Ossevatorio per la

Sicurezza Nazionale

Anno 1 - n°1 Settembre 2006

L'Osservatorio per la Sicurezza Nazionale è una pubblicazione del Centro Militare di Studi Strategici, realizzata sotto la direzione editoriale dell'Amm. Div. Luciano Callini.
Le informazioni utilizzate per l'elaborazione delle analisi provengono tutte da fonti aperte (pubblicazioni a stampa e siti web) e le fonti, non citate espressamente nei testi, possono essere fornite su richiesta.
Quanto contenuto nelle analisi riflette, pertanto, esclusivamente il pensiero degli autori, e non quello del Ministero della Difesa né delle Istituzioni militari e/o civili alle quali gli autori stessi appartengono.
L'Osservatorio per la Sicurezza Nazionale è disponibile anche in formato elettronico (file PDF) nelle pagine CeMiSS del Centro Alti Studi per la Difesa: www.casd.difesa.it

Contatti:
Dipartimento Scienze Tecnica Economia e Politica Industriale
Palazzo Salviati
Piazza della Rovere, 83 00165 - ROMA
tel. 06 4691 3205 fax 06 6879779
e-mail capostepi.cemiss@casd.difesa.it

Questo numero è stato chiuso il
15 Settembre 2006

SOMMARIO

EDITORIALE

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Amm. Giampaolo Di Paola Capo di Stato Maggiore Difesa

Editoriale

Il periodo storico attuale è definibile come una fase di rivoluzione durante la quale ciò che era valido nel passato, e avvalorato dall'esperienza, può non esserlo più, dunque è indispensabile valutare la direzione e i fattori di cambiamento agendo conseguentemente, anche con il coraggio di rischiare. Quando una rivoluzione riguarda gli scenari e il concetto di Sicurezza, tutto risulta particolarmente complesso e difficile: infatti si tratta di agire su più dimensioni, con tempi coerenti con le esigenze che spesso si manifestano sotto forma di nuove minacce, e con la valutazione e la percezione dei rischi per attuare nuove efficaci forme di risposta.
L'11 settembre rappresenta ormai la data simbolo di un periodo storico caratterizzato da profondi e veloci cambiamenti che investono la sfera politica, sociale ed economica e promuovono più ampie riflessioni sul crescente divario tra i Paesi, le modalità di accesso alla modernità per quelle popolazioni escluse dalla prospettiva di miglioramento del proprio benessere, la proliferazione delle tecnologie con particolare riferimento all'information technology, il processo di globalizzazione caratterizzato dalla perdita dei valori fondamentali e la riaffermazione di identità etniche e religiose.
Di fronte al nuovo scenario globale, contraddistinto da una forte instabilità e una accresciuta percezione di insicurezza e di vulnerabilità, occorre cambiare in maniera rivoluzionaria il nostro approccio al concetto di sicurezza: questa è la prima grande sfida della trasformazione che riguarda le Forze Armate.
Per far fronte alle nuove tipologie di intervento, nel mutato contesto di risposta alle crisi - siano esse dovute all'attentato terroristico piuttosto che a un evento naturale - non bastano più sofisticate tecnologie e personale ottimamente addestrato, ma occorre agire con un approccio integrato e olistico che impone uno sviluppo e un impiego sinergico di capacità, metodologie e strumenti differenti.
Il progetto congiunto del CeMiSS e di Elsag-Finmeccanica, che prevede la costituzione di un Osservatorio permanente per la Sicurezza Nazionale, si propone di affrontare questa sfida configurandosi come uno strumento adatto per rispondere alle nuove esigenze di sicurezza. Esso nasce da un carattere fortemente interdisciplinare e si fonda su un metodo teso a valorizzare la cross-fertilization delle competenze attraverso un approccio sistemico.
Integrazione, condivisione di obiettivi, di informazioni, di risorse intellettuali e best practices sono alcune delle parole e dei concetti chiave che delineano l'approccio che l'Osservatorio per la Sicurezza Nazionale (OSN) si propone di seguire.
L'OSN risponde all'esigenza fortemente avvertita della creazione di una cultura condivisa e trasversale sulla sicurezza, la cui diffusione l'Osservatorio pone come suo primo obiettivo e missione fondante. Rappresentanti del mondo della Difesa, dell'Industria, delle Istituzioni, dell'Università, dei Corpi di Polizia formano il tavolo di lavoro dell'OSN, ne stanno costruendo l'identità, gli strumenti, il patrimonio umano ed intellettuale.
Si tratta di un network che ha le sue radici nella valorizzazione dell'esistente - il patrimonio italiano di conoscenze in materia di sicurezza nazionale nei differenti ambiti e settori - e tende verso la creazione di un nuovo approccio fondato sulla condivisione di obiettivi, l'integrazione di orientamenti ed esperienze, il confronto di metodologie, avvalendosi di competenze specifiche declinate nei diversi campi delle scienze e provenienti da ambienti culturali differenti.
Si tratta, anche, del solo approccio mentale e concettuale idoneo ad affrontare una tematica complessa, in continua evoluzione, che segue la rivoluzione dello scenario internazionale e la trasformazione di una minaccia che si dimostra, sempre più spesso, abile nell'uso di tecnologie, così come degli strumenti della "cultura"

e della comunicazione. Pertanto, la risposta a queste minacce non può che essere ad un tempo tecnologica e culturale, ingegneristica e umanistica.
La sfida che si propone l'OSN è fare sì che la propria attività di analisi e di studio produca conoscenza, fondata su solide basi teoriche e verificata con gli strumenti della ricerca empirica, permettendo in questo modo la predisposizione di strumenti concretamente applicabili nelle diverse situazioni di rischio, facendosi altresì promotore del lancio della fattibilità di progetti e attività industriali.
Obiettivo sicurezza, dunque; una Sicurezza Nazionale che, in relazione all'evoluzione - o più propriamente - alla "rivoluzione" dello scenario e alla nuova tipologia dei rischi e della minaccia, deve essere vista in un'ottica multinazionale e che si configura sempre più come un continuum senza frontiere, in cui sicurezza interna e sicurezza esterna non possono essere separate.
Una sicurezza, quindi, affidata alla sinergia fra gli strumenti operativi interni e le Forze Armate, analizzata negli Atenei italiani e nelle nostre Industrie; una sicurezza che è anche umana e sanitaria; una sicurezza promotrice di sviluppo economico e sociale nelle zone di crisi; sicurezza come sensibilità civile, liberata da vecchi stereotipi, diffidenze e pregiudizi: questi sono i temi che l'OSN si propone di affrontare.
Ciò che si propone l'OSN è tanto ambizioso quanto di sicura utilità e arricchimento e il primo numero di questa rivista ne testimonia il primo piccolo ma importante passo avanti in questa direzione.

Anno I - n°1 Settembre 2006

Osservatorio per la Sicurezza Nazionale

Pier Francesco Guarguaglini Presidente e amm. delegato di FINMECCANICA

Editoriale

L'evoluzione della minaccia terroristica globale fino dentro i confini nazionali e la posizione geostrategica dell'Italia nel cuore del Mediterraneo hanno accresciuto l'urgenza di rivedere i nostri parametri di sicurezza. La loro trasformazione è, al tempo stesso, una sfida e un impegno. Riguarda tutti coloro che, nei diversi settori e attraverso differenti approcci e metodologie, si occupano di sicurezza nazionale: istituzioni, Forze Armate, Corpi di Polizia, atenei, industrie.

Alla globalizzazione della minaccia, sia essa di origine antropica o naturale, deve corrispondere una risposta globale. Ad essa la tecnologia deve fornire un contributo essenziale in quanto è un elemento chiave in un sistema basato su uomini preparati, organizzazioni efficaci e norme chiare. In altre parole, su una "cultura" condivisa, proprio come propone l'Osservatorio per la Sicurezza Nazionale.

Il progetto promosso dal Ce.Mi.S.S. e da Elsag, traccia una rotta per affrontare il nuovo scenario. Un'efficace azione di prevenzione della minaccia e di gestione della nostra sicurezza nazionale, deve infatti passare attraverso una razionalizzazione del quadro istituzionale, tenendo nel giusto conto l'esperienza maturata non solo dai diversi organismi e amministrazioni, ma anche nei nostri atenei e nelle nostre industrie.

Con queste premesse, riteniamo che il network che l'Osservatorio per la Sicurezza Nazionale sta costruendo intorno al concetto di sicurezza possa contribuire sensibilmente a questa innovazione. Questa rete coinvolgerà coloro che si occupano di sicurezza, ne valorizzerà il patrimonio di conoscenze e di esperienze, sarà incubatrice di nuove idee e di nuovi progetti e al tempo stesso costituirà un luogo di confronto per definire le priorità tecnologiche, ritagliate sulle esigenze di sicurezza del nostro Paese. In questo network Finmeccanica si impegna attraverso le proprie aziende, SELEX Sistemi Integrati ed Elsag in primis, a dare un contributo continuo di conoscenza, di esperienza e di innovazione tecnologica.

Riteniamo e ci auguriamo che l'Osservatorio sulla Sicurezza Nazionale formi una comunità in grado di operare un'autentica integrazione tra ricerca e sviluppo, tra strategie e dottrine, tra esperienze sul campo e simulazioni, anche attraverso un continuo confronto umano ed intellettuale. Attraverso la condivisione degli obiettivi ed il lavoro in gruppi eterogenei ma interconnessi tra loro, l'Osservatorio darà senz'altro un grande aiuto a tracciare approcci coordinati, integrati e sistemici per la Sicurezza Nazionale.

È nostra opinione che l'Osservatorio per la Sicurezza Nazionale possa dare un contributo significativo alla risposta globale nei confronti delle diverse minacce che possono interessare il territorio nazionale, e la Rivista dell'OSN, che ne rappresenterà la voce ufficiale, costituisce un lodevole esempio di lavoro di gruppo orientato a costruire, attraverso la condivisione di problematiche, competenze e soluzioni, un riferimento ed un supporto per quanti si interessino al tema della Sicurezza Nazionale.

Se l'obiettivo è "tessere insieme una cultura condivisa sulla Sicurezza Nazionale", in queste pagine si trovano i primi importanti passi nella giusta direzione.

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Amm. Div. Luciano Callini Direttore del Centro Militare Sutdi Strategici
Ing. Massimo Galluzzi, Direttore Divisione Sistemi Logistica e Difesa di Elsag

Editoriale

Sicurezza e difesa sono da sempre, e tali devono rimanere, una realtà e un binomio inscindibile che continuano forse ad evocare, nell'immaginario collettivo, un impegno specifico delle Forze dell'Ordine e delle FFAA a tutela degli spazi sovrani terrestri, marittimi ed aerei.
Avvenimenti del recente passato, come la crisi del Golfo Persico, o quella dei Balcani o l'attuale scenario libanese, hanno fatto comprendere che la sicurezza inizia ben al di là delle frontiere nazionali e che, in un mondo globalizzato come il nostro, i confini geo-strategici di un Paese vanno ben oltre i confini puramente geografici dello stesso.
Negli anni recenti si è, infatti, reso indispensabile portare stabilità in aree del mondo la cui distanza sarebbe stata giudicata, in un passato anche recente, operativamente impossibile. Le distanze di intervento si sono sensibilmente allungate e le FFAA si trovano per questo ad affrontare una fase avanzata di un processo di trasformazione che ne allungherà il braccio operativo fino a renderle proiettabili in qualsiasi parte del globo dove sono a rischio gli interessi i del nostro Paese.
Sicurezza e difesa, adeguando le proprie strutture e i propri mezzi, hanno quindi sviluppato e acquisito nella loro fisionomia le ormai famose capacità di "Peacekeeping" e di "Peacemaking" per fornire supporto concreto, quando richiesto, alle organizzazioni internazionali di cui il Paese è parte integrante.
A fronte del peggiore dei fenomeni del nostro secolo, vale a dire quello della globalizzazione della minaccia terroristica associata alla proliferazione di armi di distruzione di massa, si è resa necessaria una nuova concezione della sicurezza che deve mirare a ridurre al minimo i rischi attraverso una efficace opera di prevenzione che deve coinvolgere, non solo le Forze Armate e le Forze dell'Ordine, ma tutti gli attori che operano nella società a partire dal singolo cittadino.
Forse non è ancora diffusamente percepito, ma ogni sistema Paese è già, di fatto, in una fase permanente di assetti di "Security making " e di "Security keeping" che non hanno più le connotazioni classiche, ma che abbracciano ogni settore chiave che abbia importanza vitale per il normale procedere della società in cui viviamo. Ormai si parla di sicurezza non più solo in chiave di Forze Armate e di Polizia, ma anche a riguardo di sanità, di comunicazioni, di gestione di risorse idriche, energetiche ed alimentari, di trasporti terrestri, marittimi ed aerei, di tecnologia e di industria, di istruzione e formazione, di permeabilità delle frontiere, di catastrofi ecologiche ed ambientali.
Ecco quindi nascere, si potrebbe dire quasi naturalmente, presso il CeMiSS, dall'indissolubile legame difesa/sicurezza, e dalla collaudata e felice sinergia esistente tra difesa e industria, l'iniziativa di un Osservatorio permanente per la Sicurezza Nazionale con l'ambizioso compito di estendere e integrare tutto ciò che attiene al "security making" e al "security keeping" senza in alcun modo sovrapporsi ad alcun compito istituzionale di qualsivoglia altro ente od organismo.
Il primo obiettivo è quello di promuovere, con il fattivo contributo dei nostri partners del mondo della Pubblica Amministrazione, dell'Industria e del mondo Accademico, la diffusione di una cultura trasversale della sicurezza che serva a far meglio comprendere questa necessità del nostro tempo e a responsabilizzare maggiormente i cittadini e le strutture che hanno la responsabilità di assicurare il regolare svolgimento della vita di tutti i giorni.
E' forse solo un sassolino nello stagno, ma il primo numero di questa rivista vuole lanciare un messaggio che

possa innescare un processo virtuoso di crescita che renda consapevole il lettore che sicurezza non è solo manpower, hardware e software, bensì un processo culturale lungo e continuo che ogni singolo deve curare giorno per giorno per far si che "quello che potrebbe accadere" non accada e che, se dovesse comunque accadere, trovi una società di cittadini pronta a reagire adeguatamente all'emergenza senza cadere preda dell'impreparazione e del panico.

PRESENTAZIONE OSN

CeMiSS - ELSAG

Osservatorio per la Sicurezza Nazionale

Identità di OSN: un network per la Sicurezza Nazionale

È trascorso un anno da quando l'idea inizialmente scaturita dalle pagine di una ricerca condotta sinergicamente dal CeMiSS e da Elsag-Finmeccanica, si è trasformata in progetto. Andare sul campo rintracciando competenze, esperienze, metodologie, linguaggi inerenti alla Sicurezza Nazionale nel nostro Paese ha portato ad una consapevolezza nuova e più globale della complessità dell'argomento e del patrimonio di conoscenze da approfondire, condividere, custodire.

Per perseguire con efficacia ed efficienza l'obiettivo della conoscenza integrata è nata l'esigenza dì costituire una rete in grado di interfacciare tra loro ambienti differenti e sottoculture operanti in ambiti attigui ma non sempre comunicanti della Sicurezza.

Come hanno introdotto le pagine che inaugurano questa pubblicazione, la sensibilità e l'attenzione rivolta alla Sicurezza Nazionale sono, ormai da cinque anni, in continuo aggiornamento ed in costante evoluzione.

La sfida che ci si pone dinnanzi è nel pensare alla Sicurezza Nazionale in termini olistici, costituendo uno strumento flessibile ed incentrato sull'integrazione di approcci e metodologie così da permettere, con il contributo di tutti coloro che in Italia si occupano di sicurezza, un reale approccio trasversale alle problematiche.

L'Osservatorio per la Sicurezza Nazionale (OSN) nasce dall'intenzione di raccogliere questa sfida rappresentando il concreto tentativo di costituire un assetto operativo che soddisfi l'esigenza affatto astratta di pensare alla Sicurezza Nazionale "al plurale"; si basa dunque sulla volontà di fornire una risposta efficace alle minacce creando, con l'apporto specialistico dei diversi settori interessati alla homeland security (mondo militare, istituzionale, accademico e industriale), una diffusa e condivisa cultura della sicurezza. OSN, è un luogo di confronto, di scambio di esperienze e modelli logici, di interazione tra diversi approcci, un luogo per costruire insieme valorizzando il patrimonio esistente e, allo stesso tempo, per sviluppare strumenti condivisi a supporto dei processi decisionali nel settore della Sicurezza Nazionale.

Appare in tale ottica centrale il concetto di globalità nelle sua triplice accezione di

- *approccio multidisciplinare nella analisi delle problematiche osservate*
- *conoscenza integrata delle diverse tematiche di sicurezza in tutte le loro sfaccettature e implicazioni*
- *elaborazione di una risposta completa ed esaustiva alle minacce che lo Stato deve affrontare.*

OSN è attualmente un work in progress, "un cantiere" che coagula attorno a sé dimensioni professionali estremamente eterogenee per la prima volta chiamate ad operare sinergicamente; è un progetto nato da una precisa esigenza ma con obiettivi, modus operandi e campi d'azione ancora da definire con esattezza e da sviluppare insieme.

In questo primo numero OSN lascia il tavolo delle riunioni, intorno al quale sta' costruendo la sua identità, per presentarsi: chi è OSN dunque ?

Un network per la Sicurezza in cui, nello spirito della costituzione di una reale cultura condivisa e trasversale, lo strumento metodologico fondante sia la reciprocità dell'osservazione tra gli attori implicati nel processo dì monitoraggio delle aree di interesse.

La Rivista, che rappresenterà una delle sue espressioni, costituirà il risultato della disponibilità, dell'impegno, della competenza di un autentico lavoro di gruppo che unisce Ministeri, Atenei, Industrie, Forze Armate e di Polizia. Si decideranno gli argomenti che costituiranno i temi attorno ai quali confrontarsi, sui quali riflettere insieme per offrire al lettore non solo differenti chiavi di lettura, ma un approccio sistemico.

Attraverso le pagine di questo "numero zero" i partecipanti si presentano, descrivono le loro linee di lavoro, la propria esperienza e competenza; ognuno è parte del mosaico che è la sicurezza nazionale, ognuno un importante prezioso tassello.

Osservatorio per la Sicurezza Nazionale

Identità di OSN: un network per la Sicurezza Nazionale

Essere un sistema, formato da singolarità estremamente competenti e che, insieme, offrono un grande valore aggiunto: questo è l'Osservatorio per la Sicurezza Nazionale.
La rivista avrà la forma di monografie e potrà fornire al lettore il valore di un approccio multidisciplinare. Le Rubriche, invece, resteranno un appuntamento fisso, un approfondimento rinnovato periodicamente e dedicato ad aree di studio ed analisi particolarmente interessanti, moderne, in rapida e costante evoluzione.
Nelle pagine seguenti, il primo nucleo di OSN - al quale auspichiamo possano al più presto aderire altri partner - espressione di quanti hanno manifestato il proprio impegno e la propria disponibilità a costruire insieme qualcosa di nuovo, un approccio realmente interdisciplinare in grado di osservare meglio, con maggiore completezza, una modernità entropica nella quale la minaccia assume forme sempre più sofisticate ed imprevedibili.Questo numero zero, dunque, è il primo esempio di un lavoro integrato, condiviso, trasversale, partecipato, la prima espressione dell'impegno che ci unisce.

OSN, insieme per la Sicurezza Nazionale.

Il Project Office di OSN

Criteri ispiratori e Manifesto dell' Osservatorio per la Sicurezza Nazionale

Gli eventi dell'11 settembre 2001 hanno cambiato il mondo.
Questa è una frase, certamente scontata e condivisa, che evidenzia una linea di cesura e propone una discontinuità nei rapporti tra persone e tra paesi, avviando una nuova scommessa per ricreare equilibri di convivenza pacifica nel Mondo Globale.
Ma d'altra parte, il tempo dopo September Eleven è anche caratterizzato da una nuova sensibilità nei confronti della sicurezza, che si esprime in termini di preoccupazione per i cittadini e richiede nuove modalità organizzative e adeguate strategie alle istituzioni responsabili.
*A partire da questi presupposti nasce l'**Osservatorio per la Sicurezza Nazionale (OSN)**, un progetto promosso da Ce.Mi.S.S., Centro Militare di Studi Strategici, e Finmeccanica, a cui si sono uniti l'Università e altri partner.*
***La prospettiva** dell'OSN è quella di affrontare i temi della sicurezza secondo una molteplicità di dimensioni e, conseguentemente, una pluralità di discipline. Questa scelta articolata si fonda su alcune considerazioni:*

- *alla sicurezza nazionale attentano cause naturali e umane, la cui genesi si differenzia rispetto alla volontarietà o meno dell'evento critico (dal terremoto all'attentato);*
- *i danni conseguenti un evento critico sono commisurati sia alla mancanza di competenze nei sistemi di difesa (vulnerabilità) sia all' incremento delle competenze nei sistemi di offesa;*
- *pertanto, le pratiche di difesa e di risposta devono essere almeno tanto complesse quanto la minaccia.*

L'OSN deve dunque muoversi

- *coordinando il lavoro degli attori che, nel nostro Paese, partecipano ai processi di produzione, di gestione e di conoscenza;*
- *avvalendosi di competenze specifiche declinate nei diversi campi delle scienze e provenienti da ambienti culturali differenti;*
- *tutti impegnati secondo la prospettiva unificante della attenzione alla sicurezza nazionale.*

***La missione** dell'OSN è di creare una cultura della sicurezza insieme a strumenti per il mantenimento della sicurezza.*
Se per cultura si intende quel sistema di schemi di riferimento, di norme, di valori, di abitudini, di consuetudini che costituiscono il patrimonio di una nazione, che si trasmette, si arricchisce e si modifica tra i gruppi attraverso la comunicazione. Allora è promovendo una cultura della sicurezza, diffusa tra i cittadini, che si rende possibile affrontare la minaccia alla popolazione e al territorio attraverso una gestione del rischio e della crisi che deve essere strategica, competente, sostenibile, integrata, che sia fondata cioè su una cultura condivisa.
***Il metodo di lavoro** dell'OSN è teso a valorizzare la multidisciplinarietà e la cross-fertilization della competenze: "chi" attenta alla nostra sicurezza o "quanto" attenta alla nostra sicurezza si propone, sempre più spesso, come competente nell'uso di tecnologie, di strumenti culturali e linguistici, di strumenti della "cultura" e della comunicazione. Pertanto, la risposta a queste minacce non può che essere tecnologica e culturale, ingegneristica e umanistica. La prima sfida per l'OSN è quella di mostrarsi capace di integrare competenze diverse, affinché la propria attività di ricerca e di studio produca conoscenza, fondata su solide basi teoriche e verificata con gli strumenti della ricerca empirica, permetta la predisposizione di strumenti concretamente applicabili nelle diverse situazioni di rischio.*
***Sono obiettivi** dell'OSN:*

- *lo sviluppo di un sistema di conoscenze e competenze sulle minacce per la sicurezza;*
- *lo sviluppo di strumenti, pratiche e strategie per la riduzione della vulnerabilità e la gestione delle crisi;*
- *l'elaborazione di scenari di rischio e di pratiche di prevenzione;*
- *la proposizione di strumenti di contrasto;*
- *la diffusione dei risultati e la promozione di nuove competenze con una propria rivista e sito web, conferenze e seminari*

L'Osservatorio per la Sicurezza Nazionale è un progetto
Ce.Mi.S.S. - Centro Militare di Studi Strategici ed Elsag - Finmeccanica

Al Progetto aderiscono

CROCE ROSSA ITALIANA

Ministero dell'Interno
Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile

Ministero delle Comunicazioni
iscom
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

ENAC
Ente Nazionale per l'Aviazione Civile

TELECOM ITALIA

SELEX Sistemi Integrati
Una Società Finmeccanica

TSF
Tele Sistemi Ferroviari

ITSTIME
Italian Team for Security, Terroristic Issues & Managing Emergencies
Università Cattolica del Sacro Cuore di Milano - Dpt Sociologia

Università degli Studi di Macerata

UNIVERSITÀ DEGLI STUDI DI SIENA
FACOLTÀ DI INGEGNERIA

Polizia di Stato

Stato Maggiore Esercito

Stato Maggiore Marina

Stato Maggiore Aeronautica

Arma dei Carabinieri

ARTICOLI

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

CROCE ROSSA ITALIANA

Croce Rossa Italiana

Articoli

Mobilitare il potere dell'umanità: il contributo della Croce Rossa Italiana alla sicurezza nazionale


Roma, 8 maggio 1955
Settimana della Croce Rossa

La missione della Croce Rossa è di prevenire ed alleviare in ogni circostanza le sofferenze degli uomini.
Nata dalla preoccupazione di assistere senza distinzione chiunque sia in stato di bisogno, essa ha rivolto il suo impegno alle situazioni in cui la dignità dell'uomo risultava più gravemente minacciata: dapprima sui campi di battaglia, affiancando i servizi sanitari delle Forze Armate nei compiti di assistenza a feriti e malati, successivamente intervenendo a favore delle vittime civili ed estendendo e sviluppando la sua azione umanitaria in favore della popolazione anche in tempo di pace e nelle situazioni di emergenza non causate dall'uomo.
Questa missione - ribadita nella Strategia d'azione 2010 e nell'Agenda per l'azione umanitaria del 2003 - non si limita alla dimensione operativa: il Movimento Internazionale della Croce Rossa e Mezzaluna Rossa attraverso le sue diverse componenti (Comitato Internazionale, Federazione Internazionale e Società Nazionali) è all'origine della codificazione e protagonista delle più importanti tappe di evoluzione del diritto umanitario dei conflitti armati, sostenitore dei diritti umani, promotore del diritto internazionale di risposta ai disastri, un nuovo settore normativo di cui sostiene lo sviluppo attraverso uno specifico programma internazionale (IDRL).
Facendo appello al patrimonio di principi e valori che accomuna gli uomini ad ogni latitudine e in ogni tempo, esso sollecita dunque non solo l'azione volontaria individuale, ma anche l'assunzione di responsabilità e il rispetto da parte di governi e istituzioni di quelle norme che, stabilite a tutela della persona, definiscono il rapporto tra il rispetto dell'uomo e le esigenze di ordine pubblico, di sicurezza e - in caso di conflitto armato - la necessità militare.

2006 - Nassiriya Visita al contingente della Croce Rossa Italiana

Una competenza tanto articolata da coprire l'ambito umanitario nella sua interezza (in tempo di pace e tempo di guerra e in tutte le tipologie di crisi) e la presenza capillare su scala nazionale e globale (quasi 100 milioni di aderenti distribuiti in oltre 190 paesi), rendono la Croce Rossa un partner prezioso in tutti i settori dell'azione statale che hanno implicazioni in campo umanitario, particolarmente in contesti - come quello attuale - in cui si fa labile e incerto il confine tra gli ambiti di applicazione dei diversi settori del diritto e le competenze dei diversi organismi chiamati alla loro attuazione.

La incessante, diuturna azione svolta in oltre 150 anni di storia, è infatti svolta - nel rispetto del principio di indipendenza - attraverso un rapporto privilegiato con i governi, che hanno riconosciuto, legittimato e favorito le attività delle Società Nazionali, conferendo loro uno status ausiliario dei pubblici poteri in ambito umanitario.
I principi fondamentali del Movimento - tra cui imparzialità, indipendenza e neutralità - permettono infatti alla Croce Rossa di agire nel rispetto delle prerogative statali in merito alla definizione delle politiche di difesa e alle scelte politico-stategiche, disegnando per l'azione umanitaria uno spazio autonomo, libero da qualsivoglia connotazione politica, religiosa o ideologica. Essa è così in grado di agire in piena autonomia e di supportare al contempo le istituzioni in campo umanitario, favorendo il mantenimento e il ritorno a condizioni di normalità e di stabilità in situazioni di tensione, conflitto, calamità naturale o tecnologica, disordini interni, nonché il pieno sviluppo dell'individuo e delle sue potenzialità.
La Croce Rossa accompagna dunque il cammino dell'uomo verso la piena espressione di una umanità responsabile, nell'ambito di un rapporto di solidarietà e tutela-rispetto verso chi necessita dell'aiuto, e di dialogo e fiducia nei confronti di chi di questo aiuto è responsabile.
Un ruolo così definito acquista una precisa e chiara valenza in relazione alla nuova concezione di sicurezza.
Ampliata dalla tradizionale nozione incentrata sull'obiettivo della difesa militare del territorio a quella attuale di human security, la sicurezza vede riconosciuta oggi in sede internazionale il suo carattere multidimensionale che comprende anche gli ambiti di intervento sopra delineati (tra i quali la sicurezza economica, alimentare, sanitaria, personale e ambientale). La Croce Rossa ha sempre considerato il valore strategico della sua azione umanitaria rispetto alla promozione e al mantenimento della pace e della sicurezza, consapevole che senza solidarietà e inclusione il potenziale umano dei vulnerabili si trasforma in una risorsa al servizio della illegalità e della criminalità. La promozione di questa nuova prospettiva a livello internazionale rappresenta un esplicito riconoscimento dell'importanza dell'azione della Croce Rossa, e del suo potenziale contributo nell'ambito di un sistema di sicurezza e difesa nazionale che intenda integrare diversi livelli d'azione, stabilendo un rapporto di complementarietà tra i contributi di attori diversi.
Se "il rispetto della dignità umana è senza dubbio il migliore investimento per la sicurezza a medio e lungo termine", come ha affermato in un recente intervento il Presidente del Comitato Internazionale, le oltre mille sedi della Croce Rossa Italiana distribuite su tutto il territorio (Comitati Regionali, Provinciali e Locali, con 160.000 volontari e 5.000 dipendenti) le risorse logistiche rese disponibili attraverso i 5 Centri in Interventi Emergenza e gli 11 Centri di Mobilitazione rappresentano indubbiamente una patrimonio irrinunciabile per la realizzazione di interventi non solo di prevenzione, ma anche di risposta alle emergenze a livello nazionale.
La Croce Rossa Italiana partecipa al progetto dell'Osservatorio per la Sicurezza Nazionale offrendo il suo contributo di forza umanitaria indipendente, e confermando il suo impegno negli importanti compiti di pubblica utilità di sua competenza.
Tra questi rivestono un particolare interesse ai fini del progetto OSN i seguenti:

- servizio di assistenza sanitaria e socio sanitaria in favore di popolazioni nazionali e straniere nelle occasioni di calamità e nelle situazioni di emergenza sia interne che internazionali;
- compiti di struttura operativa nazionale di Protezione Civile (come previsto dalla legge 225 del 1992 istitutiva del sevizio nazionale di PC e successivamente precisato nei protocolli d'intesa con la Presidenza del Consiglio dei Ministri, Dipartimento di Protezione Civile e con i Vigili del Fuoco del Soccorso Pubblico e della Difesa Civile del Ministero dell'Interno, rispettivamente del 2003 e del 2004);
- concorso nell'organizzazione e nella realizzazione - attraverso la stipula di apposite convenzioni - di servizio di pronto soccorso e trasporto infermi in ambito nazionale, regionale e locale e nel raggiungimento delle finalità ed nell'adempimento dei compiti del Servizio sanitario nazionale (attraverso l'impiego di personale sia volontario sia di ruolo, nonché di personale comandato o assegnato a svolgere attività e servizi sanitari e socio-assistenziali per conto dello Stato, delle regioni e degli altri Enti pubblici e privati);
- promozione della donazione del sangue, organizzazione di donatori volontari, collaborazione con le proprie strutture alle attività trasfusionali del Sevizio Sanitario Nazionale, anche attraverso la costituzione di idonee scorte di sangue e di emoderivati;
- collaborazione con le Forze Armate per il servizio di assistenza sanitaria;

- gestione del servizio di pronto soccorso nelle autostrade, nei porti e negli aeroporti dell'intero territorio nazionale su delega, mediante convenzione;

Ulteriori ambiti di competenza rivestono inoltre una importanza che merita particolare considerazione.
Mi riferisco alle attività di diffusione e di promozione dei principi umanitari posti a fondamento dell'organizzazione: rivolte a target differenziati (pubblica opinione, mass media, giovani) esse garantiscono la sensibilizzazione ai temi dell'aiuto e della solidarietà, attivando e potenziando la capacità collettiva di prevenzione e risposta alle emergenze.
Un valore cruciale assumono in particolare le attività di diffusione della normativa a tutela dei diritti umani in tempo di pace e di conflitto armato, che la Croce Rossa include oggi tra i suoi compiti statutari, che permettono al personale delle Forze Armate e di Polizia di agire - nell'esercizio delle rispettive competenze - con piena consapevolezza del loro mandato favorendo lo spontaneo rispetto del diritto e la legalità.
Da sottolineare infine la possibilità che - mediante concessione dello Stato, delle regioni e di enti pubblici - alla Croce Rossa venga delegato lo svolgimento di altri compiti, previsione che lascia ampio spazio allo sviluppo delle sue competenze e al pieno adeguamento della sua funzione nelle nuove necessità che la rapida evoluzione dello scenario dovesse palesare.
Per la realizzazione di queste attività la CRI si avvale di un patrimonio umano di migliaia di volontari attivi all'interno di sei componenti volontaristiche, ciascuna con caratteristiche specifiche e capacità di collaborazione e integrazione multifunzionale.
Il Corpo Militare e il Corpo delle Infermiere Volontarie, con funzioni ausiliarie delle Forze Armate e inquadrati nella struttura militare; i Volontari del Soccorso, sempre presenti nelle manifestazioni pubbliche, leaders nel pronto soccorso e nel trasporto infermi con autoambulanza oltreché specializzati in soccorso cinofilo, salvataggio in acqua, soccorso in montagna su piste di sci ed altre attività speciali; i Donatori Sangue che promuovono la donazione diffondendo la cultura trasfusionale nelle comunità e tra i singoli cittadini; il Comitato Nazionale Femminile che offre assistenza morale e materiale con particolare attenzione alle categorie più emarginate; i Pionieri che prestano il proprio servizio per la diffusione delle norme di primo soccorso, per attività di animazione, di segretariato sociale e di educazione alla pace.
Ogni componente ha capacità di mobilitazione e attivazione immediata del suo personale sia in tempo di pace che di conflitto armato, e a tal fine prepara il suo personale attraverso corsi di formazione specialistici in materia di primo soccorso, risposta ad attacchi NBCR, supporto psicologico in emergenza, diritti umani e diritto internazionale umanitario, educazione alla salute, educazione alla pace, assistenza a categorie vulnerabili.
Le attività realizzate sul campo a livello nazionale in caso di terremoti (Belice, Friuli, Campania, Valnerina), alluvioni (Sarno, Vibo Valentia, solo per citare le ultime), grandi eventi (Giubileo 2000, Funerali del Papa, Olimpiadi invernali 2006), al pari di quelle di carattere internazionale a sostegno dello sviluppo (Iran, Palestina, Bosnia-Erzegovina) e di risposta all'emergenza (Iraq, Afghanistan, Siria, Sri Lanka), sono testimonianza inequivocabile della capacità di intervento della Croce Rossa Italiana. Le recenti simulazioni anche pubbliche (quali "Emercampus" nel 2003 che ha visto la partecipazione di 3000 persone) la conferma delle sue potenzialità in interventi futuri.
La partecipazione della CRI in un sistema di sicurezza integrato possiede infine un potenziale implicito: la sua specifica identità la colloca in una posizione unica, che ne fa elemento indispensabile per la costruzione della fiducia tra tutte le risorse presenti e attivabili su scala nazionale in favore della sicurezza.
Grazie alla sua funzione di supporto all'apparato istituzionale (Ministero degli Interni, della Difesa e della Sanità) e di advocacy umanitaria al fianco delle organizzazioni della società civile e a sostegno dei più vulnerabili, la Croce Rossa Italiana può facilitare l'armonizzazione dei rapporti tra attori statali e non statali, preservando il sistema da minacce interne e scollamenti.
La diffusa percezione del suo simbolo e della sua presenza come garanzia di azione disinteressata, imparziale e qualificata, conferma il suo valore aggiunto anche in relazione alla collettività nel suo insieme.


11 dicembre 2005:
eletto Presidente della Croce Rossa Italiana

Il suo inquadramento nell'ambito del Movimento la rende parte di un network mondiale che offre un canale privilegiato di confronto con le esperienze di altri paesi e un modello per lo sviluppo di relazioni con governi e partner esterni (ONG e settore privato).
La Croce Rossa con la sua storia, le sue risorse e la sua identità, rappresenta dunque un fattore ineliminabile per la messa a punto e l'ottimizzazione di un "sistema paese" che sappia affrontare e rispondere in maniera adeguata ed efficace alle grandi sfide di oggi e di domani.

Massimo Barra

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Ministero delle Comunicazioni
Istituto Superiore delle Comunicazioni
e delle Tecnologie dell'Informazione

Articoli

Il contributo dell' Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione alla sicurezza nazionale

L'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM), costituito nel 1907, opera nell'ambito del Ministero delle Comunicazioni in qualità di organo tecnico-scientifico. In considerazione del suo ruolo di istituzione pubblica super-partes, il valore aggiunto dell'ISCOM, in termini di garanzia e competenza, è l'aspetto che contraddistingue i servizi di supporto tecnico e consulenziale forniti alle imprese e ai soggetti coinvolti nel settore delle telecomunicazioni. Il ruolo dell'ISCOM nel fornire servizi alle società ICT (Information & Communication Technology), agli enti governativi e agli utenti è molteplice, spaziando dalle attività di ricerca e sperimentazione alla formazione e al training nel settore delle telecomunicazioni.
Una delle missioni principali dell'ISCOM è il suo ruolo proattivo nelle attività di normazione nazionali e internazionali, al fine di assicurare maggior trasparenza e miglior accesso ai servizi da parte degli utenti, delle aziende manifatturiere e degli amministratori di reti e servizi.
L'attività di ricerca svolta dall'ISCOM è orientata allo sviluppo e al miglioramento dei servizi di telecomunicazione e di quelli legati alla tecnologia dell'informazione. Perseguendo queste finalità, le attività investono quasi tutte le aree del settore, dalla telefonia alla televisione, dall'elaborazione e trattamento del segnale, dall'architettura delle reti alla implementazione dei servizi.
L'ISCOM gestisce la Scuola Superiore di Specializzazione in Telecomunicazioni (attiva dal 1923), cui è affidata la specializzazione post-laurea nel settore delle comunicazioni elettroniche e delle tecnologie dell'informazione; l'ISCOM provvede anche alla formazione ed all'aggiornamento tecnico del personale appartenente al Ministero e ad altre pubbliche amministrazioni nei settori delle comunicazioni elettroniche e delle tecnologie dell'informazione, della sicurezza, della multimedialità e della qualità dei servizi, attraverso la pianificazione e realizzazione di percorsi formativi mirati all'acquisizione di competenze specialistiche.
L'ISCOM collabora con Organismi di Certificazione per le attività di verifica e controllo sui Sistemi di Qualità Aziendale in osservanza delle norme UNI EN ISO 9000, è impegnato nell'attività di controllo dei Laboratori Accreditati a fronte della norma UNI CEI EN ISO/IEC 17025 ed è Organismo Notificato per le attività di cui al Decreto Legislativo 9 maggio 2001 n. 269. Inoltre è Organismo Notificato ai sensi della Direttiva riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione ed è Competent Body ed Organismo Notificato in materia di compatibilità elettromagnetica. Nel 2002 è diventato l'Ente di Certificazione internazionale per conto del TETRA[1] MoU.
Tra i numerosi campi di attività dell'ISCOM, quello della sicurezza ICT sta acquisendo una rilevanza crescente. In quest'ambito, l'ISCOM gioca un ruolo trainante in vari contesti; in particolare, in virtù di un decreto della presidenza del Consiglio dei Ministri, l'ISCOM è Organismo di Certificazione della sicurezza di prodotti e sistemi ICT commerciali (OCSI). L'OCSI (Organismo di Certificazione della Sicurezza Informatica) emette certificazioni di sicurezza di prodotti e sistemi ICT secondo gli standard Common Criteria e ITSEC (Information Technology Security Evaluation Criteria).
L'ISCOM è anche coinvolto nella diffusione della cultura della sicurezza ICT in vari ambiti (pubblica ammini strazione, utenti residenziali, infrastrutture critiche ecc) attraverso lo sviluppo di un piano coordinato di

1 TETRA: Terrestrial Trunked Radio

aggiornamento e sensibilizzazione.
Inoltre, l'ISCOM ha un ruolo di promotore e leader di varie iniziative mirate a innalzare il livello nazionale di sicurezza in ambito ICT, raccogliendo le esperienze e le competenze dei principali soggetti che operano nel settore ICT. Tra queste iniziative possiamo ricordare la redazione di tre linee guida, in lingua inglese e italiana, su "La qualità di servizio nelle reti ICT", "Analisi dei rischi e strategie di protezione per la sicurezza delle reti", e "Sicurezza delle reti nelle infrastrutture critiche", condotta con il contributo di esperti dal modo dell'industria e delle istituzioni.
Il primo volume si rivolge agli operatori e agli utenti finali di reti di comunicazioni, sia domestici che business. Viene affrontato il tema della qualità dei servizi partendo dal principio che la qualità è un aspetto imprescindibile nella caratterizzazione di prodotti e servizi di qualunque tipo. Scopo del documento è illustrare in quale modo l'utilizzatore finale possa valutare la reale qualità attesa per un certo tipo di servizio. L'utilizzatore finale dovrebbe, infatti, essere messo nelle condizioni di valutare se il tipo di servizio e di infrastruttura di rete è rispondente alle proprie esigenze di qualità. Il modello sviluppato nel volume propone gli strumenti con i quali i fornitori di servizio possono offrire all'utente informazioni oggettive in relazione alle prestazioni di rete erogate (es. effettiva velocità di download disponibile all'utente finale). In tal modo, l'utente finale e gli addetti ai lavori potranno opportunamente valutare prestazioni tecniche esistenti sul mercato. Il documento procede all'individuazione dei principali parametri per la definizione e il rilevamento della qualità dei servizi con particolare riferimento alla "larga banda" in linea con i principi contenuti nel Codice delle Comunicazioni Elettroniche (decreto legislativo 259/03).
Il secondo volume, sulla "Analisi del rischio e strategie di protezione per la sicurezza delle reti", ha lo scopo di fornire un quadro d'insieme aggiornato delle problematiche di sicurezza e delle relative soluzioni concernenti l'utilizzo di Internet e delle reti geografiche e locali ad essa connesse. Il volume è rivolto agli utenti business: liberi professionisti e studi professionali, piccole e medie imprese, grandi imprese. Nel caso degli studi professionali e delle PMI (Privilege Management Infrastructure), spesso non esiste, al loro interno, una figura professionale dedicata alla sicurezza: al massimo esiste un responsabile ICT. A lui sono dedicati molti capitoli del volume. Nel caso delle grandi imprese il destinatario del volume è il responsabile della sicurezza. Il volume può essere di utilità anche per il top management, per fornire una sensibilizzazione al problema e una percezione netta che le soluzioni esistono e sono sostenibili.
La terza linea guida rappresenta la sintesi delle attività condotte dal Gruppo di Lavoro sulle "Infrastrutture Critiche". Il gruppo di lavoro nasceva dalla necessità di analizzare le implicazioni sulla continuità di esercizio e sulla sicurezza delle infrastrutture critiche rispetto al mutato contesto socio-economico e tecnologico che ha visto crescere l'importanza e la crucialità delle infrastrutture di telecomunicazione rispetto a tutte le infrastrutture critiche nazionali. Questo si riflette in un crescente livello di interdipendenza fra le diverse infrastrutture, in gran parte dovuto alla diffusione delle tecnologie ICT. Inoltre occorre rilevare un aumento delle minacce che affliggono le infrastrutture sia legate a fenomeni naturali che ad azioni delittuose, ed in special modo terroristiche.
L'attività del Gruppo di Lavoro, costituito da rappresentanti delle più importanti pubbliche amministrazioni, insieme a rappresentanti di alcuni dei maggiori operatori di Infrastrutture Critiche Nazionali (Critical National Infrastructures, o CNI) e società specializzate in questo campo, si concentra sul ruolo delle infrastrutture di TLC rispetto alla sicurezza e alla continuità del servizio all'interno delle CNI.
Il Gruppo di Lavoro, mettendo a frutto le diverse esperienze dei componenti, ha cercato di coagulare le esigenze e le possibili soluzioni, al fine di fornire ai gestori di CNI quelle linee guida, o "best practice", che possano indirizzare verso un migliore e più consapevole uso dei sistemi di comunicazione necessari e disponibili. Il principale obiettivo del Gruppo di Lavoro è quello di aiutare le istituzioni a comprendere meglio i problemi associati alla protezione delle infrastrutture critiche e di fornire delle indicazioni di base per l'identificazione dei requisiti organizzativi per aumentare la robustezza delle infrastrutture critiche.
Sono in fase di redazione sei ulteriori linee guida; esse concerneranno degli approfondimenti sull'analisi dei rischi, l'outsourcing dei servizi di sicurezza, la Qualità del Servizio nell'UMTS (Universal Mobile Telecommunication System), la Qualità del Servizio in reti a larga banda, la gestione delle emergenze locali e la certificazione di sicurezza.

Luisa Franchina

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Ministero dell'Interno
Dipartimento dei Vigili del Fuoco del
Soccorso Pubblico e della Difesa Civile

Articoli

Direzione Centrale per la Difesa Civile e le Politiche di Protezione Civile

Il Ministero dell'Interno, per definizione istituzionale, persegue l'obiettivo della Sicurezza nel suo significato più generale. In particolare, il Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile assolve, all'interno di questa missione, un ruolo determinante sia attraverso il Corpo Nazionale dei Vigili del Fuoco sia attraverso la Direzione Centrale della Difesa Civile.
Considerate dunque le finalità dell'Osservatorio, la partecipazione al progetto appare una interessante opportunità, che deve essere raccolta nell'interesse di questa Amministrazione e degli altri interlocutori istituzionali.
Come è noto, la Difesa civile è il sistema di sicurezza chiamato a garantire, in situazioni di difficoltà, la continuità di Governo e la salvaguardia degli interessi vitali dello Stato, sostenendo la capacità economica, sociale, produttiva, logistica ed infrastrutturale della nazione. Nei confronti della popolazione, la Difesa civile opera per la riduzione dell'impatto di un evento mirando a limitarne, per quanto possibile, il suo coinvolgimento.
Ed è proprio in questa definizione la risposta al perché della nostra presenza nell'Osservatorio. Senza rinunziare alla responsabilità primaria che l'Ordinamento ci affida, questo Dipartimento vede l'Osservatorio come un importante riferimento nel più generale contesto della Sicurezza nazionale, proprio perchè scevro dai rigori del sistema istituzionale, eppure, proprio per la sua composizione, fortemente rispettoso di quello stesso sistema.
Da questo Forum ci attendiamo dunque un contributo di conoscenza, di approfondimento e un'occasione di contatti di alta qualificazione certamente utili per l'assolvimento dei compiti del Dipartimento e all'Osservatorio cercheremo di dare tutto il supporto che deriva da una continua attività in campo nazionale ed internazionale e dalla conoscenza che discende da una presenza sul territorio estremamente articolata e capillare.
La richiesta di Sicurezza, in Italia come in tutte le società avanzate, assume significati diversi a seconda delle esigenze prevalenti, dalle più manifeste alle meno evidenti. Alle molteplici esigenze l'Italia ha risposto istituendo sistemi di sicurezza diversificati e ognuno di questi sistemi ha percorso la sua strada sviluppando propri assetti organizzativi e proprie tecnologie, arrivando, ognuno per la sua parte, a notevoli livelli di efficienza. Spesso, però, questi sistemi tendono a chiudersi nei rispettivi ambiti di competenza, considerando l'aspetto della sicurezza a cui tendono come quello prevalente. Spesso, cioè, ci si dimentica che l'obiettivo è comune e ci si dimentica soprattutto che nessun sistema è isolato o isolabile dagli altri. L'esigenza emergenziale di un sistema non esclude infatti che possa, nelle sue conseguenze o convergenze, richiedere l'attivazione di un altro o di più sistemi, senza che tra essi debbano nascere forme di interferenza o addirittura di competizione.
La Difesa civile è certamente in questo contesto il sistema sicurezza più generico nella definizione delle sue competenze, che sono di carattere generale, quasi onnicomprensive, nel caso di crisi nazionali, o molto specifiche, con localizzazioni estremamente definite eppure molto complesse, come nel caso di un attacco

terroristico.
Per questo, forse più degli altri ambiti, la Difesa civile avverte l'esigenza di una forte comunicazione, mirando alla sinergia, se non addirittura alla complicità della risposta.
La prospettiva di affrontare i temi della Sicurezza nella molteplicità delle sue dimensioni, prescindendo quasi dalla particolarità delle discipline specifiche, nell'ottica di un obiettivo unico e condiviso è vista, quindi, da questo Dipartimento come una importante occasione di crescita a cui non è possibile rinunciare. L'intesa tra gli attori, che gestiscono gli strumenti della Sicurezza, contribuirà sicuramente al perfezionamento della risposta che ciascuno di essi è chiamato ad offrire nell'ambito e nel rispetto delle specifiche competenze.
In definitiva, la cultura della sicurezza che l'Osservatorio intende perseguire è un'esigenza che si profila come prioritaria certamente per chi, come la Difesa civile, opera sul territorio nella previsione di eventi che sfuggono a qualsiasi previsione e che trovano la propria organizzazione preventiva in un sistema di pianificazioni estremamente generico per l'indeterminatezza dei suoi scenari e l'inafferrabilità dei suoi obiettivi.
Inoltre, affiancandosi alla comunicazione istituzionale già presente negli Organismi nazionali di coordinamento (Nucleo Politico Militare, Commissione interministeriale tecnica per la difesa civile, Unità di crisi presso il Dipartimento della pubblica sicurezza) l'Osservatorio potrà rappresentare un momento di valorizzazione dell'approfondimento multidisciplinare consentendo al suo interno di condividere conoscenze tecnico-sociologiche e socioculturali, per una risposta adeguata ad un "nemico" agguerrito ed organizzato.
La sinergia nelle risposte.
E' questa, in estrema sintesi, la scelta che consideriamo prioritaria e la condivisione di questa esigenza deve rappresentare un'ipotesi di lavoro per una nuova cultura istituzionale fondata sul principio della sacralità dell'interesse pubblico in nome del quale tutti devono rendere disponibili le proprie conoscenze e il supporto della propria organizzazione, seppure nel rispetto delle specificità volute dal nostro Ordinamento.

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Ente Nazionale Aviazione Civile
Direzione Progetti, Studi e Ricerche
Ufficio Tecnologie Aeroportuali

Articoli

Analisi del rischio e tecnologie nella security aeroportuale.

Introduzione

Nel 1968, il 22 luglio di quell'anno, il terrorismo aereo esordì nell'aviazione civile. Tre membri del FPLP (Fronte Palestinese per la Liberazione della Palestina) dirottarono un aeromobile El Al sulla rotta Roma - Tel Aviv, e ottennero come riscatto la liberazione di numerosi palestinesi prigionieri in Israele. [2].
Dall'inizio del 1968 a oggi altri attacchi, con differenti modalità e finalità, hanno evidenziato drammaticamente le conseguenze della vulnerabilità dell'Aviazione Civile [1].
Gli aerei e gli aeroporti continuano ad essere un obiettivo privilegiato "soft target" del terrorismo internazionale in quanto permettono agli stessi di ottenere, con mezzi limitati e nell'esercizio di guerra asimmetrica, un grosso impatto mediatico della loro azione, effetti devastanti soprattutto sulla percezione di sicurezza dei cittadini ed effetti rilevanti sui sistemi economici [3,4].
L'ENAC, per il suo ruolo di Autorità Nazionale per l'Aviazione Civile, insieme ad altre amministrazioni preposte alla sicurezza dello Stato, ha avuto il delicato compito di dover dover affrontare in prima linea le problematiche della security nel trasporto aereo, sotto il diretto coordinamento della Presidenza del Consiglio dei Ministri.
L'ENAC inoltre alla presidenza del CISA (Comitato Interministeriale di Sicurezza per il Trasporto Aereo e degli Aeroporti), è continuamente impegnata ad individuare e migliorare le disposizioni relative ai controlli da effettuare sui passeggeri, bagagli, voli ritenuti sensibili, aree aeroportuali ritenute a rischio, nel rispetto delle indicazioni provenienti dalla normativa internazionale ICAO e dagli studi dell'ECAC (che già da tempo ha istituito una apposita Security Task Force).

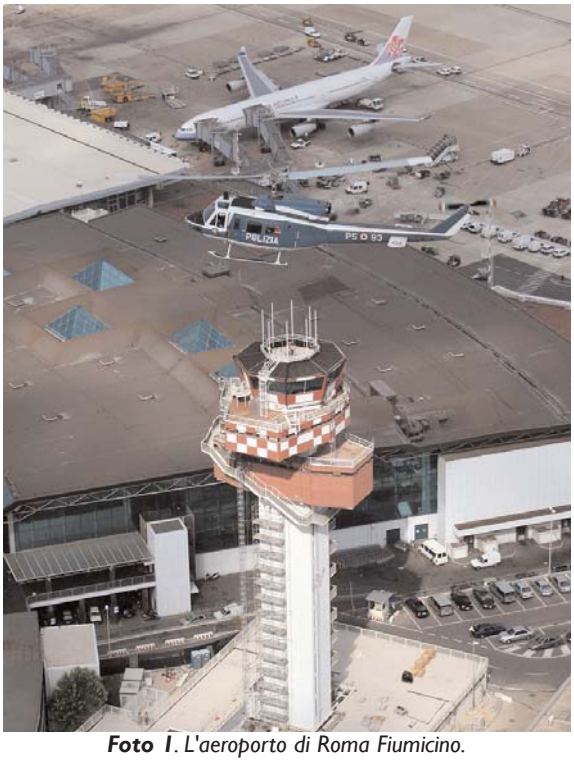


***Foto 1**. L'aeroporto di Roma Fiumicino.*
Foto di Riccardo Braccini

In particolare l' ENAC, nell'ambito della propria riorganizzione interna, ha dato maggiore enfasi al settore della sicurezza collocando la Direzione Security in staff alla Direzione Generale e potenziando le competenze dell'ex Servizio Progetti che è stato trasformato in "Direzione Progetti, Studi e Ricerche". Nell'ambito della predetta direzione opera una unità organizzativa ad alta specializzazione, l'Ufficio Tecnologie Aeroportuali, che si occupa, in stretta sinergia con le altre strutture dell'ENAC, di assicurare il governo del know how sugli aspetti tecnologici di sistemi e impianti aeroportuali finalizzati alla safety (AVL, segnaletica, ecc.) e security

(sistemi antintrusione, ecc.) coordinando le attività di approvazione dei progetti e di ricerca.
A tale intensa attività dell'Ente regolatore, rispecchiata in particolare nel Programma Nazionale di Sicurezza e nelle circolari della serie security pubblicate, è corrisposto negli ultimi anni un notevole volume economico investito dai principali operatori e gestori aeroportuali negli adeguamenti delle infrastrutture aeroportuali e degli aeromobili necessari a migliorare i livelli della security.
Le soluzioni migliorative in corso di implementazione includono controlli innovativi sui bagagli da stiva, individuazione avanzata di esplosivi, identificazione e controlli biometrici, check-in remoti, procedure di risk based threat perception analysis, utilizzo di procedure di in-flight security con gli sky marshals, evoluzione tecnologica e irrobustimento delle porte della cabina di pilotaggio con ulteriore possibilità di videomonitoraggio. Sono state prese in considerazione inoltre anche le possibilità di armare e addestrare gli equipaggi di volo a lotta non armata e la ricerca è attualmente in corso su alcune tipologie di queste contromisure [5].

Foto 2. *Aeroporto di Milano Linate.Impianto di smistamento e controllo bagagli: apparecchiatura EDS (Explosive Detection System). Foto di Galileo Tamasi.*

L'ENAV, Società Italiana per l'Assistenza al Volo ha suggerito di recente l'impiego di radar ad alta risoluzione, in corso di sperimentazione, capaci di identificare bersagli anche piccoli in maniera da "illuminare" i piazzali e la linea dei gates.
In particolare impianti e sistemi per la security sono stati migliorati nella prospettiva di minimizzare l'efficacia di atti illegali, sovrapponendosi o sostituendo impianti inadeguati a fronteggiare le nuove minacce. Le principali azioni si sono svolte nell'ottica di migliorare continuamente quanto già esistente negli aeroporti e implementare il principio della "defense in depth" già applicato nel settore della sicurezza di impianti tecnologici complessi [6].
Sistemi di controllo perimetrale, impianti di smistamento e controllo bagagli, centri di gestione di crisi, e altre installazioni, proprio per la loro complessità e per la diversità degli attori coinvolti nel loro utilizzo, richiedono nella loro progettazione e loro gestione durante il loro ciclo di vita, un approccio sistemico e multidisciplinare.
Scopo del presente lavoro è pertanto quello di mostrare in che modo l'analisi di rischio con i suoi strumenti possa essere utilizzata sia nel progetto (risk based design) che nella valutazione di impianti e sistemi per la security aeroportuale.

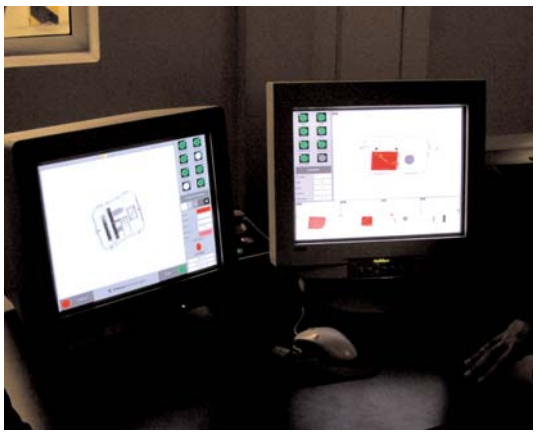


Foto 3*. Aeroporto di Milano Linate. Impianto di smistamento e controllo bagagli: postazione operatore per l'esame dei bagagli. Foto di Galileo Tamasi.*

Rischio: un approccio integrato per il trasporto aereo

In ogni tecnologia, come anche in quella di impianti e sistemi per la security per il trasporto aereo, la possibilità relativa di fallimento deve essere misurabile e predicibile.
Se il problema viene affrontato in modo diretto e con gli strumenti adatti possono sostituirsi decisioni inefficaci con altre derivanti da una classificazione di priorità ben definita.
Il rischio è un argomento complesso e inquadrabile da diversi punti di vista, ma deve essere analizzato con metodologie appropriate per agevolare il processo decisionale.
Storicamente la ricerca si è occupata del risk assessment e del risk management nel settore della safety per

la prevenzione degli incidenti aerei, nei grandi rischi naturali, nei rischi di impresa, nei rischi di operazioni finanziarie.
In queste aree le diverse organizzazioni hanno usato processi molto sistematici e strumenti per comprendere e classificare in ordine di importanza i diversi rischi, soprattutto quelli con conseguenze catastrofiche. I rischi nel settore della security sono solo un'altra ampia categoria di rischi con conseguenze potenzialmente catastrofiche. [11,12].
Le misure di security oggi esistenti sugli aeroporti mondiali non possono assicurare la protezione totale verso tutte le tipologie di minacce.
Certamente il massimo della sicurezza lo si ottiene con una profonda blindatura del sistema, ma questo, com'è facile intuire, significherebbe quasi paralizzare il trasporto aereo.
Un approccio corretto a tale problematica è pertanto l'utilizzo delle metodologie di risk assessment e risk management, così come del resto ampiamente fatto nel settore della safety. Spesso safety e security sono viste naturalmente come due discipline indipendenti con obiettivi divergenti e diverse esperienze richieste ai soggetti attori. Ma è di tutta evidenza che l'obiettivo di safety e security, pur seguendo percorsi differenti, converge nell'unico scopo di proteggere personale, passeggeri e incolumità pubblica. [7]
Anche l'ICAO nell'Annesso 17 e nel documento applicativo Doc 8973 [8,9] suggerisce un approccio mediante metodologie di analisi e gestione del rischio, evidenziando gli strumenti di threat assessment e di risk management ove tali metodologie hanno entrambe un approccio analitico e semiquantitativo basato su punteggi numerici.
Al fine di chiarire le potenzialità degli strumenti accennati verranno pertanto di seguito introdotti i concetti chiave delle metodologie per valutare qualitativamente e quantitativamente il rischio security nel settore dell'aviazione civile e il processo di risk assessment basato sui concetti di minaccia (threat), criticità (criticality) e vulnerabilità (vulnerability) evidenziando le loro specifiche interrelazioni nella determinazione del rischio complessivo.
Verrà quindi evidenziato in che modo il risk assessment può essere usato come strumento decisionale per la progettazione e il miglioramento di impianti e sistemi nel settore security, consentendo di effettuare un bilancio tra conseguenze attese e i costi sostenuti per l'implementazione di efficaci misure sul piano della security.

Analisi e gestione del rischio: il paradigma ICAO

L'ICAO, da sempre sensibile ai problemi della security, a seguito dei recenti attentati terroristici degli ultimi anni, ha avvertito l'urgenza e la necessità di ristabilire l'integrità del sistema aviazione civile incontrando nel 2001 i rappresentanti di 32 nazioni per discutere le nuove misure di sicurezza.
A tale fine l'ICAO ha raccomandato l'Universal Security Oversight Audit Program (USOAP) e ha fatto confluire le sue regole e raccomandazioni nelle Standard Recommended Practices (SRPs). Misure adeguate sono state prontamente adottate e sono riportate nella settima edizione dell'Annesso 17 e nei suoi DOC applicativi evidenziando in particolare i concetti di threat assessment e risk management.[8,9,10].
I principi fondamentali del risk assessment sono basati sul presupposto che sebbene i rischi non possono essere eliminati, le contromisure impiegate possono invece ridurlo e mitigare le conseguenze di un attacco.
Il risk assessment è un processo analitico e sistematico che consente di valutare la probabilità che una minaccia si concretizzi in una azione negativa su una infrastruttura, persone o funzioni critiche del sistema aeroportuale e consente di identificare le azioni che riducono il rischio e mitigano le conseguenze di un attacco.
La procedura del risk assessment è costituita da tre sottoprocedure primarie:

- threat assessment (verifica del livello di minaccia)
- vulnerability assessment (verifica del livello di vulnerabilità)
- criticality assessment (verifica del livello di criticità)

Il threat assessment identifica e valuta le minacce incombenti, ed è basato su vari fattori che possono tenere in considerazione la capacità di organizzazione di un gruppo, le motivazioni politiche, le capacità di reperire fondi e utilizzare equipaggiamenti speciali.
Il vulnerability assessment è una verifica che identifica le debolezze che possono essere sfruttate da

malintenzionati o da terroristi e suggerisce modifiche per eliminarle o ridurle a livelli accettabili.
Il criticality assessment è una verifica che mira ad identificare in modo sistematico le infrastrutture presenti in aeroporto in funzione del loro costo di realizzazione o ricostruzione, del loro valore di acquisto, dei ricavi diretti e indiretti che consentono di realizzare, del loro grado di importanza funzionale nell'ambito della missione svolta.
L'analisi del rischio, costituita dalle tre sottoprocedure illustrate, consente quindi di valutare la probabilità di accadimento degli effetti negativi correlati al concretizzarsi delle minacce, relativamente ad ogni componente del sistema aeroportuale, individuando la corrispondente perdita economica attesa su base annuale.
Nella maggior parte dei casi quindi, l'analisi di rischio, conduce ad una probabile perdita economica attesa ALE (Annual Loss Expectancy) che consente di realizzare, da un punto di vista degli strumenti decisionali, un immediato bilancio economico tra l'impatto dei rischi e il costo delle contromisure da implementare.
La sola comprensione e misura del rischio non è tuttavia sufficiente a fronteggiare le minacce, è necessario infatti un adeguato sistema di *security*Risk Management che consenta di implementare e mantenere attive nel tempo tutte le contromisure, confinando attraverso un processo di miglioramento continuo, il rischio entro valori ritenuti accettabili.
Il risk management si configura quindi quale migliore metodologia per organizzare una risposta effettiva a tutte le potenziali azioni illegittime e attacchi terroristici.
Gli elementi chiave del *security* risk management sono illustrati nella Figura 1 riportata di seguito [10,11,12].

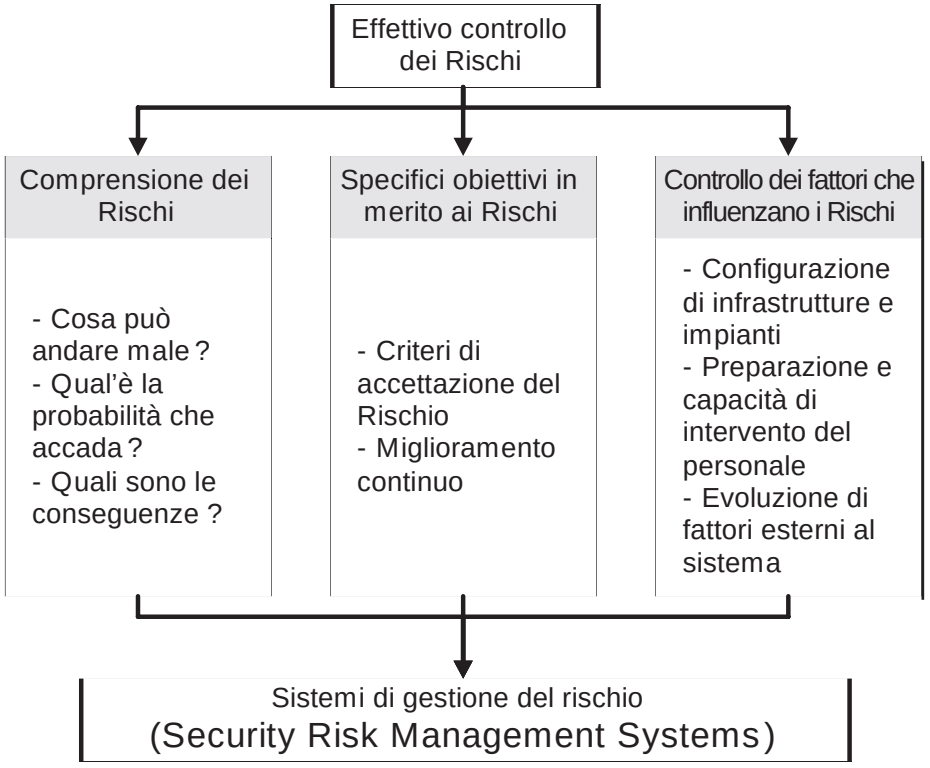


Figura 1. Security Risk Management

Analisi qualitative o analisi quantitative ?

I rischi nel settore della security richiedono un approccio differente da quello dalla safety, ma si possono applicare quasi tutti i concetti fondamentali dell'analisi del rischio. Gli attacchi terroristici, il sabotaggio e altre azioni illegittime sono differenti tipi di minacce, ma si configurano allo stesso modo di altre tipologie di eventi inizatori.
In una analisi di rischio relativa alla security aeroportuale, le metodologie di analisi sono differenti, e molte

varianti sulle procedure di valutazione del rischio residuo possono essere applicate.
Anche la metrica per esprimere il rischio residuo può essere espressa in modo qualitativo o in modo quantitativo determinando i valori economici che possono essere persi, l'impatto complessivo sulla dinamica dei trasporti aerei, le contromisure da implementare a fronte delle criticità evidenziate.
In ogni caso l'analisi deve consentire di stabilire:

a) il livello di rischio attuale
b) le possibili conseguenze di attacchi
c) le azioni da intraprendere se il rischio residuo è superiore ai valori accettabili

Solitamente le analisi di rischio quantitative tendono a confrontare le possibili perdite economiche con i costi dei sistemi di sicurezza che costituiscono adeguate contromisure. Le valutazioni quantitative possono essere realizzate mediante le seguenti relazioni generalizzate:

(1) Rischio = Frequenza (F) x Conseguenza (C)

(2) Frequenza (F) = Frequenza degli eventi iniziatori x Probabilità di fallimento di tutte le misure di protezione

(3) Rischio = [Minaccia (Threat) x Vulnerabilità (Vulnerabilità)] x Criticità (Criticality)

(4) R=[TxV]xC

Analisi di rischio

Dove T (Threats) è la frequenza attesa della tipologia di minaccia in esame, C (Criticality) sono le conseguenze degli attacchi e i valori economici perduti in conseguenza dell'attacco, V (Vulnerabilità) è la vulnerabilità dell'area critica considerata e quindi la probabilità che tutte le misure di protezione vengano superate.
Esistono ovviamente altre formulazioni che possono essere espresse sotto forma di legami funzionali differenti, ma la precedente è quella più utilizzata e più versatile.
Nella Figura 2 riportata di seguito è illustrato un approccio per condurre il risk assessment :
Ovviamente l'approccio quantitativo non è l'unica via per realizzare l'analisi di rischio, e una delle sfide più significative attualmente in corso è quella di definire dei criteri generalizzati per determinare quale livello di precisione e di tipologia di analisi sia appropriato per prendere adeguate decisioni.
L'alta o media precisione può non essere necessariamente raggiungibile, in particolar modo quando una tecnologia che consente di raggiungere una particolare difesa antiterroristica non è definita o ancora in corso di sviluppo. L'obiettivo da raggiungere è quindi quello di realizzare il minimo livello di analisi necessario a fornire informazioni adeguate necessarie a maturare le decisioni.

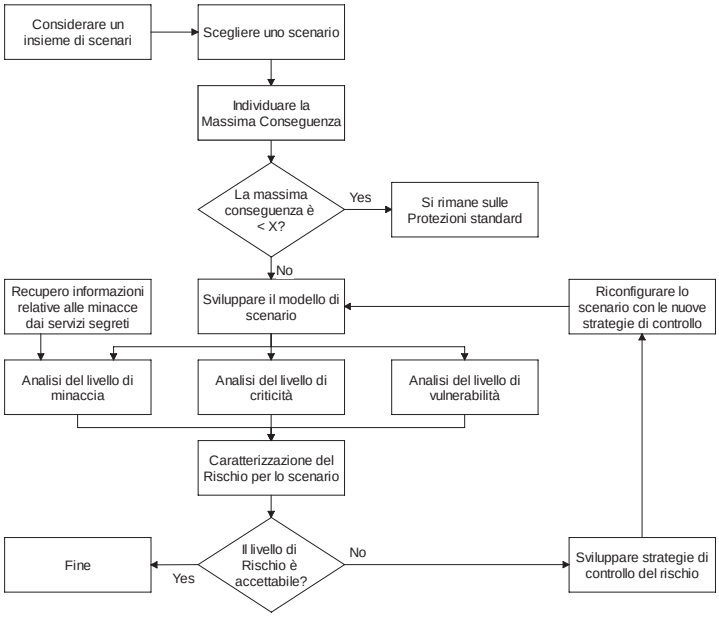


Figura 2. Procedura per realizzare il Security Risk Assessment

L'analisi qualitativa che invece viene condotta attualmente in Italia e anche in Europa, è basata su Security Audit costituiti prevalentemente da liste di controllo (check list) che sono elaborate dall'ENAC con il supporto della legislazione italiana e internazionale vigente. Le liste di controllo e le procedure ispettive sono ulteriormente integrate per tenere conto delle raccomandazioni di organismi tecnici del settore (IATA).
Il Security Audit riguarda in particolare i seguenti settori critici per la security:

- Organizzazione e amministrazione dei sistemi security a livello nazionale e cooperazione con altri stati
- Organizzazione e amministrazione dei sistemi security a livello aeroportuale
- Controllo degli accessi alle strutture aeroportuali
- Passeggeri e bagaglio a mano
- Bagagli da stiva
- Aeromobile e procedure di volo
- Cargo, posta e catering
- Capacità di risposta ad atti di interferenza illegittima e pianificazione dell'emergenza

I risultati vengono espressi qualitativamente attraverso livelli predefiniti di conformità alle norme vigenti. Per ogni area viene espresso il livello di vulnerabilità rilevato e le contromisure necessarie da implementare. Lo strumento con cui viene completata l'analisi del rischio è un report che viene sottoposto alle società di gestione aeroportuali che sono obbligate entro la scadenza prevista a risolvere le criticità evidenziate dall'analisi.

Conclusioni e prospettive future.

Le realtà del XXI secolo - l'economia globale, l'interdipendenza dei sistemi e le crescenti minacce terroristiche in uno scenario di guerra asimmetrica - necessitano di un ampio e bilanciato approccio alla sicurezza del sistema di trasporto ed in particolare di quello aereo.
L'insieme di scenari di attacco verso obiettivi sensibili in ambito aeroportuale può essere esaminato attraverso l'analisi di rischio e le sue sottoprocedure. Ogni scenario indagato è caratterizzato dal livello di rischio, che viene poi specificato in termini di perdite annuali attese, le quali consentono di realizzare un bilancio di investimenti per dotare l'aeroporto di adeguate contromisure e mitigare l'esposizione al rischio entro livelli ritenuti socialmente accettabili.
Soluzioni creative, nuove tecnologie, adeguamento dei sistemi di sicurezza allo stato dell'arte del progresso scientifico, che siano anche praticabili e sostenibili, richiedono il contributo di diverse professionalità, abilità interdisciplinari e una collaborazione tra strutture di governo e industria al fine di assicurane lo sviluppo, l'implementazione e la gestione.
Le minaccie al sistema di trasporto aereo stanno diventando sempre più sofisticate e risulta necessaria la condivisione di conoscenze ed esperienze integrate per offrire in modo continuo e aggiornato nuove informazioni, prospettive di sviluppo e best pratices nella security.
Strategie consolidate ed efficaci sono necessarie altresì per affrontare i problemi di security in modo da individuare le minacce e minimizzare i potenziali impatti. Una solida metodologia analitica come quella dell'analisi del rischio, già utilizzata nel settore della safety, è sicuramente l'elemento cruciale che consente di elaborare piani, azioni, e priorità per soluzioni adeguate.
Il processo di analisi dei rischi è una attività continua che richiede la produzione di scenari verosimili e di modelli che hanno necessità di miglioramento al fine di consentire all'autorità aeronautica, alle altre forze di stato e ai gestori aeroportuali di scegliere le giuste soluzioni e finanziarle.
Quanto evidenziato nel presente lavoro sull'analisi del rischio, chiarisce la necessità di identificare i potenziali rischi, comprendere le interrelazioni nei sistemi coesistenti in una infrastruttura aeroportuale e capire come le vulnerabilità possano amplificarsi per effetto di tali interdipendenze.
Più il sistema aeroportuale diviene complesso, come nel caso degli Hub aeroportuali di Malpensa e Fiumicino, e più aumenta la loro vulnerabilità e le conseguenze di azioni illegittime o terroristiche o di sabotaggio.
Le metodologie di analisi del rischio consentono di identificare interdipendenze fisiche, geografiche, informatiche e logiche, consentono altresì di esaminare i livelli di efficacia dei sistemi di protezione e anticipare le conseguenze negative.

L'analisi di rischio consente inoltre di effettuare un bilancio di costi e benefici per ogni soluzione necessaria a mitigare le vulnerabilità degli aeroporti, quali sistemi di tracciamento GPS, controlli biometrici, EDS e altri sistemi di identificazione. L'approccio tecnologico unito ad una integrazione sistematica dei fattori umani, fisici, informatici e operativi consentono di migliorare la risposta delle infrastrutture a minacce impreviste.
La security non è più un problema da risolvere a posteriori, ma dovrà essere integrata nel progetto, nello sviluppo e nella operatività del sistema aeroportuale
Non meno importante e altrettanto ben evidenziato dall'analisi del rischio sono lo studio della criticità delle conseguenze e l'adozione di una immediata e ben pianificata risposta in condizione di attacco che congiuntamente sono in condizioni di mitigare le conseguenze a breve e a lungo termine di un disastro. Piani di emergenza, personale ben addestrato e forti relazioni e chiarezza di ruoli e responsabilità tra le diverse entità operanti nel sistema aeroportuale sono in grado di minimizzare adeguatamente le conseguenze disastrose di un emergenza.
La gestione del rischio nel settore dei trasporti ed in particolare del trasporto aereo richiede collaborazione tra settori pubblici e privati e tra università e industria. La nascita dell'Osservatorio per la Sicurezza Nazionale è una occasione imperdibile per convogliare un ampio spettro di competenze e specializzazioni che potranno essere focalizzate sulle problematiche emergenti. Nel suo ruolo l'Osservatorio è direttamente connesso con il mondo reale e con le organizzazioni ed enti che sviluppano strategie innovative e potrà rappresentare il nodo centrale di scambio per valutare i fabbisogni di sicurezza dei cittadini, valutare gli approcci tecnologici alle problematiche e stimolare la crescita di nuove soluzioni creative.
La partecipazione dei diversi attori coinvolti a tale Osservatorio non potrà che beneficiare delle positive ricadute di una tale sinergica collaborazione con tutti gli attori coinvolti sul territorio nazionale. Collaborazione, che rappresenta di fatto l'elemento chiave per dare al cittadino adeguata protezione e qualità della vita.

Ringraziamenti
Si ringrazia la Dott.ssa Anna La Rosa per aver incoraggiato lo sviluppo del presente lavoro.

Paolo Mazzaracchio, Galileo Tamasi

***Foto 4**. Aeroporto di Milano Malpensa. Corto finale su pista 34R: le linee di atterraggio possono essere un bersaglio di entità ostili attrezzate con Manpads. Foto di Galileo Tamasi.*

Bibliografia

[1] Gerald L. Dillingham (2003) Post-September 11th Initiatives and Long-Term Challenges, United States General Accounting Office, New York, USA, April 1 2004. pp. 1-30.
[2] Choi, Jin-Tai (1994) Aviation Terrorism: Historical Survey, Perspectives, and Responses, Londra, UK, pp. 1-60
[3] Cletus C., Coughlin, Jeffrey P. Cohen, Sarosh R. Khan (2002) Aviation security and terrorism: a review of the economic issues, Working Papers 2002-009A, Federal Reserve Bank of St. Louis, St.Louis, USA, April 1 2004. pp. 1-16
[4] Harumi Ito, Darin Lee (2003) Assessing the Impact of the September 11 Terrorist Attacks on U.S. Airline Demand, Brown University Economics Department, Providence, USA, 2003. pp. 1-24.
[5] Gerald L. Dillingham (2003) Progress Since September 11, 2001, and the Challenges Ahead, United States General Accounting Office, New York, USA, September 9 2003. pp. 1-50.
[6] A. Cointet, J.Marion (2005) Defence in Depth & Uman Factors within Transport Systems, in the Proc. of ESREDA Annual Seminar: System Analysis for a More Secure World 2005, ISPRA, Italy,26-26 October 2005, pp. 193-210
[7] A. Saleem, D.Forbes (2005) Case Study in the use of an Integrated System Safety ans Security (IS3) Methodology, in the Proc. of ESREDA Annual Seminar: System Analysis for a More Secure World 2005, ISPRA, Italy,26-26 October 2005, pp. 97-109
[8] ICAO (2002) Annex 17, Annexes to the Convention on International Civil Aviation, ICAO, Montreal, Canada, 2002.
[9] ICAO (2002) DOC 8973 Restricted - Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference, Annexes to the Convention on International Civil Aviation, ICAO, Montreal, Canada, 2002.
[10] Raymond J. Decker, (2003), Key Elements of a Risk Management Approach, United States General Accounting Office, New York, USA, October 12 2001. pp. 1-11.
[11] John Moteff, (2004), Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, Congressional Research Service, Washington, USA, September 2 2004. pp. 1-27
[12] B. D. Jenkins, (1998), Security Risk Analysis and Management, Countermeasures Inc., Hollywood, USA, 1998. pp. 1-16
[13] G. Tamasi, M.Demichela (2005) Risk Assessment Techniques for Civil Aviation Security, in the Proc. of ESREDA Annual Seminar: System Analysis for a More Secure World 2005, ISPRA, Italy,26-26 October 2005, pp. 97-109

Anno I - n°1 Settembre 2006

Osservatorio per la Sicurezza Nazionale

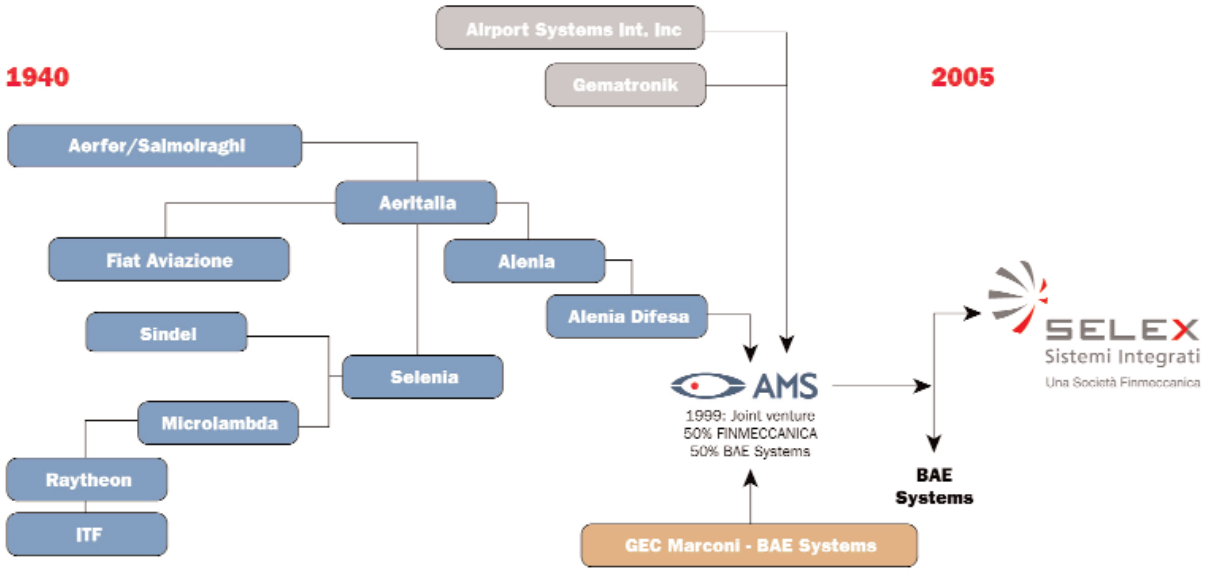
SELEX Sistemi Integrati
Una Società Finmeccanica

SELEX Sistemi Integrati

Articoli

Selex Sistemi Integrati la storia e i prodotti

SELEX Sistemi Integrati è un'azienda con una consolidata esperienza nella definizione ed integrazione di sistemi per la difesa, la sorveglianza costiera e marittima, la gestione del traffico aereo. Gli elevati standard tecnologici e il know-how raggiunti sono il risultato di una storia lunga più di 40 anni che va dalla nascita della Selenia (1960), poi Alenia (1990), attraverso l'esperienza della Joint-Venture con gli inglesi in AMS (1999) per arrivare ai giorni nostri con la ri-acquisizione completa da parte di Finmeccanica e con il nuovo nome di Selex Sistemi Integrati.

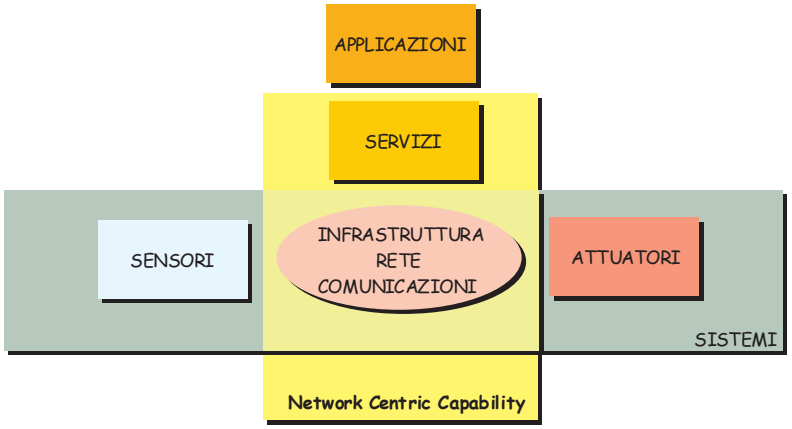


Questa lunga storia è stata caratterizzata dalla produzione e vendita in Italia e all'estero di innumerevoli apparati e sistemi la cui complessità si è evoluta nel tempo. Nel campo degli apparati il prodotto con il quale l'azienda ha raggiunto livelli d'eccellenza riconosciuti in tutto è indubbiamente il RADAR. I Radar di avvistamento, anticollisione, metrologici, di tiro, i radar terrestri, i radar navali, i radar per il controllo del traffico aereo, passando dai primi modelli pionieristici fino alle attuali nuove generazioni di radar: tridimensionali, ATC, allo stato solido, i radar navali multifunzionali. Nel campo dei sistemi sono da annoverare lo SPADA (il sistema missilistico per l'Esercito), l'ATM il sistema di gestione del traffico aereo in dotazione all'ENAV e venduto in

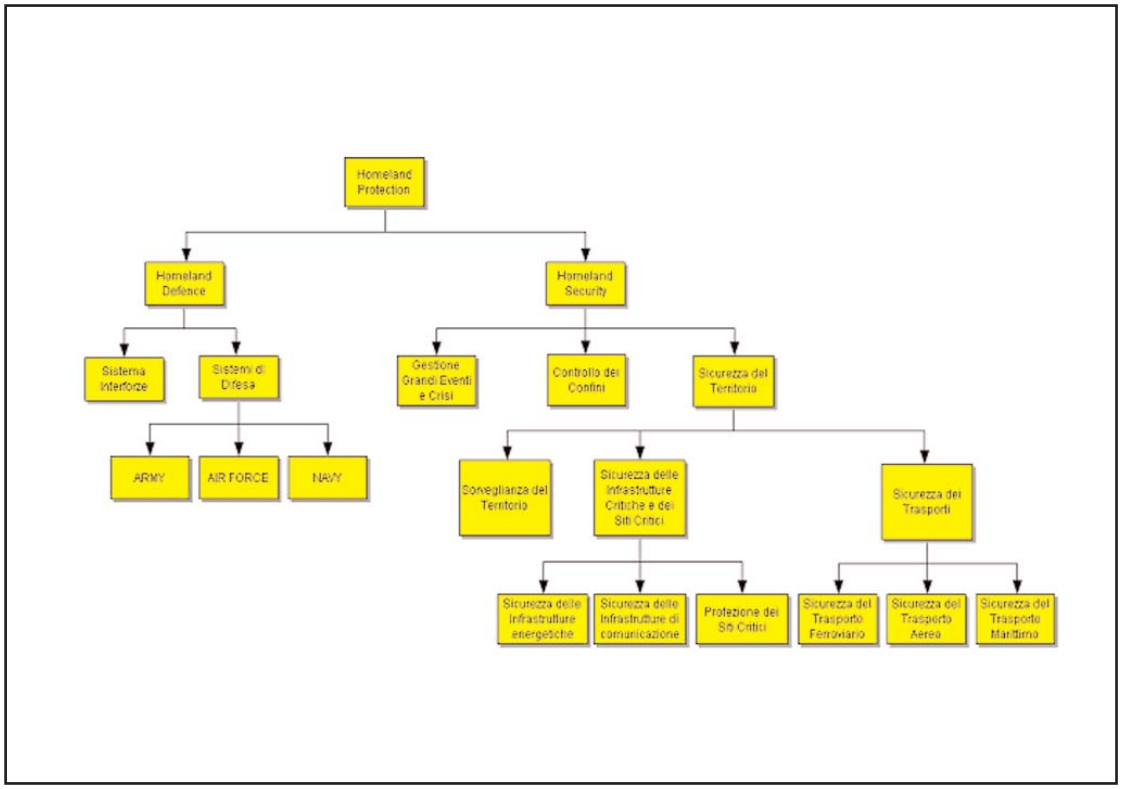
tutto il mondo, fino ai più recenti VTMS e CSS i sistemi di gestione del traffico marittimo e di sorveglianza costiera in fase di completamento in Italia e i cui moduli sono stati già venduti all'estero. Ancora in campo militare i sistemi di Comando e Controllo C4I per Esercito e Aeronautica, i sistemi Navali di combattimento per la Marina Italiana implementati nelle classi Orizzonte, NUM e FREMM.
Parte dell'Azienda è al momento impegnata nello studio e la progettazione di sistemi per la Homeland Protection, quello che si ritiene essere un mercato in netta espansione. Per quello che riguarda l'Italia, sono stati stipulati contratti con le forze dell'ordine e sono in atto studi e progetti con Clienti come le Ferrovie dello Stato e la Protezione Civile per delineare i requisiti di sicurezza a fronte di mirati studi di vulnerabilità e analisi di rischio.

Homeland Protection

Oggi per ogni regione, nazione, continente, il concetto di sicurezza è in continua evoluzione. Le minacce sono sempre meno prevedibili, la valutazione di cosa proteggere, da chi, quando, con quali modalità, diventa sempre più difficile e delicata. In un mondo globale, con scenari sempre più complessi, il livello di sicurezza è proporzionale alla possibilità di ricevere informazioni, elaborarle, trasmetterle velocemente ed integrarle in un unico grande sistema, capace di selezionare gli interventi più opportuni e consentire di prendere le decisioni di maggiore efficacia (sistema di supporto alle decisioni).
Un Grande Sistema è costituito da un insieme di sistemi che svolgono funzioni autonome, collegati tra loro tramite scambio dati, il cui collegamento si limita solamente alle strutture di interconnessione per le Comunicazioni e le cui funzionalità sono superiori alla somma delle funzionalità dei singoli sistemi componenti. I sistemi che compongono il Grande Sistema per Homeland Protection sono spesso molto complessi come nel caso del sistema di controllo del traffico marittimo (VTS), del sistema di controllo del traffico aereo (ATC), e dei sistemi di Comando e Controllo (C4ISR).
SELEX Sistemi Integrati è la società di Finmeccanica preposta alla progettazione e la realizzazione di Grandi Sistemi di Homeland Protection, realizzando l'integrazione di sistemi e tecnologie proprie, o di altre aziende, a partire da quelle del Gruppo.
L'Azienda si è recentemente dotata di una nuova struttura organizzativa di cui fa parte l'area dell'Architettura dei Grandi Sistemi che prevede il potenziamento delle preesistenti capacità nel settore dell'analisi dei sistemi integrati, dei modelli di simulazione e dell'ingegneria. Mai come in questo momento gli Organismi che gestiscono e regolano i settori nevralgici del Paese come ad esempio quello dei Trasporti, del Controllo dei Confini, della Produzione e Distribuzione dell'Energia e delle Comunicazioni, devono convincersi che, solo favorendo un approccio di livello superiore e integrato alla soluzione dei singoli problemi di sicurezza, si pone la base per una protezione globale nei confronti delle molteplici e inaspettate minacce del terrorismo internazionale. E' compito anche delle aziende introdurre e promuovere il disegno di Grande Sistema puntando sulle possibilità e sulle sinergie consentite da una logica integrazione dei sottosistemi che singolarmente rispondono alle esigenze dei vari settori.
I sistemi tradizionali di Homeland Protection sono principalmente costituiti dalle componenti di osservazione e Detezione (i sensori), di Decisione (il Comando e Controllo residente nelle applicazioni), e di Reazione (gli attuatori) messe in rete tramite un sistema di Comunicazione.
Tali sistemi sono per loro natura dei sistemi tipicamente chiusi e il sistema di Comunicazione ha una configurazione statica.
Nel Grande Sistema, il Sistema di Comunicazione è una Rete totalmente distribuita, condizione questa necessaria per realizzare la Network Centric Capability. Le Architetture che realizzano meglio tale scopo sono quelle orientate ai servizi (Service Oriented Architecture).



Lo strato SOA permette di attingere da un nutrito insieme di Servizi che, svincolati da logiche di appartenenza, vengono scelti in base alla necessità della Applicazione specifica e raggiungono gli utenti sfruttando la distribuzione e dinamicità della Rete. L'utilizzo di architetture e tecnologie SOA consente inoltre un adattamento dinamico della morfologia del Sistema alle differenti situazioni operative, garantendo la massimizzazione della propria efficacia ed efficienza.
Ne consegue che Interoperabilità, Coordinamento, Logistica, Informazione, Efficacia diventano punti di forza anche nel momento in cui il Grande Sistema per sua natura integra Sistemi gia esistenti.
L'approccio che Selex Sistemi Integrati segue e intende seguire in futuro è orientato alla Missione seguendo quello che da tempo è consuetudine in ambito militare.
Le Missioni in ambito Homeland Protection riguardano sia gli aspetti relativi alla protezione delle istituzioni del Paese (attacchi militari, destabilizzazione delle istituzioni, etc.) secondo la definizione di Homeland Defence, sia gli aspetti relativi alla protezione della popolazione da eventi indotti dall'uomo (terrorismo, sabotaggio, etc.) o naturali (inondazioni, terremoti, etc.) definita come Homeland Security.



SELEX-SI sta sviluppando lo studio architetturale per la Homeland Protection con i principali obiettivi di:
- Definire i nuovi requisiti operativi per la Homeland Protection a partire da studi di Risk Assessment e Cost Efficiency applicati ai diversi settori security-critical;
- Individuare le funzioni nuove e quelle già sviluppate che realizzano tali requisiti;
- Individuare i sistemi che implementano tali funzioni e inquadrare anche i sistemi complessi all'interno di una visione globale, assicurando interfacce predisposte per tale visione;
- Studiare la possibilità di sfruttare le nuove tecnologie alla luce anche di studi di Costo-Efficacia applicati al contesto Sicurezza.

Selex Sistemi Integrati partecipa con entusiasmo alla costituzione dell'Osservatorio per la Sicurezza Nazionale un organismo che si pone come obiettivo per prima cosa la comprensione di un fenomeno così complesso come quello della sicurezza del Paese e che nel giusto tentativo di coinvolgere il maggior numero di attori, mette ad esempio a contatto in un confronto stimolante il mondo militare con quello civile, due mondi che spesso viaggiano separatamente ma che mai come in questo periodo della storia si vedono coinvolti mutuamente nel fronteggiare una minaccia che supera gli schemi tradizionali. In questo senso la consuetudine di Selex-SI a lavorare con clienti di entrambe le sfere civile e militare si ritiene possa essere fonte di

ricchezza per contribuire agli obiettivi che OSN si propone di raggiungere.
In particolare Selex-SI potrà:

- contribuire alla proposizione di strategie e tecnologie atte a ridurre la vulnerabilità, contrastare l'azione terroristica e gestire efficacemente situazioni di crisi;
- contribuire ad elaborare scenari di rischio e pratiche di prevenzione;
- proporre strumenti di contrasto;
- contribuire a creare una rete di attori chiave in ambito Homeland Protection (Industria, Rappresentanti delle istituzioni, organismi di controllo, centri di ricerca/università) volta a facilitare l'interazione, il coordinamento e lo scambio di informazioni sulla Sicurezza.
- contribuire al confronto con l'Europa attraverso i collegamenti che l'azienda ha stabilito partecipando ai programmi europei di ricerca sul tema della sicurezza.

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

TELECOM ITALIA
Security Business
Continuity e Protezione Civile

Articoli

Gruppo Telecom Italia: organizzazione in caso di crisi

In questi ultimi anni la "filosofia dell'emergenza" ha vissuto una profonda evoluzione, passando da una visione legata esclusivamente al fronteggiamento dell'evento ad una concezione più estesa in cui viene dato un incisivo risalto anche alla previsione e prevenzione degli eventi stessi.
Questa considerazione e lo scenario sopra descritto hanno reso imprescindibile la formulazione di nuove e adeguate politiche di tutela, la cui realizzazione consentisse di concretizzare sul piano operativo anche "quell'attitudine alla prevenzione", che deve far parte del tessuto culturale dell'Azienda.
E' stata rivisitata l'organizzazione aziendale per la gestione delle situazioni di crisi secondo una logica interfunzionale pianificata che contemperasse, con un giusto mix, l'efficacia con l'efficienza.
Naturalmente la "vera" emergenza, per la quale sono necessari "strumenti" straordinari, inconsueti, scatta solo quando si è in presenza di una significativa combinazione delle seguenti condizioni:

- Gravità dell'evento
- Inapplicabilità radicale ed estesa della routine di comportamento
- Pressione temporale

Tutti gli altri eventi, che non presentino una combinazione significativa dei predetti elementi, sono quindi da considerarsi "assorbibili" dalle normali capacità reattive delle singole strutture tecniche e, pertanto, non richiedono l'applicazione delle procedure indicate nel presente documento.
Il presente documento contiene una sintesi delle procedure che Telecom Italia adotta, al fine di assicurare, in caso di emergenza, una migliore e globale risposta dell'Azienda al mantenimento del servizio pubblico, nonché a supportare gli Organi Istituzionali con una efficace infrastruttura di TLC per gestire e coordinare le operatività nelle situazioni di crisi.
In particolare di seguito sono descritti i criteri e le procedure specifiche che definiscono i ruoli, le responsabilità e le risorse umane e tecniche coinvolte, a diverso titolo, nel contrasto dell'emergenza. Inoltre sono descritti sinteticamente i singoli piani di disaster recovery per garantire la continuità del servizio svolto da Telecom.
Al fine di ripristinare condizioni di traffico accettabili, ai limiti della normalità, in tempi rapidissimi assicurando contestualmente i servizi di comunicazione a tutte le componenti, istituzionali o del volontariato, che devono gestire la crisi, il Gruppo Telecom ha elaborato un'attenta ed articolata pianificazione, che aggiorna continuamente.
Inoltre, allo scopo di garantire la continuità dei servizi di telecomunicazioni e la tutela degli impianti attraverso una presenza che possa fra fronte a qualsiasi imprevisto, ha da tempo creato, ad integrazione delle attività svolte in orario normale di lavoro, l'istituto della Reperibilità che, nel caso si manifestassero problemi nell'erogazione dei servizi, è in grado di allertare automaticamente, come previsto nel Manuale, entro pochissimo tempo, i responsabili delle varie strutture aziendali coinvolte.
Per gestire le situazioni di crisi sono stati predisposti la Procedura Organizzativa di Protezione Civile e i Piani d'emergenza Tecnici, utilizzando anche i sistemi di gestione/controllo esistenti: quello tecnico per il

monitoraggio costante della rete (NSC), quello organizzativo per il monitoraggio degli allarmi (Incident Crisis Center).
Per tutti gli aspetti inerenti alla pianificazione, al coordinamento e alla gestione dell'emergenza, fin dal 1990 la Società si è dotata, a livello centrale, di un'apposita struttura di "Difesa e Protezione Civile", che garantisce, nell'evolversi delle varie fasi dell'emergenza, il raccordo costante dell'operatività a livello territoriale.
La Procedura delinea l'organizzazione aziendale per la gestione delle crisi, definisce le attività ordinarie e/o straordinarie da mettere in campo, ed individua i canali per le comunicazioni interne ed esterne all'organizzazione, nelle fasi preventiva, concomitante e successiva alla crisi.
L'organizzazione individuata prevede la costituzione di "Operations Crisis Team" e l'utilizzo di Sale Polifunzionali (8) nelle quali si riuniscono.
Per "Operations Crisis Team" si intende l'insieme dei Rappresentanti delle funzioni aziendali che devono fornire il proprio contributo professionale per assicurare, in occasione degli eventi in parola, una più rapida ed efficace risposta aziendale, attraverso una gestione integrata delle azioni di contenimento/contrasto.
Nella Procedura, pertanto, è individuata la composizione degli Operations Crisis Team che si differenziano a seconda del tipo di emergenza.
Le Sale Polifunzionali, allestite per la gestione degli stati di crisi, sono collegate, a mezzo di circuiti diretti preferenziali in fonia, con tutte le funzioni interne ed esterne. In particolare le Sale sono dotate di:

- sistemi di telecomunicazione e collegamenti attestati su diverse centrali telefoniche;
- apparati radio per la ricezione di tutte le gamme di radiofrequenza;
- sistemi per la ricezione dai satelliti in orbita geostazionaria visibili nell'area del Mediterraneo;
- sistema informativo "CI.PRO." (Civil Protection).

In particolare il sistema informativo CI.PRO., utilizzato e commercializzato da Telecom Italia, è in grado di fornire un valido supporto da utilizzare, oltre che nelle fasi di emergenza in atto, anche in tutte le attività che precedono e seguono uno stato di crisi.
E' una banca dati, alfanumerica e grafica, contenente, tra l'altro, i dati relativi al patrimonio aziendale correlati ai rischi prevalenti (sismico, chimico/industriale, idrogeologico, e nucleare) nonché mappe territoriali digitalizzate integrate con elementi orografici e della rete dei trasporti.
Il sistema informativo facilita il Crisis Management nell'adozione di rapide ed efficaci decisioni operative, consentendogli di:

- raccogliere le informazioni relative al patrimonio Telecom correlate con i principali rischi del territorio;
- rilevare i dati dei responsabili tecnici e non e del personale in possesso di particolari specializzazioni, patentini e abilitazioni;
- individuare la dislocazione delle risorse, ivi compresi i mezzi mobili d'emergenza.

Per quanto attiene alla "rappresentanza" aziendale, l'organizzazione Telecom per la gestione delle emergenze prevede sostanzialmente:

- un presidio interno all'Azienda, garantito dagli Operarions Crisis Team, i cui componenti si riuniscono nelle Sale Polifunzionali
- un presidio esterno presso gli Organi Istituzionali centrali e periferici (es. per azioni di Protezione Civile, al centro con Dipartimento della Protezione Civile, in periferia con i Centri Operativi Misti).

Ad integrazione della struttura dedicata, sopra descritta, Telecom Italia possiede un'organizzazione diffusa in modo capillare sull'intero territorio nazionale.
Le suddette strutture territoriali sono in grado di assicurare, attraverso la presenza ed un sistema di reperibilità di coordinamento con copertura h24 domeniche e festivi compresi, un immediato allertamento dell'intera organizzazione locale, sia tecnica che relazionale, con un conseguente primo tempestivo intervento, nei limiti consentiti dalla viabilità stradale.
L'attività di ripristino dei circuiti, e la realizzazione di nuovi, sono definite dando priorità a quei collegamenti di primaria importanza finalizzati al:

- coordinamento delle operazioni di soccorso;
- assistenza sanitaria
- telefonia pubblica
- funzionamento delle stazioni radio-base, al fine di garantire le comunicazioni di telefonia cellulare.

E' da tenere presente che in funzione delle esperienze passate (calamità idrogeologiche, eventi sismici, ecc.), allo scopo di garantire sempre la disponibilità di tutto il materiale necessario alle riparazioni (cavi, armadi ripartilinea, pali, cabine, ecc.) le scorte in deposito, presso i magazzini sociali e delle imprese appaltatrici, vengono ripartite territorialmente.
Per fronteggiare, inoltre, qualsiasi emergenza dovesse interessare le acque territoriali italiane si evidenzia che Telecom Italia dispone di una rete di 71 impianti radiocostieri a totale copertura dei mari nazionali e internazionali, nonché di tutte le località costiere.

Inoltre, con l'utilizzo di un sistema satellitare (IMMARSAT) vi è la possibilità di disporre di un ulteriore sistema alternativo, attraverso il quale effettuare comunicazioni anche laddove ciò non sia possibile con i normali collegamenti terrestri.

Esistono, infine, degli apparati specifici per fornire supporto nella gestione dell'emergenza, in particolare tra gli strumenti impiegati per garantire comunque lo svolgimento del servizio nelle località colpite da eventi catastrofici, la Società dispone di Unità Mobili di Trasmissione (Ponti Radio), di Commutazione (concentratori, autocommutatori) e di Alimentazione (raddrizzatori, batterie, gruppi elettrogeni).
Allo scopo di assicurare il servizio di Telefonia Pubblica alle popolazioni colpite da eventi catastrofici sono stati attrezzati 4 TIR rimorchiabili con idonee motrici, con funzioni di "posto telefonico pubblico", ogni automezzo è dotato di 8 Terminali Telefonici Pubblici.
Inoltre sono a disposizione delle SCTP (territorio regionale di Telefonia Pubblica) dei carrelli trainabili (da normali autovetture) dotati di 5 Terminali TP.
Quanto finora descritto riguarda l'organizzazione, le strutture, i mezzi di cui Telecom Italia si avvale per fronteggiare le situazioni di crisi. Nella convinzione che una "popolazione informata" è ben preparata ad affrontare qualsiasi emergenza, il Settore di Difesa e Protezione Civile presidia tutta una serie di attività che hanno come obiettivo la diffusione di una cultura sociale sempre più attenta alle tematiche di Difesa e Protezione Civile, presupposto essenziale per una gestione dell'emergenza più efficiente.
Per il raggiungimento di tale obiettivo vengono costantemente realizzate specifiche attività quali:

- interventi formativi, mirati a:
- sensibilizzare alla gestione delle situazioni di crisi in una logica interfunzionale pianificata;
- approfondire le soluzioni organizzative previste, le modalità d'intervento in termini di risorse, mezzi e procedure;
- analizzare gli aspetti sociali/relazionali in situazioni di crisi, come ad esempio la gestione degli stati d'ansia in siffatte situazioni.
- organizzazione di periodiche esercitazioni interne per passare dalla cultura del Manuale alla cultura dell'addestramento. Partecipazione, in base alle disposizioni della legge 225/92 alle esercitazioni esterne promosse e coordinate dagli Organismi dello Stato;
- partecipazione a mostre, fiere e convegni in tema di Difesa e Protezione Civile;

In conclusione, quanto illustrato testimonia il nostro impegno al fine di raggiungere un modello organizzativo il più possibile strutturato, che per esprimere al meglio tutta la sua efficacia deve essere necessariamente supportato dalla disponibilità, competenza e professionalità delle nostre risorse, che sul campo riescono comunque e sempre a dare il "massimo" anche operando in condizioni molto difficili.

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Italian Team for SecurityTerroristic Issues & Managing Emergencies
Università Cattolica del Sacro Cuore - Dpt. Sociologia

Articoli

ITSTIME per OSN, Orientamenti e piste di ricerca.

ITSTIME - Italian Team for Security, Terroristic Issues & Managing Emergencies è un progetto nato nel Dipartimento di Sociologia dell'Università Cattolica del Sacro Cuore di Milano. E' coordinato da Marco Lombardi, sociologo ed esperto di crisis management, e si avvale di un gruppo di ricerca che comprende esperti di islam, lingua e cultura araba quale è Gabriele Crespi; di sicurezza e terrorismo con una forte esperienza maturata sul campo: Nick Ridley; di tecnologie: Chiara Fonio; di gestione della sicurezza nei grandi eventi: Jhonny Pisapia; di comportamento umano in situazione di stress: Davide Scotti. Inoltre, collabora con una ampia rete di centri e ricercatori della Università Cattolica (CRiSSMA diretto da Valeria Fiorani Piacentini) e altre università straniere. Dunque, il carattere di ITSTIME è altamente interdisciplinare in quanto coinvolge esperti capaci di affrontare i temi complessi della sicurezza secondo una necessaria molteplicità di prospettive. Per questa ragione si definisce come progetto: cioè come una realtà in divenire capace di affrontare teoricamente ed empiricamente le sfide del nuovo mondo globale post 11/9.
Nella nostra visione, infatti, teoria e pratica si completano vicendevolmente affinché una corretta analisi dei fenomeni permetta di sviluppare coerenti e concrete strategie di risposta a più livelli. Il progetto ha già avviato delle collaborazioni con soggetti pubblici e privati che hanno la necessità di monitorare le minacce a cui sono esposti; elaborare i possibili scenari di rischio; predisporre le strategie di prevenzione; definire i piani di intervento e gestire le situazioni di crisi naturale o prodotta da eventi antropici.
La missione di ITSIME si articola in tre ambiti specifici:

- Sicurezza, intesa come uno stato da conseguire e mantenere per promuovere il benessere dei cittadini e la vitalità democratica delle istituzioni;
- Terrorismo, affrontato come una minaccia destinata a perdurare nel tempo a cui è necessario fornire risposte preventive articolate;
- Gestione delle emergenze, una pratica che deve essere sviluppata e condivisa da istituzioni e cittadini per reagire alla manifestazione dell'evento possibile.

La nostra scelta è di affrontare la crisi secondo una nuova prospettiva unitaria coniugando studi e attività di prevenzione per il mantenimento della sicurezza, di analisi dettagliata dell'attuale minaccia terroristica e per essere pronti a gestire l'evento critico qualora si manifestasse. Questi tre ambiti sono quelli che, oggi con sempre maggiore frequenza, specificano la cosiddetta Homeland Security: essi forniscono le linee guida dello contributo che ITSTIME vuole portare alla rete dell'Osservatorio per la Sicurezza Nazionale.
In estrema sintesi, le attività di ITSTIME si inquadrano in una prospettiva per la quale i gruppi terroristici sono simili a organizzazioni complesse e reticolari le quali, pertanto, hanno bisogno di risorse per sopravvivere e operare.
In particolare, ciò rimanda a due dimensioni costitutive:

- il finanziamento del terrorismo
- la comunicazione del terrorismo

Questi due poli costituiscono i "bisogni primari" delle organizzazioni - anche di quelle del "terrore" - la cui

risposta promuove pratiche specifiche. A queste pratiche, che lasciano segni là dove vengono implementate, si dedicano le ricerche e le analisi di ITSTIME.

Le linee teoriche e operative della ricerca di ITSTIME

<table>
<tr><td>Il Background</td><td colspan="3">La cultura del terrorismo
La cultura della jihad e dell'Islam
Strategie e modus operandi
Competenze linguistiche e comunicative</td></tr>
<tr><td>Le dimensioni teoriche</td><td colspan="2">Finanziamento del terrorimo</td><td>Comunicazione del terrorismo</td></tr>
<tr><td>Le dimensioni operative</td><td>Contrasto ai flussi finanziari</td><td>Prevenzione dei target sensibili</td><td>Strategie di contro comunicazione</td></tr>
<tr><td rowspan="2">I risultati</td><td colspan="3">Proporre scenari</td></tr>
<tr><td colspan="3">Predisporre piani per la gestione delle emergenze</td></tr>
</table>

Il background del progetto affonda le sue radici nella necessaria conoscenza della cultura terrorista, profondamente interiorizzata dal gruppo di lavoro secondo il principio per cui è necessario "pensare da terrorista" per comprendere e combattere il fenomeno. Il risultato del progetto, infine, si declina in elaborazione di scenari e pratiche per la gestione delle emergenze.
In particolare, ITSTIME si dedica all'analisi dei processi comunicativi del terrorismo. Infatti, l'affermazione: "il terrorismo è comunicazione" orienta il nostro lavoro di monitoraggio della comunicazione jihadista.
La stessa "Al-Qaeda", che tradizionalmente si identifica come una organizzazione del terrorismo jihadista, è al tempo stesso una "rete del terrorismo" internazionale e una "griffe" che elabora e trasmette documenti e fatwe, che delinea le direttrici generali della Jihad e scandisce i tempi delle varie offensive, ma che poi delega, o semplicemente "propone", la fase operativa ai gruppi insediati localmente aventi un grado totale o parziale di autonomia. Questi gruppi possono essere tra loro indipendenti o debolmente connessi - con proprie strategie, metodi e "tecnologie di esecuzione" del terrore - e avere, con la leadership di "Al-Qaeda", una debole oppure nessuna relazione storica. In ogni caso, agire sotto la griffe di "Al-Qaeda", permetterà a questi gruppi di ottenere la massima visibilità mediatica, di raccogliere nuovi finanziamenti dalle opere di carità arabe e, in ultimo, di reclutare nuovi militanti per la Jihad totale. Gli obbiettivi di "Al-Qaeda" sono scelti, a nostro avviso, con quattro criteri: uno politico, uno religioso, uno mediatico e uno operativo. In altre parole, il paese colpito deve avere una qualche relazione di "empia alleanza" con gli Stati Uniti, e di condivisione di scelte politico-militari (per esempio l'occupazione dell'Iraq), deve rappresentare un simbolo di riferimento mondiale per le religioni alternative all'Islam, deve offrire degli obbiettivi facili dal punto di vista operativo (per esempio ad opera di imported suicider bombers o di cellule terroristiche islamiche dormienti o di gruppi locali eversivi) o altamente simbolici, che se fossero colpiti sarebbero di estrema risonanza mediatica a livello globale.
La studio che porta alla comprensione e spiegazione dell'azione terrorista deve, dunque, dotarsi di una "cassetta degli attrezzi" altamente specializzata ma interdisciplinare in cui la dimensione comunicativa offre un indirizzo interpretativo importante: la grande differenza che esiste tra un criminale e un terrorista è, infatti,

che il secondo, a differenza del primo, ha interesse per il riconoscimento simbolico che l'azione fornisce; ricerca la platea offerta dal sistema mediatico; si propone quale attore protagonista.
Una caratteristica specifica del terrorismo è di essere un "fenomeno comunicativo", nel senso che cerca e gestisce comunicazione. La tesi di fondo, dunque, è che il terrorismo ha una valenza comunicativa propria che è necessario assumere come strumento interpretativo del fenomeno. Per tale ragione è necessario leggerlo anche usando gli strumenti della media research. Ciò è tanto più rilevante in sistemi sociali in cui "l'opinione pubblica" è divenuta, con il diffondersi delle tecnologie dell'informazione in tempo reale, un fattore centrale per l'orientamento dell'azione politica e strategica.
Inoltre, gli attentati del mese di luglio 2005, pur rientrando tutti in scenari attesi, segnano una progressiva "baghdadizzazione" o "palestinizzazione" della questione terrorista con la quale ci si dovrà confrontare negli anni futuri. La differenza del "dopo luglio" sta nel fatto che il "rischio terrorismo da argomento per gli "addetti ai lavori" ha ormai assunto consapevolezza in numerosi strati della popolazione e delle amministrazioni.
La prospettiva complessa assunta da ITSTIME per affrontare i tre nodi della sicurezza, del terrorismo e della crisi, porta il progetto a muoversi sia nei campi virtuali delle comunicazioni via rete e delle relazioni sia nei campi concreti del nuovo scenario globale. I suoi esperti, infatti, hanno condotto negli ultimi cinque anni missioni in tutti i paesi dell'area nord africana, medio orientale e centro asiatica.
L'analisi della comunicazione via web del terrorismo jihadista è un ulteriore aspetto fondamentale della ricerca di ITSTIME, che da una parte applica i criteri della comunicazione per l'analisi dei fatti che si verificano e dall'altra promuove la conoscenza della comunicazione in sé, quale pratica costitutiva del terrorismo. Il presupposto è la presenza di specifiche competenze mediali tra i terroristi, da cui la costituzione di un probabile "centro media" e di strategie di promozione e reclutamento ad hoc.
Allo stato attuale si può affermare che l'informazione circa l'indirizzo di un prossimo attacco sia presente in rete, si tratta di decodificarla. Per tali ragioni, ITSTIME continua uno specifico monitoraggio del web, utilizzando strumenti di web searching and monitoring avanzati, che ha portato alla raccolta di circa 10 giga di materiali multimediali in 50.000 files e alla analisi di oltre 150 siti.
Il lavoro di ricerca è dedicato alla analisi della comunicazione del terrorismo attraverso il web, con l'obiettivo di identificare il centro mediatico di produzione della comunicazione, le strategie comunicative di promozione e reclutamento, le possibilità di elaborare azioni efficaci di risposta. Tale attività è sviluppata anche attraverso più precise analisi semiotiche, non solo linguistiche, per favorire l'identificazione dei profili dei potenziali candidati jihadisti. Inoltre, tale analisi recentemente interessa web site di diversa origine, anche in lingua italiana, e mirror, potenzialmente fiancheggiatori, di origine anarco-insurrezionalista. Questi ultimi, oggi offrono notevoli opportunità di ricerca perché spesso garantiscono la persistenza del materiale sui loro host.
Il monitoraggio sistematico dei siti web, reso difficoltoso dalla spesso scarsa permanenza dei medesimi e dalla molteplicità di livelli che ciascuno di essi offre, è particolarmente attento ai materiali audio-visivi distribuiti. Tale scelta è dovuta al forte impatto che questi hanno sul pubblico di riferimento e alla possibilità di articolazione in prodotti specifici che si offre. Tuttavia, il materiale audio e testuale risulta di grande importanza per il ruolo che gioca soprattutto in chat e forum, in quanto portatore di informazioni specifiche e, tendenzialmente, essendo materiale più adatto a sviluppare anche azioni di controterrorismo proprio nei luoghi in cui viene distribuito (chat e forum).
Oggi si può affermare con certezza che da una fase "naiv" della comunicazione terroristica si è passati a una fase più sofisticata, che richiede mezzi, competenze e strategie specifiche: tutti "oggetti" che lasciano tracce potenziali, perché implicano l'esistenza di un centro organizzativo di queste competenze per massimizzare le potenzialità del web. Specificatamente, la ricerca si svolge per comprendere:

- come questo media centre lavora: l'uso dei mezzi sia sul campo sia nella post-produzione confrontando i materiali grezzi raccolti dalle unità di fuoco e la loro successiva rielaborazione comunicativa. Si tratta di un passo importante per distinguere le strategie sviluppate e comprendere i differenti target della comunicazione, in particolare i potenziali jihadisti identificati per la comunicazione di reclutamento;
- la rete di distribuzione dei materiali, attraverso le complesse mappe di link e backlink che si creano e attraverso le pratiche di up/down load;
- l'evoluzione delle strategie di reclutamento, realizzando un'operazione di "back profiling" sulla base dei target della comunicazione.

Il percorso di ricerca qui esposto, sicuramente finalizzato ad accrescere la conoscenza intorno alla comunicazione jihadista, permette di ipotizzare anche misure strategiche di risposta al fenomeno. Per esempio:

- interrompere il circolo di imitatori di intervenendo pro-attivamente sui circuiti mediatici di "Al Qaeda";
- attaccare il mito di "Al Qaeda" dentro alla Umma virtuale e nel circuito dei media islamici, insistendo soprattutto sulla perdita di coordinamento tra le parti del sistema;
- promuovere una comunicazione che evidenzi come le recenti azioni del terrorismo siano soprattutto orientate a perseguire obiettivi di interesse locale piuttosto che ispirate da prospettive pan-islamiche;
- ostacolare la comunicazione dei messaggi ideologici di "Al Qaeda" indirizzati ai suoi imitatori ed emulatori; facilitare la nascita di una discussione critica all'interno del mondo islamico sulla natura e la legittimità degli obiettivi di "Al Qaeda" fatwas, insistendo sulla sua ortodossia, e pubblicizzando il dibattito;
- promuovere il dibattito tra gli islamici europei/occidentali per minare la loro coesione interna e ridurre la fiducia verso i leader islamici in occidente;monitorare il processo di reclutamento attraverso il web per favorire attività di profiling;
- focalizzarsi sulle strategie di web marketing di "Al Qaeda", infiltrando i siti islamici con una partecipazione attiva su chat e forum.

In conclusione, il contributo del progetto ITSTIME - Università Cattolica si propone alle attività dell'Osservatorio per la Sicurezza nazionale, come specializzato nei due ambiti della minaccia terroristica e della gestione delle crisi, entrambi interpretati nella prospettiva dei processi comunicativi. Si tratta, infine, di un contributo per la sua natura interdisciplinare, che vuole essere fortemente in relazione con tutti i partner della rete - massimizzando così i punti di vista teorici e operativi - per il raggiungimento degli obiettivi comuni.

Ulteriori informazioni, insieme ad approfondimenti e commenti sui fenomeni oggetto di studio, sono rese disponibili sul sito web *www.itstime.it*.

Marco Lombardi

Anno I - n°1 Settembre 2006

Osservatorio per la Sicurezza Nazionale

Università degli Studi di Macerata

Articoli

Sicurezza "finanziaria" e sicurezza "globale": qualche spunto di riflessione

Credo che all'avvio di questa iniziativa - meritoria e importante - si possa fornire qualche spunto ricostruttivo, purtroppo di natura (assai) operativa, sul rapporto che esiste tra le minacce alla sicurezza (intesa, qui, come concetto "sistemico") ed i reati finanziari, segnatamente gli abusi di mercato ed il riciclaggio.
Nella enumerazione che ciascuno di noi, studiosi o operatori, legislatori o regulators, può esercitarsi a redigere in materia di reati finanziari, categoria nella quale per brevità si devono necessariamente sussumere le innumerevoli fattispecie di "virus"che stanno infettando i sistemi economici internazionali soprattutto in questi ultimi anni, nonostante i richiami dell'attualità normativa, non si pone ancora l'attenzione dovuta al reato di riciclaggio.
Un reato che diventa "fenomeno", che è il sottostante di più o meno tutte le operazioni finanziarie (e non solo) compiute quotidianamente sui mercati.
Ne esaminiamo di seguito le principali caratteristiche e, soprattutto, le implicazioni economiche, non senza aver tentato una sistematizzazione giuridica del quadro normativo esistente.

La fattispecie "riciclaggio[1] "

La presa d'atto dell'esistenza del fenomeno è risalente, e si fa grazia a chi ci legge degli innumerevoli passaggi normativi, sia primari che secondari, nazionali e sovranazionali, che ancora oggi fanno di questo reato una fattispecie assai complessa, della quale in verità è più immediato comprendere le implicazioni economico-finanziarie che quelle legali[2] .
Solo tre direttive europee devono essere citate, perché ognuna di esse segna la cadenza degli interventi del legislatore nazionale e ci agevola nella comprensione delle sue scelte:
- direttiva 91/308/CEE del 10 giugno 1991, la quale ha avviato in sede europea l'imposizione di presìdi contro il riciclaggio attraverso l'apposizione di paletti all'attività degli intermediari finanziari. La logica è stata quella che ci piace chiamare "dei posti di blocco", ossia di una serie di sbarramenti che potessero consentire di prevenire, più che di reprimere, l'utilizzo del sistema finanziario a scopo di riciclaggio[3] ;
- direttiva 2001/97/CE del 4 dicembre 2001, con la quale si sono ampliati gli elenchi dei soggetti obbligati all'adozione delle misure sopra descritte. Ciò stante la recrudescenza del fenomeno, soprattutto realizzata attraverso la ricerca, da parte della criminalità organizzata, di nuovi canali e modalità mediante le quali reimpiegare il denaro di provenienza illecita o semplicemente attuare il suo inserimento nel circuito economico. Con questo provvedimento comunitario, appena recepito in Italia con i decreti del Ministero dell'Economia del 3 febbraio 2006, la lotta al riciclaggio (rectius, la prevenzione del reato e soprattutto dei suoi effetti destabilizzanti per le strutture colpite e per i mercati di riferimento) diventa non più solo appannaggio degli interme-

1 Si prescinderà, per esigenze evidenti di economia dello scritto, dalla trattazione giuspenalistica del reato, per la quale si rinvia, tra gli altri, al testo di Manna A., Riciclaggio e reati connessi all'intermediazione mobiliare, Utet, Torino, 2001, nonché alla bibliografia ivi citata.

2 Per una prima ricostruzione ci si consenta di rinviare al nostro La normativa antiriciclaggio in Italia, Giappichelli, Torino, 1999, cap. I

3 I paletti di cui trattasi sono sostanzialmente tre, e riguardano la limitazione dell'utilizzo di contante e di titoli al portatore tra privati e oltre una certa soglia, l'identificazione e registrazione in appositi archivi detenuti dagli intermediari dei clienti che compiano determinate operazioni finanziarie, la segnalazione alle autorità di settore delle operazioni cosiddette "sospette" di riciclaggio.

diari finanziari (che erano i primi ovviamente da testare sulla materia), ma, ad esempio, dei liberi professionisti (legali, revisori, commercialisti, notai)[4] e di altri soggetti non finanziari (come i grossisti di metalli preziosi, i galleristi, le case d'asta e da gioco, etc)[5] ;
- direttiva 2005/60/CE del 26/10/2005, da attuarsi entro la fine del 2007, che enfatizza - laddove ve ne fosse ancora la necessità - la "criminalizzazione" del riciclaggio come reato destabilizzante per l'economia, ma, soprattutto, essa arriva ad ipotizzare, per i soggetti obbligati (il cui novero viene tra l'altro esteso ad altre imprese non finanziarie) una vera e propria "profilatura antiriciclaggio" della clientela. La regola base del business, la nota "know your customer rule", utilizzata (ed utile) come non mai per la prevenzione di impieghi fraudolenti delle strutture dell'intermediario finanziario o della impresa sana, si trasforma da metodologia ermeneutica (che, nella prassi operativa è il maggior coadiuvante nella discoperta di anomalie censurate dalla norma), affidata alla soggettività dell'operatore, in "sistema di rating".

Rating e riciclaggio: la tesi e l'antitesi

Proprio riagganciandoci a quest'ultima proposizione cerchiamo di giungere (non senza qualche ambizione!) alla definizione di un iter comune per la prevenzione delle anomalie del mercato che rivengono da manipolazioni dello stesso e nello stesso operate.
Non è contraddittorio rispetto alle opinioni di cui al precedente paragrafo affermare che solo chi conosce il cliente, solo chi è più prossimo (poiché in qualche modo partecipe) all'operazione di mercato che si vuole attenzionare è compiutamente in grado di disporre degli elementi per poterla censurare in via preventiva e, di conseguenza, sottoporla al vaglio delle autorità preposte all'approfondimento finanziario ed investigativo.
La "oggettivizzazione" che ci si propone di raggiungere in subjecta materia non può che essere letta come deterrente "di primo livello" nei confronti delle devianze cui stiamo facendo riferimento.
In altre parole, così come nel settore del credito il rating è indubbiamente utile a catalogare e segmentare la clientela per macro aree, per poi affidare a chi dovrà materialmente erogare il credito stesso la valutazione finale circa la sua meritevolezza, nel settore della prevenzione dei reati finanziari sistemi automatizzati di monitoraggio della clientela, delle movimentazioni e dei rapporti, non possono che rivelarsi di positivo supporto al giudizio conclusivo che i responsabili delle strutture di controllo dovranno formarsi, onde segnalare eventuali anomalie a chi dovrà perseguire i crimini che ne dovessero derivare.
E' assai vivo il dibattito, e veniamo al punto, sull'obbligo di segnalazione di operazioni sospette di riciclaggio che è stato posto a carico anche di soggetti, come i liberi professionisti e taluni commercianti, di sicuro meno dotati - rispetto alle più sperimentate realtà imprenditoriali del settore della finanza - di expertise e di strumenti per una efficace ottemperanza alle prescrizioni sopra citate.
La norma italiana di riferimento, l'art. 3 della legge 197 del 1991, è in verità alquanto vaga, poiché lega la valutazione del "sospetto" a caratteristiche qualitative della/e operazione/i posta/e in essere dal soggetto da segnalare a parametri soggettivi del medesimo (quali l'attività svolta e la capacità economica) ben più difficili da approfondire date le informazioni obiettivamente in possesso dell'operatore.
Qui un rating del soggetto sarebbe una bella bombola di ossigeno per l'asmatico sistema delle segnalazioni, che continua a produrre dati sconfortanti nonostante un significativo incremento negli ultimi anni[6] : basta non fare l'errore di ritenere, lo si ripete, che esso sia esaustivo dell'obbligo!

L'obbligo di segnalazione nella normativa antiriciclaggio

Quanto appena ricordato è temperato, nelle sue conseguenze vuoi psicologiche (relazionali)[6], vuoi metodologiche, da due opportune precisazioni che la legge stessa opera, ma che le Autorità di vigilanza non si stancano di ribadire:
- la segnalazione de qua non costituisce notizia di reato, bensì un adempimento di carattere amministrativo, di vigilanza, che non porta ad alcuna conseguenza di carattere processuale per il soggetto segnalante,

4 Per un primo commento riferito all'impatto sulle libere professioni si veda il nostro "Antiriciclaggio e libere professioni", Diritto ed Economia delle Assicurazioni, 1/2003.

5 I decreti cui si fa riferimento sono i nn. 141, 142 e 143, seguiti ciascuno dalle istruzioni applicative dell'Ufficio Italiano dei Cambi. I suddetti provvedimenti, con un commento più articolato del presente, possono tra l'altro essere rintracciati sul sito www.studiorazzante.com (e sul nostro libro di prossima uscita per i tipi di Giappichelli) , mentre in dottrina si rinvia per necessità, ma con poca convinzione, ai numerosi articoli comparsi sulla rivista Il fisco, soprattutto dal gennaio 2006 ad oggi.

6 Cfr. Relazione annuale per il 2005 dell'Ufficio Italiano Cambi, sul sito www.uic.it.

sia che quest'ultimo abbia colto la negatività del comportamento del cliente, sia nel caso in cui abbia avuto un eccesso di zelo;
- in un documento del 12 gennaio 2001, noto al settore finanziario come "Decalogo-ter" della Banca d'Italia, è stato efficacemente spiegato agli intermediari finanziari (così come oggi agli altri soggetti coinvolti viene ribadito nei citati decreti ministeriali) che la segnalazione di operazione sospetta non può avere alla base alcun elemento di reato, poiché all'operatore non possono essere richieste valutazioni di tipo "parainvestigativo", ma unicamente delle sue considerazioni circa il merito delle operazioni oggetto delle anomalie. Nel documento dell'Autorità di vigilanza, scritto di intesa con l'UIC, la CONSOB e l'ISVAP, si forniscono poi tutta una serie di suggerimenti e di indicazioni operative per l'implementazioni di misure idonee, anche di controllo interno, a salvaguardare l'integrità aziendale da comportamenti (sia della clientela che degli operatori stessi) non conformi alle regole di sana e prudente gestione e di stabilità che, in buona sostanza, le prescrizioni in discorso mirano a tutelare[7] .
Malgrado queste cautele, la segnalazione continua ad essere vista come fenomeno "anticommerciale", ai limiti della delazione, per cui l'effettività e l'efficacia di questo "posto di blocco" si stanno progressivamente vanificando. Con ciò non si vuole assolutamente affermare che lo strumento segnalatorio può portare più rapidamente a soluzione le problematiche relative all'inquinamento del mercato finanziario da parte di soggetti che, non va dimenticato, sono "colletti bianchi", spesso insospettabili prestanome di articolazioni malavitose più complesse e, per ciò stesso, permeabili solo - quando vi si riesce - ad indagini condotte con sofisticati strumenti in possesso unicamente delle forze di polizia[8] .

La segnalazione di "abusi di mercato"

Come è noto, la direttiva europea 2003/6/CE sul cosiddetto market abuse ha apportato anche nel nostro ordinamento il concetto di "manipolazione del mercato" quale comportamento censurabile ai fini di una tutela del bene supremo del regolare andamento delle contrattazioni e di tutte le operazioni che siano fondate sulla fairness connaturata al luogo primario di incontro tra la domanda e l'offerta di risparmio e di investimenti.
In questa sede non appare irrilevante il parallelismo tra lo strumento scelto dal legislatore delegato e quello del già citato legislatore delle normativa contro il riciclaggio.
L'implementazione, nel Testo Unico della Finanza, delle misure previste dalla Legge n. 62/2005 (di recepimento della suddetta direttiva) ha previsto anch'essa il meccanismo della "segnalazione" quale deterrente contro comportamenti non in linea con le best practice di mercato.
In particolare, una segnalazione che possiamo definire "preventiva", statuita dall'art. 114 del TUF, il quale - al comma 7 - obbliga i soggetti che svolgono funzioni di amministrazione, controllo o direzione in un emittente quotato e tutti i dirigenti che abbiamo regolare accesso a informazioni privilegiate, nonché i soci che posseggano più del 10% del capitale sociale o il controllo dell'emittente quotato, a comunicare alla Consob e al pubblico le operazioni che essi effettuino (anche per interposta persona) sulle azioni o altri strumenti finanziari emessi dall'emittente stesso.
Quest'obbligo, pur avendo carattere preventivo e quindi comune a quello antiriciclaggio, mal si presta ad una effettiva comparazione, poiché si sostanzia in una "comunicazione al mercato" di operazioni senza alcun fumus di irregolarità.
Non appare ultroneo aggiungere che sia la citata legge 62/2005 sia la riforma del risparmio, attuata con legge n. 262/2005, hanno ampliato il novero dei momenti di confronto il tra mercato e i suoi attori, nell'ottica di una sempre più trasparente gestione sia degli emittenti che degli intermediari, nonché delle strutture organizzative coinvolte.
E' invece singolare la novità introdotta dalla Consob nel regolamento n. 11768 del 1998, peraltro a seguito dell'introduzione dell'art. 187 - nonies del TUF da parte della nominata legge 62/2005.
La norma primaria introduce un vero e proprio, questo si, obbligo di segnalazione di operazioni sospette di market abuse.

7 Per un commento più articolato al decalogo si veda R. Razzante, "Il decalogo-ter della Banca d'Italia: prime osservazioni", Diritto della Banca e del Mercato Finanziario, 2/2001.

8 Pare opportuno rammentare che la normativa antiriciclaggio assegna alla Guardia di Finanza e alla Direzione Investigativa Antimafia i compiti di approfondimento delle segnalazioni provenienti dall'UIC, il quale a sua volta metabolizza quelle rivenienti dai soggetti obbligati. E' molto più facile, questo almeno ci dicono i numeri, che reati come quello di riciclaggio vengano ad esistenza a seguito di autonoma attività investigativa di questi soggetti piuttosto che da impulsi degli intermediari o dei liberi professionisti.

In particolare, tutti i soggetti abilitati e le società di gestione del mercato devono segnalare "senza indugio" alla Consob le operazioni che, "in base a ragionevoli motivi", possono ritenersi configurare una violazione delle disposizioni di cui al titolo I-bis del TUF stesso (titolo per l'appunto dedicato all'abuso di informazioni privilegiate e manipolazioni del mercato) delle quali siano a conoscenza.
La Commissione ha fatto seguire a questa disposizione gli articoli dal 63 al 69 del citato regolamento mercati, e varie note esplicative, tra le quali la comunicazione n. DME/6027054 del 28 marzo 2006, che è seguita a quella (in questa sede più utile) del 29 novembre 2005.
Il complesso di regole e comportamenti emergente dal corpus normativo appena evidenziato appare di primario rilievo a chi scrive come il legislatore ancora una volta eserciti una opzione nei confronti della "soggettività" e "personalizzazione" del rapporto tra evento da segnalare e complesso di circostanze che inducono a segnalare il determinato evento.
In altri termini, sulla scorta dell'esperienza antiriciclaggio (che sembrerebbe qui essere quasi pedissequamente replicata), si fa ricorso all'affidamento di poteri "paraispettivi" ai soggetti obbligati, poteri che però, a ben guardare, non sono altro che una esplicitazione funzionale e finalizzata dell'ampio genus di regole e procedure ascrivibili ai controlli interni.
La prevenzione delle manipolazioni del mercato e del riciclaggio è cioè affidata alla segnalazione alle Autorità competenti, giammai a denunce all'Autorità di polizia, di comportamenti anomali dei soggetti esposti, in ossequio, peraltro, a meccanismi già sperimentati sui mercati più evoluti.
Altro elemento comune è la predisposizione, sempre da parte del regulator di settore, di una casistica esemplificativa e volutamente non esaustiva che aiuti l'operatore nella prefigurazione della tipologia di comportamento che possa essere oggetto di approfondimento.
Ci stiamo riferendo agli "indici di anomalia" contenuti nel più volte citato decalogo-ter contro il riciclaggio (cfr. parte II del documento) ed a quelli ripresi dalla Consob, e indicati dal CESR, nella comunicazione n. DME/5078692 del 29 novembre 2005.
Ci viene da fare qualche obiezione a quest'ultimo contesto segnalatorio solamente riguardo alle modalità della segnalazione, laddove al meccanismo più "blindato" previsto dall'UIC [9] per le operazioni di riciclaggio, la Consob ne preferisce uno più "aperto", in quanto l'art. 67 del regolamento mercati consenti la segnalazione anche per posta elettronica, per fax o telefono.
Positiva risulta invece, a conferma di quanto abbiamo tentato di dimostrare in questo scritto, la considerazione del grado di invasività che le due tipologie di reato hanno sul mercato e sui suoi protagonisti, operata dal legislatore del D. Lgs. 231 del 2001[10] , riguardante la responsabilità amministrativa delle persone giuridiche per i reati commessi da soggetti apicali o dipendenti e collaboratori.
Come noto, sono stati ritenuti sensibili ai fini della predisposizione dei cosiddetti "modelli di prevenzione" di cui al citato decreto anche i reati del TUF, come aggiornati dai recenti interventi legislativi e, più recentemente (con la legge comunitaria per il 2005), quello di riciclaggio, operandosi in tal modo un trait d'union tra i più efficaci ai fini della considerazione delle figure comportamentali di cui abbiamo disquisito e, soprattutto, della rilevanza sociale che il loro disvalore assume per il buon funzionamento del mercato nel suo complesso[11] .
La sintesi: come garantire una sicurezza davvero "globale" senza passare per una "tracciabilità completa" delle transazioni finanziarie che vanno ad essere (l'unica) fonte di approvvigionamento di risorse da impiegare nei reati, segnatamente di terrorismo ed eversione, che ne costituiscono la principale minaccia?

Ranieri Razzante

9 Tale meccanismo vede unicamente transitare la segnalazione dall'operatore all'UIC attraverso un software dedicato, riconoscibile dall'acronimo "SOS", mediante il quale la segnalazione di operazione anomala secondo la legge antiriciclaggio giunge all'Authority e da questa viene secretata, senza passaggi intermedi o visibili, tranne quelli interni alla struttura segnalante, che a loro volta possono avvenire solamente a mezzo di posta cartacea riservata e a protocollo dedicato.

10 Per un commento del quale rinviamo, ex multiis a Toscano F., Razzante R., La responsabilità amministrativa delle persone giuridiche, Giappichelli, Torino, 2003, nonché ai numerosi studi presenti sul sito www.reatisocietari.it .

11 Su quest'ultimo aspetto del riciclaggio ci piace segnalare la recente pubblicazione di Martucci P., La criminalità economica, Laterza, Bari, 2006.

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Università degli Studi di Siena
Dipartimento di Ingegneria dell'Informazione
Facoltà di Ingegneria

Articoli

Sistemi avanzati per la sicurezza

Definizione dello scenario e sua evoluzione

Premessa

I recenti accadimenti, sia a livello mondiale che a livello nazionale e gli scenari evolutivi che si stanno delineando, proiettano la Ns società ed i suoi stili di vita verso un futuro in cui gli aspetti di sicurezza giuocheranno un ruolo di primissimo piano. Risulta quindi evidente la necessità di trovare soluzioni: innovative, tecnologicamente all'avanguardia ed in grado di garantire adeguati livelli di sicurezza individuale e collettiva. Allo stesso tempo sta crescendo, tra la popolazione, la consapevolezza delle possibili conseguenze negative di un'invasione indiscriminata della propria sfera personale. Ciò impone di affrontare e risolvere gli aspetti relativi alla salvaguardia della libertà e della privacy di coloro che vivono nella legalità, in modo che essi possano tranquillamente usufruire dei beni e dei servizi che la società mette a disposizione.
E' evidente come tale scenario porti alla naturale identificazione di due aspetti fondamentali su cui poggia la tematica della sicurezza: un primo aspetto riguarda la sicurezza fisica, la "safety" (sorveglianza di ambienti urbani, extraurbani, di aree sensibili, ecc…); il secondo riguarda la sicurezza dei dati, la "security" (sicurezza informatica, protezione dei dati, rintracciamento di attività sospette in reti ed in INTERNET, ecc…).

Considerazioni generali

Molti sono gli aspetti che si intrecciano contribuendo a rendere articolato e complesso lo scenario della sicurezza. Un primo aspetto macroscopico, che evidenzia l'importanza di sistemi e architetture tecnologicamente avanzate (safety e security), è il fenomeno del terrorismo e della criminalità organizzata. Tale fenomeno è la principale fonte del crescente senso di disagio che si sta diffondendo capillarmente all'interno della società, seminando insicurezza e paura in larghe fasce della popolazione di ogni ceto ed estrazione sociale. Ciò è evidenziato, oltre che dagli odierni orientamenti internazionali e di politica europea, anche dalle varie iniziative a livello regionale e nazionale che hanno come obiettivo quello di affrontare seriamente il problema: "… anche mediante l'utilizzazione delle possibilità offerte dalle tecnologie in questi settori …" (si vedano, ad esempio il documento di indirizzo anci-regioni sulla sicurezza urbana giugno 2002, oppure la mappa dei progetti di sicurezza integrata realizzati dagli enti locali in italia nell'ambito del "miglioramento delle condizioni di vita nelle città" aprile 2005).
Lo sviluppo di sistemi di sicurezza: massivamente scalabili, autosostenibili ed a basso impatto ambientale (mimetici) rappresenta, pertanto, un obiettivo primario e ad elevata ricaduta sociale.
Un altro aspetto di estrema rilevanza, è quello legato agli orizzonti temporali ed ai trend internazionali in questo settore. E', infatti, opinione diffusa che le necessità di controllo e di sicurezza cresceranno progressivamente, anche a seguito di fenomeni di migrazione di massa, di sovrapopolamento e di necessaria integrazione multietnica. Tali fenomeni saranno di lunga durata, interesseranno vaste aree geografiche ed impegneranno ingenti risorse finanziarie. D'altra parte la risposta a tali esigenze risulta tuttoggi solo superficiale e par-

ziale. Esistono notevoli spazi di approfondimento, di innovazione e di ricerca scientifico/tecnologica. Da tale situazione di relativa "arretratezza" possono trarre notevoli vantaggi sia la ricerca sia le industrie operanti nel settore sicurezza.
Infine, va ricordato che esistono e sono via via in aumento, fenomeni di vandalismo che vanno da atti violenti e di aggressione su persone, ad atti di deturpazione di opere d'arte e di beni mobili e immobili, pubblici e privati. Sistemi di sicurezza innovativi, capaci di individuare automaticamente tali eventi, possono contribuire al contenimento dell'escalation di tali atti, aumentando la qualità della vita e la tranquillità di individui e comunità.

Quadro tecnologico di riferimento

Sistemi di sicurezza
La crescente miniaturizzazione nel settore della "Computer Technology" produrrà, in un prossimo futuro, processori e sensori che potranno essere integrati in maniera pervasiva nello spazio che ci circonda. Il continuo decremento dei costi dovuti alle nuove metodiche produttive ed agli sviluppi tecnologici, stanno rendendo possibili una moltitudine di nuove utilizzazioni genericamente denominate: "Pervasive Computing". La forza trainante di questi continui progressi tecnologici è stata sancita nel 1960 da Gordon More , che ha previsto un raddoppio della capacità computazionale ogni 18 mesi. Tale previsione si è rivelata esatta fino ad oggi e si ritiene continuerà ad esserlo per i prossimi 15 anni. I processori diventeranno più potenti, piccoli e poco costosi, tanto che si può ritenere che vi sarà una loro sostanzialmente illimitata disponibilità. Parallelamente, gli sviluppi delle micro e nanotecnologie stanno già consentendo la produzione di sensori minuscoli, capaci di rilevare una vasta categoria di parametri ambientali. Uno sviluppo interessante riguarda i "Radio Sensors", che possono trasmettere le loro rilevazioni a distanze di qualche decina di metri sfruttando l'energia dell'ambiente o ricavandola direttamente dal procedimento di misura. Le etichette elettroniche ("Smart Labels", RFID tags) possono operare a bassa energia, oppure ricevendola dall'esterno durante le procedure di interrogazione. Possono avere dimensioni di un millimetro quadrato ed essere più sottili di un foglio di carta. La cosa interessante è che esse abilitano la chiara e sicura identificazione degli oggetti cui sono applicate e, quindi, consentono di associare ad essi dei records informativi memorizzati in database remoti (anche su Internet). In altre parole, ogni entità del mondo reale può essere identificata univocamente a distanza e collegata alle informazioni pertinenti. Recentemente sono stati anche fatti notevoli passi avanti nel settore delle comunicazioni wireless. Sono di particolare interesse le comunicazioni autoconfiguranti a corto raggio, che richiedono bassissime potenze e consentono la realizzazione di reti di sensori interconnessi e massivamente distribuiti nelle aree da controllare (Wireless Sensor Networks). Minuscoli ed economici processori, con sensori integrati e possibilità di comunicazione wireless, capaci di collegare informazioni alle entità del mondo fisico, di localizzarle ed identificarle, capaci di muoversi e di scoprire quali altri oggetti sono nelle vicinanze e che cosa sta loro accadendo o gli è accaduto nel recente passato. Questo è lo scenario che si sta aprendo, popolato di sensori più evoluti dei semplici trasduttori di grandezze fisiche, capaci di memorizzare, di calcolare e di comunicare ("Smart Sensors"). E' con questo scenario che si devono confrontare i futuri sistemi avanzati di sicurezza.
Si può osservare come l'impiego di Smart Sensors consenta di avvicinare l'elaborazione dell'informazione di misura al fenomeno misurato. Ciò apre la possibilità di implementare paradigmi di sorveglianza più efficaci e con tempi di reazione più brevi, evitando la classica sindrome del "post-factum" tipica di molte delle attuali architetture. E' possibile: prendere decisioni direttamente in corrispondenza di un determinato evento, preaggregare eventi elementari al fine di supportare processi ragionativi di livello superiore, fornire preallarmi automatici in tempo reale (early warnings) e consentire azioni preventive (spostamento dalla "investigazione sugli eventi" alla "prevenzione degli eventi pericolosi") od evitare di sovraccaricare il sistema di controllo centralizzato con informazioni ridondanti e/o inutili. E' anche evidente che, poiché l'uomo ha capacità limitate nell'elaborare informazioni, il crescere della estensione e complessità dei fenomeni/ambienti da monitorare nonché la maggiore quantità di parametri misurabili e la maggiore capillarità di misura, rendono necessario delegare al sistema di sicurezza alcune funzionalità di livello semantico più elevato. I sistemi di sicurezza della prossima generazione devono poter supportare meccanismi preattentivi ed attentivi in modo da focalizzare le

risorse e richiamare l'attenzione sulle informazioni maggiormente utili, devono essere in grado di preaggregare e fondere (Data Fusion) dati multisensoriali/multitemporali (affetti da: incertezze, contradditorietà, incompletezze) in modo da supportare processi ragionativi deduttivi ed inferenziali. Devono poter preinterpretare i dati ed essere capaci di autoapprendere alcuni parametri di funzionamento, devono facilitare la comprensione di eventi e situazioni complesse e supportare i processi decisionali anche attraverso meccanismi automatici in grado di comprendere il contesto attuale e la sua evoluzione presentando le possibili sequenze di azioni che meglio si adattano al contesto stesso.
Solo recentemente il settore della sicurezza si è orientato verso sistemi intelligenti in grado di capire autonomamente situazioni potenzialmente pericolose e di supportare informazioni multisensoriali. Questo settore sta attraversando una fase di notevole sviluppo e ricerca le cui ricadute pratiche stanno iniziando ad affacciarsi sul mercato della safety e della security, spesso sotto forma di prototipi. Ma ancora oggi, ad esempio, la maggior parte dei sistemi di videosorveglianza funziona trasmettendo i flussi video provenienti dalla rete di videocamere ad una serie di monitor in una apposita sala di controllo in cui operano addetti umani che rilevano gli eventi anomali. È chiaro che un compito del genere è noioso e privo di stimoli, il che ingenera frequenti errori dovuti ad inevitabili cali di attenzione. Uno studio dell'US National Institute of Justice ha dimostrato che dopo soli 20 minuti di osservazione di un monitor, l'attenzione cala al disotto dei livelli accettabili. Quindi è inevitabile l'introduzione di sistemi intelligenti e proattivi nonché di opportune tecniche di Information Visualization che consentano una rappresentazione compatta delle informazioni esaltandone gli elementi salienti.
Naturalmente il moltiplicarsi delle possibilità operative, la significativa crescita di complessità dei sistemi periferici, la necessità di sfruttare la grande flessibilità offerta dalle nuove tecnologie di Pervasive Computing, il proliferare delle reti ibride (wireless e wired) e l'esigenza di garantire prestazioni affidabili, robuste, protette e rispettose della privacy, impone di ridefinire la filosofia di approccio dei sistemi di sicurezza di nuova generazione e di affrontare le relative tematiche secondo nuovi paradigmi. Per esempio, anche i sistemi di sicurezza di ultima generazione presentano il fondamentale problema che le informazioni sul contesto applicativo vengono definite in fase di progettazione ed inglobate all'interno della struttura del sistema stesso. Spesso il filtraggio degli eventi viene effettuato mediante automi a stati finiti e/o mediante espressioni booleiane applicate ai singoli eventi provenienti dai sensori di campo. Ovvero, secondo l'attuale filosofia, è necessario pensare in fase di progettazione a tutto ciò che si vuol sapere dell'ambiente esterno e costruire una logica di controllo specifica per ottenere tali informazioni. Lo svantaggio di questo approccio sta nel fatto che, una volta costruito il sistema, è complicato se non impossibile aggiungere nuove funzionalità inizialmente non prefigurate, in quanto questo significa far proliferare a dismisura gli stati degli automi e/o stravolgere le espressioni booleiane preesistenti e le relative tabelle di verità. Inoltre, le odierne metodologie di interpretazione e riaggregazione delle informazioni, sono inadatte a gestire l'ingente mole di dati provenienti dalle reti di Massively Embedded Sensors che la tecnologia sta mettendo a disposizione. In altre parole, le applicazione risultano complicate e poco scalabili soprattutto perché tendono ad accedere direttamente (od al più con pochi passaggi intermedi) al livello fisico (i sensori) dedicato alla rilevazione dell'ambiente.

Sistemi Context Aware

La Context Awareness è un campo di ricerca recente che sfrutta le informazioni di contesto per aumentare le prestazioni delle applicazioni (che vengono denominate "Context Aware"). Uno dei problemi consiste proprio nel definire che cosa sia il contesto e come si possano ottenere le informazioni di contesto. In generale si intende per contesto ogni informazione sensoriale disponibile che è rilevante per una specifica applicazione, escludendo gli input ed output forniti dall'utente. Si considerano cioé le sole informazioni implicite, quelle che pur essendo in qualche modo già presenti in forma distribuita all'interno delle varie sottoparti del sistema, necessitano di una elaborazione per poter essere riunite e ricomposte in un tutt'uno significativo. In questo senso un'applicazione Context Aware è un'applicazione che usa il contesto per migliorare le proprie prestazioni o per fornire informazioni o servizi rilevanti agli utenti.

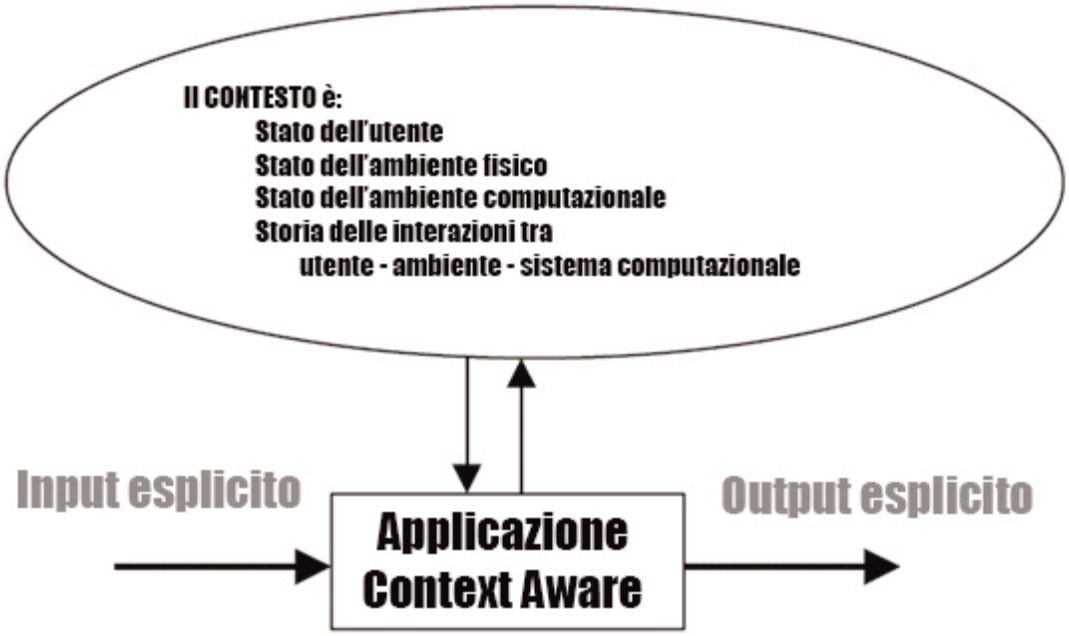


Figura I Concetto di contesto

Tipici esempi di informazioni contestuali sono:
- informazioni spaziali (ubicazione, orientazione, velocità accelerazione, per esempio, lo RFID n° 111111-111111 che si trova alle coordinate 10,300,75 è nella "sala riunioni 23 del complesso B")
- informazioni temporali (ora, data, stagione)
- informazioni ambientali (temperatura, qualità dell'aria)
- informazioni di identità (per esempio, lo RFID n° 111111-111111 è "Guido Rossi")
- situazioni sociali (presenza di persone: da sole, in gruppo)
- misure fisiologiche e fisiche (pressione sanguigna, frequenza cardiaca e respiratoria, biometria dell'iride, conformazione facciale)
- attività (parlare, leggere, camminare, correre)

La disponibilità di tali informazioni permette di:
- rappresentare il contesto attuale sintetizzando eventi di livello superiore a partire da eventi e dati di livello inferiore (più elementari)
- analizzare i cambiamenti di contesto ed agire nella maniera più opportuna sfruttando la storia del contesto stesso
- adattare la presentazione delle informazioni selezionando le più rilevanti o svolgendo azioni o sequenze di azioni nella maniera più efficace dipendentemente dal contesto
-modificare le tecniche di interazione con gli utenti e con gli altri sottosistemi in funzione del contesto corrente e/o del suo trend
- fornire suggerimenti o proporre azioni e processi sulla base del loro utilizzo passato in contesti simili a quello corrente
- semplificare lo svolgimento di azioni che coinvolgono decisioni umane dipendentemente dal contesto e dalla sua evoluzione
- aggiungere o suggerire significati e supporti informativi alternativi in funzione del contesto

Le architetture Context Aware si fanno carico delle problematiche di elaborazione distribuita, di rintracciamento delle risorse, della loro allocazione e deallocazione in funzione del contesto e delle finalità, della preelaborazione e preaggregazione dei dati, della loro fusione, mascherando la complessità fisica del sistema e fornendo informazioni significative agli strati applicativi e decisionali. Attraverso il loro operato si possono con-

trollare le attività che si stanno svolgendo in ciascun contesto e come queste attività evolvono nel tempo.
In altre parole, un sistema Context Aware e costituito da vari moduli e sottosistemi, ognuno in grado di acquisire, dall'ambiente circostante e dal contesto, tutto un insieme coordinato di informazioni. Tali moduli sono, in genere, estremamente diversificati a causa dei differenti tipi di informazioni da reperire ed a causa dei vari modi che esistono per reperire una stessa informazione. Essi devono essere facilmente aggregabili ed interfacciabili con le applicazioni che li utilizzano. L'interfacciabilità viene garantita mediante uno scambio di informazioni ottenuto attraverso un "linguaggio comune", sintetico, efficace e manipolabile semanticamente. In questo modo, le soluzioni a problemi diversi possono essere raggiunte in tempi più brevi ed in modo sistematico.
Possiamo pensare un sistema basato su Context Awareness come un sistema a tre livelli, dove il livello più basso (livello fisico) è quello dei sensori, le unità fisiche che si interfacciano direttamente con la realtà, il livello intermedio (middleware), quello della architettura Context Aware, che manipola e trasforma i dati "raw" dei sensori in una forma sintetica e, infine, il livello più alto, quello dell'applicazione, che sfrutta i dati provenienti dal middleware per prendere decisioni di alto livello.

Figura 2 Ruolo delle architetture Context Aware

Tra i livelli adiacenti c'è un continuo scambio di informazioni, mentre il livello fisico è completamente schermato da quello applicativo. Il flusso di informazione tra questi due livelli è garantito dal livello intermedio, cioè dall'architettura Context Aware. In questo modo chi deve scrivere l'applicazione non s'interessa dei di come funzionano i vari moduli, ma soltanto di come sfruttare al meglio le informazioni ed i servizi di alto livello che essi forniscono.
I "blocchi costitutivi" di cui consiste un'architettura context-aware, consentono: l'estrazione delle informazioni di contesto, la loro combinazione, la loro presentazione agli strati applicativi veri e propri. Più in particolare si distinguono:

1) i Context Widgets che forniscono le informazioni di contesto ottenute, per esempio, da sensori o da basi di dati specificamente progettate. Tali blocchi consentono di schermare gli applicativi dai dettagli di funzionamento dei componenti di livello più basso. La comunicazione distribuita avviene in maniera trasparente tanto per gli applicativi quanto per i sensori
2) i Context Interpreters che trasformano le informazioni di contesto rendendole utili alle applicazioni (per esempio, un codice identificativo di una persona rilevato da un lettore RFID può essere trasformato nel nome della persona. Oppure, determinate coordinate x-y-z possono essere trasformate in un nome simbolico come "magazzino 3 - reparto A"). Deve essere possibile usare tecniche differenziate di interpretazione (per esempio: tecniche di fusione dati, operatori logici booleiani, tecniche di autoapprendimento, tecniche di classificazione, HMM, grammatiche adatte a specificare concatenzaioni temporali di eventi, ecc...)
3) i Context Servers che aggregano contesti tra loro correlati per ottenere informazioni di livello superiore (per esempio aggregando parametri quali: rapidità di movimento, direzione, dimensioni, periodo del giorno, al fine di valutare la pericolosità di un'entità in moto in una certa regione di spazio)
4) i Context Discoverer che forniscono una descrizione dei vari componenti di un'architettura in modo che gli applicativi specifici possano esere indirizzati trasparentemente ai Context Widgets, Interpreters e Servers opportuni
5) i Context Dispatchers che provvedono a rendere disponibili le informazioni di contesto a tutti i sottosistemi che ne necessitano e che si sono "dichiarati interessati" a tali informazioni. Le informazioni di con-

testo possono derivare direttamente da sensori (eventulamente dopo l'interpretazione), oppure derivare da processi di astrazione. E' importante che i blocchi che acquisiscono le informazioni contestuali operino costantemente ed indipendentemente dalle applicazioni specifiche che ne fanno uso, in modo che le relative informazioni contestuali possano essere disponibili in parallelo per più applicazioni distinte aventi finalità distinte.

Le predette caratteristiche rendono le architetture Context Aware particolarmente adatte alle applicazioni di sicurezza, monitoraggio e controllo, abilitando lo sviluppo di sistemi facilmente scalabili ed in grado di gestire ambienti complessi, distribuiti su aree vaste e sottoposti a dinamiche di difficile interpretazione (soprattutto quando i requisiti sui tempi di risposta sono stringenti).

E' prevedibile che il futuro delle piattaforme software per la sicurezza si baserà su moduli Context Aware, facili da interconnettere e specializzati nella rilevazione e preaggregazione di dati ed informazioni tipiche degli scenari di sicurezza. Al loro interno i moduli elaboreranno e/o aggregheranno le informazioni, rendendole disponibili sotto forma di descrizioni in linguaggio simbolico sulle quale potrà agire il livello applicativo, secondo modalità inferenziali e cognitive. Ciò aumenta la capacità di discriminare gli eventi e di comprendere ciò che sta accadendo nell'ambiente sottoposto a controllo, facilita la progressiva aggiunta delle nuove tecnologie via via disponibili, rende possibile l'espansione verso nuove funzionalità e servizi, il tutto in maniera più semplice e sicura.

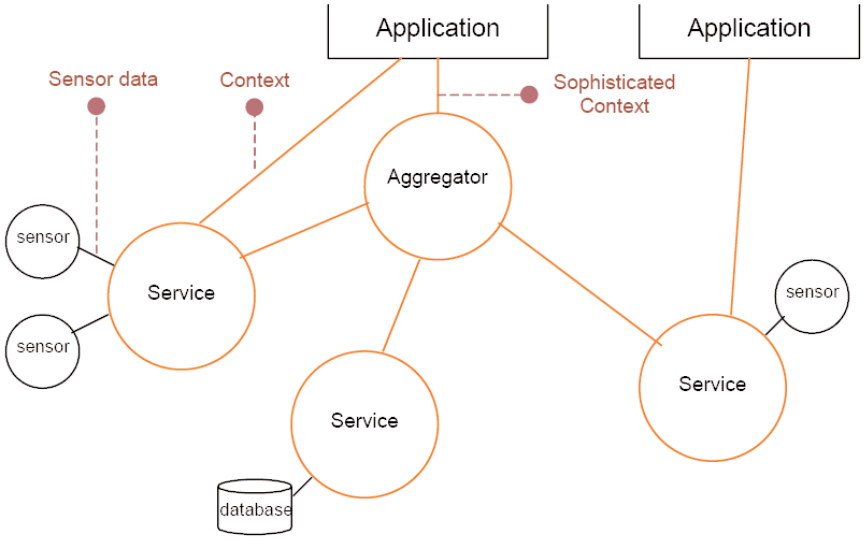


Figura 3 Struttura di un sistema Context Aware

Fig 4 Tipica catena logica di elaborazione Context Aware

Concludendo, l'introduzione di piattaforme Context Aware progettate per i sistemi di safety e security consente:

- una gestione efficiente della complessità e del vasto e variegato mondo dei sensori
- la creazione di applicazioni intelligenti basate su descrizioni semantiche e capaci di interpretazioni di più alto livello
- un approccio sistematico per affrontare problemi inerenti alla sicurezza e al controllo
- un'opportunità per incrementare le prestazioni delle applicazioni di safety e security, la loro efficienza e la flessibilità evolutiva
- un nuovo settore di ricerca che stimola la definizione di nuovi processi e servizi nella filiera della safety e della security, nel pieno rispetto della privacy

Sistemi Context Aware per la sicurezza

Le argomentazioni delle precedenti sezioni evidenziano come lo sviluppo di sistemi intelligenti ed avanzati per la sicurezza, debba confrontarsi con nuovi scenari tecnologici basati:

- sull'acquisizione massiva di dati multisensoriali/multitemporali
- sulla conoscenza di informazioni di contesto
- sull'interazione attiva con il contesto stesso
- sulla descrizione ed interpretazione semantica di quanto accade
- sul rispetto della privacy individuale
- sull'autenticazione dei dati e loro delivery sicuro

e come tutto ciò possa essere affrontato mediante lo studio e sviluppo di architetture Context Aware. Lo scopo delle architetture Context Aware per la sicurezza è quello di definire i requisiti fondamentali di tali sistemi, in quale modo essi debbano essere strutturati, quali siano i blocchi costitutivi, quali le funzioni e quali i requisiti peculiary nell'ambito sicurezza. Inoltre, devono essere considerate anche le modalità di scambio di informazione tra i vari blocchi, la loro gerarchia ed i flussi informativi.

Su queste tematiche iniziano ad emergere considerevoli conoscenze nell'ambito della comunità scientifica e sono già comparsi alcuni prototipi di architetture che supportano lo sviluppo di applicazione consapevoli del contesto. Tuttavia molto resta da fare per lo specifico settore della sicurezza.

Possibili scenari applicativi

I sistemi Context Aware pervasivi, specializzati nello svolgimento di attività peculiari nell'ambito sicurezza (safety e security), si prestano ad applicazioni in molteplici ambiti operativi, tra i quali:

- sicurezza aeroportuale e portuale
- monitoraggio di ambienti domestici abitati da persone anziane
- sicurezza nell'ambito delle raffinerie e di altre aree a rischio potenziale
- sicurezza di aree cittadine (piazze, monumenti, giardini pubblici, ecc...)
- sicurezza di aree di parcheggio e di scambio merci
- sicurezza di quartiere
- sicurezza delle stazioni ferroviarie e metropolitane
- protezione e prevenzione di atti vandalici sia a danni di persone che di beni

Aspetti scientifici e tecnologici

L'obiettivo dei sistemi Context Aware per la sicurezza, è quello di costruire una piattaforma modulare facilmente scalabile e aggiornabile per la realizzazione di sofisticate applicazioni con capacità cognitive e inferenziali avanzate rispetto a quelle degli attuali sistemi. Tale piattaforma si basa su una serie di moduli Context Aware, specializzati per la rilevazione di determinate informazioni, che cooperano sinergicamente al fine di ottenere, in tempo reale, una rappresentazione sinottica del contesto. Tale rappresentazione è il punto di partenza per operazioni semantiche e ragionative capaci di aumentare le performance ed il livello di automazione del sistema di sicurezza stesso. I punti principali che richiedono ulteriori approfondimenti sono:

- Specificazione del contesto
- Interpretazione del contesto
- Specificazione dell'interfaccia comune di accesso al contesto
- Memorizzazione e recupero del contesto
- Descrizione del contesto
- Modellizzazione del contesto

Lo studio di questi punti deve mirare ad una rappresentazione del contesto costituita da sotto-contesti, in modo da renderla dinamica. Infatti, applicazioni di sicurezza differenti possono avere bisogno di conoscere aspetti diversi del contesto, ovvero la rappresentazione deve adattarsi con facilità alla situazione specifica. Ad esempio, in un'azione di monitoraggio di una sala di attesa di un aeroporto sono aspetti importanti: la densità di persone (per capire se c'è sovraffollamento), le attività svolte dalle persone (per riconoscere comportamenti anomali), la localizzazione di oggetti smarriti e/o sospetti. In un'azione di controllo automatico della salute e dello stato di vita di una persona anziana sono aspetti importanti: le condizioni dei parametri fisio-

logici, il livello di vitalità e movimento, l'esecuzione di specifiche sequenze di azioni. È chiaro che ciascuna delle due situazioni precedenti necessita di una diversa rappresentazione del contesto. Quindi, per costruire un sistema flessibile e scalabile al variare delle situazioni, è necessario studiare una rappresentazione del contesto che possa essere scomposta in sottoparti da unire nel modo più adatto alla specifica situazione.
Accanto a questi temi di carattere più generale, si devono affrontare studi specifici per la caratterizzazione dei moduli Context Aware che costituiscono la piattaforma. Infatti, ogni modulo è dedito alla rilevazione di un aspetto differente del contesto a partire da misurazioni real-time di un insieme articolato di caratteristiche fisiche sia di tipo puntuale che di tipo areale. Le misure puntuali possono essere effettuate tramite WSN autoconfiguranti, mentre quelle areali tramite sensori video e/o audio. Ad esempio, si può pensare alla costituzione di un modulo context aware per la localizzazione dell'entità in movimento in un certo ambiente che fornisca agli applicativi informazioni di alto livello del tipo: persona che corre in posizione (x,y,z), oppure: gruppo di persone ferme vicino alla finestra. Tale modulo può ricevere informazioni da un sistema di telecamere che riprendono la scena da più viste, da una WSN che monta sensori di vario tipo (temperatura, di prossimità, magneto-resistivi, etc.) e da una serie di array microfonici.
In particolare alcuni elementi di rilievo che necessitano di ulteriori approfondimenti ed implementazioni mirate sono:

- tecniche di identificazione basate sul riconoscimento vocale e facciale
- tecniche di localizzazione di persone e cose
- tecniche di analisi del comportamento e delle attività
- stima della conforazione spaziale de della giacitura dei corpi degli individui
- riconoscimento di espressioni e gesti
- tecniche di gestione di flussi informativi "molti-ad-uno" e "molti-a-molti" tra sensori ed utenti, nonché tra sensori e sensori finalizzati all'implementazione di sistemi di sicurezza scalabili e pervasivi
- implementazione di infrastrutture massivamente scalabili in grado di supportare la memorizzazione, l'analisi ed il recupero real-time di informazioni multisensoriali
- implementazione di infrastrutture capaci di garantire il coordinamento di sensori multipli funzionanti a diverse scale spaziali e temporali

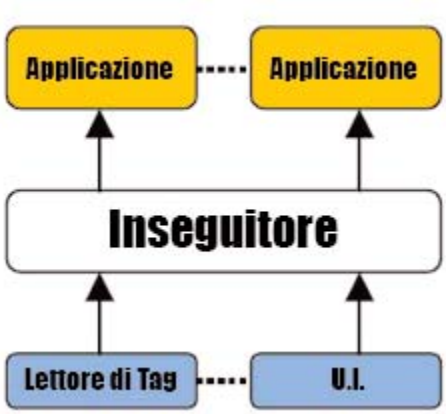


Figura 5 Integrazione di funzionalità eterogenee

Privacy

Col proliferare dei sensori distribuiti e con la crescente capacità dei sistemi computazionali Context Aware, le tecniche di sorveglianza intelligente possono risultare di grande aiuto nel controllo distribuito, nella prevenzione di crimini, nella lotta alla criminalità organizzata ed al terrorismo. Tuttavia si apre, in parallelo, una serie di problematiche di non secondaria importanza, sulle quali è opportuno riflettere attentamente.
La potenziale intrusione nella privacy personale attraverso l'uso di dispositivi di video sorveglianza è probabilmente l'aspetto più immediato da cogliere. La possibilità di un monitoraggio occulto è sicuramente molto pericolosa e può riguardare aspetti intimi della vita delle persone Tuttavia, anche il monitoraggio esplicito (cioè quello di cui le persone vengono esplicitamente avvisate) può ingenerare problemi. Tutto ciò che accade nel campo di vista di un sensore viene acquisito, sia che sia rilevante allo scopo della video sorveglianza, sia che non lo sia. Pertanto è probabile che, senza adeguate politiche di controllo, le immagini di ognuno possano progressivamente finire per popolare database informativi di varia natura e finalità.
Un altro importante aspetto riguarda la privacy delle informazioni acquisite e generate da attività di video sorveglianza. E' già accaduto, ad esempio, che spezzoni di filmati siano stati riutilizzati per spot pubblicitari televisivi. Tali spezzoni comprendevano immagini di scollature femminili e altre riprese similari, fino ad arriva-

re ad atti sessuali tra adulti consenzienti.
Le cose si complicano ulteriormente, se si considera che la video sorveglianza ha zone di sovrapposizione con altre tecnologie e in particolare con quelle dell'informazione e della telecomunicazione (Information Communication Technology, ICT). Le informazioni acquisite attraverso altri canali possono essere incrociate per registrare le abitudini delle persone attraverso le tracce lasciate durante la navigazione in internet, oppure nei log delle transazioni telefoniche e di quelle con carte di credito e similari. Le informazioni personali sono spesso il denominatore comune delle tecnologie di video sorveglianza e di ICT. La convergenza tecnologica sta assottigliando le barriere tra questi settori applicativi. Uno stesso dispositivo può essere sfruttato in ambedue le aree. Un telefono cellulare, ad esempio, è sia un mezzo di comunicazione che un mezzo di localizzazione che può essere intercettato. Le tecnologie di riconoscimento biometrico (impronte digitali, riconoscimento facciale, per esempio), possono essere usate contro le frodi, ma possono anche essere usate per monitorare dove un libero cittadino è stato durante la giornata e quali abitudini e preferenze ha esibito. I sistemi di video sorveglianza del traffico, possono essere usati per ridurre le congestioni e suggerire cammini alternativi in caso di incidenti, ma possono anche servire a monitorare gli spostamenti di un individuo. Anche se molti settori della società hanno ricevuto indubbi vantaggi dalla fusione di queste ambiti tecnologici e, pertanto, si può ipotizzare che la diffusione dei moderni sistemi di video sorveglianza continuerà a subire potenti impulsi, è necessario procedere con grande attenzione prevedendo adeguati meccanismi di controllo e garanzia, affinché tutto ciò risulti di reale vantaggio per la collettività. In questo senso l'utilizzazione di architetture Context Aware può fornire una possibile modalità di approccio, in quanto i dati e le informazioni possono rimanere distribuite nell'ambito del sistema in maniera tale che sia sostanzialmente impossibile riaggregarle in un tutt'uno significativo se non mediante operazioni di "raccolta" (Collecting) e reinterpretazione avviabili solamente sotto il controllo delle autorità competenti ed in caso di effettiva necessità investigativa.

Alessandro Mecocci

Bibliografia

R. T. Collins, A. J. Lipton, and T. Kanade, Introduction to the special section on video surveillance, IEEE Trans. Pattern Anal. Mach. Intell., vol. 22, pp. 745-746, Aug. 2000
K. Toyama, J. Krumm, B. Brumitt, and B. Meyers. Wallflower: Principles and practice of background maintenance. In Proc. International Conference on Computer Vision, pages 255-261, 1999
R.T. Collins, A.J. Lipton, H. Fujiyoshi, and T. Kanade, Algorithms for Cooperative Multisensor Surveillance, Proceedings of the IEEE, vol. 89, no. 10, October 2001
D. Koller, K. Daniilidis, and H. Nagel. Model-based object tracking in monocular image sequences of road traffic scenes. International Journal of Computer Vision, 10(3):257-281, June 1993
N. Friedman, S. Russel, Image Segmentation in Video Sequences: A Probabilistic Approach, Uncertainty in Artificial Intelligence, 1997
M. Isard and A. Blake. Contour tracking by stochastic propagation of conditional density. In Proceedings of the 1996 European Conference on Computer Vision, pages 343-356, 1996
J. Barron, D. Fleet, and S. Beauchemin. Performance of optical flow techniques. International Journal of Computer Vision, 12(1):42-77, 1994
T. Kanade, R. Collins, A. Lipton, P. Anandan, and P. Burt. Cooperative multisensor video surveillance. In Proceedings of the 1997 DARPA Image Understanding Workshop, volume 1, pages 3-10, May 1997
H. Fujiyoshi and A. Lipton. Real-time human motion analysis by image skeletonization. In Proceedings of the 1998 Workshop on Applications of Computer Vision, 1998
A. F. Bobick, J. W. Davis,,The Recognition of Human Movement Using Temporal Templates, IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 23, no. 3, march 2001

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Ministero dell'Interno
Dipartimento della Pubblica Sicurezza
Segreteria del dipartimento Ufficio Ordine Pubblico

Articoli

Contributo del Dipartimento della Pubblica Sicurezza per l' "Osservatorio per la Sicurezza Nazionale"

La delicata situazione internazionale e gli attentati perpetrati in Europa ed in altri continenti hanno imposto, nella considerazione che anche il nostro Paese doveva ritenersi esposto a rischio, l'esigenza di rivisitare le procedure e le attività da porre in essere, in caso di minaccia o di un grave evento terroristico, per la salvaguardia delle Istituzioni e dei singoli cittadini, anche alla luce delle modifiche normative intervenute a livello internazionale, soprattutto in tema di trasporto pubblico portuale ed aeroportuale.
In tale ottica, in Italia, dopo l'attentato alle Twin Towers, il Dipartimento della Pubblica Sicurezza ha avviato una profonda ed incisiva attività di rielaborazione delle pianificazioni territoriali e di rivisitazione delle risorse tecnologiche esistenti, richiedendo, in uno spirito sinergico, la collaborazione di diverse realtà pubbliche e private.
Circa due anni orsono è stato, infatti, emanato il nuovo Piano Nazionale antiterrorismo, nel quale, oltre a riaffermare il ruolo delle strutture deputate al mantenimento dell'ordine e della sicurezza pubblica, precisandone poteri e responsabilità, sono state individuate le Amministrazioni e gli Enti comunque interessati, coinvolgendoli direttamente nell'elaborazione del cennato Piano e prevedendo per ciascuno procedure e compiti.
E' indubbio che di fronte a fatti che possono mettere potenzialmente a rischio la sicurezza delle istituzioni e dei cittadini è necessaria l'azione sinergica di tutti i soggetti a vario titolo interessati, allo scopo dell'individuazione e successiva sperimentazione di un modello univoco di intervento finalizzato, qualora venga a concretarsi una situazione di crisi connessa ad un attacco terroristico, ad uniformare le procedure organizzative ed operative.
A tal riguardo, nel 2005, è stato costituito un apposito Gruppo di Esperti con l'incarico di elaborare un documento contenente le "Linee guida per la gestione delle emergenze" sul territorio nazionale.
Conseguentemente, sulla base del citato documento, le Autorità provinciali di P.S. hanno così potuto immediatamente avviare una rivisitazione anche delle pianificazioni locali antiterrorismo, al fine di adeguarne strumenti e metodologie operative.
Particolare impegno è stato, quindi, dedicato alle attività esercitative tenutesi in primo luogo nelle più grandi aree metropolitane (Roma, Milano, Torino e Napoli), alle quali hanno partecipato, in qualità di "osservatori", anche esperti internazionali.
I positivi risultati conseguiti nella gestione di scenari così articolati, hanno richiesto da un lato la disponibilità di consistenti risorse umane, adeguatamente addestrate, dall'altro l'impiego - ed in alcuni casi la sperimentazione - di strumenti e tecnologie altamente sofisticate soprattutto nel campo dell'informazione, supportate da quelle attraverso le quali è stato possibile acquisire immagini in diretta dal "cratere simulato".
Tutto questo costituisce oggi un efficace dispositivo di sicurezza nazionale, peraltro in continua evoluzione, che ha visto la sua applicazione, seppur limitatamente ad una circoscritta parte di territorio, in occasione delle recenti Olimpiadi invernali di Torino.
Quando nel febbraio 2006, a Palazzo Salviati, si è tenuto il primo incontro sul tema "Prospettive per la sicurezza nazionale" è parsa concretizzarsi l'idea di poter riunire, in tale spirito, più rappresentanti (Forze arma-

te, Forze di polizia, ecc.) con i quali condividere professionalità, lesson learnt ed informazioni, nel rispetto di ciascuna competenza.
Pur nella consapevolezza della continua evoluzione della minaccia terroristica si è oggi in grado di affermare che le attività fin qui poste in essere ed il superamento delle criticità emerse in sede esercitative hanno consentito di impiegare e sperimentare con successo, per la prima volta in contesti urbani per finalità di antiterrorismo, tecnologie diversamente impiegate e/o parzialmente utilizzate curando la professionalità degli utilizzatori, nonché perseguire la finalità di scongiurare quella confusione di ruoli che potrebbe pregiudicare il superamento dell'emergenza.

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Stato Maggiore Esercito

Articoli

L'Esercito per la sicurezza "Le Crisis Response Operations" come banco di prova dell'impiego multifunzionale dell'Esercito

Appena dieci anni fa la creazione di una struttura come l'OSN (Osservatorio sulla sicurezza nazionale) sarebbe sembrata un vezzo, una di quelle realtà nate per dare materia di studio a qualche occhialuto scienziato interessato alla filosofia della sicurezza senza alcun risvolto operativo. Questo prima che gli attentati sanguinosi di Madrid e di Londra portassero l'attacco terroristico di matrice fondamentalista islamica nel cuore dell'Europa, prima, cioè, che si capisse quanto anche l'Italia fosse a rischio.
Dopo l'11 Settembre il confine fra sicurezza e difesa è diventato molto più labile, anche in termini geografici. Delimitare la dimensione nazionale, quella europea e quella internazionale è, ormai, impossibile. In seguito alla diffusa consapevolezza che si ha a che fare con un terrorismo sempre più mondializzato in grado di colpire ovunque nel mondo, la risposta dei governi occidentali in materia di sicurezza si è orientata, giustamente, verso il superamento della dimensione nazionale per assumere una dimensione strategica e operativa globalizzata.
Ma cosa succede all'interno dei singoli Stati? Esistono delle forme di interazione operativa strutturate tra i diversi attori coinvolti sulle tematiche della sicurezza? E, soprattutto, qual è l'ottica con cui guardare alla sicurezza e di conseguenza qual è il sistema di collaborazione da costruire? L'Esercito si è interrogato spesso su questo argomento ed ha, perciò, condiviso da subito l'idea dell'Osservatorio Nazionale sulla Sicurezza, di una struttura cioè che rispondesse all'esigenza di creare una rete interna al territorio nazionale costituita da tutti gli enti e le strutture aventi causa in materia di sicurezza. L'approccio metodologico di mettere in sistema tutti gli attori è il punto di forza dell'OSN. L'integrazione dell'impegno ottimizza l'efficacia dell'azione.
L'Esercito, Forza Armata più antica, che vive ed opera sotto l'egida del Ministero della Difesa le cui politiche sono ormai strettamente intrecciate con quelle della sicurezza, da oltre quindici anni si è misurato con i profondi mutamenti dello scenario geo - politico e della situazione interna ed internazionale. Ha accolto, perciò, l'iniziativa dell'OSN come risposta all'esigenza fortemente sentita di collegare le proprie attività con tutti gli altri soggetti interessati ad operare in questa nuova dimensione della sicurezza.
La tipologia di attività che l'Esercito è chiamato a svolgere è molto ampia. Non si tratta più di opporsi ad una sola minaccia conosciuta nella sua entità, tipologia e modalità d'azione, ma di approntare forze capaci di far fronte a minacce o rischi non chiaramente conosciuti, in possesso di capacità estremamente variabili, che potrebbero concretarsi in tempi indeterminati, con modalità operative differenti, generalmente asimmetriche.
La Forza Armata in grigio - verde è pronta per fronteggiare gli attacchi alla sicurezza sotto tutti gli aspetti: da quello batteriologico a quello nucleare, a quello legato alle trasmissioni e alle comunicazioni.
Proprio perché la sicurezza, nella sua accezione più ampia, non ha più dimensioni prevalentemente militari, ma è divenuta un concetto caratterizzato da una spiccata multidimensionalità e multifunzionalità, l'Esercito costituisce uno dei principali mezzi a disposizione del Vertice politico.
Le moderne operazioni di risposta alle crisi non art. 5 "Crisis Response Operations" sono state un importante banco di prova sul quale l'Esercito ha testato la validità e la funzionalità di tutte le sua articolazioni nel dare risposta alle nuove esigenze di sicurezza. L'efficacia dello strumento rappresentato dall'Esercito nelle

operazioni per la stabilizzazione e la ricostruzione nelle aree di crisi sta, infatti, proprio nella diversificazione e specializzazione delle sue componenti. In una fase caratterizzata da elevata conflittualità ha preminenza l'impiego di unità con capacità combat, in una fase post- conflitto comprendente le attività di stabilizzazione e ricostruzione delle infrastrutture civili per il ritorno alla normalità le formazioni terrestri sul campo sono le risultanti dalla sommatoria di unità di manovra con compiti di sicurezza e di unità specializzate in vari settori: CIMIC, EOD, NBC, Sanità, COMUNICAZIONE OPERATIVA e così via. Nelle CRO (Crisis Response Operations) il passaggio dalla fase di conflittualità a quella di stabilizzazione può prevedere una transizione più o meno lunga nella quale si devono fronteggiare situazioni complesse comprendenti emergenze umanitarie, azioni di guerriglia e/o attacchi terroristici su larga scala.
Le attività militari che seguono la fase di combattimento, eventuale. richiedono, di norma, una consistente presenza di forze di manovra (Combat) al fine di garantire la necessaria cornice di sicurezza in cui far operare gli assetti Combat Support ed alcune loro componenti a spiccata specializzazione (ci si riferisce ad esempio alla sanità, ad alcune capacità del genio, ecc.) che possono favorire un rapido ritorno alla normalità . In particolare, tali componenti hanno un grado di prontezza operativa simile a quello delle forze combat e comprensive di proprie capacità di sicurezza, autodifesa e di supporto al dispositivo. Le esigenze vanno naturalmente articolate per operare sinergicamente in un contesto multidisciplinare, interforze e multinazionale, con interventi che abbracciano l'intero spettro delle situazioni a rischio, contribuendo in modo determinante allo sforzo Joint. La complessità degli obiettivi da conseguire nelle CRO e, in particolare, nell'ambito delle attività di stabilizzazione e ricostruzione, implica per le forze Combat la capacità di svolgere, insieme alle funzioni militari in senso stretto, anche delle attività più ampie, che investono il campo economico e quello del normale funzionamento della vita e delle istituzioni democratiche dello Stato interessato all'operazione.

Si tratta di un complesso di funzioni che postulano specifiche capacità in grado di garantire ad esempio: le attività umanitarie, per favorire il rimpatrio dei rifugiati, la tutela dei diritti dell'uomo, l'aiuto alle popolazioni, l'assistenza elettorale, le attività di controllo sull'ordine pubblico interno, le attività di controllo sulle strutture amministrative statali, le attività di governo locale, le attività di reintegrazione delle forze armate delle parti in lotta nella società civile e di carattere economico e sociale.
Il post-conflict management richiede una strategia di ampio respiro applicabile soprattutto attraverso interventi di tipo multifunzionale che affiancano l'azione militare alle attività nel campo civile ed economico. Infatti per assicurare l'ordine e la sicurezza, e quindi la realizzazione delle condizioni per un effettivo ritorno alla normalità nel paese in cui si opera, è necessario intervenire con un ampio spettro di capacità funzionali che consentano di sviluppare un complesso di attività eterogenee (assistenza umanitaria, disarmo, smobilitazione e reintegrazione degli ex combattenti, dei profughi e dei rifugiati nella società civile, lotta alla guerriglia e al terrorismo, ecc.) affinché l'operazione sia efficace e la pace sia effettiva e duratura.
Le attività di stabilizzazione e ricostruzione assumono, quindi, connotazioni profondamente nuove e non sono riconducibili ad un unico modello operativo e strutturale; anzi, ogni operazione è la risposta ad una particolare situazione e ciò porta ad un incremento delle opzioni da adottare per assolvere compiutamente la missione. Data la flessibilità dell'operazione e la presenza di una molteplicità di funzioni, tra loro interdipendenti, nelle operazioni di risposta alle crisi risultano sempre presenti, in misura più o meno ampia, le fasi combat e quelle di peacebuilding (consolidamento della pace), senza che esse possano essere chiaramente distinte tra

loro.
Tali scenari sono caratterizzati dall'impossibilità di distinguere nettamente tra le diverse attività quali, ad esempio, la protezione e la sicurezza, il mantenimento e l'imposizione della pace, la ricostruzione e l'aiuto umanitario, le quali diventano tutte egualmente importanti per il successo dell'operazione al livello strategico. In tale ottica si può parlare di una vera e propria evoluzione del sistema di risposta alle crisi, caratterizzata dalla concentrazione nella stessa operazione di più attività, senza che essa muti la natura e la connotazione militare dell'intervento. L'intervento si concretizza in una forma di "public service" i cui obiettivi non sono limitati al monitoraggio e all'applicazione di un accordo di pace, ma alla più ampia costruzione/ricostruzione di un framework politico-sociale sicuro e stabile.
Per realizzare questi obiettivi, gli strumenti militari devono disporre di capacità distinte ma complementari: quelle di forza combattente e quelle di forza di stabilizzazione e ricostruzione.
La possibilità di esprimere un combat power anche durante la fase di stabilizzazione e ricostruzione è resa necessaria proprio dalle condizioni ambientali particolarmente gravi e instabili che caratterizzano lo scenario in cui si svolgono le CRO e non sempre compiutamente sopite anche al termine ufficiale della conflittualità.
L'assunzione del ruolo di "stabilizzatore" implica capacità specialistiche multifunzionali sia del tipo tecnico-cooperative (genio, trasporti, sanità, NBC, intelligence, HUMINT ecc.) sia nel campo del ripristino generale degli ambiti politici, economici (es: sicurezza e ripristino fonti energetiche primarie, attività commerciali ed industriali, ecc.) e culturali del paese (sicurezza e recupero beni artistici/siti storici, ripristino istituzioni scolastiche, ecc.). Ciò a significare che tutte le componenti in campo (militare, civile, politica e umanitaria), nel condividere un'interpretazione comune della natura della situazione e dei diversi problemi - e, di conseguenza, delle possibili strategie alternative d'intervento - necessitano sempre di una unicità di direzione e controllo che sicuramente la forza militare sul campo può garantire per capacità funzionali e strumentali.
In pratica, nel quadro di un dispositivo di stabilizzazione e ricostruzione, la componente terrestre rappresenta il principale elemento cui fare riferimento nel quadro della definizione di una risposta "a tutto campo" al terrorismo transnazionale, poiché la cooperazione ed il coordinamento delle attività sono stati ampliati al di là delle classiche attività investigative di prevenzione di polizia. La componente terrestre, infatti, ha nel suo ambito le necessarie capacità per assolvere compiutamente tutte le tipologie di compiti correlati alla lotta al terrorismo (contro guerriglia, controllo della folla, assistenza alle attività umanitarie, contro terrorismo condotto dalle Forze per Operazioni Speciali, pattugliamento esteso del territorio, attività informativa ai fini operativi), essendo armonicamente strutturata per operare sinergicamente in un contesto multidisciplinare e multinazionale, con interventi che abbracciano l'intero spettro delle situazioni a rischio.
L'Esercito, un tempo espressione di "capacità in potenza" è oggi una "Forza in atto" che opera efficacemente sul campo e può fornisce un notevole contributo allo sforzo che l'OSN vuole profonde a favore della sicurezza.

Anno I - n°1 Settembre 2006

Osservatorio per la Sicurezza Nazionale

Stato Maggiore Marina
3° Reparto Pianificazione Generale

Articoli

La Sorveglianza degli spazi marittimi nel contesto della homeland security

Situazione: la minaccia all'ambiente marittimo

La situazione in cui inquadrare la sorveglianza degli spazi marittimi richiede innanzitutto un'accurata valutazione della minaccia collegabile con l'ambiente marittimo nel più ampio contesto della homeland security. Oltre agli ormai consolidati e generali connotati di imprevedibilità nei tempi e nelle forme con cui si manifesta, tale minaccia presenta infatti caratteristiche peculiari che trovano nell'utilizzo delle vie di comunicazione marittima un particolare elemento di vulnerabilità del sistema politico-economico globale. D'altra parte, la società moderna affida sempre più il proprio benessere ad attività economiche che si svolgono attraverso relazioni di interscambio marittimo, come peraltro conferma l'evidenza dei numeri. Ad esempio, sulla base di statistiche a livello internazionale, risulta che si muove via mare oltre l'80% del commercio mondiale e che viene trasportata in container circa metà del suo valore complessivo nonché il 90% della quantità dei carichi generici. L'ambiente marino ha poi grande rilevanza per le attività economiche in esso svolte, quali pesca e turismo, nonché per altre attività di natura industriale quali l'estrazione di fonti energetiche.
E' quindi importante un esame della minaccia connessa con l'ambiente marittimo per il quale si afferma in campo internazionale il modello proposto per la prima volta dal governo USA [1] che ipotizza le seguenti tipologie: Minacce collegabili con specifici paesi, Minacce di stampo terroristico, Minacce dovute alla criminalità transnazionale ed alla pirateria, Minacce all'ambiente marino, Immigrazione illegale via mare.

a. Minacce collegabili con specifici paesi
In primo luogo va considerata la possibilità di conflitti regionali che coinvolgano i Paesi occidentali nonché l'eventualità che specifici stati-canaglia (rogue states) compiano unilateralmente azioni ostili atte a minare la sicurezza marittima. Le Marine di alcuni Paesi che seguono politiche particolarmente aggressive e destabilizzanti dispongono infatti di sottomarini convenzionali e mezzi di minamento il cui impiego potrebbe avere effetti dirompenti se indirizzato verso choke-point strategici, come ad esempio Hormuz.
Questa categoria include gli attacchi sistematici dell'Iran contro il traffico mercantile durante il conflitto contro l'Iraq del 1987-88 e gli incidenti che hanno determinato, nello stesso periodo, il danneggiamento di numerose unità della US Navy da parte di mine nell'area del Golfo Arabico.

b. Minacce di stampo terroristico
Gruppi terroristici operanti a livello transnazionale possono oggi avvalersi di sistemi di comunicazioni con efficacia comparabile a quelli delle forze regolari con cui si confrontano, della disponibilità di armamenti sempre più sofisticati e letali (incluse le armi di distruzione di massa) e dell'utilizzo di tattiche basate sui principi di "sorpresa" e "concentrazione delle forze". Uno sguardo al panorama internazionale mostra inoltre che la minaccia sta acquisendo una capacità di manovra che, a livello spazio-temporale, può generare picchi di effi-

1 Vds "The National Strategy for Maritime Security" - 2005.

cacia da mettere in seria difficoltà le forze di contrasto. Un valido esempio è costituito dall'attacco all'USS Cole (Aden, 12 ottobre 2000) che ha causato la perdita di 17 uomini, il ferimento di 39 e l'uscita dalla linea operativa per alcuni anni di un'unità navale tra le più moderne e sofisticate della US Navy.
La minaccia terroristica in questo settore va peraltro esaminata secondo due aspetti:

- uno che vede le navi, le piattaforme petrolifere ed altre infrastrutture marittime come obiettivi degli attacchi (sequestro della "Achille Lauro" nel 1986 ed attacco alla petroliera Limbourg in prossimità di Al Mukalla, Yemen, il 2 ottobre 2002);
- l'altro che vede l'utilizzo di mezzi navali per portare la minaccia contro strutture militari e civili lungo la costa, in analogia a quanto fatto con vettori aerei in occasione degli attacchi dell'11 settembre (si pensi all'effetto di una "gasiera" [2] lanciata contro un terminale petrolifero o una qualunque altra struttura portuale o costiera).

A quanto sopra va aggiunto che il terrorismo può avvalersi dell'ambiente marino per infiltrare operatori subacquei via mare ovvero per la posa di mine per minacciare porti ed aree limitrofe.
Esiste poi la minaccia collegata con i *failed states* [3] ove, in mancanza di una salda autorità governativa, trovano ospitalità organizzazioni criminali, anche di stampo terroristico, che potrebbero ricorrere per le loro azioni all'impiego di armi di distruzione di massa (WMD) da trasferire via mare, possibilmente insieme agli operatori, in prossimità degli obiettivi.

c. Minacce dovute alla criminalità transnazionale ed alla pirateria

La crescita del volume dei traffici marittimi è stata accompagnata ad un aumento dell'utilizzo degli spazi marittimi per scopi criminali. Tra questi il contrabbando di armi, il traffico di droga ed altre merci illecite, il trasporto illegale di esseri umani ed altre attività criminali tra cui la rapina e la cattura a scopo di estorsione nei confronti di navi ed imbarcazioni. In particolare, la pirateria e le rapine sono concentrate in specifiche aree caratterizzate da elevata instabilità politica ed economica nonché regioni in cui le capacità degli stati rivieraschi di imporre il rispetto delle leggi sono ridotte o addirittura assenti (Golfo di Guinea, Stretto di Malacca, Mar Cinese Meridionale, Bacino Somalo e Golfo di Aden, Caraibi). I moderni pirati utilizzano, peraltro, tecnologie ed armi avanzate ed hanno anche sviluppato tecniche e capacità operative che li rendono idonei a fiancheggiare efficacemente le attività delle organizzazioni terroristiche.
Parallelamente alle linee di traffico marittimo si possono poi individuare direttrici standard per il trasferimento via mare ed il commercio di merci illegali di largo uso, primi tra tutti gli stupefacenti. Gli ingenti proventi che ne derivano, opportunamente riciclati utilizzando i canali del sistema finanziario mondiale, costituiscono fondi di grande entità che, sfuggendo ai normali controlli sui movimenti di capitali, possono essere utilizzati per la corruzione e per il finanziamento di ulteriori attività illecite e criminali incluso il terrorismo.

d. Minacce all'ambiente marino

I disastri ecologici che possono derivare da azioni ostili, dirette o indirette all'ambiente marino, possono avere contraccolpi negativi sulla stabilità e quindi sulle condizioni di sviluppo economico di intere regioni. Ciò può determinare forti impatti su vari settori industriali tra cui quelli legati allo sfruttamento ittico, dove la progressiva riduzione delle risorse determina un crescente livello di competizione.

e. Immigrazione illegale via mare

I flussi migratori illegali, che costituiscono una delle maggiori sfide per la stabilità internazionale, sviluppano negli spazi marittimi alcune delle principali direttrici di spostamento. Gli sforzi della comunità internazionale devono quindi confrontarsi con la gestione di un'emergenza umanitaria che rende il controllo di questo fenomeno quanto mai complesso. Peraltro, l'organizzazione dei flussi permette di realizzare proventi significativi che richiamano l'attenzione delle organizzazioni criminali. In questo caso si presenta un valido collegamento con la "tratta degli schiavi" che, insieme alla pirateria, rientra tra i crimini condannati dal diritto internazionale, contro cui è previsto l'intervento delle navi da guerra a prescindere dalla nazionalità. I flussi migratori possono inoltre costituire elemento di copertura per gli spostamenti dei terroristi, rendendo ancora più strin-

2 Gasiera =Unità designata al trasporto di gas liquefatti.

3 Failed States = Stati allo sbando.

gente la necessità di un'attenta e capillare azione di controllo.
Peraltro, in un momento in cui gli aeroporti ed in modo crescente anche i porti sono sottoposti a controlli molto accurati, le linee di costa si offrono quale ottimale punto di approdo ove inserirsi clandestinamente ed infiltrarsi per raggiungere gli obiettivi.
In questo settore, le iniziative regionali sono importanti per realizzare forme di coordinamento che agevolino lo scambio di informazioni e migliorino quindi l'efficacia del contrasto. Iniziative di cooperazione in tale settore sono già presenti ed attive in Mediterraneo con le operazioni Nettuno e Triton.

Dalla Maritime Surveillance alla Maritime Security

La maritime surveillance si inquadra nel più ampio contesto della maritime security che assume oggi valenza strategica per due categorie di fattori fondamentali:

- l'accresciuta importanza degli "spazi marittimi", soprattutto nel contesto di globalizzazione nonché in relazione alla necessità di salvaguardare il libero utilizzo dell'alto mare in un panorama caratterizzato dalla tendenza alla "territorializzazione" del mare, conseguenza delle crescenti rivendicazioni da parte degli stati costieri (ZEE , ZPE , ZPP , etc.) [4];
- le pressanti esigenze di "sicurezza" in presenza delle minacce precedentemente descritte, dinamiche ed imprevedibili, in grado di manifestarsi ovunque e con potenzialità devastanti per la stabilità globale; si pensi all'importanza delle fonti energetiche [5] per il sistema mondiale, al loro massiccio trasporto vie mare ed agli effetti dirompenti che potrebbero derivare da eventuali attacchi a piattaforme fisse e/o galleggianti ovvero a navi di linea con migliaia di passeggeri a bordo.

La maritime security è quindi un elemento cruciale per la stabilità mondiale che richiede un'azione a livello governativo [6] basata su tre concetti fondamentali: cooperazione, integrazione, coordinamento. In particolare, la linea d'azione da adottare dovrà prevedere:

- il conseguimento di una comune volontà di cooperazione e convergenza di obiettivi, da sviluppare in modo omnicomprensivo, a livello nazionale e transnazionale, con il supporto di idonee misure di confidence building e sulla base di una vision "collettiva e condivisa" della sicurezza;
- l'ottimizzazione delle sinergie tra le diverse agenzie/organismi coinvolti a vario titolo nella sicurezza degli spazi marittimi, al fine di realizzare una significativa integrazione delle capacità e delle risorse disponibili, incluse quelle "informative" fino al livello consentito;
- l'individuazione di entità in grado di assicurare un'adeguata opera di coordinamento in ambito nazionale e nei contesti internazionali delle Alleanze e delle organizzazioni regionali, sulla base dei trattati internazionali e del vigente corpo giuridico nazionale.

A questo punto si inserisce il concetto di Maritime Domain Awareness (MDA) che, mutuando la definizione americana, è l'efficace comprensione di tutto quanto è associato all'ambiente marittimo globale e che può avere impatti sulla sicurezza (safety & security), l'economia e l'ambiente dello stato rivierasco.
Nell'evidenza del panorama internazionale, la linea d'azione sopra descritta è in linea con una serie di iniziative emergenti che individuano nella MDA l'elemento essenziale per il suo conseguimento, oltre a confermare la centralità della maritime security. Tra queste:

- il progetto 1000 Ship Navy, promosso dalla Marina Statunitense e volto ad integrare la capacità operativa intrinseca della US Navy con risorse rese disponibili da altri attori internazionali, statali e non, incluse le compagnie di navigazione, quale contributo concreto al miglioramento della maritime security;
- il concetto per la "Alliance and Coalition Maritime Domain Awareness (MDA)", redatto dal Pentagono e diffuso allo scopo di introdurre, in ambito NATO, una discussione in merito all'opportunità di realizzare uno strumento che consenta un controllo marittimo ad ampio spettro nelle aree d'interesse per l'Alleanza, supportato da importanti elementi guida di "integrazione" delle risorse disponibili e di "coordinamento" tra gli attori coinvolti;

4 ZEE = Zona Economica Esclusiva; ZPE = Zona di Protezione Ecologica; ZPP = Zona di Protezione della Pesca.

5 La criticità del problema energetico è stata evidenziata dal Segretario Generale della NATO in un articolo sul Wall Street Journal del 14 giugno 2006 con riferimento alla Dottrina Carter (1980) che identificava il Golfo Persico quale "vital national interest" e la necessità da parte dell'Occidente di rivedere/aggiornare tale dottrina.

6 Un esempio di approccio governativo è costituito dal citato documento "National Strategy for Maritime Security" sulla base della più ampia "Strategy for Homeland Defence and Civil Support".

- la Proliferation and Security Initiative (PSI), promossa da un foro di nazioni, al cui core group appartiene anche l'Italia, mirata alla creazione di un framework concettuale ed operativo per contrastare in modo efficace la diffusione delle armi di distruzioni di massa (WMD) e con una particolare enfasi sul controllo dei traffici via mare;
- le iniziative in atto nel contesto del CHEN [7] e del CHANCOM [8] per lo sviluppo di un framework concettuale e condiviso delle Maritime Security Operations.

Ad ulteriore conferma della centralità della MDA si evidenzia che nell'ambito della Strategia nazionale USA per la maritime security sono stati realizzati dei piani di supporto (supporting plans) uno dei quali [9] tratta in modo specifico l'argomento (National Plan to Achieve Domain Awareness).
Importanti segnali in merito al ruolo delle Marine [10] giungono anche dalla Commissione dell'Unione Europea che, con l'adozione del Green Paper sul futuro della Maritime Policy dell'UE, ha dato validi spunti in merito al ruolo delle Marine nel futuro sviluppo della maritime security.

Dalla Maritime Security alla Maritime Domain Awareness

Nell'ambito della strategia perseguita dalla Difesa per soddisfare la duplice esigenza di difendere l'integrità nazionale (homeland defence) e produrre sicurezza proiettando stabilità in qualunque parte del globo, la Marina è da tempo impegnata nel dare sviluppo e concretezza a due linee guida di riferimento che costituiscono gli elementi fondanti della vision per l'impiego e lo sviluppo delle forze marittime [11] : la sorveglianza integrata degli spazi marittimi d'interesse nazionale e la proiezione di capacità sul mare e dal mare.
Tali concetti operativi hanno una importante relazione con la MDA in quanto:

- la sorveglianza integrata degli spazi marittimi è uno dei principali elementi che da un lato contribuisce alla MDA e dall'altro la utilizza per le proprie finalità di compilazione della situazione;
- la proiezione di capacità sul mare e dal mare, pur contribuendo quale effetto secondario al miglioramento della MDA, ne ha una necessità primaria per poter agevolmente estrinsecare le proprie potenzialità di proiezione e quindi svilupparsi nelle missioni ed attività discendenti.

Da quanto detto emerge la centralità del ruolo della MDA, da sempre fulcro dello sviluppo del core business della Marina, sia in termini di policy sia sul piano operativo:

- in termini di policy, attraverso il rafforzamento e l'ampliamento del livello di mutua conoscenza ed interoperabilità, concretizzatosi in misure di confidence building tra i paesi delle aree di operazioni, con picchi di eccellenza rappresentati dalla realizzazione dell'unico foro biennale tra i Capi di Stato Maggiore delle Marine della regione Mediterranea (Simposio di Venezia) e l'avvio del progetto denominato Virtual Regional Maritime Traffic Centre (V-RMTC);
- in termini operativi, con il mantenimento in efficienza di un adeguato dispositivo aeronavale, di una rete radar costiera e, soprattutto, della capacità di integrare in una maritime picture coerente e per quanto possibile completa le informazioni raccolte sia nel corso delle attività operative svolte dal citato dispositivo sia grazie agli scambi con gli altri contesti di Alleanza/Coalizione nei quali la Marina è inserita nonché quelle generate dagli altri attori statali concorrenti alla maritime security, tra cui:
- il Ministero dei Trasporti, tramite il Comando Generale delle Capitanerie di Porto per quanto afferisce alla integrazione dei dati provenienti dalla rete VTS e dai dispositivi AIS, ARES e Blue-box nonché per quanto deriva dalla legge 979 del 1982 sulla Difesa del mare e dal disposto combinato della Legge 25/97 e del DPR 556/99 relativamente ai compiti di difesa delle acque metropolitane;
- la Guardia di Finanza, la stessa Guardia Costiera e le altre Forze di Polizia inquadrate nel Ministero dell'Interno, per quanto attiene al coordinamento delle attività di controllo dei flussi migratori in attuazione dell'Accordo Tecnico-Operativo discendente dalla Legge 189/2002 cosiddetta Bossi-Fini.

7 CHEN = Chief of European Navies, forum tra i Capi di Stato Maggiore delle Marine dell'UE.

8 CHANCOM = Channel Committee, forum tra i Capi di Stato Maggiore o equivalenti delle Marine dell'area della Manica - Belgio, Francia, Germania, Paesi Bassi, Gran Bretagna - cui nel 2005 sono stati anche invitati i CSM delle Marine di Italia, Spagna e Portogallo.

9 Gli altri piani sono: Global Maritime Intelligence Integration Plan, Interim Maritime Operational Threat Response Plan, Interim Outreach and Coordination Strategy, Maritime Infrastructure Recovery Plan, Maritime Transportation System Security Plan, Maritime Commerce Security Plan, Domestic Outreach Plan.

10 Particolarmente significativo quanto riportato nell'Annesso, ove viene menzionato a titolo di esempio l'approccio canadese al problema, con lo sviluppo di un Maritime Security Operations Centre che raggruppa, sotto la direzione della Marina, rappresentanti della Guardia Costiera, Canada Border Services Agency e Trasporti.

11 Vds "Investire in marittimità - La Strategia navale nazionale", conferenza tenuta il 27 giugno 2006 dal Capo di Stato Maggiore della Marina, Amm. Sq. Paolo La Rosa presso l'Istituto Studi Ricerche Informazioni Difesa (ISTRID).

Si delinea quindi il ruolo chiave della Marina nella complessa realtà della sicurezza marittima, ove le forze aeronavali sviluppano da sempre una robusta e credibile azione di presenza e controllo nelle aree di interesse strategico in concorso, per le zone marittime limitrofe al territorio nazionale, con le altre amministrazioni dello Stato e, per l'alto mare, con tutte le Marine che contribuiscono alla sicurezza marittima.
Ciò, fermo restando che, in un'ottica interforze, la Marina, forte delle esperienze nelle missioni multinazionali degli ultimi anni nonché in virtù delle intrinseche capacità di "mobilità" e "autonomia logistica" delle proprie forze, si trova ad affermare sempre più il proprio ruolo di componente fondante della capacità expeditionary nazionale e key enabler per la proiettabilità di capacità nazionali, militari e non, nei teatri lontani.
Tale capacità expeditionary, oltre che nel concetto di "proiezione di capacità sul mare e dal mare" va considerata quale fattore essenziale per l'esercizio della sorveglianza marittima a protezione degli interessi nazionali in aree distanti dai mari circostanti il territorio nazionale. Si delinea quindi un modello, basato su un approccio sistemico al problema, che viene graficamente rappresentato in Figura 1.

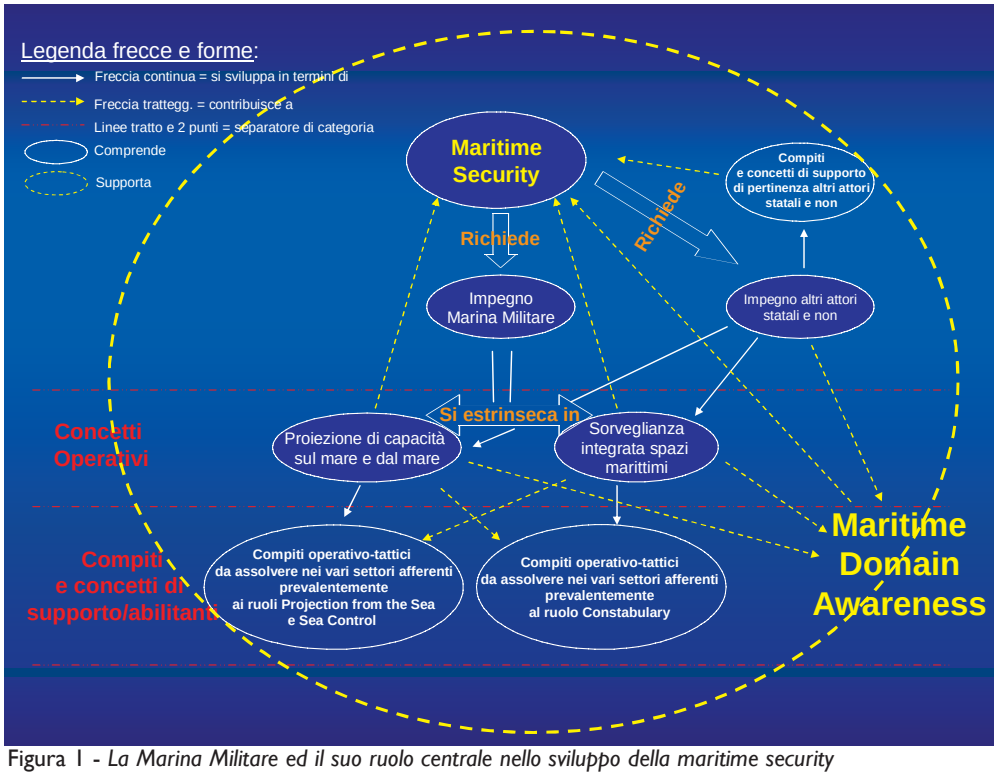


Figura 1 - *La Marina Militare ed il suo ruolo centrale nello sviluppo della maritime security*

Realizzazione della capacità di Sorveglianza degli Spazi Marittimi

In esito alle missioni derivanti dalle Direttive Ministeriali e dal discendente Concetto Strategico del Capo di SMD, la Marina deve assicurare una adeguata presenza e sorveglianza delle aree di interesse strategico, in concorso, per le zone marittime limitrofe al territorio nazionale, con le altre amministrazioni dello Stato competenti (cooperazione inter-agenzia), ed in generale in congiunzione con le forze delle Alleanze di cui il paese fa parte.
La Marina è inoltre impegnata, in attuazione di quanto previsto dalla Convenzione ONU sul Diritto del Mare ed in concorso con le altre Marine, nella salvaguardia della libertà di utilizzo delle vie di comunicazione marittima (cooperazione internazionale), nell'esercizio del proprio tradizionale ruolo constabulary, ovvero di polizia dell'alto mare.
Lo sviluppo della capacità di Sorveglianza degli Spazi Marittimi ed il suo efficace esercizio richiede quindi una linea d'azione su due livelli complementari:
- uno centrato nell'ambito del Mediterraneo;
- l'altro orientato al di fuori dell'area Mediterranea.

a. La Sorveglianza Marittima nella regione Mediterranea

Con riferimento alle zone marittime limitrofe al territorio nazionale, in attuazione dei disposti di legge e nell'esecuzione della missione assegnata, la Marina deve svolgere una attività di sorveglianza degli spazi marittimi che, per raggiungere la massima efficacia e quindi garantire un adeguato livello di MDA che sia di efficace supporto alla maritime security, deve avere due elementi di fondo: contenuti e capacità di condivisione.

I contenuti sono il risultato dall'azione di raccolta e dipendono quindi dal numero e dal livello delle fonti. Ciò implica la disponibilità di:

- una capacità autonoma di raccolta delle informazioni e, quindi, sensori allo stato dell'arte in grado di sfruttare le nuove tecnologie per estrarre dal "bersaglio" il maggior numero di informazioni possibile con l'obiettivo finale di conseguire non solo la scoperta, la localizzazione e il tracciamento (c'è, dov'è, dove sta andando) ma soprattutto il riconoscimento (chi è);
- una infrastruttura di comunicazione realizzata nell'ottica dei paradigmi NCW-NEC, adeguata a soddisfare le esigenze, in termini di capacità di banda, dei vari utenti del sistema.

L'integrazione è invece il risultato della combinazione di due fattori:

- la disponibilità di tecnologie per la fusione delle informazioni raccolte in un apposito hub che la Marina sta realizzando presso il Comando in Capo della Squadra Navale, quale ente che più di ogni altro ha le competenze tecniche e l'accesso ad informazioni ad ampio spettro, che vuol essere il nucleo sul quale far evolvere la Rete Radar Costiera a connotazione Marina Militare, verso un concetto più ampio di Dispositivo Integrato di Sorveglianza degli spazi marittimi, in cui l'attenzione si sposta dalla capacità di raccogliere informazioni (Rete Radar) alla capacità di elaborare e integrare le informazioni provenienti dai sistemi più disparati (Dispositivo Integrato) in una immagine coerente e completa da distribuire a chiunque, a livello strategico, operativo o tattico, ne abbia bisogno;
- le autorizzazioni all'accesso dei dati provenienti dalle varie fonti, come ad esempio quelle militari, per le quali sono necessarie azioni di filtro (vds in ambito NATO le procedure per la compilazione Recognised Maritime Picture RMP) ed il flusso dati del traffico mercantile proveniente per ora in determinate occasioni dal sistema del Naval Control And Guidance of Shipping (NCAGS).

La completezza della picture è tanto maggiore quanto più numerose sono le fonti che contribuiscono alla sua compilazione che implica, a livello internazionale, quanto più spinti sono gli accordi bilaterali e multilaterali che ne supportano lo scambio informativo e l'attività di confidence building svolta nei citati contesti internazionali (il Simposio di Venezia, il V-RMTC, le attività addestrative congiunte che vengono svolte in vari contesti tra cui, di particolare rilievo l'iniziativa ADRION ed il 5+5).

La centralità della Marina nella sorveglianza marittima è evidente anche esaminando le varie aree in cui essa viene attuata alla luce dei disposti di legge in campo nazionale ed in relazione agli altri attori statali che, a vario titolo, hanno attribuzioni afferenti alla maritime security.

Lo sviluppo delle capacità operative della Marina nel settore specifico della Sorveglianza Marittima nel Mediterraneo richiederà, soprattutto al fine di sviluppare il necessario connotato di integrazione:

- un adeguato supporto finanziario;
- la definizione di un appropriato supporto nell'ambito del corpo legislativo nazionale;
- un efficace collegamento con il contesto Europeo ed in modo specifico con le agenzie che trattano questioni afferenti alla sicurezza marittima ma che esulano dallo specifico contesto militare, quali:
- European Agency for the Management of operational Control at the external Borders (FRONTEX);
- European Maritime Safety Agency (EMSA);
- European Defence Agency (EDA).

b. La Sorveglianza Marittima fuori dalla regione Mediterranea

Al di fuori del Mediterraneo, la Marina concorre allo sforzo di presenza all'estero e nelle missioni internazionali del sistema paese. In tale azione, ove continua a valere la centralità del ruolo della MDA, lo sviluppo del concetto operativo di Sorveglianza Marittima si estrinseca in una forte azione di confidence building che include la partecipazione ad iniziative quali la Theatre Security Cooperation (TSC) in ambito Enduring Freedom, l'interazione con le guardie costiere dei paesi rivieraschi, e l'effettuazione di attività addestrative

congiunte con le marine nell'ottica di un loro sempre maggiore coinvolgimento nell'azione di sviluppo della stabilità delle regioni in questione, in primis nell'ottica di prevenzione del fenomeno terroristico.

Conclusioni

L'evoluzione dello scenario internazionale richiede che la pianificazione e condotta della sicurezza nazionale tenga in considerazione le peculiarità di una minaccia che presenta connotati multiformi ed una crescente imprevedibilità. Il concetto di homeland security che si sta conseguentemente diffondendo richiede pertanto l'estensione del campo d'azione della prevenzione e del contrasto ben oltre il ristretto ambito territoriale dei singoli paesi. Ne deriva una situazione molto complessa che richiede risposte integrate e coordinate nell'ambito del Paese (secondo una logica inter-ministeriale ed inter-agenzia) la cui efficacia venga poi accresciuta attraverso lo strumento della cooperazione internazionale.
In tale contesto, la maritime security rappresenta un aspetto cruciale, sia per il proprio ruolo fondamentale in relazione ai traffici marittimi, essenziali per lo sviluppo economico e sottoposti a crescenti minacce di varia natura, sia quale valido strumento che, nell'ambito di una più ampia strategia marittima, permetta il miglioramento della conoscenza reciproca e quindi delle possibilità di cooperazione tra paesi che condividono interessi comuni (confidence building).
Quale concetto operativo per la maritime security, in linea con le esigenze di presenza e sorveglianza individuate nel Concetto Strategico del Capo di Stato Maggiore della Difesa, la Marina Militare sta ponendo particolare enfasi sullo sviluppo della "capacità di sorveglianza integrata degli spazi marittimi" che, nell'area Mediterranea, si traduce nella realizzazione di specifici progetti tra cui, di particolare rilievo, il Virtual Regional Maritime Traffic Centre (V-RMTC) ed il Dispositivo Integrato di Sorveglianza Marittimo (DISM).
A fronte della necessità di investimenti, significativa soprattutto per quanto attiene al DISM, tali progetti permettono di ottimizzare l'utilizzazione delle risorse disponibili attraverso la condivisione degli sforzi e l'individuazione di soluzioni quanto più possibili sinergiche tra tutti gli attori coinvolti, approccio che risulta particolarmente idoneo in un momento di generali ristrettezze di bilancio come l'attuale.
In definitiva, la Marina Militare guarda con fiducia all'aumentata sensibilità del Paese verso la homeland security ed all'importanza che la maritime security sta assumendo in tale contesto e prosegue nella strada intrapresa quale attore in grado di assicurare la massima integrazione degli sforzi nel settore della sorveglianza degli spazi marittimi grazie alla propria posizione che la vede agire come interlocutore istituzionale nei confronti delle altre Marine, ed in particolare di quelle che operano nel Mediterraneo, nonché come elemento organizzativo che, nell'ambito del comparto Difesa, cura le relazioni operative nel settore marittimo e navale con le alleanze e le organizzazioni internazionali, prime tra tutte la NATO e l'Unione Europea.

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Stato Maggiore Aeronautica
Ufficio Generale del Capo di Stato Maggiore
Ufficio Pubblica Informazione e Comunicazione

Articoli

"Nine-Eleven" terrorismo globale e sicurezza dei cieli
L'impegno dell'Aeronautica Militare per la sicurezza dello spazio aereo

Il terrorismo[1] globale

Gli eventi del "nine-eleven" hanno dimostrato gli effetti della radicale trasformazione della natura del terrorismo che è oggi un fenomeno globale sia per il numero e la diffusione degli eventi che per le conseguenze sociali, politiche ed economiche che da essi derivano. Il terrorismo del ventunesimo secolo risulta organizzato secondo i più moderni criteri di decentralizzazione dell'iniziativa operativa mirata al conseguimento di obiettivi strategici "attraverso l'impiego di armi convenzionali, chimiche, batteriologiche, nucleari e radiologiche "[2], e di strumenti e metodi non classificabili fra quelli normalmente utilizzati in campo militare.
In Europa, l'abbattimento delle frontiere, la grande disponibilità di mezzi e vie di trasporto, l'elevata densità di abitanti, la fruibilità e la velocità delle informazioni, sembrano essere le caratteristiche dell'ambiente operativo maggiormente sfruttate dal terrorismo internazionale per operare nell'ombra progettando e perpetrando attentati in grado di condizionare una massa di persone ben più grande di quella direttamente colpita nel corso di tali eventi. I media giocano in questo contesto un ruolo fondamentale diffondendo le notizie in "tempo reale" su scala globale.
Nella scala dei valori della cittadinanza, condizionata da questa realtà, la sicurezza ha assunto una priorità sempre maggiore. Gli organi istituzionali si sono attivati per garantire il funzionamento del sistema paese prevenendo il terrorismo e predisponendo una capacità di risposta volta a fronteggiare eventuali crisi derivanti da eventi terroristici catastrofici.
La natura multi-dimensionale del terrorismo impone un forte impegno nel campo della prevenzione e delle predisposizioni finalizzate a garantire il coordinamento e la cooperazione fra tutti gli operatori di sicurezza attivi nei vari settori delle attività sociali, economiche e produttive, vitali per gli interessi del Paese ed esposte alla minaccia terroristica.
La definizione di una politica di sicurezza in grado di indirizzare univocamente tutte le iniziative di prevenzione e riduzione del rischio associato alla minaccia terroristica è ritenuta indispensabile al fine di garantire un'efficace interazione fra Ministeri, Forze Armate, Enti, Agenzie e tutte le organizzazioni direttamente o indirettamente chiamate a contribuire alla sicurezza in modo efficace, tempestivo e soprattutto sostenibile.
Come dimostrato dagli eventi dell'11 settembre 2001, uno di questi settori attiene al controllo e alla sicurezza dei cieli oggi garantita, in Italia, dall'Aeronautica Militare inserita nel contesto multinazionale della Difesa Aerea Integrata della NATO.

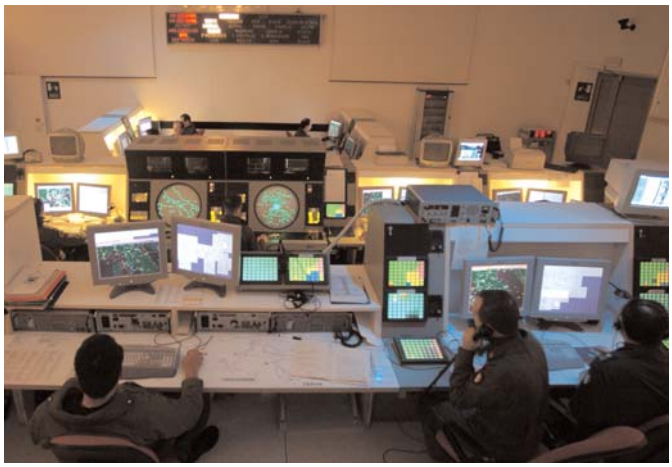
La difesa aerea

L'Aeronautica Militare assicura la sorveglianza e la difesa dello spazio aereo nazionale in maniera continuativa attraverso un sistema integrato di sensori (radar basati a terra ed in volo[3]) e con l'impiego di velivoli e

1 *Trattasi di una minaccia asimmetrica, indeterminata, volatile e, soprattutto, imprevedibile che richiede un'azione di contrasto che fa della prevenzione l'unica arma sulla quale polarizzare la strategia globale di lotta. Pur nella consapevolezza che "il fenomeno è controllabile, ma non debellabile", che ha limiti e debolezze, ma numerosi punti di forza che lo rendono pressoché invincibile. - Giulia La Volpe / Pagine Difesa*

2 *RAND - Quick scan of post 9/11 national counter-terrorism policymaking and implementation in selected European countries. Maggio 2002*

3 *Airborne Early Warning*



Una tipica sala operativa della difesa aerea - Foto Troupe Azzurra

sistemi missilistici superficie/aria.
Il dialogo continuo con gi enti di controllo del traffico aereo civile (ENAV) e con le autorità deputate alla sorveglianza dello spazio aereo dei paesi NATO europei, consente di operare efficacemente a tutela di tutti gli utenti dello spazio aereo e per garantire un adeguato livello di sicurezza.
Le funzioni di comando e controllo degli assetti della difesa aerea nazionale permanentemente assegnati alla NATO, sono devolute al CAOC 5 [4] di Poggio Renatico che, attraverso una sala operativa, dispone l'impiego dei velivoli in QRA (Quick Readiness Alert). In caso di avvistamento di una traccia radar non identificata, oppure nel caso in cui un traffico non risponda a prestabiliti requisiti o diverga dalla rotta prevista senza validi motivi, viene rapidamente ordinato il decollo (in gergo tecnico "scramble") dei velivoli intercettori che sotto la guida dei controllori di intercettazione a terra, si dirigono verso la traccia "sospetta", ne accertano visivamente l'identità e le reali condizioni ed intervengono, ove necessario, per scortarlo fino ai limiti dello spazio aereo di responsabilità, imponendo variazioni di rotta o eventualmente l'atterraggio su di un aeroporto idoneo per effettuare ulteriori verifiche da parte dell'autorità di pubblica sicurezza.
I Reparti dell'Aeronautica Militare che svolgono questo tipo attività sono il 5° Stormo di Cervia ed il 37° Stormo di Trapani, equipaggiati con i caccia F-16 e, dal 16 dicembre del 2005, il 4° Stormo di Grosseto, equipaggiato con i nuovi velivoli Eurofighter 2000. Tali aeromobili, opportunamente predisposti ed equipaggiati, sono in grado di decollare ed intervenire in tempi brevissimi su tutto il territorio nazionale e nell'area NATO di responsabilità assegnata alla nazione.
La necessità di prevenire ed eventualmente scongiurare un attacco terroristico dal cielo ha indotto la difesa aerea a modificare la propria filosofia operativa oggi orientata alla "sorveglianza attiva" piuttosto che ad una "sorveglianza vigile" intrinsecamente inerte. La struttura della catena di comando e controllo è stata modificata allo scopo di garantire la piena tutela degli interessi e della sicurezza nazionale.

Firma dell'accordo tecnico per la difesa aerea con la Svizzera - Foto Troupe Azzurra

Seppure ancora fortemente incardinato nel sistema di difesa integrata della NATO, il servizio di sorveglianza dello spazio aereo italiano consente oggi (sulla base di provvedimenti di legge recentemente adottati) di trasferire il comando e controllo degli intercettori dalla NATO alla autorità governativa nazionale nel caso in cui una "traccia" sia classificata come "RENEGADE" ovvero come un traffico aereo la cui condotta sia riconducibile ad una possibile azione terroristica.
Nella gestione di situazioni di questo tipo, un'efficace interazione fra le agenzie deputate al controllo amministrativo dello spazio aereo e la difesa aerea, è ritenuta fattore di fondamentale importanza per garantire una

4 *Combined Air Operation Centre*

5 *Servizio d'Allarme*

capacità operativa di difesa realmente credibile.
Al pari, l'opportunità di avviare un dialogo costruttivo con i paesi confinanti e, in un contesto più ampio, con i paesi che si affacciano sul bacino del mediterraneo, costituisce oggetto di attenzione in relazione alla definizione di nuove strategie per contrastare una minaccia di portata crescente. La recente sottoscrizione di accordi tecnici per la difesa dello spazio aereo con Francia e Svizzera e l'avvio di una similare iniziativa con l'Austria, consentirà certamente di incrementare l'efficacia dello strumento della difesa aerea durante gli interventi in prossimità dei confini nazionali precedentemente considerati limiti inviolabili da parte degli intercettori.

Sostenibilità e criticità del servizio di sorveglianza dello spazio aereo.
Le recenti restrizioni di bilancio hanno fortemente condizionato lo svolgimento di tutte le attività dell'Aeronautica Militare che ha avviato un processo di verifica finalizzato all'individuazione di soluzioni idonee a garantire la sostenibilità dello sforzo operativo nonostante la costante riduzione strutturale delle risorse a disposizione. Oltre a focalizzare le proprie attività sul "core business", ovvero sui prioritari compiti d'istituto (primo fra tutti quello della sicurezza dello spazio aereo), lo Stato Maggiore Aeronautica ha preso in esame la casistica delle attivazioni del sistema di sorveglianza, alla ricerca di soluzioni per garantire il desiderato livello di sicurezza al minor costo possibile.
Tale studio ha evidenziato la marcata tendenza di crescita del numero di attivazioni degli intercettori dovuta all'innalzamento del livello di attenzione ed all'applicazione di nuovi e più restrittivi criteri di sicurezza da parte dell'autorità di comando e controllo della difesa aerea nazionale. In questo campo è stato anche necessario rilevare che una gran parte delle attivazioni è stata determinata dall'inosservanza delle norme riguardanti la gestione amministrativa dello spazio aereo quali: la mancata richiesta delle autorizzazioni diplomatiche da parte di operatori stranieri ovvero l'utilizzo di autorizzazioni scadute o destinate ad altri paesi o operatori, la perdita delle comunicazioni radio terra/bordo/terra dovuta si, ad avarie tecniche ed alla vetustà dei sistemi, ma anche a leggerezza o inadeguata conoscenza delle procedure in uso, l'inosservanza spesso consapevole delle norme della circolazione aerea.
La possibilità di ridurre il numero di attivazioni generate per motivi inconsistenti consentirebbe di preservare risorse preziose ai fini della salvaguardia della sicurezza nazionale.

Periodo	Interventi
dal nov. 2000 al 11 sett. 2001	4
dal 11 sett. 2001 al 31 dic. 2001	11
2002	32
2003	19
2004	28
2005	**47**
dal 1 gen. 2006 al 14 lug. 2006	18

Numero di attivazioni degli intercettori dal 1 nov. 2000 al 14 lug. 2006.

I grandi eventi nazionali
Da diversi anni, in occasione dello svolgimento di eventi di particolare rilevanza per i quali sia prevedibile una consistente concentrazione di persone e una diretta esposizione all'attenzione dei media, l'Aeronautica Militare provvede al potenziamento del apparato di sorveglianza e difesa dello spazio aereo per prevenire e

Un HH3F del 15° Stormo CSAR in configurazione Slow Mover Interceptor - Foto Troupe Azzurra

scongiurare eventuali attacchi terroristici condotti con mezzi aerei.
La prima operazione di questo tipo si è svolta nei cieli di Genova in occasione del G8 dal 16 al 23 luglio 2001, pochi mesi prima del fatidico 11 settembre.
In tale circostanza, come del resto avviene oggi nel contesto delle operazioni di questo tipo (denominate "JUPITER" dal 2004), fu previsto l'impiego integrato di mezzi e personale appartenenti a diverse unità dell'Aeronautica Militare, delle Forze Armate e dei Corpi Armati dello Stato per prevenire e contrastare la minaccia aerea controllando sia il flusso del traffico aereo in volo che il transito di velivoli di qualsiasi categoria o dimensione presso gli aeroporti e le aviosuperfici (generalmente sprovviste di un servizio di controllo del traffico aereo). Per contrastare il segmento cosiddetto "asimmetrico" della minaccia aerea, ovvero l'attacco da parte di aeromobili/aerostati non concepiti come veri e propri sistemi d'arma, i dispositivi di sicurezza JUPITER sono dotati di una capacità di intervento specificamente orientata all'intercettazione di piccoli aeromobili (anche ultraleggeri), generalmente lenti e facilmente occultabili alla scoperta dei radar grazie a profili di volo a bassissima quota.
Avverso tali minacce, oltre a dotarsi di una catena di avvistamento visivo sul perimetro della zona di interesse (SPOTTERS), sono schierati ed impiegati velivoli MB 339 CD del XII Gruppo di Gioia del Colle unitamente ad elicotteri HH3F del 15° Stormo CSAR, opportunamente equipaggiati al fine di disporre di una capacità di intervento alle quote più basse, in prossimità dei centri abitati e soprattutto a bassa e bassissima velocità.

Un F-16 riceve l'ordine di "scramble" - Foto Troupe Azzurra

Aree di intervento ai fini del miglioramento continuo del servizio

La NATO, coinvolta nella definizione dei programmi di sviluppo dei dispositivi di difesa aerea e dei futuribili scenari d'impiego, fornisce il proprio contributo di pensiero suggerendo, alle nazioni alleate, nuovi indirizzi e procedure aggiornate alla mutevole realtà della minaccia aerea di matrice terroristica.
L'alleanza promuove, presso i paesi membri, l'armonizzazione delle procedure, della terminologia e dei protocolli di comunicazione. Sostiene lo sviluppo di dispositivi e procedure che consentano di fronteggiare potenziali situazioni di emergenza in prossimità dei confini nazionali (la recente sottoscrizione di accordi tecnici bilaterali per la difesa aerea con la Francia, la Svizzera e l'Austria sono in linea con tali suggerimenti). Supporta la pianificazione e l'esecuzione di esercitazioni per favorire l'interoperabilità in ambiente multinazionale, interforze ed interagenzia; sollecita lo sviluppo di efficaci strumenti e modalità di coordinamento fra l'autorità militare deputata alla difesa e quella civile deputata al controllo del traffico aereo.
Indipendentemente dalla capacità operativa del dispositivo di difesa aerea, la mutevole ed imprevedibile fisionomia della minaccia terroristica impone un'accurata azione nel campo delle informazioni per fronteggiare efficacemente il fenomeno. Un costante scambio di informazioni fra gli operatori di sicurezza finalizzato alla ricerca, alla pronta identificazione ed alla valutazione di "segnali deboli" che evidenzino le anomalie potenzialmente associate al fenomeno del terrorismo, è determinante ai fini dell'attuazione delle misure necessarie a garantire la sicurezza.
L'interoperabilità dei sensori, dei sistemi di comunicazione, delle procedure, unitamente alla possibilità di condividere, con tutte le organizzazioni militari e civili che concorrono a

Un RADAR della Difesa Aerea - Foto Troupe Azzurra

garantire la sicurezza, una comune strategia e linee guida inequivocabili, è indispensabile per operare insieme efficacemente.
Un quadro normativo adeguato deve necessariamente prevedere le nuove fattispecie associate a scenari fino ad ora non ipotizzabili per consentire la definizione di regole d'ingaggio commisurate al tipo di minaccia da fronteggiare e garantire la sicurezza di tutti gli utenti dello spazio aereo.
La normativa riguardante la gestione amministrativa dello spazio aereo dovrebbe tenere maggior conto delle esigenze di urgenza, flessibilità ed economicità degli utenti commerciali e non, nazionali e stranieri, prevedendo severe sanzioni per i comportamenti volontari lesivi della sicurezza dello spazio aereo che inneschino inopportune e dispendiose attivazioni del sistema di difesa.
Ancora molto è possibile fare nel campo della "cultura della sicurezza" sensibilizzando tutti gli operatori ad una professionale e scrupolosa osservanza dei comportamenti che, oltre a garantire l'ordinato utilizzo dello spazio aereo, consentono di operare in sicurezza anche in condizioni di traffico crescente.

Achille Cazzaniga

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Comando Generale dell'Arma dei Carabinieri
II Reparto - SM - Ufficio Criminalità Organizzata

Articoli

La minaccia asimmetrica: il contrasto alla criminalità transnazionale e al terrorismo

L'iniziativa di istituire un osservatorio sulla sicurezza nazionale rappresenta un passo importante per poter comprendere la complessità dell'attuale scenario geostrategico. La stessa nozione di tutela della sicurezza nazionale, ampiamente intesa, presuppone ampie sinergie tra forze armate e di polizia, tra organismi preposti al contrasto dell'illegalità o alla difesa del territorio e agenzie di protezione civile, di sicurezza tecnologica che in ogni settore, pubblico e privato, proteggono interessi nazionali fondamentali, in Italia o all'estero, dalle minacce emergenti.

In tale quadro, occorre sottolineare che la situazione internazionale è caratterizzata dalla presenza di una minaccia asimmetrica che costituisce, dopo i devastanti eventi terroristici degli ultimi anni, sicura priorità per le forze armate e di polizia, nel più ampio quadro del concetto di sicurezza nazionale.

Nell'ambito della valutazione attuale del contesto generale di sicurezza, caratterizzato proprio dall'incertezza e dall'asimmetricità della minaccia, il crimine organizzato così come il terrorismo hanno assunto importanza crescente.

Tra i potenziali fattori di rischio per lo strumento militare, spesso portato da attori non convenzionali, già il Capo di SMD nel Concetto Strategico ha evidenziato la necessità di flessibilità e capacità di reazione da parte delle FF.AA., di fronte non solo al terrorismo ma anche a fattori di destabilizzazione legati a fenomeni di natura politico - sociale, quali i traffici illegali, l'immigrazione clandestina e l'attività di gruppi criminali, che potrebbero - attraverso la corruzione - destabilizzare entità statali giungendo ad ottenerne il supporto.

Non si può poi oggi parlare di rischi per la sicurezza costituiti dalla criminalità organizzata e dal terrorismo senza considerare la dimensione europea del fenomeno, e le risposte che l'UE sta sviluppando: la transnazionalità della minaccia comporta necessariamente una risposta comune a tutela del comune interesse alla sicurezza. Al riguardo, sulla base della Strategia europea di Sicurezza delineata da Javier Solana nel 2003, viene auspicata una sempre maggiore integrazione per l'azione esterna svolta nel settore Giustizia e Affari Interni con la Politica estera e di Sicurezza Comune (PESC). Per gli obiettivi europei (politici e economici) è indispensabile associare all'azione stabilizzatrice, svolta nelle aree di crisi, il supporto fornito dal contrasto della criminalità organizzata e del terrorismo.

Dall'11 settembre 2001 il terrorismo è al centro di tutte le preoccupazioni concernenti la sicurezza europea, ma anche la criminalità organizzata continua a rappresentare in sé una minaccia contro la società, specie dopo l'allargamento dell'UE a 25 membri. E' in grado infatti di incidere sulle economie legittime e costituisce un fattore destabilizzante per l'organizzazione sociale e democratica. La Commissione europea, in particolare, ha più volte rilevato la difficoltà di individuare il concetto di criminalità organizzata, ritenendo necessario un collegamento tra i diversi settori criminali, che non in tutti i Paesi sono considerati diretta espressione di gruppi criminali organizzati ma che invece incidono sulla sicurezza comune.

Non bisogna infatti dimenticare che l'Europa si è formata ed allargata attorno al concetto di stabilità politica ed economica: questa doppia dimensione della sicurezza deve essere garantita al suo interno ed ai confini da condizioni, di democrazia e libero mercato, sane e libere da corruzione. La criminalità organizzata, che opera

proprio attraverso la corruzione, è considerata una delle principali minacce allo sviluppo e alla competitività, specie dei paesi nuovi ammessi e candidati. Sempre questa concezione europea della sicurezza ha conferito, nel tempo, particolare enfasi anche al partenariato pubblico - privato, specie nella lotta al terrorismo e nella protezione delle infrastrutture critiche nonchè, in generale, per supportare il binomio sicurezza - sviluppo.
Tradizionalmente, la minaccia asimmetrica è tipica di quelle forze antagoniste che, non disponendo di mezzi adeguati per far fronte alla preponderante forza convenzionale dell'avversario, ricorrono a strumenti alternativi a basso costo e limitato contenuto tecnologico e si servono della propaganda all'interno sia del gruppo sociale di riferimento che di quello contrapposto per massimizzare i risultati delle loro azioni. I gruppi terroristici più attivi al momento in ambito internazionale, sia di matrice confessionale che politica hanno ben compreso la forza di questo tipo di azioni verso la società occidentale: si sono concentrati quindi nelle azioni violente contro obiettivi simbolici accompagnati da un forte impiego dei media per aumentare l'effetto degli attacchi nella società italiana e far conoscere il "messaggio" a nuovi adepti. L'efficacia di questo modello si completa con un caratteristico modello organizzativo, variamente definito come cellulare, orizzontale, "a rete", addirittura "per franchising", comunque strutturato in modo da minimizzare le opportunità di contrasto esaltandone la dimensione informale e transnazionale, nonché sfruttando la flessibilità del sistema finanziario internazionale per garantirsi i finanziamenti.
Anche la criminalità organizzata internazionale costituisce un forte elemento di instabilità per la sicurezza nazionale, caratterizzata anch'essa dalla crescente diffusione di gruppi attivi in più paesi, dediti a diverse tipologie di traffici illeciti e dalla struttura orizzontale informale di tipo cellulare. Inoltre, anche dall'analisi sviluppata da Europol, è emerso che la criminalità organizzata ha adottato un modus operandi simile a quello dell'impresa nella società della globalizzazione, volto ad adottare modelli organizzativi di network cellulari, flessibili, con rapporti di dipendenza funzionali e non gerarchici, tali da creare una sorta di criminal industry, orientata al massimo profitto con il minimo rischio secondo una logica prettamente commerciale, volta a penetrare l'economia legale. I gruppi criminali gestiscono singoli settori delle medesime rotte sulle quali vengono sviluppati diversi traffici Illeciti: il contrabbando, il traffico di stupefacenti, di armi, di persone, di merci contraffatte.
Un'altra caratteristica di questo tipo di organizzazioni è la capacità di sfruttare le economie sommerse e informali, tipiche di talune comunità etniche, legate alla crescente domanda di servizi illegali ed a basso costo. Lo sfruttamento lavorativo di persone, la tratta di esseri umani anche particolarmente vulnerabili, e il favoreggiamento dell'immigrazione illegale, gestiti da parte della c.o. unitamente ad altri traffici illeciti, specie degli stupefacenti e delle merci contraffatte, determinano infatti alterazioni nella concorrenza e nel mercato, a favore di imprese illegali a danno di quelle regolari, determinando per di più gravi violazioni dei diritti umani.
Europol, in particolare, ha recentemente individuato, quali indicatori chiave della pervasività della criminalità organizzata attiva nell'Unione (di matrice autoctona o etnica), la dimensione internazionale, la struttura orizzontale - cellulare, l'uso di sistemi economico - finanziari legali, la forte specializzazione, la capacità di influire sulle istituzioni, l'impiego della violenza interna e, da ultimo, il ricorso a contro - misure anche qualificate dal punto di vista tecnologico. Fattori facilitanti, in questo tentativo della criminalità organizzata di proporsi come attore sociale ed economico a tutti gli effetti, sono stati individuati nella difficoltà di controllo a livello internazionale dei settori finanziario e dei trasporti e nella crescente capacità tecnologica, anche nella contraffazione di documenti di identità delle stesse organizzazioni.
In tale contesto, emerge l'importanza anche della tutela di settori strategici quali la sicurezza biologica, ambientale e alimentare, non solo, come spesso si ricorda, da attacchi di tipo terroristico, bio - terroristico o radioattivo, ma anche dal crescente inquinamento, dalla diffusione di patologie a livello internazionale, dal commercio e diffusione di sostanze ed alimenti pericolosi per la salute pubblica (contraffatti, igienicamente inadeguati o realizzati con sostanze tossiche o cancerogene): questi fenomeni sono facilitati dalla presenza di operatori economici che agiscono in un quadro di crescente illegalità, specie all'esterno dell'UE.
In sostanza, emerge un quadro di illegalità internazionale, che spesso trova, nella presenza di aree di crisi o di paesi a debole controllo democratico ai confini europei, un potente catalizzatore.
Come noto, l'Arma è una Forza Militare di Polizia a competenza generale ed in servizio permanente di pubblica sicurezza. In sostanza, svolge sia attività di prevenzione e repressione dei reati e di mantenimento del-

l'ordine pubblico alle dipendenze funzionali del Ministro dell'Interno, sia compiti militari alle dipendenze del dicastero della Difesa.
Tale peculiarità rende pertanto l'Arma strumento estremamente flessibile, in grado di assolvere, anche contemporaneamente, compiti fortemente differenziati, tra cui assumono particolare rilievo la gamma di attività info - investigative qualificate per contrastare terrorismo e criminalità organizzata transnazionale.
L'Arma ha avviato il contrasto a questi emergenti fenomeni criminali attraverso l'impiego del proprio tradizionale modello operativo, basato sulla territorialità del dispositivo che opera in stretta sinergia con Reparti speciali, in Italia e all'estero. In particolare, i Comandi provinciali in tutta Italia sono molto attivi nello sviluppo delle attività operative nel settore, rispondendo a una diffusa domanda di sicurezza dei cittadini nei confronti di ogni espressione dell'illecito.
Ma è sul piano della cooperazione internazionale che le attività di indagine più qualificate hanno permesso di conseguire risultati di eccezionale rilievo, che si sono imposti all'attenzione nel mondo per l'ampiezza dell'azione investigativa e la capacità di disarticolazione di organizzazioni terroristiche e criminali transnazionali. Queste indagini, sviluppate in particolare dal Raggruppamento Operativo Speciale, hanno riguardato i diversi settori: dal terrorismo confessionale e anarchico, ai traffici di stupefacenti, di armi e di persone.
A livello internazionale, l'attività dei Reparti dell'Arma nelle Missioni nei diversi teatri operativi, in ambito NATO, UE o multilaterali, è ormai simbolo di efficienza nella capacità di reale supporto e addestramento delle autorità locali.
Particolarmente qualificante, poi, l'attività dei Reparti speciali, primi tra tutti in questo settore i Comandi Carabinieri per la tutela della salute, dell'ambiente, del lavoro e delle Politiche agricole, posti alle dipendenze funzionali dei rispettivi Ministeri per salvaguardare interessi fondamentali della qualità della vita dei cittadini, che si sono imposti all'attenzione internazionale come esempio di operatori di polizia specializzati attivi nella collaborazione con i servizi ispettivi dei dicasteri e con le altre autorità competenti.
Proprio questo modello di sinergia tra le diverse componenti, che l'Arma persegue da sempre per supportare la fondamentale missione di controllo del territorio, costituisce premessa e scopo dell'adesione all'Osservatorio, nella ferma convinzione che la costruzione di un solido sistema paese potrà contribuire alla difesa nazionale nei diversi teatri operativi.

RUBRICHE

Anno I - n°1 Settembre 2006

Osservatorio per la Sicurezza Nazionale

rubriche

La Sicurezza Nazionale in Rete

a cura di Chiara Fonio
Italian Team for Security, Terroristic Issues & Managing Emergencies

Web e terrorismo

Il network terrorista sembra saper sfruttare pienamente gli strumenti offerti dalle nuove tecnologie proprio perché presenta la medesima caratteristica strutturale: la particolare architettura a maglie formata da "nodi" altamente interconnessi. Tuttavia, la cassa di risonanza offerta da Internet ha anche degli svantaggi: il riferimento è alle tracce lasciate, per esempio, attraverso i meccanismi di upload e download di materiali, o alla possibilità di analizzare nel dettaglio l'HTML dei siti, l'evoluzione delle strategie criptografiche ecc… Ognuno di questi aspetti è un inevitabile segno lasciato dal jihadismo che fornisce informazione sulle competenze specifiche e sull'organizzazione della rete. Questa puntata della rubrica Sicurezza Nazionale in Rete, si propone di esaminare il rapporto tra web e terrorismo in due modi: attraverso la descrizione delle potenzialità offerte dalle ICT (Internet Communication Technology) e attraverso alcune considerazioni di metodo e descrizione dei risultati che si possono ottenere grazie agli strumenti della media research.

ICT e terrorismo

Il coordinamento tra i membri delle cellule terroristiche nonché il reclutamento di potenziali militanti, è sempre più gestito attraverso il sapiente utilizzo delle nuove tecnologie. La "umma", ovvero la comunità di fedeli musulmani, è diventata "virtuale" grazie all'uso funzionale delle ICT. In particolare, la rete permette:

- un'elevata interconnettività: comunicazione e networking verso l'intero e verso l'esterno;
- una comunicazione "coperta", ovvero anonima; bassi costi e un campo di intervento pressoché globale;
- la moltiplicazione delle forze e la "sovra-rappresentazione" dei terroristi. Il terrorismo ha così raggiunto un livello di influenza mai avuto prima da altre simili organizzazioni grazie alla "la fine delle distanze" e all'eliminazione dei confini tra "vittima e carnefice";
- di raggiungere con facilità una molteplicità di target, indipendentemente dal sistema mediatico formale; " di diffondere i messaggi anche attraverso "siti mirror" non necessariamente appartenenti al mondo islamico (es. siti anarco-insurrezionalisti).

La maggior parte della comunicazione terrorista circola sul web sfruttando le caratteristiche sopra descritte. Inoltre, le nuove frontiere della comunicazione in rete, sono proiettate verso l'utilizzo di piattaforme - come quelle dei blog- estremamente flessibili e semplici da utilizzare. Non è più necessario conoscere l'HTML per pubblicare informazioni o diffondere video, occorrono soltanto un computer e una connessione. E' ipotizzabile che il cosiddetto Web 2.0, la nuova generazione di servizi presente all'interno della rete, in particolare i mezzi che servono per condividere risorse, diventi un ulteriore punto di forza per i gruppi fondamentalisti. Va infine ricordato che Al Qaeda, non è solamente un brand di import/esport di "suicide bombers", ma è anche un movimento politico "open source" che, grazie agli innumerevoli nodi della rete e alle peculiarità

dei gruppi locali, si rinnova e cresce in continuazione. La piattaforma mondiale del web contribuisce a mantenere le cellule costantemente operative e raggiungibili.

Come lavorare sul web

La vasta e differente quantità di materiali raccolti durante le nostre ricerche - una collezione di oltre 50.000 file - viene classificata secondo alcune macro-categorie:

- audio-video
  - sermoni, per la maggior parte discorsi dei leader jihadisti (es.: Abu Hamza, Osama, ecc.);
  - intrattenimento, soprattutto musica e clip dei gruppi islamici che promuovono la jihad;
  - formazione, video specifici di formazione all'azione;
  - informazione, sia sulla base della costruzione di "reality" (es.: uccisione degli ostaggi o azioni di fuoco) sia con la diffusione di bollettini informativi (es.: Sout Al-Khilafa - La Voce del Califfato);
    video complessi, di un'ora o più che affrontano la jihad con un mix dei prodotti precedenti;
  - video games, giochi di simulazione in rete o su CD (es: UnderAhs, UnderSiege);
  - flash, che pur facendo riferimento a un tipo tecnologico identifica bene una ormai diffusissima modalità di distribuzione di contenuti religiosi e jihadisti molto leggera (per il download) e di facile fruizione (es: jehad1, hisbah, ecc.)
- solo audio
  - a contenuto eminentemente politico;
  - a contenuto eminentemente religioso.
- solo testo
  - con riferimento a una tipologia da fonte a recettore (documenti per il pubblico);
  - con riferimento a una tipologia a rete (chat e forum).

L'analisi dei siti web che si sta conducendo permette le seguenti operazioni:

- Ping, che consiste nell'utilizzo di un protocollo chiamato UDP per inviare un pacchetto di dati al server corrispondente all'URL e mostrare i tempi di risposta in millisecondi. Si tratta di un'informazione utile per valutare l'effettiva raggiungibilità del server;
- Traceroute, ovvero il percorso nella rete che i pacchetti di comunicazione devono seguire per raggiungere il server dell'URL;
- Whols, attraverso l'utilizzo di questo strumento si ottengono informazioni specifiche riguardanti il dominio internet dell'URL, indicando chi l'ha registrato, chi ne è responsabile e altre informazioni gestite dal Network Information Center che ha concesso l'uso del dominio in questione;
- HTML, cioè il linguaggio di markup attraverso il quale è stato costruito il sito in questione;
- Emails (nascoste e non);
- Immagini;
- Links e backlinks, quest'ultima è una sorta di "navigazione al contrario" che serve a trovare tutte le pagine web che si riferiscono a una pagina data. Questo tipo di ricerca permette di analizzare graficamente le correlazioni all'interno del web. Data una URL di partenza si elabora il grafo raffigurante i suoi link, i backlink, le pagine con contenuti simili etc. e ognuno di questi risultati può diventare oggetto della richiesta successiva per creare mappe articolate che mettono in evidenza correlazioni di difficile individuazione (es siti che non si linkano direttamente tra di loro ma che sono collegati indirettamente) (cfr. figura 1);
- ricerche multiple su Google, Altavista, Yahoo, Google Newsgroup
- connessione a reti peer-to-peer per accedere a networks passando attraverso server (gateway) di ingresso.

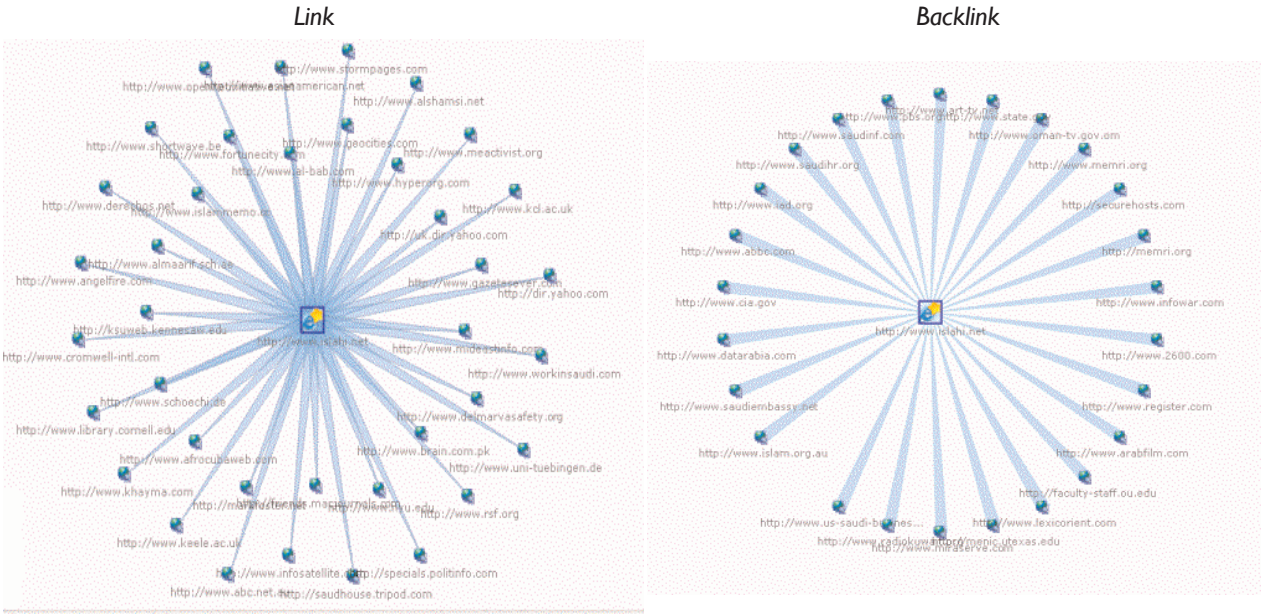


Figura 1 - Esempio di mappatura di link e back link di un sito monitorato

I risultati che si possono ottenere

Un esempio sia di come ogni evento possa essere letto nella sua dimensione comunicativa, sia di concreta applicazione degli strumenti della media research, è costituito dagli attentati terroristici che hanno colpito tre stazioni della metropolitana di Londra e un autobus il 9 luglio del 2005. Innanzitutto, occorre evidenziare le analogie con la capitale spagnola colpita l'11 marzo dell'anno precedente: l'attacco è coordinato, colpisce una grande città in orario di punta nel cuore del sistema dei trasporti; gli attentati coincidono con significativi eventi politici e mediatici. Tuttavia, le differenze sono maggiormente significative per comprendere l'evoluzione di un fenomeno che ci interessa e può essere studiato sia in riferimento ai comunicati apparsi sul web, sia quale processo di comunicazione che "svela" alcuni caratteri dell'organizzazione.

E' interessante soffermarsi sulle rivendicazioni e le subitanee smentite: entrambe di origine islamica. La rivendicazione è comparsa sul sito di Qal3ah, che è connesso a Sa'ad Rashed Mohammad Al-Fagih, considerato appartenente ad Al Qaida e alla jihad da circa dieci anni. Fagih - saudita con residenza a Londra - secondo gli USA ha fornito supporto logistico agli attentati alla ambasciata americana in Africa nel 1998 e poi si è occupato di mantenere la comunicazione via rete tra i jihadisti. Queste operazioni rimandano alla sua organizzazione "MIRA" e, appunto, a un'altra identità in rete denominata "Il Castello". Inoltre, la pista informatica porta a islah.org e miraserve.com, che non sono registrati a nome di Al-Fagih o di MIRA, tuttavia re-indirizzano al sito di MIRA (islahi.net). Le informazioni di registrazione dei domini portano a Al-Fagih, attraverso la "charity" di Hamas con base in Gran Bretagna, denominata Interpal. Pertanto, almeno il luogo virtuale in cui la rivendicazione ha avuto manifestazione è congruente. La smentita ha, anch'essa, avuto una origine jihadista e ha fornito ad alcuni l'alibi della speranza: se la smentita è vera forse non è jihad. Tale atteggiamento è spia significativa di una cultura del rifiuto della possibilità di essere oggetto del terrorismo islamico che ormai non ha più senso e crea debolezza. Ma soprattutto pone un interrogativo: perché smentire?

Un altro aspetto comunicativo allarga le dimensioni del problema. Immediatamente dopo Londra ecco l'uccisione, rivendicata, dell'Ambasciatore egiziano in Iraq. Perché tanta fretta? In fin dei conti era nelle loro mani, assassinarlo contiguamente a Londra significa avere perso una opportunità comunicativa: le due notizie penetrano su "mercati" - cioè pubblici - diversi, uno occidentale e uno arabo. Le due notizie tendono a elidersi a vicenda e non a rafforzarsi. Al contrario, l'assassinio dell'Ambasciatore oggi, avrebbe rinforzato l'allarme generato dall'attacco del 7/7. Allora perché? Probabilmente si tratta di una comunicazione interna e di un assassinio di reazione tra una jihad medio orientale e una jihad europea che non sono coordinate. Insomma, una sorta di affermazione di potere tra entità attive su un progetto comune ma senza una comune centrale di

controllo. Da questo punto di vista si è trattato di un errore, che ci aiuta a comprendere una struttura cellulare in evoluzione in Europa, fatta di imitatori di una rete in "franchising". Se questa lettura è corretta, la jihad può attraversare un momento di difficoltà organizzative (questo è l'aspetto positivo) ma anche può presentarsi sempre più frammentata e imprevedibile (e questo è l'aspetto negativo). Il caso di Londra, dunque, sembra essere interessante per una molteplicità di ragioni e dimostra che l'approccio "comunicativo" al fenomeno terrorista è molto utile per mettere a nudo logiche e dinamiche non sempre evidenti.

Anno I - n°1 Settembre 2006

Osservatorio per la Sicurezza Nazionale

rubriche

Tecnologie Intelligenti per la Sicurezza Nazionale

a cura di Enrico Appiani

Tecnologie intelligeti per la sicurezza

Nei paesi avanzati, il presidio della sicurezza del territorio nazionale, definita anche Homeland Security negli Stati Uniti dopo l'11 settembre, é un compito sempre piú complesso a causa della ricchezza di fattori politici, sociali, economici, informativi, organizzativi e territoriali di cui tenere conto. Il caso italiano é ulteriormente complicato dalla densitá di popolazione, dal territorio non vasto ma molto articolato, e dalla conseguente articolazione di infrastrutture e vie di comunicazione. Inoltre, le attrattive turistiche del paese e la ricchezza di beni storici e culturali lo rendono sede di grandi flussi di viaggiatori e di frequenti Grandi Eventi.
In questo contesto risulta fondamentale l'organizzazione gerarchica delle Forze di Pubblica Sicurezza, che gestiscono le proprie attivitá su diversi livelli territoriali in accordo alla rilevanza di attivitá, eventi, risorse e decisioni. Le tecnologie di informazione e comunicazione (ICT) svolgono da anni un ruolo fondamentale nelle operazioni di Polizia e Carabinieri, dalla periferia dei sensori al "cervello" delle sale operative, passando per il "sistema nervoso" distribuito delle reti informative. I sensori aumentano la capacitá di osservazione e detezione di eventi; le comunicazioni fisse e mobili supportano la cooperazione e lo scambio informativo fra tutti gli operatori coinvolti sul territorio; le sale operative, infine, forniscono una visione elaborata, centralizzata e condivisa delle informazioni rilevanti.
Al crescente uso del supporto ICT corrisponde tuttavia una crescente quantitá di informazioni multimediali a disposizione degli operatori, generate internamente ed esternamente alla Pubblica Sicurezza, con crescente difficoltá ad isolare le informazioni utili, classificare e archiviare i dati, e rispettare le norme sulla privacy, identificando i dati sensibili ed eliminando quelli non rilevanti alle attivitá di prevenzione e indagine. Basti pensare per esempio a quanti milioni di telecamere si trovino in luoghi pubblici e privati di una nazione, dove la telesorveglianza si é spinta in molti casi fino all'ambito domestico. Molti crimini vengono risolti grazie alla visione delle sequenze registrate dai privati, che tuttavia vengono periodicamente cancellate e non sono in genere indicizzate ai fini della ricerca automatica delle sequenza piú utili.
La nuova frontiera del supporto ICT alla sicurezza diventa quella delle "tecnologie intelligenti", in grado non solo di raccogliere, elaborare e presentare dati dal territorio, ma anche di assolvere una parte dei compiti umani nella loro interpretazione e valutazione, a partire dai segnali fisici generati dai sensori fino al supporto decisionale su situazioni complesse per la vita nazionale.
Il concetto di per sé non é una novitá: la disponibilitá di potenza di elaborazione a basso costo e la miniaturizzazione dei dispositivi spingono a porre software complesso dovunque, aumentando l'autonomia dei nodi periferici (es. sensori o attuatori) e la loro capacitá di dialogare sulle reti. Agli alti livelli di elaborazione, cresce l'uso di tecnologie in grado di supportare la comprensione e interpretazione umana dei dati, come la business intelligence, l'analisi semantica di testi, l'analisi di scene, l'indicizzazione multimediale e i motori inferen-

ziali per svolgere catene deduttive di concetti. In campi civili e industriali, l'intelligenza delle tecnologie ICT viene intepretata sotto forme diverse, come piú elevata automazione, autonomia di funzioni e dispositivi, facilitá d'uso e adattamento alle esigenze degli utenti, fino all'emulazione del ragionamento umano.
Ma quale puó essere un significato appropriato di supporto intelligente nel contesto della Sicurezza Nazionale? Si fa sicurezza perché esistono minacce da fronteggiare e rischi da mitigare, la cui capacitá di analisi é una qualitá essenzialmente umana, in quanto legata alla percezione di pericolo e insicurezza. Tale percezione é anche molto soggettiva e legata a fattori storici e culturali. Inoltre, il presidio della sicurezza é un processo organizzativo che si svolge parallelamente al resto della vita civile, ben organizzato dalle Forze di P.S. nei compiti di prevenzione, intervento e indagine.
Quindi la sicurezza non é completamente automatizzabile, ma il relativo supporto ICT diventa piú "intelligente" se comprende caratteristiche che aiutano gli operatori della sicurezza a svolgere piú efficacemente i propri compiti, concentrandosi sulle proprie capacitá umane di sintesi della situazione anziché sull'intepretazione di grandi moli di dati: il che significa dare automazione almeno parziale alle fasi tipicamente umane di monitoraggio - percezione - analisi - decisione - azione. L'obiettivo é quello di ridurre lo stress degli operatori e di conseguenza la possibilitá che eventi rilevanti per la sicurezza vengano percepiti e gestiti in modo scorretto o ritardato.
Oltre alla dimensione delle azioni di cui sopra, c'é quella della complessitá del territorio che, similmente ad un sistema informativo geografico (GIS), va modellato come sovrapposizione di strati tematici che concorrono a determinare i rischi e gli eventi da fronteggiare:
1) ambiti infrastrutturali, con famiglie di infrastrutture potenzialmente sensibili che ammettono scomposizione gerarchica (es. reti di distribuzione di energia a diffusione nazionale);
2) caratteristiche del territorio, che incrociato alle infrastrutture determina i rischi e le criticitá di protezione (es. zone montuose, siti isolati);
3) popolazione e attivitá, ordinarie e straordinarie, che hanno luogo sul territorio e sulle infrastrutture, determinando l'evoluzione dei rischi e degli eventi da gestire.
Infine, l'automazione delle sale operative deve tenere conto di diversi livelli di gestione della sicurezza nazionale, come illustrato nella figura 1 che riassume il contesto descritto.

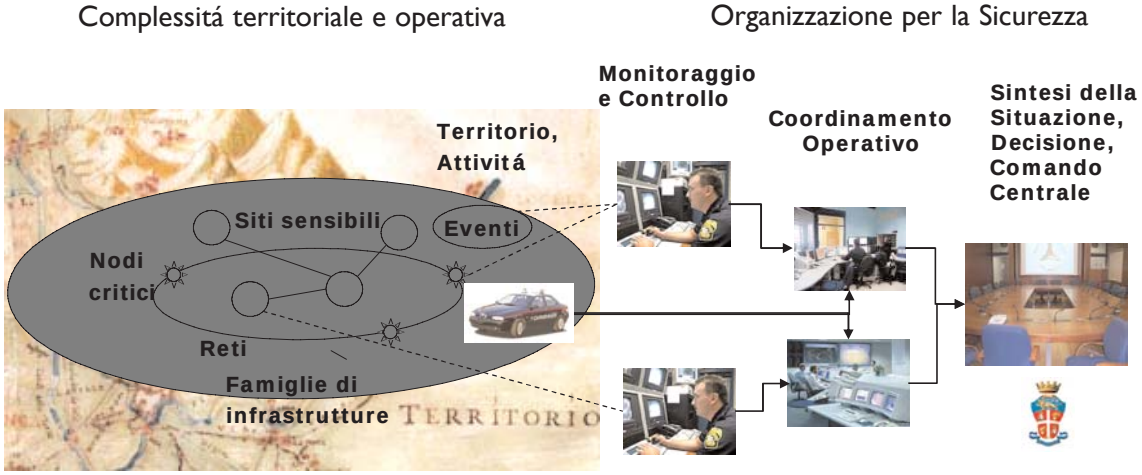


Figura 1 - Gestione del territorio e livelli di decisione

Vediamo di seguito alcuni requisiti e caratteristiche che possono trasformare una sicurezza informatizzata in sicurezza intelligente:
- condivisione di risorse con la gestione di processi diversi dalla sicurezza; es.: sorveglianza di infrastrutture critiche, giá dotate di sensori e sale controllo;
- utilizzo di sensori e fonti informative come sopra e in comune a diverse missioni; es: indagini o prevenzione con accesso condiviso a sensori e basi dati di dati per la sorveglianza di siti privati; monitoraggio di sorgenti aperte;

- interpretazione di informazioni multimediali per la sicurezza; es. indicizzazione di sequenze audio-video per ricerca di personaggi specifici o di comportamenti anomali, con finalitá diverse da quelle dell'archiviazione storica;
- interfacce e funzionalitá che si adattano ai ruoli degli operatori, sia per mansioni che per collocazione territoriale; es.: situazione provinciale, regionale o nazionale; supporto a gestione di interventi, gestione segnalazioni o analisi di informazioni; informazioni specializzate per operatori di comandi inter-forze;
- sintesi di situazioni da diversi elementi indicatori; es: detezione di esplosione, attentato o altro incidente in luogo affollato a partire dalla correlazione di dati da sensori video, audio, antincendio e segnalazioni dei cittadini ai numeri di emergenza;
supporto alle decisioni tramite inferenze e modelli predittivi; es: ragionamento automatico su regole di sicurezza; previsione delle conseguenze di incendio o esplosione; correlazione di fatti utili alla medesima indagine;
- analisi dinamica del rischio, sia come livello di rischi giá modellati, sia come individuazione di nuovi rischi;
- flessibilitá di cooperazione fra processi di sicurezza che riflettono diversi approcci e punti di vista; es: condivisione di dati fra Polizie di diversi stati europei, armonizzando diverse proritá, concetti sensibili e reati connessi alle rispettive legislazioni e forze di sicurezza.

Speriamo fin qui di aver presentato efficacemente al lettore, in modo preciso ma non troppo tecnico, il contesto della sicurezza intelligente nella visione di Elsag. Questo primo numero della rubrica si conclude presentando alcune tecnologie abilitanti sviluppate e integrate nelle soluzioni dell'azienda, che saranno approfondite nei numeri successivi.

< Sensori intelligenti - Componenti software che, applicati a normali sensori, in particolare video, diventano unitá sensoriali dotate di capacitá autonome di connessione al sistema, gestione dei dati rilevati e detezione/analisi di eventi significativi. Fra questi spiccano i lettori automatici di targhe di veicoli, fissi e mobili, e gli analizzatori di scene in grado di tracciare presenza e moto di persone e veicoli.
< Sale di monitoraggio e controllo - Evoluzione della sorveglianza verso una gestione integrata, grafica e intuitiva, degli eventi ed allarmi rilevati dal campo attraverso una pluralitá di sensori, con classificazione degli eventi, guida per la gestione da parte degli operatori in sala e comunicazione con le forze sul campo.
< Sale informative di comando e decisione - Raccolta, classificazione e analisi di informazioni da sorgenti eterogenee, sia aperte sia interne alle Forze di P.S., classificandole per contenuti e rilevanza tramite Integrazione di tecnologie di indicizzazione avanzata multimediale, analisi di sequenze audio-video, analisi linguistica e semantica, e correlazione delle informazioni estratte. Ricerca su tecniche avanzate di intelligence, come i sistemi cognitivi, i motori inferenziali e l'analisi di novitá nei comportamenti delle fonti monitorate. In altra rubrica si trova "Web e terrorismo" sull'analisi di informazioni sensibili di supporto al terrorismo da fonti Web.

Settembre 2006
Anno I - n°1

Osservatorio per la Sicurezza Nazionale

Stato Maggiore Aeronautica
Ufficio Generale del Capo di Stato Maggiore
Ufficio Pubblica Informazione e Comunicazione

Articoli

"Nine-Eleven" terrorismo globale e sicurezza dei cieli
L'impegno dell'Aeronautica Militare per la sicurezza dello spazio aereo

Il terrorismo[1] globale

Gli eventi del "nine-eleven" hanno dimostrato gli effetti della radicale trasformazione della natura del terrorismo che è oggi un fenomeno globale sia per il numero e la diffusione degli eventi che per le conseguenze sociali, politiche ed economiche che da essi derivano. Il terrorismo del ventunesimo secolo risulta organizzato secondo i più moderni criteri di decentralizzazione dell'iniziativa operativa mirata al conseguimento di obiettivi strategici "attraverso l'impiego di armi convenzionali, chimiche, batteriologiche, nucleari e radiologiche "[2], e di strumenti e metodi non classificabili fra quelli normalmente utilizzati in campo militare.
In Europa, l'abbattimento delle frontiere, la grande disponibilità di mezzi e vie di trasporto, l'elevata densità di abitanti, la fruibilità e la velocità delle informazioni, sembrano essere le caratteristiche dell'ambiente operativo maggiormente sfruttate dal terrorismo internazionale per operare nell'ombra progettando e perpetrando attentati in grado di condizionare una massa di persone ben più grande di quella direttamente colpita nel corso di tali eventi. I media giocano in questo contesto un ruolo fondamentale diffondendo le notizie in "tempo reale" su scala globale.
Nella scala dei valori della cittadinanza, condizionata da questa realtà, la sicurezza ha assunto una priorità sempre maggiore. Gli organi istituzionali si sono attivati per garantire il funzionamento del sistema paese prevenendo il terrorismo e predisponendo una capacità di risposta volta a fronteggiare eventuali crisi derivanti da eventi terroristici catastrofici.
La natura multi-dimensionale del terrorismo impone un forte impegno nel campo della prevenzione e delle predisposizioni finalizzate a garantire il coordinamento e la cooperazione fra tutti gli operatori di sicurezza attivi nei vari settori delle attività sociali, economiche e produttive, vitali per gli interessi del Paese ed esposte alla minaccia terroristica.
La definizione di una politica di sicurezza in grado di indirizzare univocamente tutte le iniziative di prevenzione e riduzione del rischio associato alla minaccia terroristica è ritenuta indispensabile al fine di garantire un'efficace interazione fra Ministeri, Forze Armate, Enti, Agenzie e tutte le organizzazioni direttamente o indirettamente chiamate a contribuire alla sicurezza in modo efficace, tempestivo e soprattutto sostenibile.
Come dimostrato dagli eventi dell'11 settembre 2001, uno di questi settori attiene al controllo e alla sicurezza dei cieli oggi garantita, in Italia, dall'Aeronautica Militare inserita nel contesto multinazionale della Difesa Aerea Integrata della NATO.

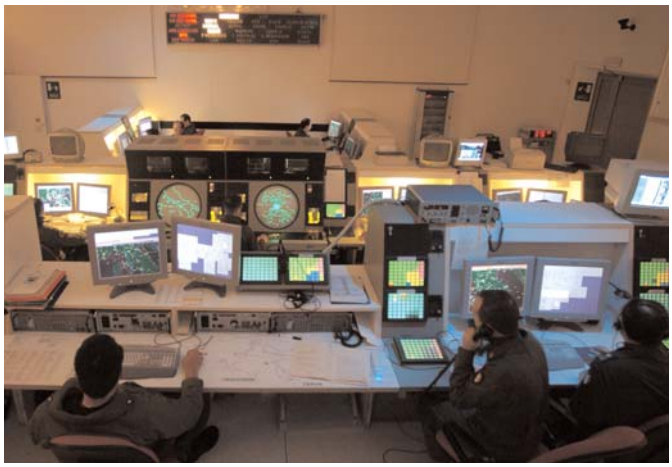
La difesa aerea

L'Aeronautica Militare assicura la sorveglianza e la difesa dello spazio aereo nazionale in maniera continuativa attraverso un sistema integrato di sensori (radar basati a terra ed in volo[3]) e con l'impiego di velivoli e

1 *Trattasi di una minaccia asimmetrica, indeterminata, volatile e, soprattutto, imprevedibile che richiede un'azione di contrasto che fa della prevenzione l'unica arma sulla quale polarizzare la strategia globale di lotta. Pur nella consapevolezza che "il fenomeno è controllabile, ma non debellabile", che ha limiti e debolezze, ma numerosi punti di forza che lo rendono pressoché invincibile. - Giulia La Volpe / Pagine Difesa*

2 *RAND - Quick scan of post 9/11 national counter-terrorism policymaking and implementation in selected European countries. Maggio 2002*

3 *Airborne Early Warning*



Una tipica sala operativa della difesa aerea - Foto Troupe Azzurra

sistemi missilistici superficie/aria.
Il dialogo continuo con gi enti di controllo del traffico aereo civile (ENAV) e con le autorità deputate alla sorveglianza dello spazio aereo dei paesi NATO europei, consente di operare efficacemente a tutela di tutti gli utenti dello spazio aereo e per garantire un adeguato livello di sicurezza.
Le funzioni di comando e controllo degli assetti della difesa aerea nazionale permanentemente assegnati alla NATO, sono devolute al CAOC 5 [4] di Poggio Renatico che, attraverso una sala operativa, dispone l'impiego dei velivoli in QRA (Quick Readiness Alert). In caso di avvistamento di una traccia radar non identificata, oppure nel caso in cui un traffico non risponda a prestabiliti requisiti o diverga dalla rotta prevista senza validi motivi, viene rapidamente ordinato il decollo (in gergo tecnico "scramble") dei velivoli intercettori che sotto la guida dei controllori di intercettazione a terra, si dirigono verso la traccia "sospetta", ne accertano visivamente l'identità e le reali condizioni ed intervengono, ove necessario, per scortarlo fino ai limiti dello spazio aereo di responsabilità, imponendo variazioni di rotta o eventualmente l'atterraggio su di un aeroporto idoneo per effettuare ulteriori verifiche da parte dell'autorità di pubblica sicurezza.
I Reparti dell'Aeronautica Militare che svolgono questo tipo attività sono il 5° Stormo di Cervia ed il 37° Stormo di Trapani, equipaggiati con i caccia F-16 e, dal 16 dicembre del 2005, il 4° Stormo di Grosseto, equipaggiato con i nuovi velivoli Eurofighter 2000. Tali aeromobili, opportunamente predisposti ed equipaggiati, sono in grado di decollare ed intervenire in tempi brevissimi su tutto il territorio nazionale e nell'area NATO di responsabilità assegnata alla nazione.
La necessità di prevenire ed eventualmente scongiurare un attacco terroristico dal cielo ha indotto la difesa aerea a modificare la propria filosofia operativa oggi orientata alla "sorveglianza attiva" piuttosto che ad una "sorveglianza vigile" intrinsecamente inerte. La struttura della catena di comando e controllo è stata modificata allo scopo di garantire la piena tutela degli interessi e della sicurezza nazionale.

Firma dell'accordo tecnico per la difesa aerea con la Svizzera - Foto Troupe Azzurra

Seppure ancora fortemente incardinato nel sistema di difesa integrata della NATO, il servizio di sorveglianza dello spazio aereo italiano consente oggi (sulla base di provvedimenti di legge recentemente adottati) di trasferire il comando e controllo degli intercettori dalla NATO alla autorità governativa nazionale nel caso in cui una "traccia" sia classificata come "RENEGADE" ovvero come un traffico aereo la cui condotta sia riconducibile ad una possibile azione terroristica.
Nella gestione di situazioni di questo tipo, un'efficace interazione fra le agenzie deputate al controllo amministrativo dello spazio aereo e la difesa aerea, è ritenuta fattore di fondamentale importanza per garantire una

4 *Combined Air Operation Centre*

5 *Servizio d'Allarme*

capacità operativa di difesa realmente credibile.
Al pari, l'opportunità di avviare un dialogo costruttivo con i paesi confinanti e, in un contesto più ampio, con i paesi che si affacciano sul bacino del mediterraneo, costituisce oggetto di attenzione in relazione alla definizione di nuove strategie per contrastare una minaccia di portata crescente. La recente sottoscrizione di accordi tecnici per la difesa dello spazio aereo con Francia e Svizzera e l'avvio di una similare iniziativa con l'Austria, consentirà certamente di incrementare l'efficacia dello strumento della difesa aerea durante gli interventi in prossimità dei confini nazionali precedentemente considerati limiti inviolabili da parte degli intercettori.

Sostenibilità e criticità del servizio di sorveglianza dello spazio aereo.
Le recenti restrizioni di bilancio hanno fortemente condizionato lo svolgimento di tutte le attività dell'Aeronautica Militare che ha avviato un processo di verifica finalizzato all'individuazione di soluzioni idonee a garantire la sostenibilità dello sforzo operativo nonostante la costante riduzione strutturale delle risorse a disposizione. Oltre a focalizzare le proprie attività sul "core business", ovvero sui prioritari compiti d'istituto (primo fra tutti quello della sicurezza dello spazio aereo), lo Stato Maggiore Aeronautica ha preso in esame la casistica delle attivazioni del sistema di sorveglianza, alla ricerca di soluzioni per garantire il desiderato livello di sicurezza al minor costo possibile.
Tale studio ha evidenziato la marcata tendenza di crescita del numero di attivazioni degli intercettori dovuta all'innalzamento del livello di attenzione ed all'applicazione di nuovi e più restrittivi criteri di sicurezza da parte dell'autorità di comando e controllo della difesa aerea nazionale. In questo campo è stato anche necessario rilevare che una gran parte delle attivazioni è stata determinata dall'inosservanza delle norme riguardanti la gestione amministrativa dello spazio aereo quali: la mancata richiesta delle autorizzazioni diplomatiche da parte di operatori stranieri ovvero l'utilizzo di autorizzazioni scadute o destinate ad altri paesi o operatori, la perdita delle comunicazioni radio terra/bordo/terra dovuta si, ad avarie tecniche ed alla vetustà dei sistemi, ma anche a leggerezza o inadeguata conoscenza delle procedure in uso, l'inosservanza spesso consapevole delle norme della circolazione aerea.
La possibilità di ridurre il numero di attivazioni generate per motivi inconsistenti consentirebbe di preservare risorse preziose ai fini della salvaguardia della sicurezza nazionale.

Periodo	Interventi
dal nov. 2000 al 11 sett. 2001	4
dal 11 sett. 2001 al 31 dic. 2001	11
2002	32
2003	19
2004	28
2005	**47**
dal 1 gen. 2006 al 14 lug. 2006	18

Numero di attivazioni degli intercettori dal 1 nov. 2000 al 14 lug. 2006.

I grandi eventi nazionali
Da diversi anni, in occasione dello svolgimento di eventi di particolare rilevanza per i quali sia prevedibile una consistente concentrazione di persone e una diretta esposizione all'attenzione dei media, l'Aeronautica Militare provvede al potenziamento del apparato di sorveglianza e difesa dello spazio aereo per prevenire e

Un HH3F del 15° Stormo CSAR in configurazione Slow Mover Interceptor - Foto Troupe Azzurra

scongiurare eventuali attacchi terroristici condotti con mezzi aerei.
La prima operazione di questo tipo si è svolta nei cieli di Genova in occasione del G8 dal 16 al 23 luglio 2001, pochi mesi prima del fatidico 11 settembre.
In tale circostanza, come del resto avviene oggi nel contesto delle operazioni di questo tipo (denominate "JUPITER" dal 2004), fu previsto l'impiego integrato di mezzi e personale appartenenti a diverse unità dell'Aeronautica Militare, delle Forze Armate e dei Corpi Armati dello Stato per prevenire e contrastare la minaccia aerea controllando sia il flusso del traffico aereo in volo che il transito di velivoli di qualsiasi categoria o dimensione presso gli aeroporti e le aviosuperfici (generalmente sprovviste di un servizio di controllo del traffico aereo). Per contrastare il segmento cosiddetto "asimmetrico" della minaccia aerea, ovvero l'attacco da parte di aeromobili/aerostati non concepiti come veri e propri sistemi d'arma, i dispositivi di sicurezza JUPITER sono dotati di una capacità di intervento specificamente orientata all'intercettazione di piccoli aeromobili (anche ultraleggeri), generalmente lenti e facilmente occultabili alla scoperta dei radar grazie a profili di volo a bassissima quota.
Avverso tali minacce, oltre a dotarsi di una catena di avvistamento visivo sul perimetro della zona di interesse (SPOTTERS), sono schierati ed impiegati velivoli MB 339 CD del XII Gruppo di Gioia del Colle unitamente ad elicotteri HH3F del 15° Stormo CSAR, opportunamente equipaggiati al fine di disporre di una capacità di intervento alle quote più basse, in prossimità dei centri abitati e soprattutto a bassa e bassissima velocità.

Un F-16 riceve l'ordine di "scramble" - Foto Troupe Azzurra

Aree di intervento ai fini del miglioramento continuo del servizio

La NATO, coinvolta nella definizione dei programmi di sviluppo dei dispositivi di difesa aerea e dei futuribili scenari d'impiego, fornisce il proprio contributo di pensiero suggerendo, alle nazioni alleate, nuovi indirizzi e procedure aggiornate alla mutevole realtà della minaccia aerea di matrice terroristica.
L'alleanza promuove, presso i paesi membri, l'armonizzazione delle procedure, della terminologia e dei protocolli di comunicazione. Sostiene lo sviluppo di dispositivi e procedure che consentano di fronteggiare potenziali situazioni di emergenza in prossimità dei confini nazionali (la recente sottoscrizione di accordi tecnici bilaterali per la difesa aerea con la Francia, la Svizzera e l'Austria sono in linea con tali suggerimenti). Supporta la pianificazione e l'esecuzione di esercitazioni per favorire l'interoperabilità in ambiente multinazionale, interforze ed interagenzia; sollecita lo sviluppo di efficaci strumenti e modalità di coordinamento fra l'autorità militare deputata alla difesa e quella civile deputata al controllo del traffico aereo.
Indipendentemente dalla capacità operativa del dispositivo di difesa aerea, la mutevole ed imprevedibile fisionomia della minaccia terroristica impone un'accurata azione nel campo delle informazioni per fronteggiare efficacemente il fenomeno. Un costante scambio di informazioni fra gli operatori di sicurezza finalizzato alla ricerca, alla pronta identificazione ed alla valutazione di "segnali deboli" che evidenzino le anomalie potenzialmente associate al fenomeno del terrorismo, è determinante ai fini dell'attuazione delle misure necessarie a garantire la sicurezza.
L'interoperabilità dei sensori, dei sistemi di comunicazione, delle procedure, unitamente alla possibilità di condividere, con tutte le organizzazioni militari e civili che concorrono a

Un RADAR della Difesa Aerea - Foto Troupe Azzurra

garantire la sicurezza, una comune strategia e linee guida inequivocabili, è indispensabile per operare insieme efficacemente.
Un quadro normativo adeguato deve necessariamente prevedere le nuove fattispecie associate a scenari fino ad ora non ipotizzabili per consentire la definizione di regole d'ingaggio commisurate al tipo di minaccia da fronteggiare e garantire la sicurezza di tutti gli utenti dello spazio aereo.
La normativa riguardante la gestione amministrativa dello spazio aereo dovrebbe tenere maggior conto delle esigenze di urgenza, flessibilità ed economicità degli utenti commerciali e non, nazionali e stranieri, prevedendo severe sanzioni per i comportamenti volontari lesivi della sicurezza dello spazio aereo che inneschino inopportune e dispendiose attivazioni del sistema di difesa.
Ancora molto è possibile fare nel campo della "cultura della sicurezza" sensibilizzando tutti gli operatori ad una professionale e scrupolosa osservanza dei comportamenti che, oltre a garantire l'ordinato utilizzo dello spazio aereo, consentono di operare in sicurezza anche in condizioni di traffico crescente.

Achille Cazzaniga

SOMMARIO