

# LA TRASFORMAZIONE NET-CENTRICA

IL FUTURO DELL'INTEROPERABILITÀ  
MULTINAZIONALE E INTERDISCIPLINARE



STATO MAGGIORE DELLA DIFESA



Periodico dello Stato Maggiore della Difesa fondato nel 1981  
Via XX Settembre, 11 - 00187 Roma - Tel. 06-4884925 - Fax 06-46912950

# LA TRASFORMAZIONE NET-CENTRICA

IL FUTURO DELL'INTEROPERABILITÀ  
MULTINAZIONALE E INTERDISCIPLINARE

NCW - AL CENTRO DELLA TRASFORMAZIONE .....	4
UNA RETE GLOBALE .....	12
ITALIA: SITUAZIONE E OBIETTIVI.....	26





**L**a sostanza del concetto net-centrico risiede nell'interconnessione in rete – in termini di binomio uomo-sistema - fra sensori, valutatori, decisori e attuatori mirata a sfruttare sinergicamente informazioni e capacità operative allo scopo di conseguire effetti coerenti con gli obiettivi desiderati.

La trasformazione net-centrica delle Forze Armate italiane, per certi versi già avviata e operante in analogia con quanto avviene nei principali Paesi alleati, rappresenta un'esigenza assolutamente prioritaria e, al tempo stesso, ineludibile.

Non possiamo rimanere attardati; dobbiamo muoverci nella direzione di sviluppare concetti e capacità operative coerenti con quelli dei nostri partners: se non lo faremo resteremo inesorabilmente tagliati fuori dalla possibilità di interoperare nell'ambito delle missioni multinazionali - alle quali oggi forniamo un apporto importante - e che sempre più domani costituiranno il focus del contributo della componente militare all'azione del nostro Paese nell'ambito delle iniziative della comunità internazionale per la stabilità e la sicurezza. Ciò a supporto e a tutela della pace e della nostra stessa sicurezza.

La questione non è pertanto "se" dovremo acquisire capacità NCW/NEC ma "quando", "come" e "in che misura" saremo in grado di acquisirle. Occorre cioè essere consapevoli che non ha senso, per l'Italia, uno strumento militare "sconnesso" da quello dei principali Paesi che formano le alleanze e le organizzazioni internazionali – in primis la NATO e l'Unione Europea - di cui noi stessi siamo parte.

La piena integrazione e l'interoperabilità multinazionale rappresentano requisiti irrinunciabili; rinunciarvi vorrebbe dire rinunciare ad essere membri partecipi e attivi del sistema di sicurezza internazionale e scadere ad un livello che, certamente, non corrisponde al ruolo

e alle responsabilità del Paese, che scaturiscono dagli orientamenti consolidati a livello politico-istituzionale.

In questa direzione occorre quindi procedere ed investire con chiarezza di idee e dinamicità. In futuro saremo destinati, probabilmente, a disporre di un numero più ridotto di piattaforme e di sistemi: e questo sarà accettabile in una certa misura. Ma quelli che avremo – e questo sarà assolutamente indispensabile – dovranno essere pienamente in grado di dialogare e interagire con quelli degli altri partners. Il nostro personale dovrà essere addestrato ad operare in tale contesto e con un'ottica focalizzata sugli effetti da conseguire.

E'una scelta di cui sono pienamente convinto e sulla base della quale sono determinato ad incentrare l'accelerazione della trasformazione dello strumento militare che, insieme al sostegno alle missioni internazionali, costituisce l'imperativo quotidiano delle Forze Armate.

La trasformazione in senso net-centrico richiede, innanzitutto, un salto di mentalità - una vera e propria rivoluzione culturale - e una partecipazione attiva e convinta dell'elemento umano, che della trasformazione deve divenire "motore" e protagonista a tutti i livelli e in tutti i settori: concetti e dottrina operativa, formazione e addestramento, sostegno logistico, strutture organizzative, procedure di lavoro, ottimizzazione dell'impiego delle risorse umane e finanziarie. Il contributo di pensiero, l'iniziativa e l'azione di tutti è ugualmente necessaria, e sarà determinante.

Il secondo fattore su cui è indispensabile puntare è la tecnologia. L'Italia è certamente un Paese che sa esprimere capacità e tecnologie di alta qualità, e su questo fronte è necessario andare oltre l'intensa e proficua cooperazione che, fino ad oggi, ha caratterizzato il rapporto fra le Forze Armate e l'industria della difesa. Occorre raggiungere e consolidare tutte le sinergie possibili, al fine di "mettere in rete" e indirizzare al meglio esigenze, conoscenze, esperienze, energie e risorse verso un obiettivo comune.

Il processo di trasformazione che le Forze Armate stanno sviluppando è destinato, inevitabilmente, ad avere effetti diretti e correlati anche sul sistema industriale: questo percorso non può essere affrontato in modo autarchico, in particolare in termini di risorse e di tecnologie sulle quali poter contare.

Non ho dubbi che l'Industria sarà in grado, come in passato, di rispondere alle nuove esigenze dello strumento militare e di fornire un contributo determinante all'acquisizione delle capacità che ci sono necessarie. Ciò anche ricorrendo alle più opportune alleanze strategiche con i partner europei e transatlantici, che consentiranno alle nostre aziende di sviluppare, al tempo stesso, il proprio "know how", la propria competitività e, quindi, la capacità di guadagnare quote di mercato a livello globale.

Ci troviamo dunque di fronte ad una sfida che investe formazione, tecnologia, dottrina e sistema industriale; la trasformazione net-centrica è un obiettivo a largo spettro coerente con quello più generale, e strategico per il "sistema Paese", che chiama tutte le sue componenti ad un impegno sinergico per rispondere efficacemente alle esigenze di un mondo sempre più globalizzato, nel quale sicurezza e stabilità rappresentano condizioni imprescindibili e determinanti per le prospettive di sviluppo.

Ammiraglio Giampaolo Di Paola  
Capo di Stato Maggiore della Difesa

# NCW - AL CENTRO DELLA TRASFORMAZIONE

IL CONCETTO DI NETWORK CENTRIC WARFARE (NCW) RAPPRESENTA LA RISPOSTA DEL COMPARTO MILITARE ALLE ESIGENZE OPERATIVE DELL'ERA DELL'INFORMAZIONE

I profondi cambiamenti che hanno accompagnato l'ingresso nel nuovo millennio – il passaggio dall'era industriale a quella dell'informazione, la globalizzazione e la fine del confronto bipolare, sostituito da quello asimmetrico e dalla minaccia terroristica – hanno inciso non solo sulla società e sull'economia ma, inevitabilmente, anche sul mondo "sicurezza" in generale, e militare in particolare.

In quest'ultimo, la necessità di una trasformazione per molti versi radicale deriva da diversi fattori:

- la modifica degli scenari di sicurezza, che richiedono di adeguare la struttura delle forze nel senso di una maggiore flessibilità, mobilità, modularità e proiettabilità, in modo da poter reagire alle crisi, prontamente e con uno strumento qualitativamente e dimensionalmente efficace, là dove esse si manifestano;

fianco degli alleati atlantici ed europei, con un elevato grado di interoperabilità e la più completa integrazione;

- il progresso tecnologico (particolarmente incalzante nel campo dell'Information Technology, IT, e delle comunicazioni), che impone il progressivo e coerente adeguamento di ogni strumento militare che non intenda rinunciare ad essere moderno, efficace e compatibile con quelli dei Paesi alleati e quindi, in ultima analisi, efficace e utilizzabile;
- i vincoli economici che, agendo sulle capacità di spesa, impongono sempre più scelte lungimiranti, intelligenti, efficienti e rivolte all'acquisizione e allo sviluppo delle capacità prioritarie, in un contesto in cui non è più possibile guardare alla Difesa come a una realtà "autarchica", ma saldamente inserita nel sistema di sicurezza nazionale ed internazionale.

Al centro di questa trasformazione si pone – col conforto degli insegnamenti tratti dalle operazioni più recenti e da quelle in corso, dalle esercitazioni, dalle simulazioni e, non ultimo, dall'esperienza dei Paesi che, come gli Stati Uniti, hanno già compiuto significativi passi in questa direzione – il concetto di Network Centric Warfare (NCW): concetto che rappresenta la "risposta" con cui il comparto militare si adegua alla condotta delle operazioni nell'era dell'informazione.

Il termine identifica, in senso lato, una combinazione di elementi dottrinari, procedurali, tecnici, organizzativi e umani che, opportunamente collegati fra loro ("messi in rete" ovvero "networked", secondo la terminologia anglosassone), interagiscono creando una situazione di decisiva superiorità per la forza che ne dispone.

L'implementazione dell'NCW riguarda prima di ogni altro l'elemento umano, e per chiarirlo è sufficiente una semplice considerazione. La tecnologia,

4



- la connotazione spiccatamente interforze e multinazionale delle operazioni attuali e future, non solo belliche ma anche di Peace Support Operations (PSO) e di soccorso umanitario, che richiedono la capacità di inserirsi efficacemente nell'ambito di contesti "joint e combined", a

e in particolare l'IT, è essenziale per creare il "sistema", la "rete": ma "operare in rete" implica l'intervento coordinato e sinergico di persone e di elementi organizzativi (comandi, reparti, strutture di supporto) che, sotto la guida di una nuova dottrina e avvalendosi delle più appropriate procedure, riescono a relazionarsi in un modo nuovo, sfruttando le capacità della rete per la raccolta, analisi, trattazione e distribuzione delle informazioni, trasformandole in un vantaggio decisivo nella condotta delle operazioni. L'uomo – non la tecnologia – è al centro della "rete", perché l'ha concepita, l'ha progettata, la usa e ne è parte integrante e interattiva.

Il principio organizzativo che sta alla base del concetto di NCW non è nato nell'ambiente militare, ma può essere fatto risalire alle dinamiche di crescita e competizione che già negli ultimi decenni del secolo scorso hanno caratterizzato lo sviluppo dell'economia mondiale. Anche in questo caso l'Information Technology è stata il motore principale del rinnovamento della moderna economia e in particolare del suo segmento più avanzato e reattivo, quello americano. I massicci investimenti commerciali nel settore dell'IT sono all'origine della diffusione esponenziale dei computer nel mondo degli affari e nella vita domestica e della parallela introduzione di Internet, intranet, browser, motori di ricerca, router e altri sistemi e tecnologie per l'accesso e la distribuzione veloce di dati ed informazioni, che sono all'origine della "rete" globale e della conseguente rivoluzione nei campi dell'economia, delle comunicazioni e della vita sociale.

### LA POTENZA DELLA RETE

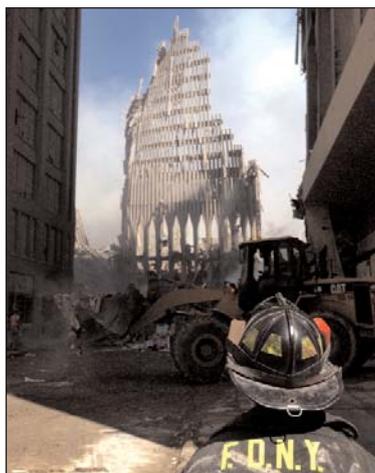
Secondo la legge di Metcalf, la potenza di una rete è maggiore della somma dei suoi componenti: essa è infatti proporzionale al quadrato del numero dei nodi (elementi) che ne fanno parte. Questo semplice assunto ha stimolato una trasformazione altrettanto radicale del mondo militare, anch'esso interessato a trarre vantaggio dalle capacità consentite dal "networking" in termini di

**Non potendo contare su grandi masse di manovra, dobbiamo puntare sulla qualità e sulla capacità di più limitati assetti in grado di operare con la massima sinergia, sincronizzazione ed efficacia.**

miglioramento e diffusione della conoscenza, compressione dei tempi di valutazione, di risposta e possibilità di coordinare e sincronizzare le azioni di forze anche fisicamente disperse in vista di un comune obiettivo. Internet è diventato un fenomeno "reale" quando il collegamento ha interessato una massa critica di utenti: una volta superata questa soglia, il valore dello strumento è aumentato esponenzialmente e, ad oggi, non ha ancora raggiunto il suo massimo sviluppo.

Lo stesso vale per l'NCW: una volta che una porzione critica di una forza è saldamente connessa in rete, i vantaggi crescono in maniera esponenziale e la spinta alla trasformazione diviene irreversibile. È un processo che occorre affrontare con attenzione e responsabilità, ma anche con una visione chiara del futuro: senza compromettere l'interoperabilità a medio e lungo termine per lasciare spazio a preoccupazioni di breve termine, e badando a sviluppare ed acquisire i nuovi sistemi (che si tratti di piattaforme, sensori o attuatori) in un'ottica "net-ready", "pronti per la rete".

Alla base del concetto di NCW sta lo sfruttamento della superiorità informativa (Information Superiority) che deriva dal collegamento in rete e dalla conseguente



### INFORMATION SUPERIORITY

*L'espressione indica una condizione di controllo (prevalenza, superiorità) nel campo dell'informazione tale da consentire la condotta delle operazioni senza che l'avversario sia in grado di esprimere un contrasto efficace. In altre parole, la superiorità informativa corrisponde a una situazione di squilibrio nel dominio dell'informazione a favore di una delle parti in causa. Chi (nazione, gruppo, forza militare) dispone della superiorità informativa è in grado di raccogliere, elaborare, disseminare e sfruttare un flusso ininterrotto e mirato di dati e informazioni, a fronte di un antagonista limitato o impedito nell'avvalersi della stessa possibilità.*



possibilità di accesso e condivisione delle informazioni, sino ad acquisire quella conoscenza condivisa della situazione (Shared Situational Awareness, SSA) che rappresenta ad un tempo un potente moltiplicatore di forza e un fattore chiave del successo, specie nell'ambito delle operazioni interforze e multinazionali (di Coalizione).

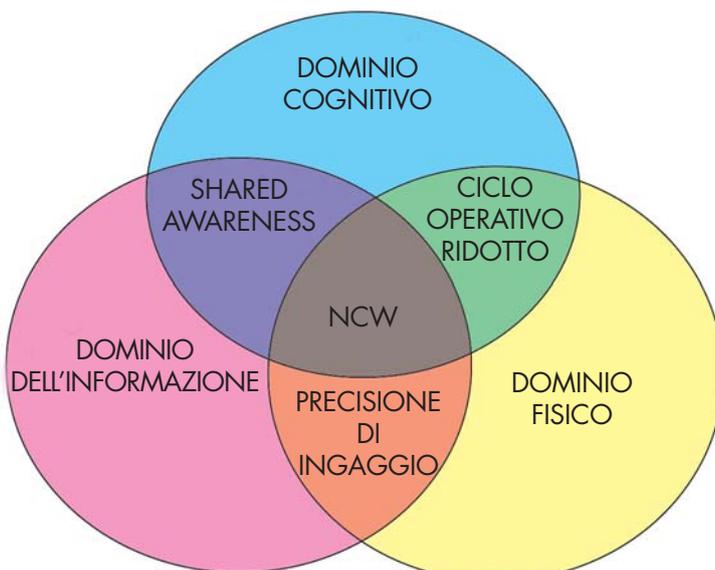
condivisa; e infine quello cognitivo, che coincide con la mente del singolo soldato e combattente, dove operano fattori quali leadership, morale, spirito di corpo, addestramento, esperienza e livello di conoscenza della situazione e dove risiedono dottrine, tattiche, procedure e l'obiettivo dell'azione di comando), una forza dotata di capacità NCW è in grado di agire con maggiore efficacia perché:

6

Con riferimento ai tre domini fondamentali in cui hanno luogo le operazioni militari (quello fisico, che coincide con lo spazio aereo, marittimo e terrestre in cui si sviluppa la manovra e risiedono le piattaforme, i sensori e i sistemi di comunicazione, comando e controllo; quello dell'informazione, dove l'informazione stessa viene generata, acquisita, elaborata, trasmessa, protetta e

- nel dominio fisico, tutti i suoi elementi (piattaforme, sensori, attuatori e decisor) sono collegati saldamente e senza discontinuità;
- nel dominio dell'informazione, l'intera forza ha la capacità di raccogliere, distribuire e condividere le informazioni, sino ad acquisire un decisivo vantaggio sull'avversario;

## LA GUERRA NELL'ERA DELL'INFORMAZIONE



## SHARED SITUATIONAL AWARENESS (SSA)

La situational awareness (conoscenza, consapevolezza della situazione) indica il grado di precisione con cui la percezione di una situazione da parte di un individuo corrisponde alla realtà effettiva. Quando la conoscenza della situazione è patrimonio comune di un insieme di attori (nel caso specifico, sensori, decisor) e attuatori), si parla di "conoscenza condivisa" (shared). I fattori che possono ridurre la consapevolezza della situazione sono fatica, stress, sovraccarico di lavoro, insufficienza della comunicazione, degrado dell'ambiente operativo; fra quelli che al contrario contribuiscono a migliorarla vi è in primo luogo un efficiente "networking" della forza, che abilita la distribuzione tempestiva e capillare di informazioni precise, aggiornate e affidabili.

- nel dominio cognitivo, tutti gli elementi della forza hanno la possibilità di sviluppare e condividere una migliore conoscenza della situazione, di essere informati sulle intenzioni del comandante e di sincronizzare le proprie azioni.

Grazie a questo insieme di fattori, una forza "networked" è in grado di operare in un'area geografica più ampia, con risorse quantitativamente inferiori e distribuite nello spazio, con maggiore precisione, portata e capacità di sopravvivenza, in modo sincronizzato e con un ciclo decisionale estremamente ridotto rispetto a una forza convenzionale, accrescendo proporzionalmente l'efficienza della propria azione e le probabilità di successo.

Nelle future operazioni – che avverranno in misura predominante, se non esclusiva, in contesti multinazionali – lo strumento militare dovrà essere in grado di conseguire l'obiettivo strategico assegnato avvalendosi delle dottrine, procedure e strumenti utili ad attuare il concetto delle Effects

**Capacità, metodi e strumenti d'intervento devono essere sviluppati in vista del raggiungimento di effetti coerenti con gli obiettivi da conseguire (EBO).**

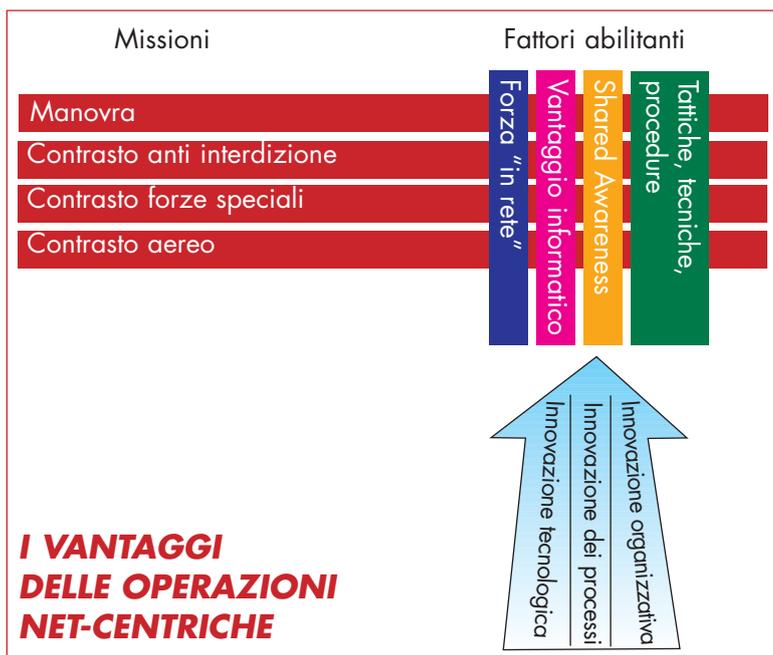
Based Operations (EBO), per la cui condotta le capacità NCW rappresentano un fattore abilitante. L'integrazione in rete di sensori, decisori e attuatori è infatti determinante per riuscire ad acquisire i risultati ("effetti") voluti grazie all'impiego parallelo, sinergico e sincronizzato degli assetti necessari. Senza la disponibilità di una robusta struttura connettiva e dei vantaggi che derivano dall'utilizzo delle capacità netcentriche sarà praticamente impossibile, all'interno di una Coalizione, l'esecuzione coordinata e simultanea di operazioni EBO da parte dei singoli partners.

A parità di altre condizioni, una forza dotata di capacità NCW è destinata a prevalere su una forza non netcentrica: lo provano i risultati delle operazioni su larga scala effettuate in Afghanistan e Iraq, nonché delle numerose esercitazioni e simulazioni condotte in diversi Paesi e in ambito multinazionale. Tali attività hanno consentito di mettere a fuoco i quattro principi fondamentali che stanno alla base del concetto NCW e della relativa dottrina:

- la connessione in rete aumenta la diffusione e la condivisione delle informazioni all'interno di una forza;
- la condivisione migliora la qualità dell'informazione disponibile e la conoscenza condivisa della situazione;
- la conoscenza condivisa della situazione facilita la collaborazione e la sincronizzazione, migliorando la sostenibilità dello sforzo e la velocità di comando;
- tutti questi fattori, a loro volta combinati ed interagenti, aumentano drasticamente l'efficacia dell'azione.

I principi che governano l'azione di una forza netcentrica non hanno soppiantato i criteri classici su cui si fonda la condotta delle operazioni militari (massa critica, obiettivi, manovra, unità di comando ecc.), ma forniscono quel "di più" necessario per un'efficace condotta delle operazioni nell'era dell'informazione, sia nel settore strettamente militare che in quelli strettamente collegati e interdipendenti della "homeland security", delle PSO, delle operazioni di stabilizzazione e di soccorso umanitario e dell'esercizio della deterrenza contro varie forme di minaccia.





**I VANTAGGI DELLE OPERAZIONI NET-CENTRICHE**

**INFORMATION SUPERIORITY**

In questo quadro, l'elemento determinante è la conquista della superiorità informativa, che da un lato richiede di realizzare una rete sicura in grado di assicurare a tutti gli elementi della forza amica l'accesso illimitato e tempestivo all'informazione e, dall'altro, di negare la stessa capacità all'avversario, accrescendo la sua dipendenza dalle informazioni e il suo grado di incertezza. Il frutto della superiorità informativa è una migliore conoscenza condivisa della situazione fra tutti i partecipanti a un'operazione, resa possibile dalla creazione di una "rete delle reti" alimentata da tutte le fonti collegate (ciascu-

**Per sostenersi e sostenere l'intero strumento militare, la trasformazione deve poggiare su un'architettura net-centrica, quale "sistema dei sistemi".**

**EFFECTS BASED OPERATIONS (EBO)**

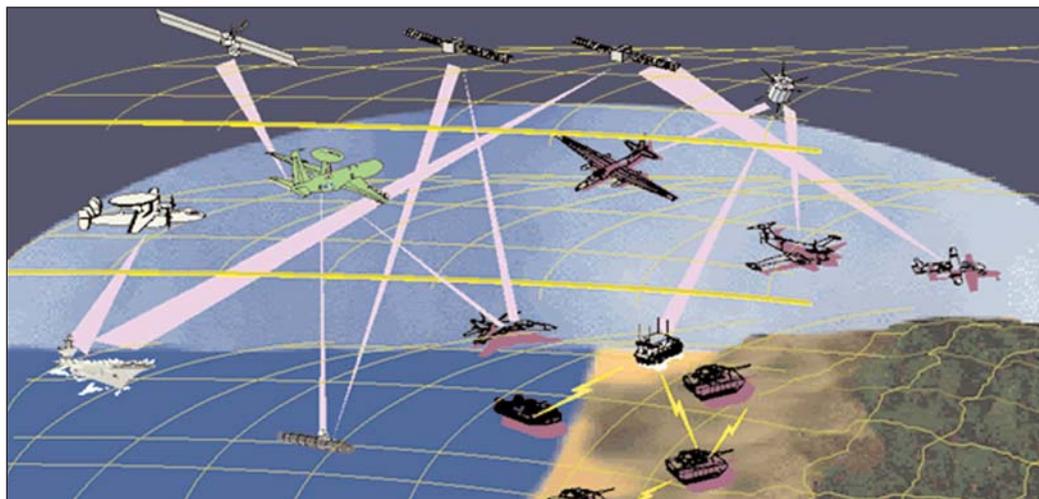
Per Effects Based Operations s'intende in generale un insieme di azioni dirette a influenzare il comportamento di soggetti amici, neutrali o avversari in situazioni di pace, crisi o conflitto. Con riferimento alla realtà militare, le EBO puntano ad ottenere l'effetto desiderato sull'avversario attraverso l'applicazione cumulativa, sinergica e coordinata di tutte le capacità disponibili (militari e non) a livello tattico, operativo e strategico. La capacità NCW rappresenta un fattore abilitante per la condotta delle EBO, in quanto rende disponibile la struttura informativa (rete) necessaria per pianificare ed eseguire le operazioni e valutarne i risultati.

na delle quali può operare, a seconda delle circostanze, come utilizzatore o come fornitore di informazioni) con dati (grezzi e/o elaborati) affidabili, disponibili in "real time" o "near real time", accessibili a tutti secondo necessità e indipendentemente dalla posizione geografica e protetti contro l'accesso o il disturbo da parte dell'avversario.

La superiorità informativa si trasforma in un vantaggio decisivo nel momento in cui consente di ridurre i tempi del processo decisionale, alterando le condizioni iniziali con una serie di cambiamenti tanto rapidi da impedire all'avversario di reagire in maniera tempestiva e coerente,

sino a paralizzare la sua capacità di rispondere all'evolvere della situazione in maniera efficace. La "shared awareness" permette di adattare dinamicamente e rapidamente

la forza ai cambiamenti che intervengono nello spazio della manovra, aumenta il grado di iniziativa dei subordinati migliorandone la reattività e la tempestività di risposta e facilita l'attuazione delle intenzioni del comandante, grazie al fatto che queste sono prontamente e chiaramente note a tutti gli elementi (nodi) di una forza professionale e bene addestrata.



## RICERCA TECNOLOGICA E PROCUREMENT



Il concetto di NCW/NEC abbraccia un insieme di dottrine, tattiche, tecniche e procedure emergenti e innovative che consentiranno a un complesso di forze pienamente integrato di creare a proprio vantaggio una situazione di superiorità decisiva sull'avversario. Una delle conseguenze del nuovo approccio sarà il superamento dell'attuale modo di condurre le operazioni, centrato sull'utilizzo delle piattaforme, grazie a una rete informatica in grado di acquisire e gestire in tempo quasi reale banche dati e informazioni provenienti da tutti i sensori disponibili, a vantaggio di decisori e attuatori fisicamente dispersi, ma fra loro connessi in un "continuum" rappresentato dalla cosiddetta "Global Information Grid". In altre parole, è necessario passare da un concetto d'impiego per piattaforme a uno per sistemi fortemente integrati in rete.

Per quanto riguarda le competenze del Segretario Generale della Difesa/Direzione Nazionale degli Armamenti, questo percorso di trasformazione investe due aree in particolare: la ricerca

tecnologica e il procurement. SGD/DNA ha avviato da tempo numerose attività di ricerca tecnologica finalizzate allo sviluppo di capacità di tipo NCW/NEC, ad esempio nei settori delle comunicazioni digitali, del trasferimento dati, del comando e controllo, dei radar multifunzione, della guerra elettronica e dei velivoli non pilotati (UAV). I risultati sin qui conseguiti sono incoraggianti e lasciano intravedere buone possibilità di ulteriore sviluppo, a condizione che la disponibilità di risorse adeguate consenta di definire e perseguire un programma pluriennale di investimenti per la ricerca coerente con gli obiettivi generali della Difesa.

SGD/DNA condivide pienamente l'importanza fondatrice dell'acquisizione di capacità NCW/NEC, come è confermato da un'analisi delle attività di procurement. Da tempo sono in atto, anche in questo settore, programmi di carattere abilitante e di assoluto rilievo tecnologico: è sufficiente ricordare il satellite per comunicazioni SICRAL, il sistema di osservazione spaziale Cosmo-Skymed, le reti di comunicazione in fibra ottica e HF della Difesa, i sistemi di comando e controllo di Vertice e per le singole Forze Armate e, ancora, i sistemi informatici di gestione che la Difesa sta acquisendo per far fronte alle esigenze in campo amministrativo, finanziario, logistico e sanitario.

Si tratta di programmi che richiedono un vasto impegno organizzativo anche in considerazione della loro natura "trasversale", che li porta spesso ad interessare non una, ma più Direzioni Generali, che di conseguenza sono a loro volta chiamate a "mettersi in rete" per condividere obiettivi, indirizzi e risorse.

Condizione determinante per far fronte agli impegni che ci attendono già nel breve e medio termine sono un rapporto di collaborazione Difesa-Industria sempre più intenso ed aperto e, soprattutto, un quadro di risorse coerente e affidabile, in assenza del quale qualsiasi disegno rischia inevitabilmente di rimanere incompiuto.

Generale C.A. Gianni Botondi  
Segretario Generale della Difesa/DNA



È importante sottolineare che i vantaggi derivanti dall'introduzione di capacità netcentriche non si applicano esclusivamente alla componente "combat" ma riguardano in misura altrettanto significativa la logistica (che viene messa in condizione di far fronte in maniera più efficace, tempestiva e mirata alle diverse richieste provenienti dal campo, gestendo sulla base di una conoscenza in "real time" aggiornata e globale della situazione il flusso

**Lo sviluppo e l'attuazione di concetti net-centrici non rappresenta un "nice to have", ma la condizione indispensabile per far sì che lo strumento militare sia in grado di rispondere alle esigenze di sicurezza.**

dei rifornimenti, delle parti di rispetto, delle riparazioni e delle sostituzioni), la gestione del personale, la componente amministrativa e quella di vertice, ciascuna delle quali è fortemente supportata e agevolata, nello svolgimento delle proprie funzioni, dall'uso combinato dell'Information Technology e delle comunicazioni.

L'altro aspetto che occorre avere ben chiaro è l'estensione della trasformazione associata all'implementazione della NCW: si tratta di un fenomeno di portata globale, al quale non sfuggono nessun Paese e nessuna Forza Armata. Tutte le maggiori nazioni, sulla scia degli Stati Uniti, stanno infatti costruendo la propria strategia di risposta alle sfide e alle opportunità offerte dall'era dell'informazione, sviluppando e adattando tecnologie, concetti operativi, procedure e dottrine utili ad accrescere le capacità NCW delle proprie forze. Alcuni di questi paesi, fra cui l'Italia, hanno già avuto modo di sperimentare le opportunità e i vantaggi offerti da un approccio netcentrico, sia pure parziale, nel corso delle operazioni in Afghanistan, Iraq,

nei Balcani, nel Mediterraneo e altrove, oltre che in esercitazioni condotte in ambito NATO (quali la "First Wave", che nel 2004 ha coinvolto le forze aeree di sette paesi collegate in rete mediante simulatori, e che si prevede di estendere in futuro a livello interforze) e multinazionale, dove l'Italia partecipa attivamente alle attività più significative (Coalition Warrior

Interoperability Demonstration e Combined Endeavours).

## CONDIZIONE ESSENZIALE

Guardando al futuro, il possesso di capacità NCW sarà essenziale per consentire la partecipazione efficace alle operazioni in ambito alleato e multinazionale: gli strumenti militari che non ne saranno dotati si troveranno progressivamente emarginati e, al limite, esclusi da ogni possibilità di coinvolgimento. Questa consapevolezza ha spinto anche la Difesa italiana ad occuparsi attivamente del problema, avviando studi e azioni in ambito nazionale e partecipando a diverse iniziative in ambito internazionale. Fra queste è il caso di ricordare l'iniziativa (che verrà esaminata in maggiore dettaglio nel capitolo successivo) assunta nel novembre del 2003 da nove Paesi NATO (Canada, Francia, Germania, Gran Bretagna, Italia, Norvegia, Olanda, Spagna e Stati Uniti, cui si sono aggiunti successivamente Belgio, Danimarca e Turchia) che, coerentemente con le decisioni assunte nel 2002 al Vertice di Praga, hanno deciso di cofinanziare lo studio di fattibilità di una NATO Network Enabled Capability (NNEC).

Lo studio, affidato alla NATO Consultation, Command and Control Agency (NC3A), è stato avviato nel gennaio del 2004 e si è concluso nel giugno del 2005 con l'individuazione di una roadmap per lo sviluppo e l'introduzione, in fasi successive e distribuite nel periodo 2006-2020, di capacità adeguate a consentire ai Paesi dell'Alleanza di partecipare insieme ad operazioni di tipo netcentrico. Sempre in ambito NATO, un importante contributo allo sviluppo delle capacità NCW viene dall'Allied Command Transformation (ACT) di Norfolk, nel cui ambito un Project Team integrato si occupa della NNEC e del contesto strategico in cui la stessa si verrà ad inserire.

I vantaggi della trasformazione sono chiari, la sua necessità è acquisita, e il percorso che renderà possibile l'introduzione delle capacità NCW è tracciato: occorre tuttavia essere coscienti che restano numerose difficoltà da superare, e che la Network Centric Warfare non rappresenta una "formula magica" in grado di sgomberare il teatro delle operazioni da tutti i possibili problemi. Il ricorso a NCW, EBO e alla superiorità informativa non è sufficiente a garantire il successo nelle operazioni che restano, al di là di ogni trasformazione dottrinarica e tecnologica, un fenomeno dinamico estremamente complesso, il cui esito non può essere determinato a priori ma solo governato ed indirizzato nella direzione voluta sfruttando i fattori favorevoli.

Gli stessi sforzi di adeguamento e trasformazione che vengono intrapresi dall'Italia e dai Paesi alleati sono d'altra parte all'attenzione anche degli antagonisti e dei potenziali avversari, inclusi quelli determinati a sfruttare il potenziale dei conflitti asimmetrici, del terrorismo e delle armi di distruzione di massa. In altre parole, se da un lato si cerca di utilizzare i vantaggi del concetto



NCW, dall'altro si lavora con altrettanto impegno per sfruttarne i punti deboli e le limitazioni. Non va infine dimenticato che, nel momento in cui tutti dovessero disporre di capacità NCW, si tenderà a ricreare una situazione di equilibrio, nella quale il vantaggio residuo sarà dato dalla capacità di adattare, assimilare e cambiare dottrine, organizzazioni e tecnologie ad un ritmo maggiore di quello dell'avversario.

### NCW E NEC

*Accanto al termine Network Centric Warfare (NCW) è frequente imbattersi nel "quasi equivalente" Network Enabled Capability (NEC). Il concetto di fondo cui fanno riferimento le due espressioni è lo stesso, dal momento che riguarda in entrambi i casi lo sfruttamento dell'IT per la creazione, secondo i criteri esposti in queste pagine, di una rete in grado di operare come moltiplicatore di forza per gli assetti coinvolti in un'operazione. Di fatto il concetto NCW, introdotto dagli Stati Uniti, corrisponde a un approccio più radicale, basato su un'acquisizione di capacità netcentriche rapida e diffusa, destinata a trasformare in tempi brevi l'intero strumento militare. Il concetto NEC, di origine britannica, punta all'acquisizione delle stesse capacità attraverso un'evoluzione graduale e sostenibile, adattando parte delle piattaforme e dei sistemi attuali all'uso in ambiente NCW in attesa del completo rinnovamento.*

# UNA RETE GLOBALE

DAGLI USA ALL'ALLEANZA ATLANTICA ALL'EUROPA: L'APPROCCIO AMERICANO, QUELLO BRITANNICO E LA "ROADMAP" DELLA NATO C3 AGENCY

Una panoramica sullo "stato dell'arte" e sulle iniziative in atto in diversi paesi occidentali per l'introduzione di capacità net-centriche non può che iniziare dagli Stati Uniti, dove il concetto NCW è nato e dove una combinazione unica di fattori favorevoli (il livello di ambizione nazionale, il grado di sviluppo tecnologico e, non ultima, la disponibilità di rilevanti risorse da impiegare nei settori della ricerca e del procurement) ne sostiene una crescita e un'implementazione estremamente dinamiche.

Questo vale non solo in campo militare (dove il Segretario alla Difesa Rumsfeld è stato ed è uno dei più ferventi sostenitori della "trasformazione", tanto da costituire all'interno del Department of Defense (DoD) un Office of Force Transformation

Le origini del processo che ha portato allo sviluppo e all'affermazione del concetto NCW possono essere fatte risalire alle lezioni tratte dal fallimento dell'operazione "Eagle Claw", che avrebbe dovuto portare nell'aprile 1980 alla liberazione degli ostaggi americani detenuti nell'ambasciata di Teheran. L'insuccesso mise in luce in particolare l'ancora limitata interoperabilità fra le singole forze armate, che portò negli anni successivi a dare forte impulso (anche attraverso la legge Goldwater-Nichols del 1986) alla creazione di una struttura rigorosamente "joint" avvalendosi delle possibilità offerte dal progresso tecnologico, dell'esperienza operativa (in particolare quella della guerra del Golfo del 1991) e di aggiornamenti organizzativi; fra questi ultimi va ricordata la decisione, presa nel 1992 dall'allora Presiden-

12



di cui è stato direttore sino alla sua scomparsa, avvenuta alla fine del 2005, il vice ammiraglio Arthur K. Cebrowski, uno dei "padri" della NCW), ma anche in quello governativo più in generale (dove lo sfruttamento delle sinergie consentite dall'Information Technology è un obiettivo ampiamente condiviso e perseguito) e in quello industriale.

te del Comitato dei Capi di Stato Maggiore generale Colin Powell, di attribuire all'US Atlantic Command la responsabilità dell'addestramento di reparti di tutte le forze armate alla condotta di operazioni interforze.

Nel gennaio del 1998 il vice ammiraglio Arthur K. Cebrowski e John J. Garstka pubblicarono

sulla rivista *US Naval Institute Proceedings* un articolo in cui si affermava che gli Stati Uniti erano al centro di una "rivoluzione degli affari militari" di portata ineguagliata dall'epoca napoleonica, ponendo il concetto di NCW al centro della trasformazione. I fatti dell'11 settembre 2001, mettendo tragicamente in luce la trasversalità e l'imprevedibilità della minaccia terroristica, hanno dato un'ulteriore spinta alla trasformazione come passaggio decisivo per sfruttare tutte le capacità disponibili, a partire da quelle offerte dall'NCW, per ridurre la vulnerabilità nei confronti delle minacce asimmetriche.

Nell'ottobre del 1999 l'US Atlantic Command ha mutato il nome in US Joint Forces Command al fine di sottolineare il suo ruolo guida nella trasformazione dello strumento militare americano, che lo ha visto affiancare alla responsabilità di comando "geografica" un preciso mandato funzionale, consistente nell'indirizzo del processo di passaggio delle forze armate americane verso il XXI secolo. Tale ruolo è stato confermato ed ampliato dal vertice NATO di Praga del novembre 2002, in seguito al quale anche il Comando Supremo dell'Atlantico (SACLANT) di Norfolk è



**Le attuali capacità sono destinate a degradare rapidamente, fino ad essere compromesse, se non saremo in grado trasformarci coerentemente con quanto stanno facendo gli alleati e le strutture di sicurezza di cui siamo parte.**

stato "convertito" in Comando Alleato per la Trasformazione (Allied Command Transformation, ACT). Risale infine al 26 novembre 2001 la decisione di costituire, nell'ambito del Pentagono, il già citato Office of Force Transformation.

Per quanto riguarda l'apporto dell'industria, va ancora ricordato che negli Stati Uniti hanno sede gruppi quali Boeing, Lockheed Martin e Northrop Grumman che – grazie alle loro dimensioni, al possesso di uno straordinario patrimonio di conoscenze e tecnologie e al fatto di operare nel primo e più ricco mercato mondiale – sono in grado di svolgere a livello globale un ruolo trainante nello sviluppo e nell'introduzione di nuovi concetti, tecnologie e sistemi. Non va infine sottovalutata l'esigenza, nell'attuale fase iniziale (rispetto all'obiettivo di una piena implementazione delle capacità NCW), di definire un'architettura e degli standard comuni per far sì che i diversi sistemi netcentrici in fase di sviluppo siano pienamente compatibili e interoperabili: un ruolo decisivo viene svolto in tal senso dal consorzio NCOIC (vedi riquadro), che raggruppa le maggiori aziende del mondo occidentale.

### NCOIC

Il Network Centric Operations Industry Consortium (NCOIC), costituito nell'agosto 2004, è un organismo internazionale che riunisce oltre 80 aziende di 16 Paesi (principalmente americane ed europee), accomunate dall'intento di migliorare l'interoperabilità interforze e multinazionale fra USA e paesi alleati e dalla "visione" di un rapporto collaborativo fra utenti e industria per lo sviluppo di un ambiente networkcentrico dove tutti i sistemi basati sull'IT possano interoperare grazie alla definizione e alla condivisione di standard comuni. Il Consorzio (fra i cui soci fondatori figurano aziende come Finmeccanica, Boeing, IBM, Microsoft e BAE Systems) affianca i membri e i clienti nell'analisi e nella valutazione di requisiti, architetture, modelli e standard idonei ad accelerare la fattibilità delle operazioni netcentriche (NCO).





### LA "VISIONE" AMERICANA

Per il Pentagono, l'introduzione delle capacità netcentriche e il parallelo spostamento da una "visione" centrata sulle piattaforme a una centrata sulla rete è un processo continuo, basato su un'evoluzione parallela in sette aree chiave (dottrina, organizzazione, addestramento, materiali, leadership, personale e infrastrutture) all'interno delle quali i cambiamenti sono collegati e si influenzano reciprocamente. Le iniziative rivolte alla netcentricizzazione interessano sia l'ambito interforze che le singole forze armate, e riguardano lo sviluppo e l'affinamento di nuovi concetti, nuovi assetti organizzativi e nuovi sistemi, alla luce dell'esperienza accumulata sia grazie a programmi-pilota, sia alle operazioni condotte nell'ambito della guerra globale al terrorismo.

È il caso del sistema Force XXI Battle Command Brigade and Below/Blue Force Tracking (FBCB2/BFT), le cui capacità netcentriche (basate sulla combinazione di piattaforme satellitari e trasmettitori GPS) sono state utilizzate nel corso dell'operazione "Iraqi Freedom" da unità dell'US Army, dei Marines, delle Forze Speciali e anche della 1ª Divisione Corazzata del British Army per monitorare con continuità la posizione di velivoli e mezzi terrestri, creando (in combinazione con l'uso di mappe digitali e di input dell'intelligence sullo schieramento avversario) un'immagine della situazione del campo di battaglia che veniva poi distribuita e "condivisa" grazie alla disponibilità di un potente assetto di comunicazioni satellitari.

Il programma "Horizontal Fusion" (dove il termine "orizzontale" si riferisce alla capacità di connettere e integrare le forze al di là dei limiti tipici delle tradizionali organizzazioni "stove-piped", ovvero verticali), avviato all'inizio del 2003 dal DoD col

concorso delle forze armate, del Dipartimento di Stato e di diverse Agenzie di intelligence, è destinato a concludersi nel 2008 e rappresenta il catalizzatore della trasformazione delle forze in senso netcentrico, attraverso lo sviluppo e l'introduzione di mezzi e strumenti che consentano, nell'ambito della "Global Information Grid" (GIG) prevista dal Pentagono sin dal 1999, capacità di accesso e scambio di informazioni tali da migliorare la conoscenza della situazione in tempo reale sull'intero spazio di manovra, consentire la disseminazione di intelligence di importanza critica e promuovere la collaborazione fra gli assetti accomunati da un preciso obiettivo operativo.

Ad "Horizontal Fusion" si affiancano, nello sforzo di trasformazione del DoD verso la capacità di condotta di operazioni netcentriche (Network Centric Operations, NCO), una serie di programmi diretti ad eliminare le attuali limitazioni legate all'ampiezza della banda utilizzabile per le trasmissioni e a rendere disponibili servizi affidabili nel settore dell'IT. Di tali programmi fanno parte:

- il Global Information Grid Bandwidth Expansion, (GIG-BE), rivolto alla creazione di una "rete globale" in fibra ottica a larga banda, elevato grado di copertura e assoluta affidabilità che, utilizzando protocolli tipo IP, consenta un massiccio scambio di informazioni;
- il Joint Tactical Radio System (JTRS), per le comunicazioni voce, video e dati a livello tattico;
- il TCA SATCOM, per integrare nella rete gli

### GIG

*La Global Information Grid è una singola infrastruttura integrata, concepita dal DoD nel 1999 e approvata da una direttiva del Segretario alla Difesa del settembre 2002, destinata a soddisfare tutte le esigenze di raccolta, elaborazione, immagazzinamento, distribuzione e gestione delle informazioni a supporto del DoD, delle forze armate e delle Agenzie di Sicurezza e di Intelligence degli Stati Uniti. La GIG deve assicurare la connessione di tutti i siti e le piattaforme di interesse operativo (basi, comandi, piattaforme mobili, sedi di rischieramento fuori area), oltre a prevedere opportune interfacce da/per utenti e sistemi appartenenti a Coalizioni, paesi alleati e Agenzie esterne alla Difesa. L'ambiente di elaborazione e trasporto delle informazioni è di tipo joint, dinamico, flessibile e dotato di capacità di autoriconfigurazione.*

utenti mobili a livello tattico e ad offrire opportunità di accesso globale ai dati di intelligence attraverso canali EHF e collegamenti IP;

- il Net-Centric Enterprise Services (NCES), per la fornitura di servizi di informazione e dati a tutti i nodi della GIG;
- l'Information Assurance (IA), per mettere a disposizione degli utenti della GIG sistemi di processazione dati, collegamenti e servizi affidabili.

Questi ed altri programmi, fra i quali si possono ancora citare quelli rivolti all'acquisizione di stazioni comuni per il segmento destinato alla gestione del flusso informativo di terra, di sistemi globali di comando e controllo e di dispositivi crittografici destinati a garantire l'inviolabilità e la protezione delle comunicazioni, sono destinati ad assorbire entro il 2009 investimenti per un totale di oltre 30 miliardi di dollari, una cifra sicuramente rapportabile alle capacità di spesa di una superpotenza quale gli Stati Uniti e che, al tempo stesso, serve a dare una misura dell'importanza prioritaria attribuita alla tempestiva introduzione di capacità NCW efficaci e diffuse.

Fra le iniziative avviate a livello "joint" dall'Office of Force Transformation figurano ancora:

- la Sense and Respond Logistic (SRL), volta a introdurre un nuovo concetto di logistica basato sulla conoscenza condivisa della situazione, la rapidità, il coordinamento e la sincronizzazione degli interventi, l'adattabilità e la flessibilità della risposta grazie allo sfruttamento delle capacità NCW e in grado di accrescere la disponibilità operativa delle piattaforme e dei reparti attraverso una gestione ottimale del supporto distributore-utilizzatore;



**Lo sviluppo di concetti e capacità net-centriche coerenti e integrabili a livello multinazionale diventa l'elemento abilitante per garantire l'operatività dello strumento militare.**



- su un piano più generale, un preciso sforzo diretto a rivedere la formazione del personale, con l'obiettivo di influenzarne percezioni e valori per stimolare un'attitudine "innovativa" ed infondere la consapevolezza dell'urgenza della trasformazione.

Al di là dei programmi a carattere interforze, anche le singole forze armate hanno tracciato delle roadmap che definiscono, in un'ottica rigorosamente interforze, il rispettivo

percorso di trasformazione verso l'obiettivo di una "full-spectrum dominance" basata su capacità NCW. Per quanto riguarda l'US Army, i due programmi chiave in corso sono il Future Combat System (FCS) e il Warfighter Information Network - Tactical (WIN-T). L'FCS è una

famiglia di sistemi destinati ad equipaggiare la nuova struttura operativa basata sui Brigade Combat Teams, composta da 18 diversi tipi di piattaforme con e senza equipaggio (robotizzate) e una rete integrata C4ISTAR che assicurerà ai soldati la capacità di "vedere per primi, capire per primi, agire per primi e condurre un'azione risolutiva".

Il WIN-T è un sistema di comunicazioni digitale tattico, mobile, sicuro, con elevate doti di sopravvivenza e in grado di supportare un sistema informativo multimediale, che si avvale anche di tecnologie commerciali per mettere a disposizione dei soldati un'elevata capacità di scambio di informazioni. Il WIN-T rappresenta l'evoluzione finale di una serie di sistemi, in parte già sperimentati sul campo da alcune Grandi Unità, che l'US Army intende acquisire attraverso un processo cosiddetto di "spiralizzazione", che consiste nel rendere progressivamente disponibili alla

componente operativa determinati “pacchetti” di capacità, man mano che le tecnologie sottese giungono a maturazione.

Per l’US Navy e l’US Marine Corps, uno dei quattro pilastri capacitivi su cui si basa l’attuazione del concetto operativo di Seabasing (che prevede di sfruttare l’incontrastato dominio del mare per realizzare la proiezione di potenza e l’immissione e il sostegno di assetti interforze in teatri terrestri) è rappresentato da FORCEnet, che costituisce



il quadro di riferimento per l’architettura destinata a realizzare una forza pienamente integrata e collegata a sua volta alla GIG. Va ricordato che già negli anni ‘90 l’US Navy aveva avviato l’introduzione di capacità netcentriche, prevalentemente finalizzate alla difesa antiaerea e antimissile in ambiente “littoral”, con lo sviluppo della Cooperative Engagement Capability (CEC). Il concetto, testato nel corso di diverse esercitazioni a partire dal 1995, è entrato nella fase di realizzazione nel 1998 ed entro il 2012 l’US Navy conta di acquisire oltre 200 sistemi CEC da integrare sulle maggiori piattaforme navali ed aeree.

L’US Air Force basa l’implementazione delle capacità NCW sull’iniziativa C2 Constellation, che prevede il passaggio dall’attuale sistema di raccolta e distribuzione delle informazioni basato su una varietà di assetti indipendenti (AWACS, JSTARS, Rivet Joint, satelliti per l’osservazione e le comunicazioni) a una nuova architettura in cui ciascuna piattaforma, indipendentemente dal tipo, potrà agire come sensore e/o attuatore nell’ambito di una rete pienamente integrata. Per provare la fattibilità di un sistema netcentrico in grado di integrare orizzontalmente assetti aerei, spaziali e di superficie ai fini della gestione delle operazioni è stata avviata col programma

***Se non riusciremo ad essere parte integrata della rete finiremo per restare esclusi dalla globalizzazione delle operazioni e, quindi, della sicurezza.***

Network Centric Collaborative Targeting (NCCT) la realizzazione di un dimostratore tecnologico avanzato di una rete C4ISTAR a larga banda.

Gli USA sono particolarmente attivi anche nello sviluppo di capacità di Combat Identification, considerate un aspetto chiave in un contesto NCW. L’identificazione tattica sul campo di battaglia consente infatti di discriminare le forze amiche da quelle nemiche o sconosciute, incrementa l’efficacia del combattimento, riduce il rischio di fuoco fratricida e concorre alla definizione della Situational Awareness. Gli Stati Uniti sono gli ispiratori e il motore trainante dei due programmi NATO/multinazionali nel settore dell’identificazione:

- il New Generation Identification Friend or Foe (NGIFF) per l’identificazione “air-to-air”;
- il Battlefield Target Identification Device (BTID) per l’identificazione “ground-to-ground”.

Tali attività (alle quali partecipa, tra gli altri paesi, anche l’Italia) s’inquadrano nel più ampio programma “joint” NATO CCID (Coalition Combat Identification), che punta al raggiungimento della piena interoperabilità dei sistemi di identificazio-

ne nei settori "air-to-air", "ground-to-ground", "air-to-ground" e "ground-to-air". Le tecnologie allo studio sono state di recente sperimentate con successo, in forma prototipale, nel corso dell'esercitazione "Urgent Quest" che si è svolta in Gran Bretagna nel 2005.

In conclusione, è il caso di sottolineare ancora una volta i principali fattori che qualificano lo sforzo in atto negli USA per la realizzazione del concetto NCW: la profonda convinzione della necessità della trasformazione come chiave per il mantenimento di un predominio assoluto ("full dominance") in campo militare; il ricorso – continuo, ampio e condiviso in ambito interforze – alla sperimentazione per la validazione dei nuovi concetti, procedure, sistemi e organizzazioni; l'apertura all'utilizzo delle tecnologie commerciali (COTS), hardware e software, per la realizzazione delle architetture e dei sistemi richiesti.

### NATO NEC: OBIETTIVI E SCADENZE

I Capi di Stato e di Governo della NATO, riuniti a Praga nel novembre 2002, hanno preso atto del radicale mutamento dello scenario geostrategico determinato dalla minaccia del terrorismo globale, includendola fra quelle da contrastare con le forze militari dell'Alleanza. Fra le più importanti iniziative varate nel corso del summit per incrementare le capacità di risposta della NATO figurano la creazione dell'Allied Command Trasformation (ACT), motore concettuale per lo studio e la definizione del percorso di trasformazione dell'Alleanza, e la creazione della NATO Response Force (NRF), una forza di reazione rapida joint, agile e flessibile, in grado di intervenire col minimo preavviso in ogni area del mondo dove si manifesti una minaccia alla sicurezza.

Al fine di facilitare lo sviluppo delle nuove capacità da acquisire in linea con gli impegni di Praga, i Comandi strategici della NATO hanno



individuato una serie di "traguardi della trasformazione" e di "aree obiettivo della trasformazione" fra le quali figura la superiorità informativa (Information Superiority), da conquistare attraverso lo sviluppo di una Network Enabled Capability. Per definire questo concetto, che corrisponde a quello americano di NCW e a quello britannico di NEC, è stato coniato il termine di NATO NEC (NNEC), che esprime la volontà di perseguire un analogo obiettivo, senza però adottare la "formula" precostituita di una singola nazione.

Le capacità richieste investono un'ampia gamma di elementi tecnologici, operativi ed organizzativi, con impatti diretti sulla gestione del flusso di informazioni (per assicurarne la fruibilità agli interessati prevenendo possibili sovraccarichi), sulla sicurezza della rete (per limitarne le inevitabili vulnerabilità) e sulle risorse, sicuramente significative, necessarie per avviare e completare la trasformazione. Al fine di affrontare il problema, riconosciuta l'improponibilità di ricorrere (soprattutto per ragioni di tempo) a una politica di finanziamento con fondi comuni dell'Alleanza, nove paesi (Canada, Francia, Germania, Gran Bretagna, Italia, Norvegia, Olanda, Spagna e Stati Uniti, cui si sono aggiunti successivamente Belgio, Danimarca e Turchia) hanno deciso di farsi carico direttamente di uno studio di fattibilità (NNEC Feasibility Study) della durata di 18 mesi, affidato alla NATO C3 Agency e avviato nel gennaio del 2004.

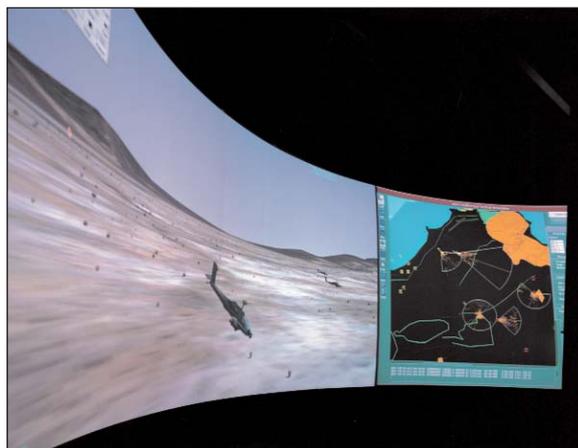
Lo studio, indirizzato a diversi destinatari (vertici decisionali politici e militari, responsabili della



programmazione finanziaria, program e project managers e staff tecnici), si è concluso il 27 ottobre 2005 indicando una serie di passi idonei a supportare lo sviluppo del concetto NNEC, delineando il quadro di riferimento generale ("Overarching NEC Architecture") su cui insistono le diverse applicazioni (ingaggio di precisione, superiorità informativa, capacità expeditionary ecc.) già individuate dai Comandi supremi della NATO e in cui va inquadrata l'evoluzione dei requisiti capacitivi, e tracciando una strategia e una roadmap per il loro sviluppo e attuazione.

Concordando con le indicazioni dell'ACT, lo studio di fattibilità individua nel processo volto a realizzare gli obiettivi della NNEC quattro fasi, definite rispettivamente di "deconfliction", "coordination", "collaboration" e "coherence". La prima, riferibile alla situazione attuale (prima dell'avvio della trasformazione), è caratterizzata dall'uso di applicazioni stand alone, data base separati e tipologie di reti di comunicazione diverse da forza armata a forza armata e da paese a paese, che determinano una condizione di ridotta possibilità di collaborazione dovuta alla sostanziale incompatibilità di applicazioni, reti e dati.

La seconda, che prende il via con l'inizio della trasformazione, vede la progressiva caduta delle barriere che si frappongono a un'effettiva integra-



zione delle forze grazie all'introduzione di nuove capacità di comunicazione e condivisione delle informazioni e alla realizzazione di una rete unica per il traffico di voce, dati e video, che consentirà un'accresciuta interoperabilità tra reti fisse, rischierabili e mobili e rafforzerà la possibilità di condivisione di una "Common Operational Picture". In questa fase continuerà ad essere utilizzabile la dottrina corrente, mentre occorrerà procedere ai primi aggiustamenti dell'assetto organizzativo.

La terza fase, di piena transizione, vedrà l'introduzione di capacità avanzate di collaborazione e pianificazione e un deciso miglioramento della shared situational awareness e dell'interoperabi-

## ACT

*Nel corso del vertice di Praga (novembre 2002) i leader dei paesi NATO decisero di adattare la struttura dell'Alleanza per meglio rispondere alle sfide emergenti. Sono nati così due nuovi comandi strategici: l'Allied Command Operations, responsabile della pianificazione e della condotta delle operazioni, e l'Allied Command Transformation (ACT), incaricato di sovrintendere alla trasformazione delle capacità militari, sia della NATO che dei singoli paesi membri. Istituito formalmente il 19 giugno 2003, l'ACT ha sede a Norfolk, Virginia, ha uno staff di circa 750 persone e controlla l'attività di altri 8 enti dipendenti, fra cui il Joint Warfare Centre di Stavanger, Norvegia, il Joint Analysis Lessons Learned Centre di Monsanto, Portogallo, e il NATO Undersea Research Centre di La Spezia. I due principali campi in cui opera l'ACT al fine di assolvere la sua missione sono quelli della ricerca tecnologica e dello sviluppo di nuovi concetti e dottrine.*

lità, accompagnati da cambiamenti più profondi all'assetto organizzativo, alle procedure e alla dottrina. La quarta fase sarà infine quella della piena maturazione della NNEC, che grazie alla massiccia integrazione in rete di tutti gli assetti consentirà alle forze di reagire con prontezza e flessibilità al rapido variare rapido delle circostanze, operando con nuove dottrine e nuovi modelli organizzativi in un ambiente totalmente netcentrico.

I risultati dello studio di fattibilità sono condensati in due serie di "raccomandazioni", una prima di carattere strategico e una seconda che riguarda gli obiettivi raggiungibili già nel breve-medio termine e a costi relativamente contenuti. Del primo gruppo fanno parte suggerimenti relativi ad esempio alla necessità di concordare i criteri per la realizzazione di una infrastruttura comune (Networking and Information Infrastructure, NII), definire una policy, anch'essa comune, per l'immagazzinamento e l'accesso alle informazioni, giungere a una standardizzazione dei sistemi radio sulla base della tecnologia Software Defined Radio (SDR) e definire un quadro di riferimento per la definizione dei criteri "net-ready" sulla base dei quali impostare la pianificazione dello sviluppo delle future capacità.

Un'altra importante "raccomandazione strategica" riguarda l'opportunità di avvalersi, nella fase di sviluppo, di infrastrutture di test, modellizzazione e simulazione dove Difesa e indu-

stria possano lavorare fianco a fianco per la verifica dei requisiti operativi e di sicurezza, la definizione dell'architettura di sistema, la sperimentazione e la validazione delle soluzioni proposte per realizzare la piena interoperabilità delle forze in un contesto NNEC e la formazione e l'addestramento del personale. La seconda serie di raccomandazioni, definite "quick wins", riguarda invece la possibilità di avvalersi di soluzioni e tecnologie già disponibili, anche in campo commerciale, per accelerare lo sviluppo e l'introduzione di capacità netcentriche.

***Occorre essere realisti e muoversi con grande pragmatismo; in primo luogo, partire dalla situazione attuale e dalle capacità disponibili, di fatto del tutto coerenti con quelle dei paesi alleati.***

In sintesi, lo studio raccomanda l'adozione dei concetti NCW/NEC sia alla NATO che ai singoli Paesi dell'Alleanza e delinea una roadmap per sviluppare e introdurre i relativi elementi tecnici e sistemistici, indicando un obiettivo di breve termine (introduzione di una capacità netcentrica "minima" nell'ambito della NRF a partire dal 2008), uno di medio (incremento delle capacità precedenti sino ad estenderla a livello Coalizione entro il 2012) e uno di più lungo termine (realizzazione di una piena capacità netcentrica sul piano dell'interoperabilità, dell'armonizzazione degli assetti e dell'architettura complessiva entro il 2020).

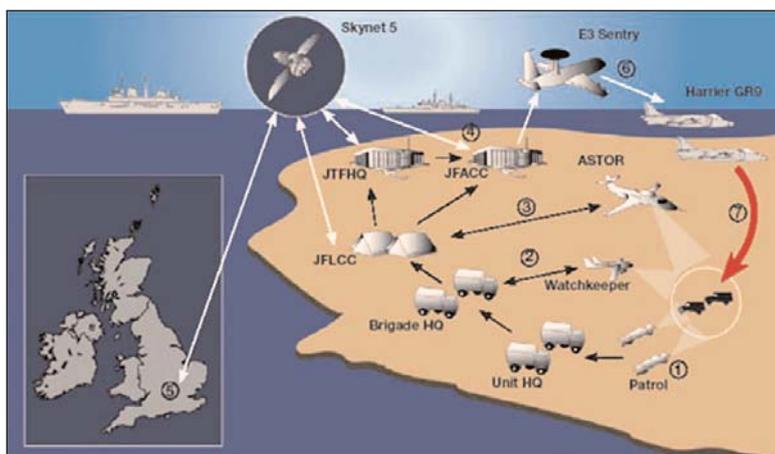
## **L'APPROCCIO BRITANNICO**

L'acquisizione di una Network Enabled Capability, secondo l'interpretazione data dalla Gran Bretagna al concetto NCW, è al centro dell'ultima edizione della Strategic Defense Review e del Joint High Level Operational Concept, che indica come si dovranno sviluppare le forze armate britanniche e i relativi criteri d'impiego. Attraverso la NEC il Ministry of Defence (MoD) punta ad acquisire, in tre fasi successive (Initial, Transitional e Mature NEC), la capacità di raccogliere informazioni, fonderle, analizzarle, condividerle con gli Alleati, distribuirle in tempo quasi reale ai decisori e agli operatori sul campo di battaglia.



L'MoD punta a realizzare il "valore aggiunto" della NEC attraverso lo sviluppo di un certo numero di funzioni, le più importanti delle quali prevedono di:

- abilitare gli utenti (nodi) alla ricerca, manipolazione e scambio di informazioni caratterizzate da vari livelli di classifica, da inserire o già residenti all'interno dello spazio di manovra;



- favorire la conoscenza condivisa della situazione e dell'evoluzione degli eventi nello spazio di manovra;
- consentire una rapida riconfigurazione e/o un'aggregazione delle forze in "mission groups", in vista di interventi sinergici fra elementi anche geograficamente non contigui;
- conseguire un effetto travolgente nelle operazioni attraverso una pianificazione dinamica e il coordinamento di tutti gli assetti disponibili.

Lo sviluppo, secondo criteri di costo-efficacia e minimo rischio, di una capacità complessa e articolata quale la NEC richiede il coordinamento degli sforzi della Difesa, dell'industria, dei centri di ricerca e di partner internazionali: un compito che l'MoD ha deciso di affidare al Directorate of Equipment Capability - Command, Control and Information Infrastructure (DEC - CCII) e a un apposito Integrated Project Team (IPT) che opera nell'ambito della Defence Procurement Agency (DPA). I due organismi hanno individuato in tre distinte fasi il percorso ottimale per conseguire l'obiettivo voluto, secondo un approccio incrementale che parte dalle piattaforme, dai sistemi e dalle capacità esistenti:

- la prima fase, denominata "Initial NEC", prevede di migliorare entro il 2007 le capacità di collegamento in rete fra le principali famiglie di

- sensori, i sistemi e i reparti in servizio;
- la seconda fase, denominata "Transitional NEC", si spinge fino al 2015 e prevede un forte potenziamento dell'integrazione fra i



- nuovi assetti che si renderanno man mano disponibili, e che dovranno essere sviluppati fin dall'inizio tenendo conto dei requisiti NEC;
- la terza fase, "Mature NEC", ha infine come obiettivo entro il 2030 una piena capacità di integrazione e sincronizzazione fra tutte le componenti che, a quella data, faranno parte dello strumento militare britannico.

L'impegno complessivo di spesa previsto è dell'ordine di alcune decine di miliardi di sterline, da recuperare in parte attraverso l'efficiamento delle forze consentito dalla progressiva introduzione di capacità NEC. Al fine di assicurare uno sviluppo coordinato, coerente e col minimo rischio, il Ministero della Difesa ha avviato nel 2003, con un investimento iniziale di 50 milioni di sterline e un'ampia partecipazione dell'industria, il programma NITeworks (Network Integration, Test & Experimentation), che prevede la creazione di un ambiente sperimentale in cui valutare i benefici del concetto NEC e le alternative per la sua efficace attuazione. Del NITeworks fa parte anche la Joint Multi National Interoperability Assurance Network (JMNIAN), che collega attraverso una WAN sicura e canali a larga banda tre centri di test e ricerca in Gran Bretagna (RAF Waddington per i sistemi aerei, un Land System Reference Centre, gestito da QinetiQ, per i sistemi terrestri e interforze e un Land Based test Site

per quelli navali) con analoghi centri statunitensi e NATO.

In quanto ai programmi già avviati, a livello tattico il più importante è il Bowman, che copre le bande di comunicazione VHF e HF e prevede l'acquisizione di oltre 46mila radio e 26mila computer da installare a bordo di 20mila veicoli da combattimento e trasporto terrestri, 150 unità navali e 275 velivoli, per un valore di 2,4 miliardi di sterline. Il sistema è già stato testato nel corso delle operazioni "Enduring Freedom" e "Iraqi Freedom", ed entro il 2008 ne è prevista l'estensione a cinque brigate del British Army e alla 3<sup>a</sup> Command Brigade dei Royal Marines.

L'architettura delle comunicazioni è completata dai segmenti Falcon (che prevede una rete di terminali mobili per collegamenti operativi sicuri), Cormorant (relativo al sistema di comando e controllo che interfaccia i comandi fissi di alto livello con quelli proiettabili) e Skynet 5 (un sistema satellitare per le comunicazioni strategiche nelle bande UHF e SHF, basato su due piattaforme di nuova generazione). Per il potenziamento della componente ISTAR sono stati invece avviati i programmi Watchkeeper, basato sull'omonimo UAV di origine israeliana equipaggiato con

sensori Thales, e ASTOR (Airborne Stand-Off Radar), che prevede l'installazione di un radar SAR sul velivolo Sentinel.

## ULTERIORI INIZIATIVE IN EUROPA E IN ALTRI PAESI

Oltre che a livello di singole Nazioni (molte delle quali, peraltro, parte della NATO e già coinvolte nel gruppo dei 12 che hanno finanziato il NATO NEC Feasibility Study), il concetto NCW/NEC è al centro dell'interesse anche delle organizzazioni che in Europa si occupano di Difesa. È il caso dell'EDA (European Defence Agency), dove nell'ambito del Direttorato per la Ricerca Tecnologica sono state individuate numerose aree di interesse correlate al tema, e della Lol (Letter of Intent, l'accordo quadro che lega i sei paesi europei – Belgio, Francia, Germania, Gran Bretagna, Italia, Spagna e Svezia – nei quali l'industria per la difesa è più sviluppata), dove già nel 2003 il

**La strada verso le capacità net-centriche può essere vista come un'evoluzione, ma costituisce in realtà una rivoluzione che deve partire già da ora per interessare tutti i settori provocando un cambio radicale di mentalità.**

Gruppo dei Direttori della Ricerca (GRD) ha approvato un programma di studio congiunto relativo alla NEC.

All'iniziativa hanno aderito tutti i paesi membri, assegnando la leadership dell'attività alla Svezia, mentre in parallelo le organizzazioni industriali organizzavano un gruppo di supporto (guidato da Saab e comprendente tutte le maggiori industrie del settore dei paesi partecipanti, inclusa SELEX Sistemi Integrati per l'Italia). Lo scopo del programma, inizialmente finalizzato alla realizzazione di un dimostratore entro un termine di



### NATO C3 Agency

La NATO Consultation, Command and Control Agency (NC3A) è stata creata nel 1996 con l'obiettivo di ristrutturare le attività C3 nell'ambito dell'Alleanza, riunendo sotto un'unica responsabilità le funzioni di pianificazione, ricerca scientifica, sviluppo e acquisizione nei settori dei sistemi di comando, controllo, comunicazione e informatici. L'Agenzia opera con un totale di circa 450 addetti, fra civili e militari, suddivisi fra la sede centrale di Bruxelles (Belgio), dove vengono svolte le funzioni di pianificazione e procurement, e quella distaccata dell'Aia (Olanda), dove invece sono concentrate le attività di ricerca e supporto in campo scientifico.



tre anni, è stato successivamente modificato in un pre-studio di fattibilità, cui farà eventualmente seguito la realizzazione del dimostratore. Nel giugno 2005 è stato assegnato a un gruppo di industrie delle sei Nazioni un primo contratto, del valore di 1,2 milioni di euro, finanziato in parti uguali da ciascuno dei Paesi membri.

Gli obiettivi dello studio riguardano sul piano generale l'acquisizione di know-how per l'introduzione di capacità NCW nelle forze armate, l'integrazione dei programmi nazionali e il miglioramento della cooperazione fra le industrie del settore. Sul piano tecnico il programma prevede invece la definizione dei requisiti per un dimostratore tecnologico, quella degli scenari per una dimostrazione di "Shared Situation Awareness" in un ambiente di peace keeping/peace enforcing (in accordo con le missioni che potranno essere assegnate ai Battlegroups europei sulla base della dichiarazione di Petersberg) e infine la dimostrazione dei benefici derivanti dall'introduzione di una capacità NCW

iniziale. La conclusione del pre-studio è prevista nel luglio 2006 e, dopo la valutazione dei risultati, le Nazioni della Lol decideranno l'eventuale realizzazione del dimostratore.

Fra i paesi europei, a parte la Gran Bretagna (il cui contributo è già stato esaminato) e l'Italia (oggetto del successivo capitolo), un cenno particolare merita, anche in relazione alle dimensioni del Paese, l'iniziativa della Svezia, che in materia di NCW è impegnata col programma Ledssystem in un radicale sforzo di innovazione e trasformazione delle procedure, delle dottrine, dei sistemi C2 e della struttura organizzativa della Difesa. Il programma di trasformazione, avviato nel 2001, prevede un investimento complessivo di oltre 100 milioni di euro e si articola in tre fasi. La prima, relativa all'analisi dei sistemi e della struttura esistente, alla valutazione della loro adattabilità al contesto NCW e/o dell'opportunità di dismetterli (operazione "Leave behind") e alle decisioni circa nuove iniziative di sviluppo, si è conclusa



nel 2004; la seconda, centrata sulla sperimentazione degli assetti attuali "adattati" e di quelli di cui è previsto lo sviluppo in uno scenario d'impiego riferito a un Battlegroup europeo, si concluderà nel 2006 e sarà seguita dalla terza, che fissa al 2010 la scadenza per l'introduzione di capacità NCW per un Battlegroup UE impiegabile in operazioni multinazionali.

Il progetto della Svezia – che non nasconde l'ambizione di rendersi protagonista delle future operazioni di PSO in ambito Unione Europea – è sostenuto da una vigorosa collaborazione fra forze armate, organizzazione del procurement e industria ed è stato accompagnato dalla creazione a Enköping di un avanzato centro di sviluppo e test delle soluzioni NCW relative a reparti, piattaforme, sensori, sistemi di comunicazione e C3I, dove è possibile verificare con tecniche di modelling e simulazione e con esercitazioni reali la validità delle scelte operate prima di passare alla fase di procurement.

Un breve cenno, per concludere la panoramica europea, alle attività della Francia, dove la presenza di una forte industria della difesa e la notevole disponibilità di risorse hanno favorito l'avvio di iniziative per lo sviluppo e l'acquisizione di capacità NCW (acronimo che diviene, in francese, ORC, per "Opérations Réseaux-Centrées") anche con l'obiettivo di creare una solida base per l'esportazione. I principali programmi rivolti alla digitalizzazione delle forze sono il RIFAN in

campo navale, lo STRIDA in quello aereo, l'OE SIC Terre (che riguarda l'interoperabilità dei sistemi di comunicazione e informazioni operative al fine di creare la cosiddetta BOA, "Bulle Operative Aéroterrestre) per l'esercito e lo Spatio Nav per la sorveglianza costiera.

In campo spaziale il rafforzamento delle capacità di sorveglianza e comunicazione è affidato ai programmi Helios 2, SAR Lupe, Pleiades, Cosmo SkyMed (alcuni condotti in un quadro di collaborazione internazionale con diversi paesi europei, fra cui l'Italia) e Syracuse, mentre nel settore delle infrastrutture sono previsti nel 2006 il completamento della rete INTRACED per la distribuzione di informazioni classificate ad alta velocità e nel 2008 quello della rete SOCRATE NG per le comunicazioni end-to-end user. Anche in Francia le atti-

vità di sviluppo, sperimentazione e validazione dei sistemi sono sostenute da diversi centri di ricerca e sperimentazione gestiti da Difesa e DGA col concorso dell'industria.

L'impatto innovativo del concetto NCW e, al tempo stesso, la necessità di non rimanere ai margini del processo di trasformazione, nella consapevolezza che una scelta di questo tipo finirebbe inevitabilmente col pregiudicare ogni effettiva ed efficace partecipazione alle future operazioni multinazionali (a framework USA, NATO e/o UE), sono all'origine di studi e programmi in

**Un sistema o sarà integrato nella rete o non sarà operativo, e quindi sarà un "non-sistema".**

## **NRF**

La NATO Response Force (NRF) è una forza di elevata prontezza operativa, composta da assetti navali, aerei e terrestri, interoperabile, flessibile e facilmente rischierabile e supportabile in teatro, destinata ad intervenire sia per la difesa collettiva dell'Alleanza (ex Art. 5) che per operazioni di gestione delle crisi e stabilizzazione (non Art. 5). L'NRF ha conseguito la capacità operativa iniziale a fine 2003, mentre la piena capacità operativa dell'intera forza (composta da circa 20mila uomini suddivisi in una componente navale, una terrestre basata su un Brigade Combat Team e una aerea in grado di generare sino a 200 sortite al giorno) è prevista dopo la verifica da attuare nel giugno 2006 con l'esercitazione "Steadfast Jaguar".



ambito netcentrico che interessano, oltre a quelli già citati (e all'Italia, cui è riservato il prossimo capitolo), numerosi altri paesi occidentali.

Una panoramica di tutte le attività in corso rischia sempre di essere incompleta e, in qualche caso, ripetitiva; è comunque opportuno ricordare, anche per sottolineare la diffusione e l'ampiezza del fenomeno innescato dalla NCW e l'attenzione che il concetto ha destato su scala mondiale, le iniziative avviate da alcuni Paesi particolarmente significativi in relazione alle dimensioni del loro strumento militare, al grado di sviluppo dell'industria della difesa o al coinvolgimento nella politica di sicurezza globale, quali Australia, Canada, Germania e Singapore.

L'Australia, parte attiva della politica di sicurezza soprattutto nella regione Asia-Pacifico e presente con proprie forze nelle operazioni "Enduring Freedom" e "Iraqi Freedom", assegna alle capacità NCW un ruolo importante nell'implementazione del disegno strategico tracciato dal documento "Force 2020", che prevede una trasformazione delle forze armate in senso decisamente



netcentrico attraverso un percorso in tre tappe. Partendo dalla situazione attuale di una "Network Aware Force", cioè di uno strumento militare consapevole dell'importanza dell'NCW, l'Australia prevede di creare nel prossimo quinquennio le basi della trasformazione, operando in particolare sul piano della formazione del personale e della progressiva integrazione di sistemi C2, sensori e piattaforme.

Questa prima fase dovrà consentire di raggiungere, poco oltre il 2010, una "massa critica" in ter-

**Occorre essere concreti:  
nel breve-medio termine  
è prioritario perseguire  
obiettivi di elevata  
interoperabilità, piuttosto  
che inseguire lo  
sviluppo di sistemi  
futuribili.**

mini di capacità NCW che, insieme all'esperienza nel frattempo maturata con la sperimentazione e l'impiego dei nuovi sistemi e di una nuova dottrina, permetterà di presentarsi alla soglia del 2015 con una forza militare sostanzialmente integrata e supportata da un'adeguata infrastruttura IT, in grado di condurre operazioni di tipo NCO su una base di piena interoperabilità con i principali alleati e partner di colazione. Per il 2020 l'obiettivo è di estendere queste capacità all'intero strumento militare, senza soluzioni di continuità. Accanto agli assetti "tradizionali" (quali UAV, sistemi di comunicazione satellitare, sistemi C2/C4I ecc.) previsti a questo scopo, l'Australia dispone di un assetto originale nei sistemi radar HF "oltre l'orizzonte", di cui ha avviato da tempo la realizzazione per la sorveglianza degli adiacenti spazi oceanici (programma "Jindalee").

Un approccio più vicino a quello britannico, quindi di tipo NEC, è stato scelto dal Canada, dove la Difesa ha avviato un processo di adattamento evolutivo, basato su un adattamento pragmatico dei sistemi esistenti e sulla parallela maturazione di



nuove esperienze, organizzazioni, dottrine, cultura e mentalità. Oltre ad investire le tre forze armate, il processo punta a uno stretto coordinamento interministeriale sulle tematiche generali della sicurezza e prevede tre successive fasi di attuazione: "Horizon 1" (entro il 2008) per l'implementazione di un sistema di comando e controllo interforze, interoperabile e interconnesso, in grado di chiudere il "capability gap" nei confronti degli alleati; "Horizon 2" (entro il 2013) per l'implementazione degli aspetti netcentrici del sistema C2 e l'avvio di programmi di investimento lo sviluppo tecnologi-

co, l'adeguamento delle risorse umane e il rinnovo dei materiali; e infine "Horizon 3" (fissato al 2018) per il conseguimento di una piena Situational Awareness a tutti i livelli di comando e controllo e una conseguente flessibilità e agilità delle forze consentita dalla netcentricizzazione, dall'integrazione dei sensori, dalla conoscenza e dalla consapevolezza della situazione.

In Germania l'enfasi è per il momento diretta alla maturazione di una nuova mentalità e all'adeguamento delle strutture organizzative, più che all'avvio di specifici programmi di procurement. Il Paese è presente in alcuni dei fori multinazionali che trattano la materia, a partire dalla NATO NEC e dalla Concept Development and Experimentation (CD&E) condotta dall'US Joint Forces Command, ed è consapevole delle esigenze collegate alla partecipazione ad operazioni multinazionali. In questo contesto, il processo di trasformazione della Bundeswehr tracciato dal Ministro della Difesa Peter Struck nell'agosto del 2004 indica chiaramente il dominio della "dimensione informativa", l'acquisizione di adeguate capacità di comando, controllo, intelligence, ricognizione e ingaggio efficace, la totale "jointness" di pensiero e di azione e la massima interoperabilità con le forze alleate fra gli obiettivi chiave da conseguire.

Le azioni in corso in vista di questo traguardo sono molteplici e, in relazione agli specifici settori di eccellenza dell'industria nazionale, riguardano in particolare il campo delle reti per comunica-



zioni sicure, degli UAV e dei sensori aeroportati; è inoltre in fase di sperimentazione il sistema "Infanterist der Zukunft" (soldato futuro) per la digitalizzazione sino al minimo livello del campo di battaglia, sistema di cui è prevista l'acquisizione entro il 2007 di un primo lotto di 1.600 esemplari nella versione V1.

Per quanto riguarda infine Singapore, lo sviluppo di quello che viene localmente definito il "sistema IKC2" (Integrated Knowledge-based Command and Control) è affidato a un approccio collaborativo (in particolare con gli USA e l'Australia) e di verifica sperimentale, sia attraverso un centro di simulazione interforze (aperto anche ai paesi alleati) di cui è prevista l'apertura presso la base navale di Changi che di esercitazioni multinazionali. Per ridurre il gap di interoperabilità tutt'ora esistente fra le forze aeree, navali e terrestri è stata da poco completata l'introduzione di regole operative comuni, mentre l'ambiente operativo netcentrico è stato analizzato da uno studio denominato DIANE (Digital ANalysis Environment).

In vista dell'introduzione di capacità NCW, Singapore punta in particolare sullo sfruttamento della tecnologia commerciale (soprattutto nel campo dei sistemi di rappresentazione e di comunicazione mobile), sull'adeguamento della dottrina (che in un ambiente netcentrico deve prevedere ove necessario la possibilità di delegare/decentrare rapidamente il potere decisionale), sul superamento delle barriere che tuttora si frappongono all'utilizzo operativo dei dati di intelligence e sul pieno dominio della dimensione informativa.

#### **C4ISTAR**

*È l'acronimo risultante dalle iniziali di Comando, Controllo, Comunicazione, Computer (termine che in una più recente interpretazione, fatta propria anche dalla Difesa italiana, è stato sostituito da Consultazione, a sottolineare l'importanza di poter consultare tempestivamente l'autorità politica nel corso della condotta delle operazioni), Intelligence, Sorveglianza, Acquisizione obiettivi (in inglese, Target Acquisition) e Ricognizione. Con questa sigla si identificano le capacità essenziali di cui un comando di alto livello deve disporre per poter esercitare in maniera efficace e tempestiva la direzione di un'operazione militare, sfruttando la migliore conoscenza del proprio schieramento e di quello avversario e la possibilità di comunicare in maniera rapida, sicura e capillare con le proprie forze.*

# ITALIA: SITUAZIONE E OBIETTIVI

IL PUNTO SULLA SITUAZIONE E SUI PROGRAMMI AVVIATI E ALLO STUDIO PER CONSOLIDARE ED ESTENDERE LE CAPACITÀ NCW, IN SINTONIA CON GLI OBIETTIVI E LA ROADMAP DELLA NATO. LA COOPERAZIONE FRA DIFESA E INDUSTRIA

// I nuovi concetti d'impiego e le nuove dottrine operative dovranno essere focalizzate sull'utilizzo integrato di tutte le capacità e di tutti i mezzi disponibili nel corso di tutte le fasi di un'operazione (pre-crisi, "combat", post-conflittuale) per il conseguimento di effetti EBO (Effects Based Operations) coerenti con l'obiettivo da perseguire. Le operazioni future saranno focalizzate più sui risultati da conseguire che sui sistemi e i mezzi disponibili per conseguirli, e la dottrina netcentrica costituirà la struttura portante di questa nuova impostazione concettuale".

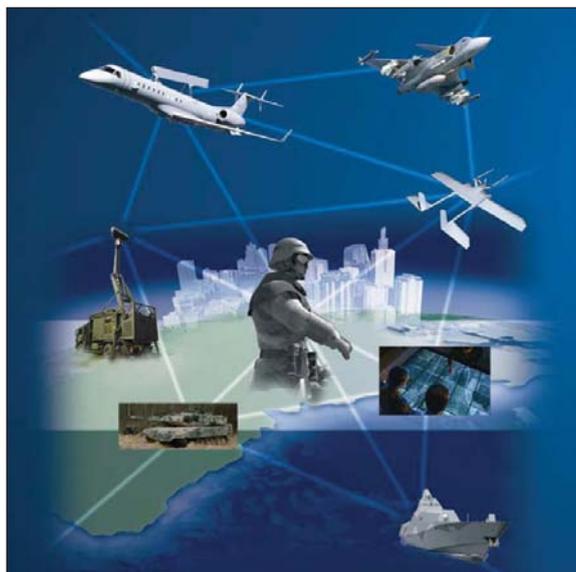
"Non possiamo permetterci di non trasformare le nostre Forze Armate in accordo con quanto sta avvenendo negli altri Paesi coi quali ci troviamo ad operare in ambito multinazionale. La questione non è "se", ma "quando" riusciremo ad acquisire le capacità necessarie ad operare in un ambiente netcentrico. [...]. Uno strumento militare italiano "scollato", non interoperabile con quelli dei nostri alleati, non ha senso, e l'approccio netcentrico è l'asse portante della struttura che dobbiamo costruire".

Queste due citazioni, tratte rispettivamente dal "Nuovo Concetto Strategico" approvato all'inizio del 2005 dal Capo di Stato Maggiore della Difesa e dall'intervento effettuato dallo stesso Capo di SMD al Seminario sulla Network Centric Warfare/Network Enabled Capability organizzato a Roma il 13 e 14 dicembre 2005 dal Reparto Telecomunicazioni, Elettronica ed Informatica (TEI) di SMD, ben sintetizzano le ragioni e l'obiettivo della trasformazione di cui anche la Difesa e le Forze Armate italiane sono protagoniste.

## SISTEMA DI COMANDO E CONTROLLO DELLA DIFESA (C4I DIFESA)

Con la riforma dei Vertici della Difesa e la costituzione del Comando Operativo di vertice Interforze (COI) è stato avviato un progetto per la realizzazione di un sistema di comando e controllo apicale, con l'obiettivo di rendere interoperabili i sistemi C2 di Esercito (SIACCON), Marina (MCCIS) e Aeronautica (SICCAM), rendere disponibilità di comando e controllo per il COI e assicurare l'interfacciamento verso analoghi sistemi NATO. La realizzazione del sistema, avviata nel 2000, è stata affidata all'Industria nazionale con un contratto unico, suddiviso per fasi, e ad oggi ha già assicurato al COI la possibilità di comunicare in sicurezza coi Comandi Operativi di Forza Armata e coi Comandi in zona di operazione attraverso lo scambio di posta elettronica, nonché di rappresentare graficamente la situazione terrestre, navale ed aerea ricavata dalle differenti "pictures" di Forza Armata. Il completamento del programma, previsto per il 2007, renderà disponibili funzioni operative per la pianificazione, la gestione delle operazioni, il supporto alle decisioni, la presentazione e valutazione di situazioni e funzioni di simulazione operativa.





Tutti i principali paesi del mondo si stanno muovendo verso una dottrina e un modo di operare netcentrico, con iniziative che abbracciano (e spesso travalicano, considerata la natura multidimensionale della netcentricità) l'ambito militare: se anche l'Italia non sarà in condizione di operare secondo questi concetti, si troverà emarginata. Non c'è – già oggi, ma sempre di più in futuro – operazione militare che possa prescindere da una piena capacità di integrazione in un contesto netcentrico: è un'affermazione che si applica tanto alle

***Il concetto net-centrico, al momento assorbito soprattutto dalla componente militare, dovrà essere esteso quanto prima anche a quanti sono chiamati ad interagire con la componente militare.***

operazioni ad alta intensità, di tipo combat, che a quelle di PSO e di assistenza umanitaria, per le quali la possibilità di gestione netcentrica rappresenta ugualmente un fattore in grado di incrementare la tempestività, la precisione, la sicurezza e l'efficacia.

La Difesa italiana è pienamente convinta della necessità di questa scelta e, al tempo stesso, consapevole di svolgere un

ruolo di "front runner" nello sviluppo e nell'approfondimento dei concetti e delle strutture necessarie ad attuare la trasformazione: è un ruolo che i militari sono particolarmente preparati e portati a svolgere – vuoi per la natura stessa della loro professione (che li porta ad analizzare e definire aspetti dottrinari e concettuali), vuoi per le operazioni in cui si trovano correntemente impegnati (che li mettono a continuo e diretto contatto con le realtà di altri paesi), vuoi infine perché rappresentano la struttura e il "collante" degli interventi nazionali fuori area (anche quando questi coinvolgono altri Enti e Organizzazioni) – e proprio per questo sono i più sensibili e ricettivi nei confronti delle nuove idee ed esigenze.

## PROGRAMMA SICRAL

*Il satellite per comunicazioni SICRAL 1, lanciato nel febbraio del 2001, è frutto di un progetto avviato nel 1995. Le sue capacità si sono già rivelate determinanti ai fini della condotta delle missioni nazionali fuori area, e costituiscono una preziosa risorsa per la Protezione Civile in caso di emergenza. Dopo la vittoria di Italia, Francia e Gran Bretagna nella gara per la realizzazione del sistema di comunicazioni NATO Satcom post 2000, l'esigenza di disporre di ulteriori canali di comunicazione ha portato alla decisione di utilizzare la piattaforma di riserva SICRAL 1B, il cui lancio è previsto nel 2007; una parte dei canali in banda EHF di questo satellite verrà usata anche dall'Arma dei Carabinieri. Nel 2010 è previsto il lancio di SICRAL 2, destinato a rimpiazzare il SICRAL 1 al termine della sua vita utile.*

## LA PROVA DELL'ESPERIENZA

Il percorso di trasformazione che la Difesa e le Forze Armate italiane sono impegnate a percorrere sono del tutto coerenti con le esperienze maturate in ambito nazionale e internazionale, col livello di ambizione del Paese (e la conse-



guente necessità di contribuire in maniera attiva e responsabile al sistema di sicurezza globale), col livello tecnologico e con le capacità dell'industria.

Le pietre miliari di tale processo (i cui contenuti e obiettivi generali, in termini di capacità, sono gli stessi già illustrati nel primo capitolo) sono rappresentate da:

- l'acquisizione e la maturazione, da parte del personale, di una nuova mentalità e di una visione concettuale ormai ben definita: ognuno deve essere consapevole che, in un ambiente netcentrico, è collegato e interagisce con altri attuatori e decisori, quale parte di una rete in cui ciascun elemento influenza ed è al tempo stesso influenzato dagli altri, per effetto di una condivisione sempre più spinta delle informazioni, della consapevolezza e della responsabilità;
- uno spostamento dell'enfasi dalle piattaforme alla rete, vale a dire alla struttura che le interconnette. Le piattaforme esistenti, se prive della capacità di operare in rete, sono e saranno



sempre meno utili e necessarie: potranno avere ancora (specie se adeguabili ad operare in un contesto NCW) un'utilità transitoria in determinate attività, ma per i futuri sistemi oggi in fase di sviluppo il requisito di una piena compatibilità netcentrica è determinante e irrinunciabile;

- la conseguente necessità di indirizzare in via prioritaria le risorse verso sistemi e piattaforme "network enabled", privilegiando le capacità rispetto alla quantità. Ogni assetto che le Forze Armate italiane porteranno ad operare in teatro dovrà essere pienamente integrabile in un contesto NEC, sia a livello interforze che nei confronti degli assetti delle alleanze e delle possibili coalizioni.

Si tratta di una scelta che non solo risulta indispensabile per consentire allo strumento militare italiano di continuare ad essere componente efficace ed utilizzabile di ogni più ampio dispositivo alleato e multinazionale, ma che presenta anche significativi vantaggi sul piano dell'economia delle forze e delle risorse, come prova l'esperienza sin qui maturata nelle operazioni reali.

Due esempi possono essere utili per provare quest'ultima affermazione. Il primo viene dall'impiego degli UAV nel corso dell'operazione "Antica Babilonia", dove la disponibilità del Predator ha dato un impulso decisivo alle capacità ISTAR del contingente nazionale, consentendo di controllare in maniera continuativa ed efficace l'area di responsabilità (provincia del Dhi Qar) con un dispendio limitato di risorse laddove in passato,

## UAV PREDATOR

L'UAV (Unmanned Aerial Vehicle) si è dimostrato uno strumento estremamente efficace per lo sviluppo delle capacità ISTAR, specialmente in un ambiente NCW. Nel 2002 l'Italia ha avviato un programma interforze per l'acquisizione di cinque UAV Predator, tre dei quali equipaggiati con sensori EO/IR, una stazione di guida e controllo, una console di pianificazione della missione, un simulatore di volo e il necessario supporto logistico. Le consegne dei materiali e l'addestramento del personale sono stati completati nel 2004, e dalla fine dello stesso anno il Predator è impiegato con ottimi riscontri operativi nel teatro iracheno, tanto che nel 2005 è stata decisa l'acquisizione di altri due UAV e una stazione di controllo a terra.

## MODELLI E ARCHITETTURE



“La prima dote di un comandante in capo è avere una mente fredda, nella quale le informazioni che si succedono simultaneamente e che riceve nel corso d'una giornata siano ordinate ed occupino esattamente il posto che meritano”.

Questo era il modo con cui Napoleone conduceva le operazioni. L'approccio Network Centric Warfare, invece, è diametralmente opposto: pone al centro di tutto la diffusione delle informazioni. Le piattaforme, i sistemi e perfino i concetti operativi devono essere pensati e realizzati in funzione di una rete e della qualità e quantità d'informazione che essa mette a disposizione a tutti i livelli di comando.

Un approccio innovativo e radicale, che presuppone in linea di principio il rinnovamento completo delle piattaforme, ma anche del *modus operandi* di comandanti e sottoposti.

Nata negli Stati Uniti, la dottrina del Network Centric Warfare è stata concepita

per sviluppare un'architettura di riferimento nella quale tutti i tipi d'informazione possano essere integrati grazie alla definizione e all'utilizzo di standard comuni.

Ma anche in Europa, sempre più spesso coinvolta in operazioni fuori area per far fronte alle situazioni di crisi in diverse parti del mondo, la necessità di migliorare l'efficacia degli interventi è oggi una priorità evidenziata da tutte le forze armate del continente e questo nonostante i budget della Difesa dei Paesi europei, e quello dell'Italia in particolare, siano molto inferiori rispetto a quello degli Stati Uniti.

In Europa, pertanto, si è scelto di sviluppare il concetto meno radicale e dispendioso della Network Enabled Capability, che ha l'obiettivo di integrare i sistemi e le piattaforme esistenti in una rete di comunicazione efficace.

Per ottenere ciò all'Amministrazione Difesa spetta la responsabilità di definire la dottrina e i requisiti operativi, mentre l'industria ha il compito di definire i modelli ingegneristici e le architetture complessive, da cui derivare sistemi e piattaforme.

Finmeccanica vuole giocare un ruolo da protagonista in campo europeo quando un programma NEC sarà definito compiutamente, e ha tutte le carte in regola per farlo.

Negli Stati Uniti ha sviluppato partnership strategiche con Boeing, Northrop Grumman e Lockheed Martin; fa parte del Network Centric Operations Industry Consortium (NCOIC, che raggruppa circa 80 aziende di tutto il mondo) per la definizione degli standard con un ruolo da leader a livello europeo; nel Regno Unito siamo in grado di fornire soluzioni sensor-to-effect, in grado di integrare le capacità sensoristiche e di piattaforma delle proprie società; infine, in Italia, stiamo conducendo lo studio di fattibilità, finanziato dal Ministero della Difesa, per lo sviluppo e l'interoperabilità del sistema di comando e controllo nazionale.

Questi sforzi daranno i risultati attesi se la collaborazione sempre più stretta ed efficace tra Ministero della Difesa, Forze Armate e industria porterà allo sviluppo di un programma NEC nazionale credibile e di assoluto livello.

Pier Francesco Guarguaglini  
Presidente e AD di Finmeccanica



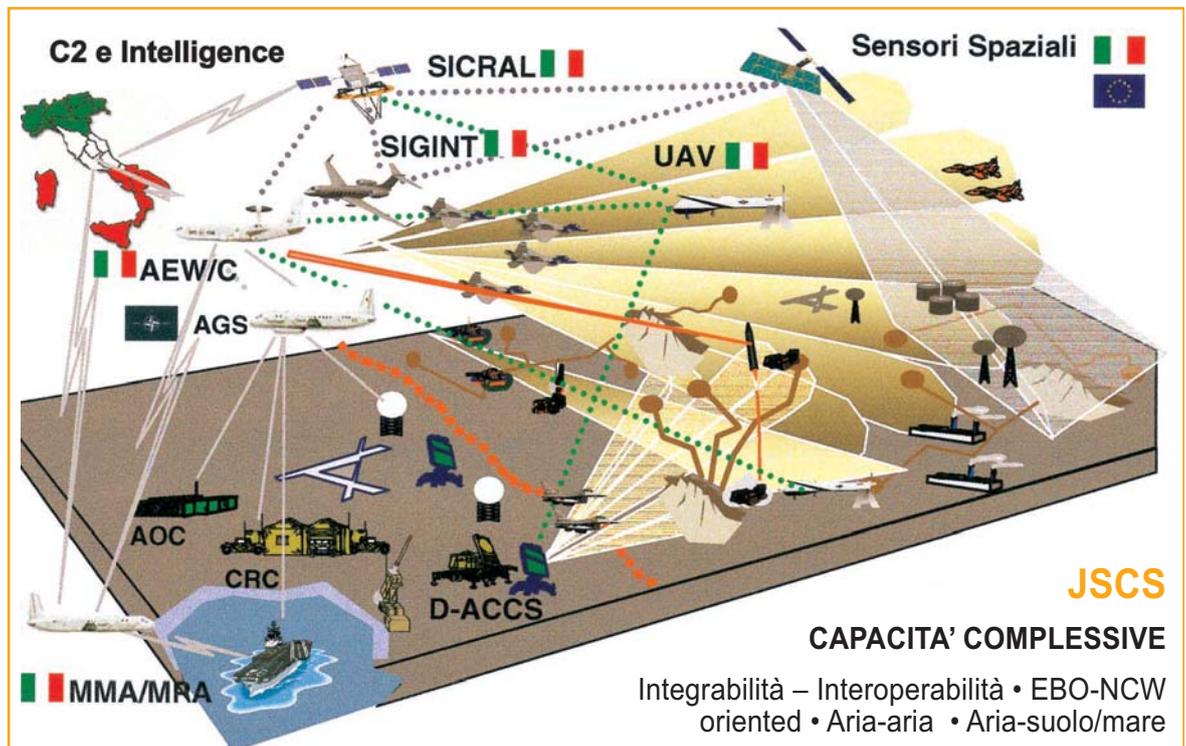
Generale (mentre il resto ne supporta l'azione dalla madrepatria grazie alle possibilità offerte dall'IT e dai collegamenti satellitari) rappresenta un'altra prova evidente dei molteplici benefici offerti dal ricorso a capacità netcentriche.

Altri due aspetti di carattere generale che è opportuno sottolineare, prima di passare a un esame dell'attuale situazione italiana e degli sviluppi futuri, riguardano rispettivamente l'esigenza di assicurare piena unitarietà di indirizzo, in ambito Difesa, nel disegno dell'architettura della struttura C4ISTAR e quella di mettere a punto una metodologia valida, coerente e ben definita per lo sviluppo dei nuovi sistemi, basata su un'ampia interazione e collaborazione fra Difesa e Industria.

per disporre di una "situation awareness" comparabile, sarebbe stato necessario schierare sul terreno centinaia di uomini impegnati in una continua attività di pattuglia.

Un altro significativo esempio è dato dalle capacità di "reach back" consentite già dagli attuali assetti C4ISTAR, che permettono ad esempio – a parità di efficacia dell'azione svolta – di proiettare in teatro terrestre o marittimo solo un'aliquota di un comando complesso, mantenendo la parte rimanente nella sede stanziata in Italia. Il vantaggio che deriva dal dover schierare, mantenere, proteggere e alimentare fuori area solo una frazione del personale che compone il Quartier

La necessità di avere una direzione unitaria nell'ambito Difesa per la definizione dell'architettura, intesa come quel complesso degli aspetti attinenti i requisiti operativi, standard tecnici, requisiti di interoperabilità e requisiti di sistema, da parte del reparto TEI dello Stato Maggiore Difesa (che opera beninteso fianco a fianco di SEGREDIFESA, degli altri Reparti di SMD e degli Stati Maggiori di Forza Armata e dell'Industria, per gli aspetti amministrativi, dottrinari, formativi e specialistici di rispettiva competenza) deriva dalla consapevolezza che solo in questo modo



è possibile procedere a uno sviluppo degli assetti "intelligente" e armonizzato con le indicazioni e gli standard nazionali, internazionali e NATO, al fine di garantirne la piena interoperabilità.

Per quanto riguarda la metodologia di sviluppo dei sistemi NCW e i rapporti che devono intercorrere, in questo contesto, fra Difesa e Industria, l'esperienza dei singoli Paesi e delle Organizzazioni internazionali che hanno preceduto e/o affiancano l'Italia sullo stesso cammino dimostra che l'approccio più razionale, promettente e a basso rischio è quello basato su un ampio ricorso a procedure di modelling e simulazione in tutte le fasi previste, dalla verifica dei requisiti operativi, alle attività di sviluppo, al test e all'accettazione dei sistemi. Sia le metodologie che i centri di prova e simulazione devono essere armonizzati e condivisi da Difesa e Industria, in qualità di co-protagonisti interattivi e sinergici di un'impresa comune.

#### UN PERCORSO AVVIATO

È bene chiarire subito che, nel processo di trasformazione in senso netcentrico, la Difesa e l'Industria italiane non si trovano oggi a partire da zero, né sul piano concettuale né su quello degli strumenti disponibili né su quello dei programmi in corso di realizzazione: questo grazie

***Non è importante ciò che le Forze Armate o l'Industria della Difesa hanno fin qui realizzato, ma ciò che deve e dovrà essere ancora realizzato: e questo dipende da noi e da come sapremo metterci in rete al nostro interno e con l'esterno.***

#### PROGRAMMA SICCONA

*Il programma SICCONA (Sistema di Comando, Controllo e Navigazione) prevede di dotare i veicoli da combattimento dell'Esercito Italiano di un sistema di comando, controllo, navigazione e comunicazione in grado di fornire in tempo reale al personale di bordo tutte le informazioni tattiche e logistiche (cartografia, messaggistica, database, comunicazioni sicure dati e voce) utili allo svolgimento della missione, avviando il processo di digitalizzazione dello spazio di manovra e contribuendo alla realizzazione della "information dominance". Entro il 2006 è prevista la fornitura di tre prototipi da installare rispettivamente su una blindo Centauro, un MBT Ariete e un IFV Dardo; nel 2007, dopo la conclusione delle prove operative, seguirà una prima serie di 40 sistemi accompagnati dal relativo supporto addestrativo e logistico.*



anche all'appartenenza all'Alleanza Atlantica, che ha permesso di conoscere e condividere tempestivamente orientamenti dottrinari, impostazioni operative e soluzioni tecnologiche con i maggiori Paesi occidentali; al rafforzamento del potere di indirizzo e decisionale di SMD conseguente alla ristrutturazione dell'assetto di Vertice della Difesa avviata nella seconda metà degli anni '90; e infine alle capacità dell'industria italiana, che hanno consentito di impostare già nel recente passato programmi precursori di (o pienamente compatibili con) una visione NCW quali il sistema C4I di Vertice, i sistemi di comando e controllo e di supporto al comando di Forza Armata, la rete digitale interforze in fibra ottica, il sistema di comunicazioni satellitare SICRAL, il sistema di osservazione militare/civile Cosmo-SkyMed e la digitalizzazione dello spazio di manovra, come pure di partecipare ad analoghi, importanti programmi internazionali.

Non è importante ciò che le Forze Armate o l'Industria della Difesa hanno fin qui realizzato, ma ciò che deve e dovrà essere ancora realizzato: e questo dipende da noi e da come sapremo metterci in rete al nostro interno e con l'esterno.

Anche se in origine – prima degli anni '90 – lo sviluppo di sistemi nazionali idonei a consentire la progressiva introduzione di capacità di comando e controllo, l'automazione di alcune funzioni operative e una crescente condivisione delle informazioni è avvenuto principalmente in un'ottica "single service", vale a dire in base alle specifiche esigenze di ciascuna Forza Armata, non va dimenticato che le stesse Forze Armate hanno sempre operato, in particolare fuori area, in un contesto NATO e multinazionale: il che significa che ciascun "Component



Command" ha comunque sviluppato concetti e sistemi allineati con quelli adottati o avallati all'epoca dall'Alleanza. Questo vale in particolare per l'Aeronautica e la Marina Militare, le cui operazioni hanno sempre avuto una più forte connotazione multinazionale, mentre per l'Esercito un'analogia esigenza si è manifestata in tempi successivi.

La supervisione e il coordinamento attuati da SMD nei confronti delle singole Forze Armate si sono sensibilmente rafforzati dopo la Riforma del 1997, che ha consentito al Vertice della Difesa di esercitare una più robusta azione d'indirizzo e controllo sia in campo dottrinario che sulla condotta delle operazioni: si sono così consolidate una visione "joint" e le conseguenti iniziative destinate a realizzare uno strumento militare allineato a questa visione. In questo quadro vanno ricordate in particolare la creazione, alla fine degli anni '90, del Comando Operativo Interforze (COI) e la costituzione di un gruppo di lavoro interforze, coordinato dal Reparto TEI di SMD, per lo sviluppo di un sistema di comando e controllo joint (il cosiddetto "C4I") destinato allo stesso COI, attività iniziata nel 2000 e di cui si stanno attualmente raccogliendo e validando i risultati.

Altri assetti tipicamente interforze, già disponibili oppure in fase di acquisizione e/o di potenziamento nell'ambito di programmi nazionali o bilaterali già in corso, riguardano le comunicazioni satellitari (SICRAL 1, 1B e 2), la rete terrestre digitale in fibra ottica interforze (RNI), la sorveglianza e ricognizione dallo spazio (Cosmo-Skymed) e mediante velivoli non pilotati (Predator) e l'automazione delle funzioni gestio-

nali, amministrative e logistiche di vertice dell'Amministrazione Difesa (SIV e programmi analoghi). L'insieme di tali programmi ha già comportato, a partire dagli anni '90, investimenti per un ammontare complessivo di parecchie centinaia di milioni di euro, a ulteriore conferma dell'attenzione e del tempismo con cui la Difesa italiana si è mossa in relazione alle iniziative abilitanti ai fini della trasformazione.

Per quanto riguarda i programmi avviati per le esigenze e/o nell'ambito delle singole Forze Armate, è ancora il caso di ricordare:

- per l'Esercito il SIACCON (Sistema Informatico Automatizzato di Comando e

### **PROGRAMMA "SOLDATO FUTURO"**

*Il programma, che s'inserisce nella più ampia iniziativa della digitalizzazione dello spazio di manovra terrestre, punta ad adeguare le capacità operative del singolo combattente ai futuri scenari d'impiego. Del sistema "Soldato Futuro" fanno parte un fucile d'assalto di nuova generazione, completo di lanciagranate e sistema di controllo del tiro, un sistema modulare di protezione balistica e NBC, un sistema di mobilità/visione notturna, un sistema per lo scambio di informazioni in ambito NCW/NEC e un sistema di alimentazione con batterie al litio. A seguito della sperimentazione effettuata col dimostratore tecnologico consegnato nel 2004, nel 2005 sono state approvate le specifiche tecniche del sistema nella versione definitiva e ha avuto inizio la fase di sviluppo e progettazione e dei prototipi, che si prevede di completare nell'estate del 2006.*



CONtrollo), articolato su un Centro Analisi e Selezione delle Informazioni (CASI), un Centro di Fusione (CF) che ospita la banca dati aggiornata e un Centro Decisionale (CD) in cui i dati di sintesi sono presentati ai decisori, destinato ad automatizzare le procedure dei Posti Comando delle Grandi Unità in zona di operazioni; il SIACCON MLO (Minori Livelli Operativi), destinato ad integrare il precedente estendendolo verso le Unità di più basso livello (da reggimento a plotone); il SICCONA (Sistema Integrato di Comando, Controllo e Navigazione) per l'interconnessione in rete delle piattaforme da combattimento terrestri e il "Soldato Futuro" (rivolto ai combattenti individuali), che insieme rientrano nella più generale iniziativa rivolta alla digitalizzazione dello spazio di manovra terrestre;

- per la Marina Militare il sistema di comando e controllo strategico MCCIS (Maritime Command and Control Information System), la rete radar di sorveglianza costiera, il NILE (NATO Improved Link Eleven) per lo scambio dei dati tattici e il MIDS-LTV (Multifunctional Information and Distribution System - Low Volume Terminal) per la distribuzione delle informazioni;
- per l'Aeronautica Militare l'ACCS (Air Command and Control System) e il SICCAM (Sistema di Comando e Controllo Aeronautica Militare), per il controllo e la gestione dello spazio aereo ai fini rispettivamente delle esigenze NATO e nazionali;

**La trasformazione è un processo continuo; arrestarsi significa retrocedere ad un passato dal quale le Forze Armate sono uscite grazie allo sforzo di modernizzazione che hanno saputo compiere.**

- per l'Arma dei Carabinieri lo sviluppo e il potenziamento dell'infrastruttura informatica e delle reti di comunicazione fisse e mobili terrestri e satellitari (attraverso l'uso di canali dedicati sul satellite SICRAL 1B) al fine di migliorare l'efficienza dei reparti, il controllo del territorio e l'efficacia delle attività operative.

A questi programmi se ne affiancano, nell'ambito di ciascuna Forza Armata, altri rivolti all'automazione e al rafforzamento delle capacità di interconnessione di specifici settori operativi e/o delle maggiori piattaforme, quali ad esempio il SOATTC per la gestione dello spazio aereo sull'area di battaglia terrestre, i sistemi C4ISTAR delle maggiori unità navali (in particolare quelli di Nave *Garibaldi* e Nave *Etna*, certificate dalla NATO per ospitare il Maritime Component Commander), il sistema di Comando e Controllo per la Lotta Anfibia, il JAMMS (Joint Airborne Multi-Mission System) per l'elaborazione e distribuzione di dati e informazioni di interesse strategico e operativo per l'AMI, l'acquisizione di pod da ricognizione optronica per i velivoli, ecc.

STRATEGIA COMUNE

In un panorama nazionale già ricco di iniziative concrete s'inserisce la volontà di continuare con decisione sul percorso dell'integrazione dei sistemi esistenti (per quanto riguarda la parte adeguabile a capacità NEC) e di quelli in corso di acquisizione o in fase di sviluppo (che nascono e nasceranno con una precisa caratterizzazione di netcentricità) nella "Information Grid" che costi-



tuirà il tessuto connettivo delle future operazioni NCO "joint" e multinazionali. La "rete" al cuore di questo progetto non è una semplice "Internet militare" ma molto di più, in quanto deve possedere due caratteristiche peculiari: essere "intelligente" e "sicura". L'aspetto della sicurezza riguarda la protezione, mediante opportune barriere logiche e fisiche, delle informazioni che viaggiano nella rete, sia contro le possibilità di intrusione o disturbo da parte dell'avversario che in relazione alle esigenze di riservatezza politica e militare che ciascuna Nazione comprensibilmente esige e ha diritto di

**Un driver della trasformazione è comunque il problema delle risorse: è indispensabile poter contare, in proiezione a medio-lungo termine, su risorse strutturali coerenti.**



esercitare, stabilendo liberamente se condividere o meno certe informazioni e determinati data base con altri membri di un'Alleanza o di una Coalizione.

L'aspetto dell'intelligenza riguarda invece l'idoneità della rete ad adeguarsi in modo dinamico e flessibile alle esigenze di tutti gli operatori, distribuendo le informazioni in modo pianificato e secondo necessità (inclusa l'applicazione di criteri selettivi) e consentendo a tutti coloro che hanno bisogno di dati di poter accedere. Un risultato di questo tipo può essere conseguito solo attraverso una seria e consapevole armonizzazione di tutti i segmenti programmatici deputati a gestire le informazioni, sia sul piano nazionale che a maggior ragione su quello internazionale (di Alleanza o di Coalizione), dove "essere netcentrici con se stessi" non è di utilità alcuna. In altre parole è necessario, come si è già avuto modo di sottolineare, un "architetto unico" che armonizzi la struttura informativa sia a livello nazionale che multinazionale, in linea con le indicazioni emergenti nel contesto internazionale e segnatamente dalla NATO.

I tempi di attuazione del disegno complessivo restano, per quanto riguarda l'Italia, quelli tracciati dalla roadmap dell'Alleanza, che prevede l'acquisizione di una capacità minima NCW per operare con la NRF entro il 2008, una crescita armonizzata, all'orizzonte 2012, per conseguire significative capacità NCW di Coalizione e, a più lungo termine (2016-2020), una piena capacità NCW. Il contesto in cui continuare e perfezionare la trasformazione è rigorosamente di collaborazione internazionale, sia per quanto riguarda la Difesa che l'Industria, a sua volta impegnata a dialogare con Organismi internazionali quali il consorzio industriale NCOIC in materia di standardizzazione, ad avvalersi delle partnership strategiche (sviluppate in particolare con aziende americane quali Boeing, Lockheed Martin e Northrop Grumman) per acquisire know-how e rafforzare le proprie capacità sistemiche e a consolidare un livello di conoscenze e tecnologie che le consenta di accedere al maggior numero di mercati.

Per conseguire i propri obiettivi di breve, medio e lungo termine la Difesa italiana si è già mossa



con diverse iniziative, sia in ambito nazionale che internazionale, prevedendo di:

- analizzare, nel quadro di uno studio affidato a Finmeccanica da completare entro il 2006, gli assetti esistenti (i cosiddetti "sistemi di legacy") in un'ottica netcentrica, al fine di valutare quali siano idonei ad operare, mediante opportuni aggiornamenti, nel futuro ambiente NCW/NCO, e quali sia invece preferibile dismettere gradualmente;
- creare, insieme con l'industria, un'adeguata capacità di modelling e simulation al fine di

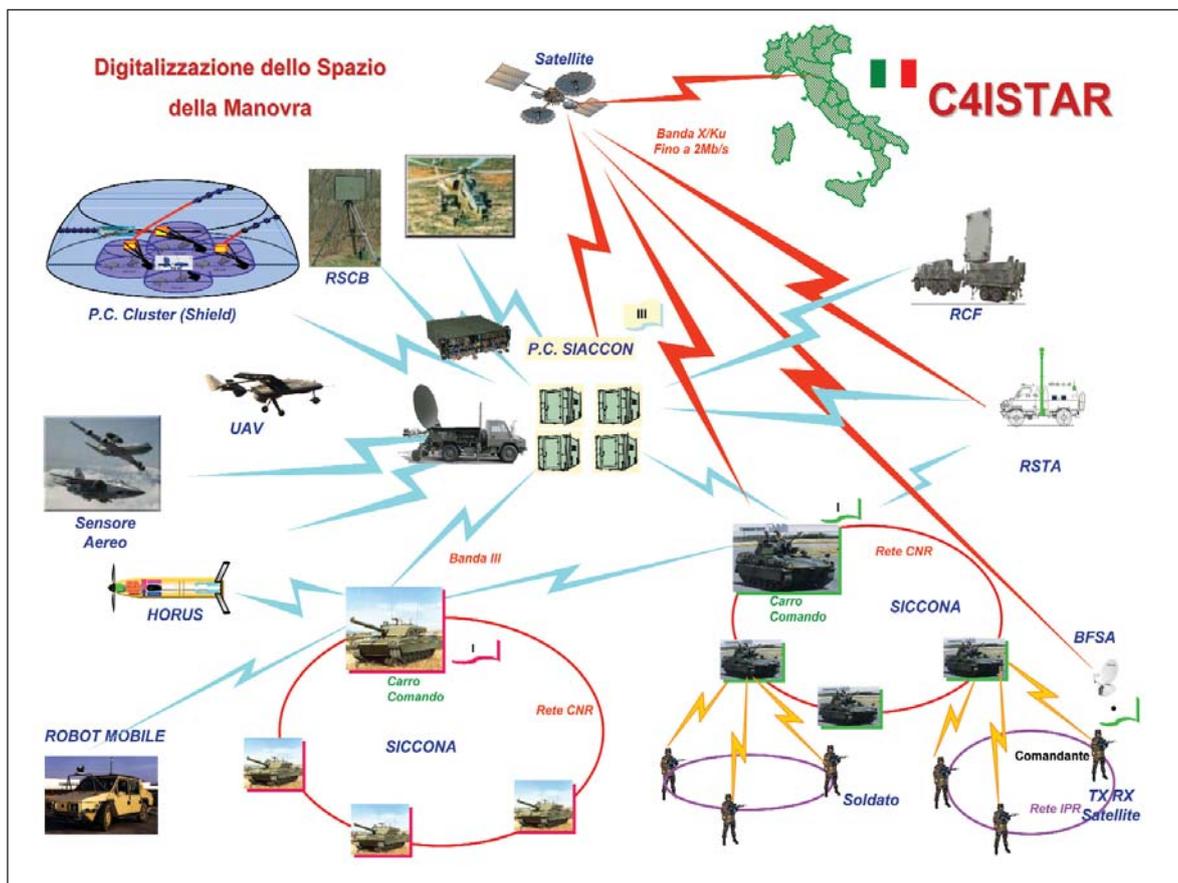
### SISTEMI E SERVIZI INFORMATICI

*A complemento dei sistemi operativi, inclusa la "rete" per lo scambio delle informazioni, l'attuazione del concetto NCW presuppone lo sviluppo di sistemi e servizi informatici per l'automazione di una vasta gamma di funzioni, incluse quelle gestionali di vertice, amministrative e logistiche. In ambito Difesa è in fase di avviamento operativo il SIV (Sistema Informativo di Vertice), che consentirà al vertice politico-militare un'ampia visibilità e una conseguente capacità di controllo della situazione amministrativa e finanziaria, mentre è in corso lo sviluppo di analoghi sistemi per la gestione del personale (SIPAD), della Sanità Militare (SISAD), delle attività di procurement (SIDAT) e della Logistica interforze (SILAD). Nel settore dei servizi è in fase di realizzazione una carta "sicura" per il personale dell'Amministrazione Difesa, contenente i dati anagrafici, biometrici e sanitari, mentre il servizio di Telemedicina consentirà di mettere tempestivamente a disposizione dei pazienti, anche se ubicati in aree remote, le capacità consultive e diagnostiche proprie di un Ospedale Militare.*



verificare preliminarmente, attraverso una simulazione il più accurata possibile dei requisiti tecnico-operativi, delle caratteristiche dei sistemi e dell'ambiente operativo, che i sistemi NCW/NEC allo studio siano conformi alle aspettative. L'obiettivo è di interfacciare per via telematica i centri di sviluppo e sperimentazione interessati, sia della Difesa (quali quelli di Pratica di Mare, MARICENPROG a Taranto, Anzio, Civitavecchia, Sabaudia, Treviso) che dell'Industria (segnatamente quelli operati da Finmeccanica, SELEX Sistemi Integrati e SELEX Communications a Roma, Napoli, Genova e La Spezia), al fine di assicurare il coordinamento e l'armonizzazione dei rispettivi sforzi e la piena interoperabilità dei risultati. È necessario contestualmente procedere a un robusto ed autonomo consolidamento delle attività dei predetti centri. Si tratta di un'iniziativa che, una volta attuata, consentirà





non solo di far convergere e allineare le rispettive metodologie di lavoro ma, fatto altrettanto importante, di far "crescere assieme" una futura generazione di Ufficiali (per quanto riguarda le Forze Armate) e di specialisti (dal lato

dell'Industria) accomunati da una preziosa condivisione di idee, esperienze e obiettivi nel campo dell'NCW;



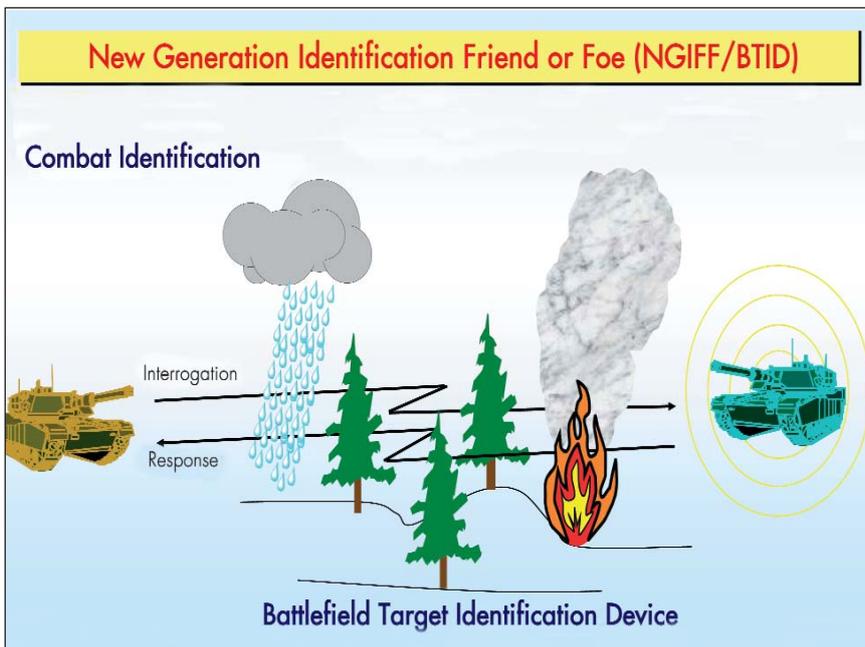
### PROGRAMMI NGIFF E BTID

Il programma NGIFF (New Generation IFF) ha come obiettivo di rendere disponibili sistemi di identificazione amico-nemico (Identification Friend or Foe, IFF) di nuova generazione in grado di operare in accordo con gli standard NATO e ICAO (modo ATC civile), mantenendo nella fase di transizione la capacità di interoperare con gli apparati IFF esistenti. L'impiego del NGIFF è previsto su una varietà di piattaforme terrestri, navali ed aeree, in accordo coi requisiti operativi delle Forze Armate. Un interrogatore NGIFF sarà integrato anche nel sistema missilistico superficie-aria SAMP/T, mentre per l'identificazione dei mezzi sul campo di battaglia terrestre è previsto lo sviluppo di una versione denominata BTID (Battlefield Target Identification Device). Per i programmi nazionali di sviluppo NGIFF e BTID, nel periodo 2001-2005 sono già stati investiti complessivamente circa 50 milioni di euro.

- sviluppare, nell'ambito di programmi nazionali e internazionali, gli ulteriori assetti necessari ad implementare le successive fasi della trasformazione in senso netcentrico.

Per quanto riguarda quest'ultimo aspetto, è il caso di ricordare ancora i programmi:

- NGIFF/BTID (New Generation IFF/Battlefield Target Identification), condotto in collaborazione con Stati Uniti, Gran Bretagna, Francia e Germania per lo sviluppo di un sistema di identificazione amico-nemico di nuova generazione, idoneo a risolvere i problemi posti dal rischio di fuoco fratricida negli scenari operativi aerei e terrestri;
- MAJIC (Multisensor Aerospace-ground Joint Interoperable ISR Coalition), coordinato dall'US Joint Forces Command di Norfolk e destinato a sviluppare



***In un mondo in continua e rapida evoluzione, nel quale il Paese è chiamato a fornire un contributo attivo alla sicurezza, alla stabilità e alla pace, il futuro delle Forze Armate rappresenta una questione focale.***

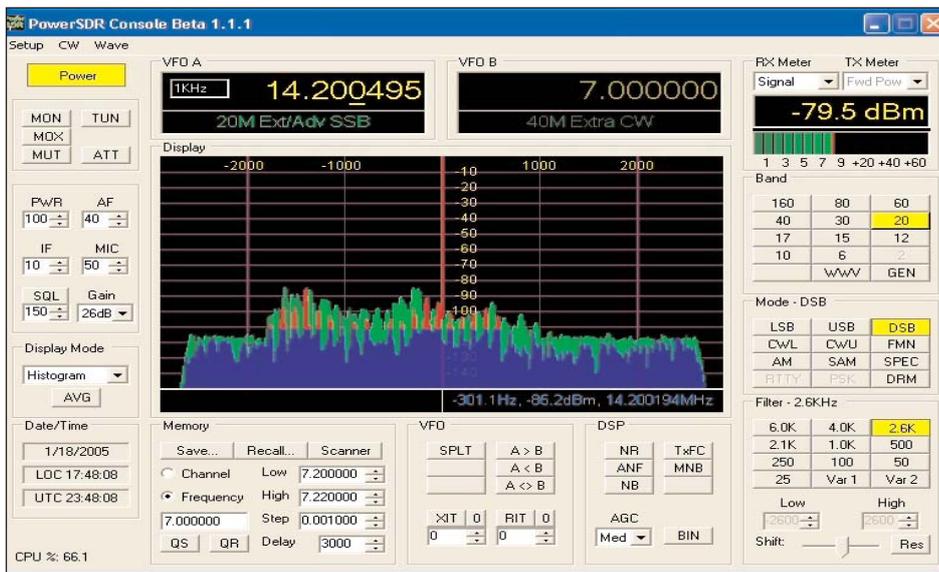
un'architettura che consenta ai partners di scambiare in tempo reale i rispettivi dati di intelligence, sorveglianza e designazione bersagli;

- SDR/JTRS (Software Defined Radio/ Joint Tactical Radio System), per lo sviluppo di una nuova generazione di sistemi radio tattici interoperabili, multibanda/multimodo e

riconfigurabili via software;

- MIP (Multilateral Interoperability Programme) e STP (Shared Tactical Picture), programmi a partecipazione multinazionale che prevedono l'uso di soluzioni tecniche a livello software per consentire la condivisione delle informazioni tra sistemi operativi e tattici anche già esistenti, senza la necessità di re-ingegnerizzazione degli stessi. Tali programmi introducono l'approccio architetturale Service-Oriented, considerato centrale in un contesto netcentrico;

- BFSA (Blue Force Situation Awareness), programma di sviluppo intrapreso dalla Difesa e assegnato all'Industria nazionale per il tracciamento e la positiva identificazione delle forze amiche in campo tattico, nonché gli studi/iniziativa in atto per acquisire le necessarie capacità abilitanti nei settori dei sistemi aeroportati di sorveglianza, comando e controllo



mand System, JSCS) con tutti gli assetti utili a sviluppare le capacità richieste.

In ambito industriale Finmeccanica, coerentemente con le missioni assegnate alle singole Aziende all'interno del Gruppo, ha individuato in SELEX Sistemi Integrati la società leader incaricata di occuparsi, in qualità di prime contractor, del disegno e dell'architettura dei "grandi sistemi", incluso quello netcentrico, e dell'integrazione in questo contesto dei diversi sistemi/prodotti interessati. A tal fine si è costituito all'interno

(AEW&C, AGS), pattugliamento marittimo multi-ruolo (MMA) e intelligence (SIGINT), al fine di completare il futuro sistema interforze di sorveglianza e comando (Joint Surveillance and Com-

della Società un gruppo di lavoro dedicato alla definizione dell'architettura, che affronta il tema in stretta collaborazione (per gli aspetti specifici relativi alle comunicazioni, ai sensori, agli attuatori ecc.) con le altre aziende del Gruppo e del settore difesa e in un'ottica di riduzione dei rischi, per la quale Finmeccanica si avvale anche della partecipazione al consorzio NCOIC e dei rapporti di collaborazione stabiliti con importanti partners industriali nei paesi più avanzati sul fronte dello sviluppo del concetto NCW/NEC, quali USA e Gran Bretagna.

## SDR/JTRS

La Software Defined Radio (SDR) è una nuova concezione della tecnologia delle comunicazioni militari nel campo tattico, secondo la quale il segnale che trasporta l'informazione non viene generato da componenti hardware, ma da un microprocessore in grado di eseguire un programma (forma d'onda) specifico; ne deriva che per riconfigurare un sistema radio è sufficiente aggiornarne il software, anziché intervenire sull'hardware. In tale ottica è di fondamentale importanza lo sviluppo di una piattaforma radio comune in grado di garantire l'interoperabilità degli apparati, l'implementazione di forme d'onda standard e una grande flessibilità d'impiego. A questo scopo gli USA hanno avviato il programma Multifunctional Information Distribution System - Joint Tactical Radio System (MIDS-JTRS), che prevede la migrazione del MIDS verso nuove tecnologie del tipo SDR. La Difesa Italiana, già coinvolta nel MIDS, è fortemente interessata alla SDR per le evidenti ricadute sull'interoperabilità e sull'applicazione del concetto NCW, nel cui ambito la SDR è considerata il "pilastro wireless". Nel gennaio 2005 è stata pertanto riconfermata la partecipazione italiana al programma MIDS-JTRS, col proposito di far acquisire all'industria nazionale il know-how da riversare nel parallelo programma di sviluppo di una famiglia di Radio Software Digitale Italiana.



## ACCELERARE LA TRASFORMAZIONE NET-CENTRICA



L'acquisizione delle capacità NCW/NEC necessarie per mantenere e rafforzare l'interoperabilità dello strumento militare italiano con i dispositivi alleati avverrà nell'ambito di una strategia e di un percorso che sono stati già tracciati dalla NATO, come risultato di uno studio cui anche l'Italia ha dato il suo attivo e convinto contributo. Questo rappresenta un obiettivo primario per la Difesa, come già stabilito dal vertice militare, che deve essere recepito anche a livello interdisciplinare nella prospettiva di estendere l'approccio net-centrico all'intero ambito di applicazione del concetto di "homeland security" – ovvero alle strutture degli altri dicasteri che contribuiscono alla funzione sicurezza – e, più in generale, alle organizzazioni che operano nel campo della sicurezza e degli aiuti umanitari. "interagenzia" dell'intera amministrazione dello Stato.

I sistemi C4ISTAR della Difesa Italiana sono oggi paragonabili, sul piano delle capacità, a quelli delle altre nazioni alleate, come è provato sia nelle attività congiunte nei vari teatri operativi, sia dai test di interoperabilità effettuati a più riprese in ambito internazionale. Si tratta di una situazione destinata a migliorare una volta che saranno completati i programmi, in parte già avviati, destinati a colmare le criticità residue: ma è chiaro che la costruzione di una struttura C4ISTAR in chiave NCW/NEC adeguata alle esigenze dello strumento militare futuro resta un percorso ambizioso e difficile, superabile solo con un impiego intelligente e sinergico di energie e risorse umane, tecnologiche e finanziarie.

Questo vale in uguale misura per la Difesa e l'Industria, che sono chiamate a coordinare i loro sforzi, concentrandoli in primo luogo sulla razionalizzazione e l'ottimizzazione dei centri di modellizzazione e simulazione, integrati a livello informatico e connessi con le analoghe realtà che operano nei paesi alleati, utilizzabili per la verifica dei requisiti operativi, la definizione unitaria dell'architettura di sistema, la riduzione dei rischi di sviluppo e la validazione dei sistemi, oltre che per la formazione e l'addestramento del personale. Si tratta solo di un primo passo, ma indispensabile per assicurare una maturazione coerente di mentalità, cultura, metodologia, strategie, tecnologie, operatività e capacità produttive.

Nello sviluppo dell'NCW la componente tecnologica riveste un'importanza fondamentale, ma non bisogna dimenticare che – prima di qualsiasi tecnologia – è l'uomo a costituire l'elemento cardine per il successo.

L'ottimizzazione dei benefici consentiti dall'utilizzo delle nuove tecnologie non può infatti prescindere da una profonda evoluzione del modo di pensare, agire e relazionarsi delle persone – siano esse decisori, "sensori" o attuatori – nel futuro ambiente net-centrico; un ambiente che la realtà attuale già consente di intravedere ma che, una volta pienamente attuato, porterà con sé trasformazioni ancora più profonde.

La velocità con la quale riusciremo a realizzarle sarà una misura della volontà e della capacità di tenere il passo con le nazioni più avanzate, rispetto alle quali è essenziale evitare ogni "perdita di contatto" per non compromettere la capacità, la credibilità e la competitività del sistema Paese.

Amm. Div. Gino BIZZARI  
Capo Reparto TEI/SMD

## ABBREVIAZIONI

ACCAM	Automazione Centri Comunicazione Aeronautica Militare
ACCS	Air Command and Control System
ACT	Allied Command Transformation
BFSA	Blue Force Situational Awareness
BTID	Battlefield Target Identification Device
C2	Comando e Controllo
C3	Comando, Controllo e Comunicazioni
C4I	Comando, Controllo, Comunicazioni, Computer e Informazioni
CAESAR	Coalition AERial Surveillance And Recon
CEC	Cooperative Engagement Capability
CMS	Combat Management System
COI	Comando Operativo Interforze
COP	Common Operational Picture
COTS	Commercial Off The Shelf
EBO	Effects Based Operations
FCS	Future Combat System
GIG	Global Information Grid
IP	Internet Protocol
JAMMS	Joint Airborne Multi Mission System
MAJIIC	Multimission Aerospace-ground Joint Interoperable ISR Coalition
MCCIS	Maritime Command and Control Information System
MIDS-LVT	Multifunctional Information Distribution System-Low Volume Terminal
MIP	Multilateral Interoperability Programme
NADGE	NATO Air Defence Ground Environment
NATO	North Atlantic Treaty Organization
NC3A	NATO Consultation, Command and Control Agency
NCO	Network Centric Operations
NCOIC	Network Centric Operations Industry Consortium
NCW	Network Centric Warfare
NEC	Network Enabling Capability
NGIFF	New Generation Identification Friend or Foe
NRF	NATO Response Force
PSO	Peace Support Operations
RNI	Rete Numerica Interforze
SDR/JTRS	Software Defined Radio/Joint Tactical Radio System
SIACCON	Sistema Informativo Automatizzato di Comando e CONTROLLO
SICCAM	Sistema di Comando e Controllo Aeronautica Militare
SICCONA	Sistema di Comando, Controllo e Navigazione
SICRAL	Sistema Italiano per Comunicazioni Riservate ed Allarmi
SIGE	Sistema Informativo Gestionale dell'Esercito
SIGINT	SIGNAL INTELLIGENCE
SILEF	Sistema Informativo Logistico Euro Fighter
SILI	Sistema Informativo Logistico Integrato
SIV	Sistema Informativo di Vertice
SMD	Stato Maggiore Difesa
SOATCC	SOTTOSISTEMA di Avvistamento Tattico contraerei, Comando e Controllo
SORAO	SOTTOSISTEMA di SORveglianza di Acquisizione Obiettivi
SOTRIN	SOTTOSISTEMA di TRASmissioni INtegrate
SSA	Shared Situational Awareness
STP	Shared Tactical Picture
TEI	Telecomunicazioni, Elettronica, Informatica
UAV	Unmanned Air Vehicle
US DoD	United States Department of Defense
WAN	Wide Area Network
WIN-T	Warfighter Information Network-Tactical

Il testo di questo documento può essere liberamente ripreso a condizione che la riproduzione sia fedele e non utilizzata in contesti fuorvianti. Il materiale deve essere citato come proprietà intellettuale dello Stato Maggiore Difesa, specificando il titolo del documento. Le immagini e i grafici sono stati forniti da: Alenia Spazio, AMI/Troupe Azzurra, Australian Dept. Of Defence, Boeing, Dept. of National Defence - Canadian Forces, Ericsson, Fincantieri, Finmeccanica, Maristat/Ucom, NATO, NATO ACT, OTO Melara, Power SDR, Sagem, SELEX Sistemi Integrati, SEGREDIFESA, SMD, R. Stanglini, UK Ministry of Defence, USAF, US Army, US Dept. of Defense, US Navy, P. Valpolini, e sono protette dal copyright delle rispettive fonti originarie.

Stampa: Imago Media Editrice - Piedimonte Matese (CE)  
tel 0823 866710 - [www.imagomedia.it](http://www.imagomedia.it)  
maggio 2006



STATO MAGGIORE DELLA DIFESA