportuni limitati poteri

On. Ramponi: Ringrazio il Sen. Erroi. Ringrazio tutti coloro che si sono prodigati per questo convegno. In coscienza credo di poter dire che lo sforzo, che abbiamo fatto, ha permesso a tutti voi e anche agli organi di informazione di avere indicazioni ben precise delle linee lungo le quali si deve sviluppare questa azione di contrasto alla minaccia terroristica. Grazie ancora a tutti.

INDICE

Il convegno nasce dalle conclusioni
del precedente «Contro il nuovo terrorismo,
una nuova strategia globale»:
le Istituzioni pubbliche non possono da sole
assumere l'onere totale della
prevenzione - protezione
nei confronti della minaccia che è globale
nel dove, nel come e nel quando.

L'attentato terroristico del 11 marzo u.s. in Spagna
è stato la tragica conferma che una
efficace strategia di contrasto al nuovo terrorismo
deve prevedere un
impegno sinergico del pubblico e del privato.

Il convegno è stato aperto con l'intervento
del Capo del Dipartimento della Protezione Civile
e si è sviluppato su tre sezioni,
ENERGIA, TRASPORTI e TELECOMUNICAZIONI;
ha concluso i lavori del mattino
l'Amministratore Delegato della Finmeccanica.

Il dibatto che si è innescato è stato
intenso, brioso ed avvincente,
non solo per l'alto consesso dei relatori
ma anche perché le sezioni hanno avuto come moderatori
tre esperti giornalisti che lo hanno abilmente condotto.

L'alto rango bipartisan dei politici
che hanno partecipato alla tavola rotonda,
che ha concluso i lavori,
ha contribuito a esaurire l'argomento
convenendo ad unanimi e convergenti vedute.

Il presente volume riporta integralmente
i lavori del convegno.