quaderni IAI

ISSN 0075-1448

Innovazione tecnologica e difesa: Forza NEC nel quadro euro-atlantico

a cura di Alessandro Marrone, Michele Nones
e Alessandro R. Ungaro

Edizioni Nuova Cultura

IAI
Istituto Affari Internazionali

Quaderni IAI

INNOVAZIONE TECNOLOGICA E DIFESA: FORZA NEC NEL QUADRO EURO-ATLANTICO

a cura di
Alessandro Marrone, Michele Nones e Alessandro R. Ungaro

Edizioni Nuova Cultura

Ringraziamenti
Il team di ricerca intende ringraziare per le informazioni e i suggerimenti ricevuti lo Stato Maggiore dell'Esercito, in particolare il Dipartimento per la Trasformazione Terrestre, e Finmeccanica-Selex ES.
Gli autori si assumono la piena ed esclusiva paternità e responsabilità per i contenuti dello studio. Questa ricerca è stata realizzata col contributo di Finmeccanica-Selex ES.
Si ringrazia infine Carolina Coradeschi, che è stata tirocinante nel programma Sicurezza e Difesa dello IAI nel primo semestre 2015, per la traduzione dall'inglese del capitolo sul caso americano.

Hanno contribuito:
Nick Brown, IHS Jane's International Defence Review
Tommaso De Zan, assistente alla ricerca, Istituto Affari Internazionali (IAI)
Maren Leed, Senior Adviser, Center for Strategic and International Studies (CSIS)
Alessandro Marrone, responsabile di ricerca, Istituto Affari Internazionali (IAI)
Michele Nones, direttore del Programma Sicurezza e Difesa, Istituto Affari Internazionali (IAI)
Alessandro R. Ungaro, ricercatore, Istituto Affari Internazionali (IAI)

Quaderni IAI
Direzione: Natalino Ronzitti

Per Istituto Affari Internazionali (IAI)
Via Angelo Brunetti 9 - I-00186 Roma
www.iai.it

ISBN: 9788868125066
Copertina: Luca Mozzicarelli
Composizione grafica: Luca Mozzicarelli

Indice

Executive Summary

Innovazione tecnologica e mondo militare sono da sempre in costante interazione, un fenomeno molto importante che ha visto una significativa accelerazione nel periodo post-Guerra Fredda. In questo contesto, il Quaderno si concentra in particolare sul rapporto tra l'Information Communication Technology (ICT) e le forze armate di Italia, Stati Uniti, Gran Bretagna, Francia e Germania. Si intende così analizzare nel quadro euro-atlantico il percorso intrapreso dall'Esercito Italiano (EI), nell'ultimo decennio, per sviluppare delle capacità militari netcentriche (Network Enabled Capabilities, NEC) attraverso il programma Forza NEC. Con l'acronimo NEC ci si riferisce all'interconnessione di diversi elementi delle forze armate in un'unica rete, in modo da ottenere la loro interazione per raggiungere una marcata superiorità strategica. Ciò si realizza tramite un'adeguata architettura di Comunicazione, Comando, Controllo e Computer (C4), e la digitalizzazione degli equipaggiamenti delle forze armate per connetterli alla rete stessa.

Il Quaderno si articola in tre capitoli, che offrono rispettivamente un'analisi del caso studio americano, una panoramica degli sviluppi in Francia, Germania e Gran Bretagna, ed infine una approfondita disamina della situazione italiana. Il volume mira, a quattro anni di distanza dal Quaderno IAI "La trasformazione delle Forze Armate: il programma Forza NEC", a fare il punto rispetto ad una relazione tra innovazione tecnologica e difesa in piena evoluzione. Evoluzione segnata dal fatto che gli sforzi per digitalizzare ed interconnettere gli equipaggiamenti delle forze terrestri, sfruttando le potenzialità dell'ICT, si scontrano con realtà operative e di bilancio che rendono particolarmente difficile per le forze armate dei Paesi analizzati percorrere la propria strada verso capacità netcentriche.

* * *

Nel caso americano, le tecnologie ICT e le capacità netcentriche sono divenute così profondamente e irrevocabilmente radicate nelle operazioni mi-

litari statunitensi che il dibattito in corso ruota attorno a "come" esse possano essere utilizzate più efficacemente, piuttosto che sul "se" impiegarle o meno. Le reti – siano esse cablate, wireless, space-based e terrestri – ricoprono un ruolo fondamentale in ognuna delle "funzioni di combattimento" delineate nella dottrina interforze degli Stati Uniti – Comando e Controllo (C2), Intelligence, Fuoco, Movimento e manovra, Protezione Supporto logistico. Ci sono decine di programmi, sia interforze che a livello di singola forza armata, volti a fornire capacità in una o più di queste funzioni.

Dal momento in cui le tecnologie ICT hanno sviluppato e creato la premessa alle capacità netcentriche, esse hanno presentato sia un'opportunità che una sfida. L'opportunità consiste nell'incrementare non solo le capacità delle singole piattaforme, ma anche quelle tra le piattaforme. Una delle sfide invece è infondere tale potenziale a tutto l'insieme degli equipaggiamenti militari, straordinariamente ampio e complesso. Ognuna della quattro forze armate adotta un approccio alquanto simile per raggiungere un adeguato equilibrio tra le risorse a disposizione e l'incremento di capacità. Sebbene il finanziamento per i nuovi programmi sia costantemente in diminuzione, ogni nuovo progetto sarà disegnato per essere net-enabled, con un'architettura aperta che consenta i necessari aggiornamenti di capacità alla luce dei continui progressi nel campo dell'ICT. L'equipaggiamento esistente viene continuamente ri-aggiornato per fornire, in alcuni casi, un supporto sufficiente per ottenere un maggior collegamento tra i diversi sistemi mentre in altri, per incorporare direttamente capacità più aggiornate.

L'Aeronautica e la Marina stanno tentando di uniformare i principali, rispettivi, sistemi d'arma, riducendo ad esempio il numero di versioni delle unità navali e di velivoli e puntando a raggiungere una capacità equivalente attraverso la loro piena connessione NEC. Il Corpo dei Marines e l'Esercito, che dispongono tipicamente di un ampio ventaglio di equipaggiamenti, devono disporre necessariamente di piattaforme simili ma con differenti livelli di capacità, con il rischio di generare criticità in termini di interoperabilità tra le loro stesse unità nel caso di operazioni su larga scala. L'intento è minimizzare il più possibile queste differenze, anche se le restrizioni finanziarie hanno costretto, in particolar modo l'Esercito, a orientarsi più decisamente verso una strategia di aggiornamento incrementale attraverso molteplici programmi, con ovvie differenze capacitive tra e nelle varie unità. Nel complesso comunque, il desiderio dell'Esercito di evolversi da sistema "stand alone a networked" è condiviso dall'intera forza armata statunitense, e l'intero establishment militare si muove in

questa direzione. Al tempo stesso però si riconosce che se da una parte le capacità "stand-alone" manchino di sinergia, dall'altra quelle "networked" offrano agli avversari l'opportunità di provocare conseguenze ben maggiori, ad esempio se fossero in grado di penetrare o negare l'accesso a tali reti. Non è un caso infatti che le forze armate americane stiano investendo ingenti risorse economiche nel settore della cyber defense.

Un primo e ampio riconoscimento del potenziale che le tecnologie ICT erano in grado di offrire alle forze armate americane avvenne con il sistema di navigazione satellitare Global Positioning System (GPS) e con le informazioni che esso forniva in termini di Positioning, Navigation and Timing (PNT). I dati PNT hanno rivoluzionato ogni area funzionale di combattimento, dai sistemi Blue Force Tracker – che permettono ai comandanti di "vedere" in tempo reale la posizione di ogni veicolo della loro unità – alla comunicazione di precise coordinate, fino all'impiego di velivoli unmanned in grado di provvedere ai necessari rifornimenti in luoghi e postazioni remote nelle montagne dell'Afghanistan. Come già accennato, l'impatto piuttosto rivoluzionario dei dati PNT sulle operazioni militari americane ha comunque generato alcuni rischi, e non solo in termini di attacchi cibernetici. Sempre più frequentemente, i vertici delle forze armate evidenziano come lo spazio stia diventando sempre più congestionato e conteso. Ciò rappresenta una grave minaccia (volontaria o meno) ad ogni aspetto delle operazioni militari americane, dalla comunicazione all'intelligence, fino alla fornitura di supporto logistico.

Nonostante le informazioni fornite dai dati PNT siano state per molti aspetti rivoluzionarie, al momento i requisiti delle forze armate in termini di capacità netcentriche tendono ad estendersi su vari fronti. Per quanto riguarda l'Esercito, l'ultimo decennio e più di operazioni di combattimento ha persuaso i vertici della forza armata che la capacità di "vedere" se stessi e il nemico così come di diffondere rapidamente quest'informazione al campo di battaglia sono di cruciale importanza, e che tutto ciò si basa quasi esclusivamente su una solida struttura di network. Anche il Corpo dei Marines, che si avvale considerevolmente del supporto delle altre forze armate, riconosce che le NEC offrono alle sue unità capacità ben superiori, e che si rivelano centrali per l'interazione con le altre forze armate. Quindi, mentre le specificità delle ICT continuano a evolversi rapidamente, l'establishment militare americano concorda sul fatto che il successo delle forze armate dipenda in maniera significativa dall'abilità di sfruttare più adeguatamente tali progressi attraverso le capacità netcentriche.

Ogni principale programma di procurement delle forze armate americane ha già incorporato al suo interno le capacità netcentriche. Alcuni di questi sono concepiti esplicitamente con l'obiettivo di fornire un sistema di reti interconnesso, mentre altri sfruttano indirettamente le capacità netcentriche per incrementare la loro performance complessiva. Ogni "funzione di combattimento" ha al suo interno uno o più programmi, soprattutto terrestri, che riguardano più direttamente le NEC.

Le ICT e le capacità netcentriche, così come il loro impiego, sono chiaramente destinate a permeare il tessuto militare e industriale degli Stati Uniti. Oltretutto, molti ritengono che il loro potenziale sia ancora tutto da scoprire e che solo in parte sia stato adeguatamente sfruttato. Persistono però ancora diverse difficoltà – a livello tecnico e di interoperabilità – limiti finanziari, ostacoli istituzionali, giuridici e di policy.

a) Tecnologia. Malgrado il ritmo vertiginoso dell'innovazione tecnologica, rimangono ancora irrisolte diverse incognite di natura tecnica legate alle capacità netcentriche. Probabilmente le criticità maggiori sono quelle poste da vincoli strettamente fisici; dimensione, peso e potenza continuano a limitare il pieno sfruttamento delle capacità sia a livello di sistemi d'arma sia a livello del singolo soldato.

b) Interoperabilità. L'interoperabilità con le altre forze armate americane e con i principali partner internazionali è solo in parte un problema tecnico ed è soprattutto un problema politico. Continua ad essere una priorità a vari livelli: all'interno di ogni singola forza armata, tra le forze armate, e con i maggiori partner internazionali. Tuttavia, nonostante la retorica, a livello pratico c'è ancora molto da fare. Le forti pressioni sul bilancio sembrano incoraggiare ognuna delle forze armate a "start at home", ossia ad attribuire priorità al miglioramento dell'interoperabilità a livello interno, poi in un'ottica joint e solo in seguito in prospettiva multinazionale. Al tempo stesso ognuna di esse sembra voler confermare, per quanto possibile, la propria partecipazione alle esercitazioni internazionali (sia per ragioni militari che diplomatiche), che rimarranno probabilmente nei prossimi anni la principale occasione per lavorare sulle questioni dell'interoperabilità multinazionale. A livello di policy in materia di acquisizioni, la Difesa stabilisce che l'equipaggiamento sarà interoperabile nel suo complesso, e che quello specificatamente acquisito per determinate operazioni sarà interoperabile con tutti i partner della coalizione. Allineare gli investimenti e gli standard tra i principali Paesi rimane però una sfida da affrontare. Come ha fatto notare un ufficiale dell'Esercito americano di base in Europa, i Paesi NATO sono ancora in-

capaci di dispiegare dei dispositivi radio capaci di fornire comunicazioni dirette, in parte perché l'aspetto dell'interoperabilità a livello NATO non sembra costituire un fattore sufficientemente rilevante nelle scelte di procurement adottate a livello nazionale.

c) Ambito istituzionale. Uno dei punti cardine emersi durante l'ultimo dibattito sulla riforma è costituito dalla necessità della Difesa di adoperare un approccio più sfumato – meno "one-size-fits-all" – circa l'acquisizione di diverse tipologie di capacità militari. In ambito NEC, alcuni hanno suggerito che il sistema tradizionale può essere adatto nel caso di reti fisse ma – per altri sistemi e servici ICT – è necessario un sistema più rapido, meno rigido e quindi più flessibile. Altri invece sostengono che il sistema attuale sia praticabile se attuato in modo diverso: per esempio, alcuni centri di ricerca hanno pubblicato delle sorta di linee guida volte ad assistere il Pentagono a migliorare il suo processo di acquisizione. Prendendo atto delle sfide da affrontare, la Difesa ha preferito adottare quest'ultimo approccio, impegnandosi a utilizzare al meglio le procedure esistenti piuttosto che rielaborarle in toto. A tal fine, lo Stato Maggiore ha recentemente modificato il sistema ufficiale di acquisizione per creare una nuova "categoria" riferita ai programmi IT, consentendo una maggiore delega del potere decisionale.

I diritti di proprietà intellettuale sono un ulteriore elemento di criticità. Il Dipartimento della Difesa, sostenuto dal Congresso, è stato sempre più esplicito circa la sua intenzione di evitare l'acquisizione di sistemi con interfacce hardware e software brevettate. Tuttavia, le aziende con modelli di business strutturati su diritti di proprietà di lunga data sono restie a muoversi verso architetture più aperte, specialmente quando percepiscono che il tempo è dalla loro parte. Le aziende che hanno sviluppato componenti chiave di sistemi più complessi – i quali stanno divenendo obsoleti e necessitano di sostituzioni o aggiornamenti – devono decidere se vogliono continuare a competere per un ruolo che forse potrebbe essere minoritario col passare del tempo.

d) Livello concettuale. Come discusso poc'anzi, sia le forze armate che più in generale il Dipartimento della Difesa riconoscono sia le opportunità che le vulnerabilità associate ad una forte dipendenza dalle reti. Ciononostante non sembra emergere al momento una visione condivisa su come affrontare soprattutto le seconde, ossia le vulnerabilità. La naturale propensione delle forze armate è stata quella di difendersi, specialmente in campo cyber – aumentando la spesa per le capacità di difesa e quelle per l'infrastruttura e la progettazione di reti. In campo spaziale, tale

approccio si è tradotto piuttosto in un'attenzione più bilanciata verso l'incremento sia delle capacità di difesa sia della resilienza, in termini di payloads, satelliti e costellazioni. Nell'ambito relativo allo spettro elettromagnetico, il tradizionale filone di studi e ricerca sulla guerra elettronica ha accentuato l'attenzione sulle capacità di difesa.

e) Questioni politiche/regolamentari. Infine, come spesso accade, gli sviluppi nel campo dell'ICT evolvono in molti casi più velocemente di quanto non facciano gli "impianti" politici e regolatori che dovrebbero permettere la loro piena applicazione. Il tema dell'interoperabilità è già stato in parte discusso, ma le criticità si annidano e si estendono anche ad altri campi. Ad esempio, le politiche americane che regolano l'utilizzo delle tecnologie cloud da parte delle forze armate riflettono alcune tensioni tra i timori circa la sicurezza, l'accessibilità economica e, appunto, l'interoperabilità. Alla fine, il Dipartimento della Difesa si è orientato verso un approccio decentralizzato affinché ciascuna delle forze armate possa procurarsi autonomamente sistemi cloud digitalizzati se conformi agli standard comuni.

Un altro settore in cui i progressi tecnologici mettono a dura prova l'impianto giuridico esistente è quello relativo alle attività militari nello spettro elettromagnetico. Via via che si sviluppano nuove capacità, molti cercano di integrare le informazioni di intelligence con l'abilità di produrre effetti. Ciò crea una tensione intrinseca tra il Titolo 50 del Codice della legislazione federale degli Stati Uniti (U.S. Code), che disciplina le attività di intelligence, con il Titolo 10 che regolamenta le operazioni militari. Le operazioni di guerra elettronica sono state condotte nell'ambito del Titolo 10 ma, ad esempio, la volontà di coniugare le attività di guerra elettronica (che cercano di interrompere i segnali) con operazioni cyber (che potrebbero cercare di influenzare le informazioni all'interno di tali segnali) presenta nuove sfide di tipo giuridico che non sono ancora state pienamente esaminate, né tanto meno risolte.

In conclusione, le forze armate americane sono e saranno in futuro completamente dipendenti dalle capacità netcentriche, in ogni funzione e dominio di combattimento: aria, terra, mare, spazio e cyber. Il grado con cui le capacità netcentriche sono impiegate per scopi offensivi e difensivi varia in ogni dominio e funzione, così come il bilanciamento tra un approccio difensivo rispetto a quello "dispersivo" per mitigare le vulnerabilità loro associate. E sebbene le ICT e le capacità netcentriche abbiano trasformato le modalità di condotta, odierne e future, della guerra da parte degli Stati Uniti, rimangono ancora irrisolti molti ostacoli circa il loro

potenziale sfruttamento. Detto questo, il momento è propizio; la sfida, per l'Esercito americano e il Corpo dei Marines, sarà quella di massimizzarne i benefici minimizzando i rischi.

* * *

Il secondo capitolo offre una panoramica dei programmi di digitalizzazione ed interconnessione delle forze terrestri nei principali Paesi del Vecchio Continente, dove il punto di partenza e le ambizioni in fatto di capacità netcentriche sono parzialmente diversi dal caso americano. Francia, Germania e Regno Unito hanno intrapreso un proprio percorso per la trasformazione netcentrica delle rispettive forze armate, che è stato influenzato anche dall'esperienza nelle missioni internazionali dell'ultimo quindicennio.

Ad esempio, la Francia ha intrapreso rapidamente la digitalizzazione del livello del singolo soldato appiedato – con il programma Fantassin à Équipement et Liaisons Intégrés (FELIN) – e ha potuto sviluppare il processo in senso verticale senza la pressione di impegni operativi quali quello in Iraq ed in Afghanistan – dove Parigi ha assunto un ruolo relativamente piccolo e per un tempo limitato. Viceversa, il Regno Unito ha dovuto ricorrere ai "requisiti operativi urgenti" (Urgent Operational Requirements, UOR) per equipaggiare le proprie brigate impegnate massicciamente nei teatri iracheno ed afgano, acquisendo spesso sul mercato equipaggiamenti da diversi fornitori e complicando così la messa in rete degli assetti e la costruzione di una architettura netcentrica – senza contare il drenaggio di risorse dai programmi di procurement ordinari verso gli UOR. La Germania si è collocata in una posizione mediana rispetto ai due estremi francese e britannico, con una certa coerenza nell'impegno per la digitalizzazione delle proprie forze armate e al tempo stesso uno sforzo militare significativo e prolungato in Afghanistan (ma non in Iraq).

Quanto alla minaccia alle reti che costituiscono il sistema nervoso delle capacità netcentriche, la sicurezza cibernetica ha acquisito sempre maggiore importanza nella concezione sia britannica che francese. Entrambe le forze armate stanno sviluppando capacità non solo di difesa cibernetica ma anche di offesa, come compensazione per la riconosciuta vulnerabilità intrinseca al processo di digitalizzazione dei rispettivi strumenti militari. A tale impegno corrisponde altresì un certo attivismo dell'industria della difesa nei due Paesi. Anche la Germania si è mossa in questa direzione, soprattutto in seguito alla recente crisi in Ucraina, in particolare quanto a capacità di prevenzione ed interdizione rispetto ad attacchi cibernetici.

In termini di C2, la vicenda britannica dell'architettura di comunicazione a livello tattico Bowman è un buon esempio della difficoltà per le forze armate di tenere il passo con l'innovazione tecnologica nel campo dell'ICT. Il sistema Bowman è entrato in servizio nel 2008, dopo una lunga fase di gestazione a causa delle difficoltà di digitalizzare e mettere in rete gli assetti dell'Esercito, e nel 2015 è in via di introduzione la sua versione più aggiornata. Eppure già nel 2018 è prevista la sostituzione del Bowman con un nuovo sistema, anche noto come Morpheus, che si spera sia più facilmente aggiornabile nel tempo per restare al passo con gli sviluppi dell'ICT. In Francia, il programma Synergie du COntact Renforcé par la Polyvalence et l'InfovalorisatiON (SCORPION) adotta un approccio centralizzato e integrato all'acquisizione di veicoli, sistemi d'arma e di comunicazione al fine di ottenere capacità netcentriche. In parallelo, tuttavia, viene finanziato l'ammodernamento dell'attuale architettura di comunicazione, il Système d'Information et de Combat SCORPION (SICS), per mantenere operativi i veicoli che non saranno riconfigurati in ambito SCORPION. Il combinato dei due programmi cerca sostanzialmente di bilanciare il bisogno di tenere il passo con l'ICT con l'impossibilità di poter rimpiazzare tout court gli equipaggiamenti già in uso (il c.d. asset legacy) dall'Esercito francese. Anche la Germania ha dovuto affrontare problemi simili. Il programma Infanterist der Zukunft (IdZ) di digitalizzazione degli equipaggiamenti del singolo soldato – l'equivalente del FELIN francese – è iniziato nel 2004, ma ha visto la consegna del primo lotto di prodotti solo nel 2012, lotto che si è rivelato per certi versi obsoleto a causa del rapido avvento dei dispositivi smartphone. Al tempo stesso, il fatto che i veicoli dell'Esercito tedesco siano nuovi o in fase di acquisizione è un fattore positivo nella misura in cui sono già disegnati per soddisfare le esigenze netcentriche.

In generale, in tutti e tre i Paesi si è adottato un approccio più cauto rispetto agli Stati Uniti nella digitalizzazione delle forze terrestri, anche a causa dei limiti di bilancio e/o delle esigenze di breve periodo legate alle operazioni in corso. Tuttavia, gli stessi Paesi hanno riconosciuto l'importanza delle capacità netcentriche, in particolare del dominio cyber, investendo ingenti risorse economiche nell'affrontare le difficoltà che la trasformazione netcentrica comporta, in termini di asset legacy, interoperabilità, e obsolescenza dei sistemi acquisiti anche a causa della lentezza del loro processo di sviluppo, produzione ed entrata in servizio.

* * *

Il terzo capitolo di questo Quaderno fornisce una panoramica di Forza NEC, il programma di procurement guidato dall'EI ed iniziato nel 2007, che mira alla creazione di un'architettura netcentrica in grado di fornire una condizione di "superiorità dell'informazione" attraverso la digitalizzazione della forza armata. Forza NEC intende soddisfare le esigenze operative dell'Esercito attraverso l'acquisizione di determinati assetti e/o l'ammodernamento di quelli già in suo possesso, adottando un approccio molto mirato: infatti, ha intrapreso una significativa fase di sviluppo e sperimentazione – fase in cui Forza NEC si trova tuttora – per validare soluzioni tecnologiche ai requisiti operativi che man mano vengono dettagliati, anche tramite un dialogo tra forza armata ed industria.

Soprattutto dalla fine della Guerra Fredda in poi, le forze armate italiane hanno assunto dei compiti che sono andati al di là della sola protezione dell'integrità territoriale dello stato, nella fattispecie compiti relativi alla prevenzione, gestione e risoluzione di crisi internazionali. Nelle ultime due decadi, l'Esercito ha impiegato mediamente 9.000 unità in missioni internazionali e 4.000 in operazioni nazionali, con punte complessive di 19.000 soldati contemporaneamente impiegati nei teatri operativi. L'EI è dal punto di vista quantitativo la forza armata maggiormente dispiegata in operazioni, fornendo circa il 75% dei militari italiani complessivamente impiegati in teatro. Nel 2014, l'Esercito è stato impiegato in due operazioni sul territorio nazionale e in dodici missioni all'estero, con un totale di 10.361 soldati coinvolti. Se si volesse generalizzare in estrema sintesi quelle che sono state, e sono attualmente, le necessità principali dell'Esercito, le missioni in teatro hanno evidenziato che in futuro sarà auspicabile: sviluppare un'architettura di C2 in grado di convogliare le informazioni a supporto di un processo decisionale più tempestivo ed efficace; ampliare la capacità di aggiornamento in tempo reale della situazione in teatro attraverso sofisticate capacità di intelligence; potenziare tutte le nuove piattaforme con sistemi di protezione attiva e passiva.

In futuro l'Esercito continuerà ad avere un ruolo fondamentale a sostegno della politica di difesa nazionale, a maggior ragione a fronte del deterioramento del contesto di sicurezza in cui si trova l'Italia. In riferimento ai possibili scenari di impiego futuri, sembra più probabile che l'Esercito sarà impiegato in missioni internazionali in contesti operativi affini a quelli dove la forza armata ha operato negli ultimi 25 anni. Le aree situate nell'immediato vicinato dell'Italia – Nord Africa e Africa sub-sahariana, Medio Oriente, Europa Orientale e Caucaso – sembrano particolarmente inclini a questo tipo di situazioni, aree dove prevalgono ancora regimi non pienamente de-

mocratici e dove sono tuttora presenti "conflitti congelati". Questa opzione sembra più probabile rispetto a quella, comunque non escludibile, della protezione dello spazio atlantico da minacce dirette, viste le condizioni attuali in cui versa la Libia ed il permanere della crisi in Ucraina.

I primi segnali dell'interesse italiano verso la capacità netcentrica vennero espressi nel Concetto Strategico del Capo di Stato Maggiore della Difesa nel 2005. Alla luce anche della rapida evoluzione dei processi di ammodernamento dello strumento terrestre negli altri Paesi NATO, nel gennaio 2007 prendeva avvio lo studio del programma Forza NEC, che si delineava come programma interforze a guida dell'Esercito. La digitalizzazione delle forze armate rappresenta il primo passo verso la realizzazione di un sistema netcentrico, ovvero l'integrazione in un sistema C4I di sistemi e tecnologie per acquisire, scambiare, mettere in correlazione e utilizzare nel momento appropriato le informazioni ottenute durante le varie fasi di un'operazione. Questo processo di raccolta delle informazioni permette di acquisire una "Shared Situational Awareness", ossia "la conoscenza della situazione operativa tra le forze". È attraverso la Shared Situational Awareness che è possibile acquisire la cosiddetta "Information Superiority" – la superiorità delle informazioni – la quale rappresenta un moltiplicatore di forza, un elemento chiave nel raggiungimento del successo, soprattutto nel quadro di operazioni interforze e multinazionali.

Inoltre Forza NEC, nell'indicare "la via" per la digitalizzazione dei sistemi, si pone come catalizzatore di altri programmi in essere, andando ad intervenire sia sugli aggiornamenti di programmi consolidati sia sulla definizione delle specifiche tecniche per quelli non ancora avviati. Anche per questo, il programma Forza NEC è un programma di procurement sui generis, in quanto i suoi esiti andranno a influire e confluire nell'ambito più generale dell'ammodernamento dell'EI. A dimostrazione di ciò, esso coinvolge e fa convergere al suo interno altri programmi come il SIACCON (Sistema Automatizzato di Comando e Controllo), il SICCONA (Sistema di Comando, Controllo e Navigazione), il BFSA (Blue Force Situational Awareness) e Soldato Futuro.

Inizialmente la durata prevista del programma era stata stimata in 25 anni, dal 2007 al 2031. Tuttavia la natura stessa dei finanziamenti, che ha visto l'approvazione degli stanziamenti solo per la fase di sviluppo e sperimentazione di concetti (Concept Development & Experimentation, CD&E), unita ad una serie di complicazioni di natura tecnico-tecnologica, ha successivamente condizionato in maniera significativa lo sviluppo e l'attuazione del programma.

Lo scopo primario della CD&E è effettuare una serie di test per valutare attentamente quelle tecnologie che saranno alla base della digitalizzazione dell'Esercito. In altre parole, la fase di CD&E mira a fornire le capacità necessarie per testare e validare l'architettura della forza digitalizzata attraverso la realizzazione su piccola scala di tutti i principali componenti dell'architettura NEC. Ciò nonostante, la natura stessa della fase CD&E – sperimentazione e sviluppo concetti appunto – ha comportato alcune problematiche da un punto di vista amministrativo e tecnico che hanno prodotto un allungamento dei tempi del programma, giudicato però prevedibile sia dalla Difesa che dalla controparte industriale. Per questo motivo la sua fine è oggi fissata indicativamente al 2020. Dall'altra parte, invece, due note positive della fase di CD&E si sono registrate nel dialogo venutosi a creare fra la Difesa e l'Industria e nell'identificazione di un primo insieme di sistemi e strumenti maturi per un'eventuale loro produzione.

Nel 2006 il costo totale del programma Forza NEC era stato stimato dal comparto industriale attorno ai 22 miliardi di euro. Tale stima era da considerarsi puramente indicativa perché antecedente alla fase stessa di CD&E, e quindi volta a definire l'ordine di grandezza economica dell'intero programma di ammodernamento. Ad oggi, il costo complessivo del programma Forza NEC per le finanze pubbliche ammonta a 815 milioni di euro, considerando i 15 milioni per la fase di Project Definition (PD) e i circa 800 milioni per la fase di CD&E.

Il programma Forza NEC presenta molte sfide che, se affrontate positivamente, possono tramutarsi in opportunità da sfruttare. Fra queste sfide/opportunità le maggiori sono:

1) produzione degli assetti frutto della CD&E;
2) formazione e addestramento delle forze armate;
3) asset legacy;
4) interoperabilità interforze;
5) gestione dei dati in teatro;
6) sicurezza cibernetica.

La produzione degli assetti frutto della CD&E rappresenta la vera incognita del programma per via delle importanti decisioni che si dovranno assumere rispetto alla produzione – e quindi all'acquisto – dei sistemi, assetti e piattaforme sviluppati da Forza NEC entro il 2020. Le risorse limitate di cui dispone attualmente la Difesa impediscono di poter pianificare con estrema certezza in che modalità, e in quali quantità, si passerà

dallo sviluppo e produzione di modelli pre-serie alla fase di produzione di modelli in serie di determinati assetti. Ciononostante, da un punto di vista operativo, ma anche finanziario e industriale, appare evidente quanto sia necessario dare seguito alla fase di ricerca e sperimentazione con un piano di industrializzazione, per soddisfare le esigenze delle Forze armate e non rendere la fase di CD&E un esercizio fine a se stesso.

La digitalizzazione dell'EI e la sfida netcentrica coinvolgono l'organizzazione dell'Esercito in tutte le sue parti, e questo non esclusivamente da un punto di vista di scelte legate all'acquisto di nuove tecnologie, ma anche riguardo a modifiche sostanziali nella formazione e nell'addestramento del personale. L'addestramento dovrà per forza di cose riprodurre nella maniera più realistica possibile gli scenari di impiego più probabili e preparare il soldato ad affrontare le complesse minacce future, anche considerando il venire meno dell'impegno in un teatro operativo come quello afgano. In quest'ottica, il Sistema Integrato di Addestramento Terrestre (SIAT) ha un grande potenziale di sinergie con l'ITB (Integration Test Bed), per assicurare un adeguato training dell'EI rispetto alla tecnologia netcentrica.

Forza NEC pone delle sfide legate ad alcune questioni "strutturali" del programma stesso, quali la notevole durata e la complessità tecnologica del processo di digitalizzazione, in particolare rispetto all'asset legacy. In termini procedurali, per rendere netcentrici i mezzi e i sistemi dell'EI si è deciso di aggiornare alcuni degli equipaggiamenti attualmente a disposizione della forza armata agli standard netcentrici, in attesa che questi siano successivamente sostituiti da nuovi assetti che incorporino sin dalla fase di design la tecnologia netcentrica. Di conseguenza, nella fase di CD&E di Forza NEC saranno presenti all'interno dell'EI sia sistemi aggiornati che verranno poi sostituiti alla fine del loro ciclo di vita operativo, sia nuovi sistemi con tecnologie netcentriche già incluse. Qualche timore in più desta la gestione dell'obsolescenza dei nuovi sistemi portati alla luce dell'attuale CD&E, data la rapidità con cui successive innovazioni tecnologiche renderanno non più allo stato dell'arte sistemi che comunque sono stati prodotti relativamente di recente. Per ovviare al problema, durante la fase di sperimentazione e prototipazione i sistemi dovrebbero essere configurati secondo una "architettura aperta", in grado cioè di recepire le repentine evoluzioni tecnologiche derivanti dallo sviluppo del mondo ICT.

Un'altra sfida di carattere tecnico è rappresentata dalla necessità di garantire l'interoperabilità fra le forze armate italiane alla fine del processo di digitalizzazione dell'Esercito, ovvero che le piattaforme e gli

assetti utilizzati da quest'ultimo, dalla Marina e dall'Aeronautica siano messi nelle condizioni di comunicare e interagire fra di loro e con quelli di altri stati alleati dell'Italia. Proprio per questo, il design e lo sviluppo dell'architettura netcentrica ha prefigurato la definizione di componenti specifici con il fine di supportare l'interoperabilità fra forze armate nazionali ed internazionali.

La possibilità di mettere in rete e far comunicare fra di loro una quantità ingente di nodi costituisce un'altra importante problematica da affrontare. Questo problema è intrinseco al programma stesso, che mira a connettere in uno spazio virtuale migliaia di elementi. L'Esercito deve da un lato partire da un livello di digitalizzazione più basso rispetto alle altre due forze armate, e dall'altro rendere netcentrici una quantità di elementi di molto superiore rispetto a Marina e Aeronautica. Affrontata l'incognita della messa in rete di migliaia di sensori, si pone l'ulteriore quesito di come elaborare l'ingente quantità di dati che da essi giungeranno. Attualmente sono in fase di sperimentazione alcuni software in grado di elaborare i dati provenienti sul terreno in maniera "intelligente", ovvero di raccogliere le informazioni provenienti da punti critici evitando di intasare la catena di comando con informazioni non totalmente rilevanti.

Infine, quanto alla sicurezza cibernetica, ovviamente il programma Forza NEC nasce in un contesto fortemente influenzato dagli sviluppi dell'ICT. Se attraverso la tecnologia netcentrica si mira a raggiungere l'Information Superiority tramite la comunicazione dei dati fra i vari nodi della rete, bisogna porsi il problema di come intervenire qualora queste informazioni vengano intercettate o la rete venga manomessa da nemici. In un sistema con migliaia di sensori, ogni "nodo" può diventare un elemento di vulnerabilità. Similmente, qualora non si avessero dei mezzi avanzati per contrastare efficacemente i pericoli derivanti dalla guerra elettronica si rischierebbe di rendere più vulnerabile una forza armata. Per questo l'approccio "Information Security Engineering" ha avuto l'obiettivo di rendere i sistemi più robusti e sicuri di fronte a possibili minacce informatiche. Oltretutto, la sicurezza è ulteriormente incrementata grazie ad attività di "security hardening" successive a valutazioni dei sistemi di sicurezza informatica in teatro. Inoltre, si è voluto promuovere alcune componenti tecnologiche innovative atte a gestire l'interconnessione tra domini a seconda del diverso livello di classificazione dell'informazione.

In conclusione, l'ammodernamento netcentrico della componente terrestre dello strumento militare italiano è una necessità imprescindibile. Gli investimenti in tecnologia permetterebbero la sostituzione dei ma-

teriali logorati dalle operazioni in teatro operativo, una razionalizzazione delle risorse e una protezione maggiore del soldato. Di conseguenza, quella che oggi è una realtà – ossia una stretta collaborazione che vede Difesa e Industria e lavorare fianco a fianco sin dalla fase di analisi delle esigenze e di concezione dei discendenti sistemi – si spera si consoliderà sempre più in futuro per consentire allo strumento militare di essere in linea con i progressi tecnologici delle altre forze armate, mantenendo i costi su un binario sostenibile, in un'ottica di condivisione degli sforzi in ambito europeo e NATO.

* * *

Infine, alla luce dell'analisi svolta nei suddetti tre capitoli, le conclusioni dello studio prendono in considerazione la portata della rivoluzione dell'ICT e valutano se, come e quanto le forze armate italiane, e dei principali Paesi NATO considerati nel Quaderno, stiano riuscendo a cogliere le opportunità offerte dall'ICT e a gestirne i rischi connessi. L'assunto di base è che la tecnologia non è e non può diventare la soluzione a tutti i dilemmi di sicurezza, in quanto il futuro ambiente operativo sarà ancora caratterizzato dalla dimensione umana che alberga in ogni conflitto. Se è vero che la tecnologia non è di per sé sufficiente per raggiungere gli obiettivi militari di un Paese come l'Italia, è altrettanto vero che è assolutamente necessaria – una vera e propria conditio sine qua non. In particolare, oggi e nel prossimo futuro, la trasformazione netcentrica delle capacità militari rappresenta un passaggio irrinunciabile per mantenere l'operatività e l'efficacia delle forze armate.

Prefazione

Come giustamente evidenziato dalle conclusioni di questo Quaderno, l'evoluzione delle forze armate italiane, ed in particolare dell'Esercito, concretizzata nel programma Forza NEC, ancorché non sufficiente a garantire l'efficacia dello strumento militare nazionale, è assolutamente necessaria e, nel caso inverosimile che non vada in porto, nessun 'Libro Bianco' o riforma della governance della Difesa potrebbero rendere utilmente impiegabile questo elemento essenziale della sovranità nazionale.

Appare infatti chiaro che la progressiva riduzione numerica delle forze armate nazionali, che va di pari passo con quanto avviene nei Paesi alleati ed amici, sia in ambito NATO che in quello dell'Unione Europea, pone un problema di adeguatezza di fronte a ipotesi di minaccia proveniente da attori che non hanno problemi 'quantitativi', e che la risposta deve basarsi su una serie di elementi tra cui la tecnologia è uno di quelli fondamentali. In altre parole, la demografia ci dice che uno dei fattori essenziali della potenza militare, la 'massa', non sarà mai più a nostro favore e che pertanto, se non vogliamo soccombere in un ipotetico futuro conflitto o in qualsiasi altra circostanza che veda l'impiego della forza militare, dobbiamo necessariamente dotarci degli strumenti offerti dalla tecnologia che rientrano nella categoria dei moltiplicatori di forze. Come conseguente corollario, occorre che adeguate risorse dovranno essere dedicate alla ricerca applicata, al fine di mantenere sempre un vantaggio tecnologico sui potenziali avversari.

L'applicazione dell'ICT alle strutture militari e, per quanto concerne l'analisi condotta dal Quaderno, il programma Forza NEC dell'Esercito Italiano, rispondono esattamente a questa imprescindibile esigenza. La decisione dell'avvio di questo percorso è stato quindi un atto lungimirante, pur nella consapevolezza dell'impegno finanziario e tecnologico cui si andava incontro. Un po' meno lungimirante, invece, è stata l'incapacità di trovare una comunalità di requisiti con gli eserciti di altri Paesi alleati che avevano analoga visione. Ma tale questione è così rilevante da meritare trattazione a parte in altra sede: basti qui sottolineare che i Paesi europei

e l'UE in quanto tale hanno perso un'ulteriore straordinaria occasione per fare un passo avanti verso l'integrazione, negandosi le economie di uno sviluppo comune e complicandosi la vita con gli inevitabili futuri problemi di interoperabilità.

È chiaro che siamo ancora solo agli inizi dello sforzo tecnico e finanziario necessario per cogliere i frutti del programma Forza NEC, sforzo che, a compimento, si rivelerà il più oneroso tra quelli intrapresi dalla Difesa negli ultimi anni. Si tratta di uno sforzo la cui realizzazione e il cui successo dipenderanno in larga misura dalla capacità industriale di sviluppare sistemi realmente aperti, che possano man mano incorporare i progressi che la tecnologia offrirà nel tempo, dal momento che l'orizzonte temporale comprende e supera il prossimo decennio.

Merita ancora una riflessione il tema culturale. Una forza netcentrica è, e sempre più sarà, ben più di un insieme di sistemi d'arma più moderni, sicuri, efficaci e precisi, ma come bene esemplificato dal concetto dello "Strategic Corporal", comporterà una vera e propria 'degerarchizzazione' delle strutture militari, in quanto l'uomo (o la donna) sul campo, ben preparato ed educato ad assumere responsabilità e consapevole delle finalità della sua azione, sarà in grado di prendere efficacemente decisioni finora riservate ai superiori livelli gerarchici. L'Esercito che maturerà questi concetti potrà conseguire i risultati voluti. Al contrario, chi rimarrà ancorato alle procedure del passato e non saprà sfuggire alla diabolica tentazione del micro-management, reso ampiamente possibile dai nuovi sistemi sviluppati con l'applicazione dell'ICT al mondo militare, rischia di fare la fine dei generali francesi durante la Seconda Guerra Mondiale ricordati nelle conclusioni del quaderno, irrimediabilmente sconfitti sulle poderose fortificazioni della linea Maginot.

Vincenzo Camporini
Vicepresidente IAI

Lista degli acronimi

A2/AD	Anti-Access/Area Denial
ACV	Amphibious Combat Vehicle
AD	Amministrazione Difesa
AEHF	Advanced Extremely High Frequency
AFATDS	Advanced Field Artillery Tactical Data System
ALAT	Aviation Légère de l'Armée de Terre
AMPV	Armored Multi-Purpose Vehicle
AOC	Army Operating Concept
BatCIS	Battlefield Tactical Communications and Information System
BCIP	Bowman and Combat and Information and Platform
BFSA	Blue Force Situational Awareness
BIGSTAF	Breitbandiges IntegriertesGefechtsSTAndFernmeldenetz
BISA	Battlefield Information Systems Applications
BIT	Brigata Integrata Terreste
BMI	Bundesministerium des Innern
BND	Bundesnachrichtendienst
BTID	Battlefield Target Identification Device
C2	Command and Control
C2I	Command, Control, Intelligence
C2N	Command, Control and Navigation
C2PC	Command and Control Personal Computer
C4I	Command, Control, Communications, Computers and Intelligence
C4ISTAR	Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition, Reconnaissance
CAC2S	Common Aviation Command and Control System
CALID	Centre d'analyses en lutte informatique défensive

CANES	Consolidated Afloat Networks and Enterprise Services
CAP	Common Air Picture
CD&E	Concept Development and Experimentation
CDR	Critical Design Review
CEC	Cooperative Engagement Capability
CEMA	Cyber Electromagnetic Activities
CEMP	Capacité d'Engagement Multi Plates-Formes
Ce.Si.Va.	Centro di Simulazione e Valutazione dell'Esercito
CEWCC	Cyber and Electronic Warfare Coordination Cell
CFI	Connected Force Initiative
CIA	Capabilities Integration Assessment
CID Server	Combat Identification Server
CIS	Communication and Information Systems
CMF	Cyber Mission Force
COMCEPT	COMplément de Capacités en Elongation, Projection et Théâtre
CONTACT	Communications Numériques Tactiques et de Théâtre
COP	Common Operational Picture
DARPA	Defense Advanced Research Projects Agency
DCGS	Defense Common Ground System
DCPP	Defence Cyber Protection Partnership
DGA	Délégation Générale pour l'Armement
DII-LD	Defence Information Infrastructure - Land Deployable
DISA	Defense Information Systems Agency
DNA	Direzione Nazionale degli Armamenti
DSB	Defense Science Board
EI	Esercito Italiano
EF	Expeditionary Force
EMARSS	Enhanced Medium Altitude Reconnaissance and Surveillance System
EMS	Electromagnetic Spectrum
EMPs	Electromagnetic Pulse
ESB	Enterprise Services Bus
ESCPC	European Satellite Communication Procurement Cell

FAC	Forward Air Controller
FAS	Functional Area Services
FCS	Future Combat System
FIST	Future Infantry Soldier Technology
FELIN	Fantassin à Équipement et Liaisons Intégrés
FMN	Federated Mission Network
G/ATOR	Ground/Air Task Oriented Radar
GBA	Generic Base Architecture
GCSS	Global Command Support System
GCHQ	Government Communications Headquarters
GdP-TT	Gruppo di Progetto Trasformazione Terrestre
GDUK	General Dynamics UK
GIP	Gruppi Integrati di Progetto
GIS	Geographic Information System
GPS	Global Positioning System
GrATS	Ground Asset Tracking System
GSA	Generic Soldier Architecture
GTIA	Groupements Tactiques Interarmes
GTWLFD	Gateway della Landing Force Digitalizzata
GVA	Generic Vehicle Architecture
HCDR	High Capacity Data Radio
HeATS	Helicopter Asset Tracking System
HF	High Frequency
HMT	Helicopter Mission Trainer
ICC	Integrated Command and Control
ICT	Information and Communication Technology
IdZ	Infanterist der Zukunft
IdZ-ES	Infanterist der Zukunft Erweitertes
IEDs	Improvised Explosive Devices
IOC	Initial Operating Capability
IoE	Internet of Everything
IP	Internet Protocol
ISAF	International Security Assistance Force

ISAF HQ	ISAF Headquarter
ISAF JC HQ	ISAF Joint Command Headquarter
ISAF SOF HQ	ISAF Special Operation Forces Headquarter
IT	Information Technology
ITB	Integration Test Bed
JBC-P	Joint Battle Command-Platform
JIE	Joint Information Environment
JLTV	Joint Light Tactical Vehicle
JPADS	Joint Precision Air Drop Systems
JRD	Joint Regional Detachment
JSF	Joint Strike Fighter
JSTARS	Joint Surveillance and Target Attack Radar System
JTAC	Joint Terminal Attack Controllers
JTRS	Joint Tactical Radio System
JUICE	Joint Users Interoperability Coalition Exercise
KFOR	Kosovo Force
LEAPP	Land Environment Air Picture Provision
LETacCIS	Land Environment Tactical Communications and Information System
LFD	Landing Force Digitalizzata
LOSA	Land Open Systems Architecture
4G LTE	Quarta Generazione Long Term Evolution
LRS-B	Long-Range Strike Bomber
M&S	Modeling and Simulation
MCCIS	Maritime Command and Control Information System
MILS	Multiple Independent Levels of Security
MIP	Multilateral Interoperability Programme
MiSE	Ministero dello Sviluppo Economico
MLRS	Multiple Launch Rocket System
MND-SE	Multi-National Division South-East
MSU	Multinational Specialized Unit
NATO	North Atlantic Treaty Organization
NATO HQ	NATO Headquarters
NATO NTM-A	NATO Training Mission - Afghanistan

NCIRC	NATO Computer Incident Response Centre
NEC	Network Enabled Capability
NG	Next Generation
NIE	Network Integration Evaluation
ONU	Organizzazione delle Nazioni Unite
OSCE	Organization for Security and Co-operation in Europe
PC	Posto Comando
PD	Project Definition
PFI	Private Finance Initiative
PIM	Paladin Integrated Management
PNT	Positioning, Navigation and Timing
PO	Project Office
PRR	Personal Role Radio
RAF	Royal Air Force
RAP	Recognised Air Picture
RFID	Radio-frequency IDentification
RITA	Réseau Intégré des Transmissions Automatiques
RMP	Recognised Maritime Picture
RPAS	Remotely Piloted Aerial Systems
RSTA	Reconnaissance Surveillance and Target Acquisition
SAIM-NG	Système d'Aide à l'Interprétation Multi-capteurs
SATCOM	Satellite Communication
SCA	Software Communications Architecture
SCORPION	Synergie du COntact Renforcé par la Polyvalence et l'InfovalorisatiON
SDR	Software Defined Radio
SDSR	Strategic Defence and Security Review
SEGREDIFESA	Segretariato Generale della Difesa
SIACCON	Sistema Automatizzato di Comando e Controllo
SIAT	Sistema Integrato di Addestramento Terrestre
SICCONA	Sistema Integrato di Comando Controllo e Navigazione
SICF	Système d'Information pour le Commandement des Forces
SICS	Système d'Information et de Combat SCORPION

SIR	Système d'Information Régimentaire
SitComDé	Système d'information terminal du Combattant Débarqué
SIT-ALAT	Système d'Information Terminal de l'ALAT
SMD	Stato Maggiore della Difesa
SME	Stato Maggiore dell'Esercito
SOP	Standing Operating Procedures
SOTM	SATCOM-On-The-Move
SBIRS	Space-Based Infrared System
SVFFuA	StreitkräftegemeinsameVerbundfähigeFunkgeräteausstattung
TAAC-W	Train Advise Assist Command-West
TCN	Tactical Communications Networking
TENCAP	Tactical Exploitation of National Capabilities
TG	Task Group
TRADOC	Training and Doctrine Command
TSMPF	Tenue de Situation Multi Plates-Formes
TTP	Tactics, Techniques & Procedures
UAV	Unmanned Air Vehicle
UGV	Unmanned Ground Vehicles
UNIFIL	United Nations Interim Force in Lebanon
UOR	Urgent Operational Requirements
US	United States
WGS	Wideband Global SATCOM
WIN-T	Warfighter Information Network-Tactical
VMF	Variable Message Format
VTLM	Veicolo Tattico Leggero Multiruolo
VTMM	Veicolo Tattico Medio Multiruolo

1.

Forze armate americane e capacità netcentriche: alla ricerca di un equilibrio

Maren Leed

1.1 Il dibattito americano sulle Network Enabled Capabilities (NEC)

Qualcuno potrebbe sostenere che la Difesa americana intrattenga una sorta di relazione alquanto schizofrenica con l'idea di network-centric warfare. I fautori delle forze terrestri in particolare hanno storicamente opposto resistenza alla concezione secondo cui i progressi nell'Information and Communications Technology (ICT) abbiano generato o determineranno in futuro una "revolution in military affairs". Tuttavia, l'ICT costituisce per molti aspetti la base dei concetti militari e dei piani di ristrutturazione delle forze armate statunitensi, a maggior ragione in un contesto di riduzione degli stanziamenti finanziari destinati alla Difesa americana. A livello strategico, il dibattito riguarda soprattutto se l'ICT presenti circostanze che alterino fondamentalmente la natura stessa della guerra. A livello operativo, ovvero in termini di concetti, dottrina e procurement, il consenso è invero più ampio sul fatto che l'ICT offra significative capacità che sono sempre più centrali nelle future attività militari americane.

Sebbene le capacità netcentriche originate dai progressi ICT stiano diventando fondamentali per il futuro delle forze armate degli Stati Uniti, è altresì generalmente riconosciuto che le reti in sé presentano delle significative vulnerabilità. Nello specifico, l'interesse è alquanto marcato nel campo della cyber defense, anche alla luce delle sempre più evidenti tensioni tra il desiderio di sfruttare tutte le opportunità che le capacità netcentriche sono in grado di offrire e il timore che questa dipendenza porti con sé i semi di una eventuale e futura debacle[1].

[1] Si veda ad esempio, US Dept of Defense, *Quadrennial Defense Review 2014*, March

Secondo le parole di un funzionario del Dipartimento della Difesa

> [Gli Stati Uniti] hanno speso centinaia di miliardi di dollari lavorando [su comunicazioni] e [intelligence, sorveglianza e ricognizione] e sistemi d'arma che nessuno può eguagliare…ma il problema con quei sistemi è che…per quanto avanzati, sono tanto vulnerabili quanto le reti che li connettono[2].

Il riconoscimento della necessità impellente di difendere il complesso sistema di reti è stato sottolineato per diversi anni, motivo per cui le misure adottate per mitigarne le eventuali vulnerabilità sono piuttosto numerose e variegate. Viceversa, sebbene i tentativi di sfruttare il potenziale offensivo delle capacità netcentriche non sembrino così ben coordinati ed efficaci, i vertici dell'establishment americano sono fortemente impegnati per far leva sulle tecnologie ICT e le capacità netcentriche come parti integranti delle future operazioni militari.

Tale consenso si è rafforzato con il progredire delle guerre in Iraq e in Afghanistan. Malgrado lo schieramento di capacità netcentriche sia stato eterogeneo in ognuna di queste operazioni, le esigenze emerse in entrambi i conflitti ne hanno accelerato il loro impiego nonché il loro sviluppo. Prima dell'inizio dell'Operazione Enduring Freedom in Afghanistan, l'interesse nelle capacità netcentriche era piuttosto limitato, e tendeva a focalizzarsi soprattutto sulle reti cablate. Il rapido sviluppo commerciale da una parte e il pieno impegno in operazioni militari complesse e asimmetriche dall'altra, hanno fondamentalmente alterato il rapporto tra ICT e capacità netcentriche per le forze armate degli Stati Uniti.

Quest'ultime complessivamente sono ampiamente interessate nello sfruttare le reti sia cablate che wireless, e nel comprendere adeguatamente le implicazioni di queste attività nel contesto delle operazioni all'interno dello spettro elettromagnetico (Electromagnetic Spectrum, EMS). Le tecnologie ICT e le capacità netcentriche sono così divenute profondamente e irrevocabilmente radicate nelle operazioni militari statunitensi che il dibattito in corso ruota attorno a "come" esse possano essere utilizzate più efficacemente, piuttosto che sul "se" impiegarle o meno.

2014, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf; US Dept of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2012, http://www.defense.gov/news/ Defense_Strategic_Guidance.pdf.

[2] Jordana Mishory, "Official: DoD needs to better coordinate, oversee electronic warfare efforts", in *InsideDefense.com*, 15 October 2014.

Questo capitolo fornisce una breve panoramica su alcuni passi fondamentali che le forze armate americane, in particolari quelle terrestri, stanno adottando per sviluppare l'utilizzo delle capacità netcentriche in ognuna delle sei "funzioni di combattimento" delineate nella dottrina interforze degli Stati Uniti. Queste funzioni sono state concepite per rispecchiare gli elementi fondamentali che sarebbero richiesti per sviluppare un piano o un'attività militare volto ad assicurare un insieme completo e integrato di forze. Mentre ognuna delle forze armate fa proprie terminologie leggermente differenti, il quadro di riferimento della dottrina interforze[3] le descrive nel seguente modo:

1. Comando e Controllo (C2) o, come lo chiama l'Esercito, comando di missione. In termini generali, l'acronimo C2 si riferisce alla capacità di indirizzare le forze verso un obiettivo comune;
2. Intelligence, o la capacità di raccogliere, sintetizzare e distribuire informazioni sull'ambiente operativo attraverso mezzi sia tecnici (come signals intelligence) e non tecnici (human intelligence);
3. Fuoco, o la capacità di produrre in maniera precisa "effetti" sul bersaglio desiderato (che potrebbe essere una struttura, un'organizzazione, un individuo, ecc.) siano essi cinetici (fisici) o non-cinetici (come la guerra elettronica o le operazioni psicologiche);
4. Movimento e manovra, o il movimento pianificato e disciplinato delle forze militari verso un obiettivo;
5. Protezione, o l'abilità di evitare e/o difendersi da attacchi, sia cinetici che non-cinetici. Questo può riferirsi ad individui, unità, basi, equipaggiamento, ecc.;
6. Supporto, o l'abilità di fornire alle forze sul campo ogni tipo di fornitura nel tempo (come cibo, munizioni, parti di ricambio, ecc.).

Le reti – siano esse cablate, wireless, space-based e terrestri – ricoprono un ruolo fondamentale in ognuna di queste funzioni. Ci sono decine di programmi, sia interforze che a livello di singola forza armata, volti a fornire capacità in una o più di queste suddette funzioni. Infatti, delle sette aree prioritarie elencate nella richiesta di bilancio del Dipartimento della Difesa per l'anno fiscale 2015, quella relativa alle attività cyber rappresentava la priorità principale. Ciascuna delle sei rimanenti – difesa missilistica; deterrenza nucleare; spazio; attacchi di precisione; intelligence, sorveglianza e ricognizione; contro-terrorismo e ope-

[3] US Dept of Defense, Chairman of the Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operations*, 11 August 2011, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

razioni speciali – supportano o dipendono dalle capacità netcentriche.

Dal momento in cui le tecnologie ICT hanno sviluppato e creato la premessa alle capacità netcentriche, esse hanno presentato sia un'opportunità che una sfida. L'opportunità consiste nell'incrementare non solo le capacità delle singole piattaforme, ma anche quelle tra le piattaforme. Una delle sfide invece è infondere tale potenziale a tutto l'insieme degli equipaggiamenti militari, straordinariamente ampio e complesso. L'Esercito americano dispone di oltre diecimila veicoli da combattimento ed elicotteri. Sostituire o ammodernare quei sistemi affinché essi possano incorporare architetture netcentriche richiede una spesa ingente, e in alcuni casi risulta tecnicamente impossibile e inefficiente. La Difesa si trova attualmente in una posizione in qualche modo paradossale. Da una parte, i tagli di bilancio rendono la transizione verso flotte net-enabled molto più ardua e complessa ma, dall'altra, tale transizione risulta ancora più necessaria dal momento che gli stessi tagli – riducendo il volume degli assetti militari – richiedono una maggiore produttività degli equipaggiamenti rimasti in servizio.

Ognuna della quattro forze armate adotta un approccio alquanto simile per raggiungere un adeguato equilibrio tra le risorse e l'incremento di capacità. Sebbene il finanziamento per i nuovi programmi sia costantemente in diminuzione, ogni nuovo progetto sarà disegnato per essere net-enabled, con un'architettura aperta che consenta i necessari aggiornamenti di capacità alla luce dei continui progressi nel campo dell'ICT. L'equipaggiamento esistente viene continuamente riaggiornato per fornire, in alcuni casi, un supporto sufficiente per ottenere un maggior collegamento tra i diversi sistemi e, in altri, per incorporare direttamente capacità più aggiornate.

Quelle versioni per cui sarebbe inefficiente o impossibile realizzare sistemi netcentrici, vengono rapidamente dismesse. L'Aeronautica e la Marina stanno tentando di uniformare i principali, rispettivi, sistemi d'arma, riducendo ad esempio il numero di versioni delle unità navali e di velivoli e puntando a raggiungere una capacità equivalente attraverso la loro piena connessione NEC. Il Corpo dei Marines e l'Esercito, che dispongono tipicamente di un ampio ventaglio di equipaggiamenti, devono disporre necessariamente di piattaforme simili ma con differenti livelli di capacità, con il rischio di generare criticità in termini di interoperabilità tra le loro stesse unità nel caso di operazioni su larga scala. L'intento è minimizzare il più possibile queste differenze ma le restrizioni finanziarie hanno costretto, in particolar modo l'Esercito, a orientarsi più decisamente verso

una strategia di aggiornamento incrementale attraverso molteplici programmi, con ovvie differenze nelle varie unità. Nel complesso comunque, il desiderio dell'Esercito di evolversi da sistema "stand alone a networked"[4] è condiviso dall'intera forza armata statunitense, e l'intero establishment militare si muove in questa direzione.

1.2 I requisiti delle forze armate e le capacità netcentriche

Nel corso del '900, gli Stati Uniti hanno preferito impostare la loro strategia di difesa su un approccio qualitativo piuttosto che quantitativo. Tale approccio si fonda su due presupposti: 1) che gli Stati Uniti abbiano un vantaggio competitivo sia nell'accesso che nell'utilizzo di tecnologie avanzate; 2) che il personale volontario, qualificato e addestrato (specialmente dai tempi della guerra in Vietnam) impieghi queste capacità più efficacemente rispetto a quanto sarebbero in grado di realizzare forze coscritte, sebbene numericamente maggiori. I progressi nelle ICT sembrano sposarsi in modo coerente con l'approccio qualitativo americano, dal momento che le reti offrono un potenziale perfino maggiore in grado di incrementare l'efficacia di una qualsiasi unità sul terreno. Ciò detto, le forze armate degli Stati Uniti riconoscono che se da una parte le capacità "stand-alone" manchino di sinergia, dall'altra quelle "networked" offrano agli avversari l'opportunità di provocare conseguenze ben maggiori, ad esempio se fossero in grado di penetrare o negare l'accesso a tali reti. Non è un caso infatti che le forze armate americane stiano investendo ingenti risorse economiche nel settore della cyber defense.

Un primo e ampio riconoscimento del potenziale che le tecnologie ICT erano in grado di offrire alle forze armate americane avvenne con il sistema di navigazione satellitare Global Positioning System (GPS) e con le informazioni che esso forniva in termini di positioning, navigation and timing (PNT). I dati PNT hanno rivoluzionato ogni area funzionale di combattimento, dai sistemi Blue Force Tracker – che permettono ai comandanti di "vedere" in tempo reale la posizione di ogni veicolo della loro unità – alla comunicazione di precise coordinate, fino all'impiego di velivoli unmanned in grado di provvedere ai necessari rifornimenti in luoghi e postazioni

[4] US Dept of the Army, *Army Equipment Program in Support of President's Budget 2015*, May 2014, http://usarmy.vo.llnwd.net/e2/c/downloads/348286.pdf.

remote nelle montagne dell'Afghanistan[5]. Come già accennato, l'impatto piuttosto rivoluzionario dei dati PNT sulle operazioni militari americane ha comunque generato alcuni rischi, e non solo in termini di attacchi cibernetici. Sempre più frequentemente, i vertici delle forze armate evidenziano come lo spazio stia diventando sempre più congestionato e conteso. Ciò rappresenta una grave minaccia (volontaria o meno) ad ogni aspetto delle operazioni militari americane, dalla comunicazione all'intelligence, fino alla fornitura di supporto logistico. In particolare, si prospetta il rischio che i collegamenti GPS non siano più disponibili. Al momento si stanno compiendo vari sforzi per mitigare tali rischi e per quanto riguarda la resilienza dei collegamenti GPS, gli Stati Uniti stanno vagliando una serie di opzioni tra cui lo sviluppo di programmi mirati ad utilizzare microtecnologie per migliorare l'accesso ai dati PNT, così come sviluppare approcci alternativi alle correzioni di navigazione fornite dal GPS[6].

Nonostante le informazioni fornite dai dati PNT siano state per molti aspetti rivoluzionarie, al momento i requisitivi delle forze armate in termini di capacità netcentriche tendono ad estendersi su vari fronti. L'attuale Chief of Naval Operations, l'Ammiraglio Jon Greenert, esprime da molto tempo la sua opinione secondo la quale la rete non sarebbe più una funzione di supporto, bensì un sistema di combattimento a sé stante[7]. A questo proposito, l'orientamento della Marina americana ha trovato riscontro in alcuni importanti cambiamenti organizzativi volti a combinare responsabilità di intelligence, comunicazioni e sorveglianza.

L'Aeronautica, la forza armata tendenzialmente più orientata all'innovazione tecnologica, è stata meno esplicita nell'articolare la centralità del-

[5] Si veda Lockheed Martin, *U.S. Marine Corps to Keep K-Max Unmanned Cargo Re-Supply Helicopter in Theater for Second Deployment Extension*, 31 July 2012, http://lmt.co/1F-88Va1.

[6] Si veda a titolo di esempio: Defense Advanced Research Projects Agency (DARPA), *Micro-Technology for Positioning, Navigation and Timing (Micro-PNT)*, http://www.darpa.mil/Our_Work/MTO/Programs/Micro-Technology_for_Positioning,_Navigation_and_Timing_(Micro-PNT).aspx; Defense Advanced Research Projects Agency (DARPA), *Adaptable Navigation Systems (ANS)*, http://www.darpa.mil/Our_Work/STO/Programs/Adaptable_Navigation_Systems_(ANS).aspx. Oltre a questi due progetti, l'Esercito persegue lo sviluppo di un programma volto a incrementare la protezione dei segnali GPS e diversificare la relativa rete di sensori. Justin Doubleday, "Congress approves Army funding for 'assured' navigation technology", in *InsideDefense.com*, 10 October 2014.

[7] Henry Kenyon, "Navy views network infrastructure as a vital combat component," in *DefenseSystems.com*, 9 June 2011, http://defensesystems.com/articles/2011/06/09/naval-it-day-greenert-network-as-combat-system.aspx.

le capacità netcentriche nelle sue operazioni. Tuttavia, dato il suo ruolo centrale nel provvedere alle capacità in campo spaziale, la sua precoce attenzione e interesse alla miriade di questioni cyber e, infine, i suoi progressi per potenziare le reti di comunicazioni aeree dimostrano come la forza armata sia sulla stessa lunghezza d'onda della Marina. Per quanto riguarda l'Esercito, l'ultimo decennio e più di operazioni di combattimento ha persuaso i vertici della forza armata che la capacità di "vedere" se stessi e il nemico così come di diffondere rapidamente quest'informazione al campo di battaglia sono di cruciale importanza, e che tutto ciò si basa quasi esclusivamente su una solida struttura di network. I vertici dell'Esercito dichiarano regolarmente, con affermazioni che poi trovano riscontro e si riflettono sull'allocazione delle risorse, che la rete costituisce la priorità di acquisizione principale. Anche il Corpo dei Marines, che si avvale considerevolmente del supporto delle altre forze armate, riconosce che le NEC offrano alle sue unità capacità ben superiori, e che si rivelano centrali per l'interazione con le altre forze armate. Quindi, mentre le specificità delle ICT continuano a evolversi rapidamente, l'establishment militare americano concorda sul fatto che il successo delle forze armate dipenda in maniera significativa dall'abilità di sfruttare più adeguatamente tali progressi attraverso le capacità netcentriche.

Allo stesso tempo però, si riconosce la possibilità che altri attori abbiano simili opportunità o che stiano sviluppando analoghe capacità. Gli Stati Uniti ad esempio non sono stati i soli a fare progressi nel fuoco di precisione, motivo per cui le forze armate americane stanno indirizzando la loro attenzione sulle cosiddette "dispersed or distributed operations", nelle quali le unità sono distribuite in modo disaggregato per poi essere capaci di riaggregarsi rapidamente in un determinato luogo e tempo per sfruttare i benefici del concetto di massa. Quest'aspetto è particolarmente importante per le forze terrestri americane, Marines ed Esercito: incrementare l'addestramento per tale tipologia di operazioni costituisce la terza priorità[8] del comandante del Corpo dei Marines, mentre la capacità di "operare in maniera decentralizzata" rappresentava uno dei sette concetti principali del precedente Army Operating Concept (AOC)[9]. A questo

[8] US Marine Corps, *Service Campaign Plan for 2014-2022*, 21 May 2014, https://marinecorpsconceptsandprograms.com/sites/default/files/files/United%20States%20Marine%20Corps%20Service%20Campaign%20Plan%202014-2022.pdf.

[9] US Army Training and Doctrine Command (TRADOC), *The United States Army Operating Concept, 2016-2028*, TRADOC Pamphlet No. 525-3-1, 19 August 2010, p. 17, https://fas.org/irp/doddir/army/opcon.pdf. Sebbene il richiamo a tale principio sia meno espli-

proposito, entrambe le forze armate hanno recentemente rilasciato due versioni aggiornate dei rispettivi concetti strategici che delineano le relative visioni sulle future modalità di impiego e, in entrambi i casi, le capacità netcentriche svolgono un ruolo centrale.

Nel marzo 2014, il Corpo dei Marines ha pubblicato il suo ultimo concetto operativo intitolato Expeditionary Force 21 (talvolta noto come EF 21)[10]. L'EF 21 tratteggia la visione futura del Corpo dei Marines, e svolge una funzione cardine e omnicomprensiva per lo sviluppo della forza armata nei prossimi anni. Il concetto ribadisce che lo scopo del Corpo dei Marines è quello di focalizzarsi sulla risposta alle crisi come principale missione, e di ripristinare il suo retaggio "expeditionary"[11]. Il documento descrive un approccio che tende ad enfatizzare una maggiore "presenza avanzata" (forward presence), una conoscenza più dettagliata del livello regionale, una migliore flessibilità della catena di comando e controllo e dell'assegnazione delle forze nel passare dalle operazioni circoscritte a quelle relativamente più grandi, un rapido schieramento di forze distribuite e organizzate per funzione, maggiori capacità di operare in ambienti elettromagnetici complessi (con relative tecnologie), e una più efficace integrazione con le forze speciali.

Al concetto operativo del Corpo dei Marines fa seguito quello dell'Esercito, il cosiddetto AOC, rilasciato nell'ottobre 2014[12]. L'AOC è inoltre atto a guidare lo sviluppo futuro della forza, e pone una forte e rinnovata enfasi sulla capacità di predisporre condizioni adeguate per l'impiego in

---

cito nell'ultimo documento relativo al concetto operativo dell'Esercito, esso rimane ancora un elemento chiave nei piani odierni e futuri della forza armata. US Army Training and Doctrine Command (TRADOC), *The U.S. Army Operating Concept: Win in a Complex World, 2020-2040*, 31 October 2014, TRADOC Pamphlet No. 525-3-1, 31 October 2014, http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf.

[10] US Marine Corps, *Expeditionary Force 21. Forward and Ready: Now and in the Future*, 4 March 2014, http://www.mccdc.marines.mil/Portals/172/Docs/MCCDC/EF21/EF21_USMC_Capstone_Concept.pdf.

[11] Ciò è conseguenza, forse, di una sorta di timore da parte del Corpo dei Marines che le operazioni in Iraq e Afghanistan abbiano richiesto alla forza armata di operare più "staticamente" – rimanendo vincolati a infrastrutture fisse sul terreno – rispetto a quanto fosse prestabilito e desiderato in termini di retaggio istituzionale, cultura e missioni. Non a caso, si afferma frequentemente che una "generazione di Marines" non ha avuto la possibilità di essere impiegata su unità navali e che il relativo set di capacità operative e conoscenze marittime dovrà essere reimpostato e ripristinato.

[12] US Army Training and Doctrine Command (TRADOC), *The U.S. Army Operating Concept: Win in a Complex World*, cit.

teatro, così come determinate azioni volte a condizionare il contesto di sicurezza. Mette altresì in evidenza come le operazioni interforze e multinazionali costituiranno il futuro delle operazioni militari, sostenendo che "le forze dell'Esercito sono particolarmente adatte a condizionare i contesti di sicurezza attraverso una "presenza avanzata" (*forward presence*) e azioni di combattimento durature e continuative con le forze di terra alleate e dei Paesi partner"[13]. Ancora, l'AOC identifica specificamente le tecnologie di processo informativo e di comunicazione come strumenti utili per sviluppare delle Common Operational Pictures (COPs) e ridurre così la complessità tecnologica per gli operatori[14]. Sebbene non riconosca esplicitamente la centralità delle capacità netcentriche, l'idea di base prevista nel documento prevede "unità multinazionali in grado di agire a livello globale e di compiere manovre da diverse posizioni [...] rapidamente adattabili alla missione [...] e che combinino capacità interforze e multinazionali."[15]

Sia per il Corpo dei Marines che per l'Esercito, realizzare le rispettive visioni sulle modalità di impiego futuro delle operazioni richiederà un affidamento finanche maggiore sulle ICT e sulle capacità netcentriche. Comprendere quali siano le implicazioni a livello di aree funzionali di combattimento agevola certamente il significato di questa affermazione.

Comando e controllo (C2). L'abilità dei comandanti di comunicare e dirigere le proprie forze costituisce il presupposto per operazioni efficaci e, sia per l'Esercito che per il Corpo dei Marines, tale funzione è strettamente dipendente dalle possibilità di disporre di network[16]. Come ha dichiarato un generale dell'Esercito americano, la priorità d'investimento per la forza armata è costituita dal continuo sviluppo delle reti wireless. Quest'ultime permettono le comunicazioni a livello di plotone, squadra e perfino a livello del singolo operatore, e sono elementi fondamentali per

[13] Ibid., p. 8.

[14] Ibid., p. 13.

[15] Ibid., p. 15.

[16] Per esempio, il Corpo dei Marine afferma che il C2 è: "leader-centric, *network-enabled* (enfasi aggiunta), and is intended to support the continuous decision-making cycle of commanders at every level to ensure they are positioned to best plan, direct, coordinate and control." US Marine Corps, *USMC Concepts and Programs 2013*, http://www.hqmc.marines.mil/pandr/ConceptsandPrograms/ConceptsandPrograms2013.aspx. L'Army Mission Command Strategy sostiene inoltre che "The network and various other technological systems are key parts of a commander's [mission control] system". US Army Combined Arms Center, *U.S. Army Mission Command Strategy, FY13-16*, June 2013, http://usacac.army.mil/cac2/Repository/Army_Mission_Command_Strategy_dtd_12June%202013.pdf.

lo sviluppo e l'aggiornamento di una "situational awareness" condivisa (shared situational understanding), dalla quale derivano e fluiscono tutte le attività di comando e controllo[17]. Per le forze di terra in particolare, i concetti relativi al comando e controllo attualmente stabiliscono che i vari comandanti di ogni livello disporranno in futuro di informazioni di base (ma precise) sulle unità superiori, adiacenti e subordinate ad essi.

Si presume inoltre che i comandanti disporranno di canali di comunicazione multipli, ridondanti, per consentire operazioni sempre più decentralizzate. Inoltre, varie entità del Dipartimento della Difesa stanno esaminando come meglio sfruttare i benefici tecnologici di sensori sempre più piccoli e interconnessi, cercando di automatizzare la raccolta e la visualizzazione di dati supplementari relativi alle unità, per arrivare a includere anche il livello del singolo operatore. Per esempio, la Defense Advanced Research Projects Agency (DARPA) sta portando avanti un approccio integrato per mettere in rete varie tecnologie a livello di soldato che fornirebbero automaticamente dati sullo stato di salute del personale sul terreno (e.g. temperatura, livello di ossigeno o idratazione) o sullo stato della logistica (e.g. quantità di munizioni utilizzate)[18].

Il Corpo dei Marines identifica le ICT come enabler fondamentale per lo sviluppo della funzione C2, facendo notare che

> data la complessità, il tasso di impiego delle capacità e la natura distribuita delle operazioni future di proiezione della forza, le forze navali richiederanno sia un'information technology (IT) avanzata che strutture di comando flessibili per sostenere un livello maggiore di coordinamento e integrazione tra tutti gli elementi della forza armata[19].

Le operazioni in Iraq e in Afghanistan, contraddistinte dalla presenza di piccole ma numerose unità dislocate in luoghi remoti e in aree piuttosto

[17] Sydney J. Freedberg, "The Army gropes toward a cultural revolution", in *Breaking Defense*, 22 October 2014, http://breakingdefense.com/?p=16597.

[18] Si veda Scott Maucione, "DARPA wants white papers on 'Squad X' dismounted info-sharing", in *InsideDefense.com*, 31 July 2014.

[19] US Marine Corps, *Expeditionary Force 21*, cit., p. 33. Il documento prosegue poi con l'identificare un certo numero di capacità di supporto (supporting capabilities) per includere specifici requisiti associati ad una incrementata robustezza delle comunicazioni, l'abilità di supportare il processo collaborativo di pianificazione e decision-making, una migliore interoperabilità e sicurezza, e un più efficace accesso alle formazioni provenienti da fonti esterne.

estese, hanno evidenziato la necessità per le forze di terra americane di incrementare la loro capacità di essere connesse ai livelli più bassi possibili. A tale scopo, sia l'Esercito che il Corpo dei Marines stanno sviluppando delle tecnologie volte a realizzare connessioni di rete non solo per i quartier generali mobili più grandi, ma anche per le postazioni minori avanzate. Detto ciò, è interessante notare come, nonostante entrambe le forze armate riconoscano che gli sviluppi nel campo dell'ICT continueranno a stimolare rapidi progressi tecnologici con ricadute importanti in termini di capacità, i rispettivi piani per indirizzarli e sfruttarli a pieno sembrano ancora divergere.

Guardando al futuro delle comunicazioni, l'approccio dell'Esercito nel fornire la connettività operativa e tattica si basa generalmente su forme d'onda comuni. L'assunto di base prevedrebbe che il Dipartimento della Difesa identifichi determinati standard per le forme d'onda, così come i protocolli per la gestione delle reti e la codifica delle informazioni. Una volta specificati gli standard, le aziende sarebbero in grado di progettare sia dispositivi hardware che software attorno a queste determinate forme d'onda, che potrebbero essere tra l'altro trasferite da un device all'altro.

Il Corpo dei Marines, d'altro canto, ha ritenuto che tentare di condurre i fornitori verso la realizzazione di specifiche forme d'onda risulta dispendioso e alquanto irrealistico. La forza armata invece prosegue nell'elaborazione di software riprogrammabili in grado di supportare una rapida traslazione di diverse forme d'onda tra differenti componenti dell'equipaggiamento[20]. A tale scopo, il Corpo dei Marines ha portato avanti una serie di sperimentazioni per creare dei "ponti" di reti (network bridges) tra i veicoli e piattaforme aeree, puntando sulla interoperabilità digitale che fa leva sugli equipaggiamenti esistenti.

Sussistono varie indicazioni sul fatto che l'Esercito, il quale ha dovuto fronteggiare diverse sfide dal punto di vista tecnico e finanziario per i programmi disegnati su specifiche forme d'onda, stia adesso considerando un approccio più commerciale. A scopo di esempio, nel settembre 2014 il centro per la ricerca elettronica dell'Esercito ha rivelato l'intenzione di valutare se la tecnologia di quarta generazione Long Term Evolution (4G LTE) possa soddisfare le esigenze operative in termini di comunicazioni e intelligence[21].

[20] Matthew Glavy, "The Flight MAP: The Marine Aviation Plan Through 2040", in *CSIS Events*, 28 April 2014, http://csis.org/node/48793.

[21] Bob Brewin, "Army Eyes 4G Cellular Tech for Combat Communications", in *Nextgov*, 10 September 2014, http://www.nextgov.com/defense/2014/09/army-eyes-4g-cellu-

Entrambe le forze armate si stanno impegnando per migliorare la condivisione delle informazioni e la connettività. Per esempio, nel 2013 il Corpo dei Marines ha affermato la volontà di sviluppare ulteriormente la capacità di ottenere aggiornamenti di intelligence in tempo reale mentre gli uomini sono impegnati in missioni a lunga distanza a bordo dei convertiplani[22] V-22[23], combinando comunicazioni e intelligence al fine di informare più efficacemente e prontamente gli operatori. I Marines stanno inoltre sviluppando applicazioni aggiuntive per sfruttare il vantaggio tattico degli ambienti "cloud"[24] per grandi quantità di dati e informazioni pianificate, mentre l'Esercito è fortemente intenzionato a favorire la convergenza tra le sue operazioni e reti di intelligence[25].

Oltre alle operazioni di terra, il Corpo dei Marines pone un'attenzione sempre più crescente sul miglioramento dei suoi legami C2 (e relative capacità di supporto) con altri elementi navali, sia afferenti la Marina che la Guardia Costiera. Per supportare più adeguatamente la cooperazione operativa interforze, i Marines puntano ad incrementare i legami esistenti a livello operativo attraverso una maggiore sperimentazione e addestramento ai livelli più bassi, così come ai livelli più alti del personale addetto alla pianificazione[26].

Intelligence. I progressi nel campo dell'ICT sono certamente determinanti per le future necessità di intelligence. Le guerre in Iraq e Afghanistan hanno generato sostanziali miglioramenti nella capacità di integrare i dati di intelligence "all-sources" provenienti da fonti elettroniche, umane, geospaziali, ecc. Ciò ha generato una nuova gamma di strumenti disegnati per rendere l'intelligence più veloce e più rilevante per i vari comandanti di ogni livello. Dall'inizio dei conflitti, le forze speciali americane hanno

---

lar-tech-combat-communications/93689.

[22] Il convertiplano è un aeromobile in grado di decollare e atterrare verticalmente, alla stregua di un elicottero, ma che al tempo stesso può volare ad una altitudine e velocità comparabili a quelle di un aereo, e per tragitti di simile lunghezza/durata.

[23] Amy Butler, "USMC to outfit Ospreys with comms node", in *Aviation Week & Space Technology*, 14 October 2013, http://aviationweek.com/node/4026.

[24] Bob Brewin, "The Navy wants a tactical cloud", in *Defense One*, 25 September 2014, http://www.defenseone.com/technology/2014/09/navy-wants-tactical-cloud/95129.

[25] US Senate, Committee on Armed Services, Subcommittee on AirLand, *Statement of Gen. John F. Campbell, Vice Chief of Staff, United States Army, on Fiscal Year 2015 Ground Force modernization and individual equipment modernization programs*, 9 April 2014, http://www.armed-services.senate.gov/imo/media/doc/Campbell-Barclay-Williamson_04-09-14.pdf.

[26] US Marine Corps, *Expeditionary Force 21*, cit., pp. 29-30.

sviluppato e ridefinito tutta una serie di processi – grazie a particolari analisi rese possibili da sistemi connessi in rete – volti a trovare rapidamente gli obiettivi di interesse, bloccarli in una determinata posizione, ed eliminarli attraverso raid aerei o altre tipologie di attacco ritenute necessarie e/o più adeguate. I suddetti raid hanno generato ulteriori dati (sia fisici che virtuali) che sono stati inseriti nel ciclo intelligence, portando a loro volta a scoperte aggiuntive di obiettivi, e così via. Tali processi si sono estesi altresì alle forze convenzionali, evolvendo sempre di più a prassi ormai consolidata tra le unità terrestri.

La capacità di trasmettere informazioni a vari livelli di classificazione, oltre ad integrarle o visualizzarle attraverso diverse modalità, ha rappresentato un forte cambiamento per le forze terrestri americane. Una maggiore conoscenza delle loro unità, insieme ad una maggiore consapevolezza delle popolazioni locali e degli avversari, ha fornito ai comandanti una migliore "situational awareness" che le generazioni precedenti avrebbero solo potuto immaginare. Le sfide rimangono nella gestione dei dati con diversi livelli di classificazione, e nella loro condivisione tra i membri della coalizione, ma molti di questi problemi si basano più su scelte politiche che sulle reali disponibilità e possibilità tecnologiche.

Fuoco. Le tecnologie netcentriche hanno inoltre aperto la strada per lo sviluppo e potenziamento della capacità di fuoco interforze in modi fino a quel momento inimmaginabili. L'aggiunta di kit a sistemi aerei, terrestri e marittimi che incorporano il sistema GPS o il puntamento laser – uniti all'istallazione di reti di comunicazione – ha significato per i comandanti di terra la possibilità di "chiamare il fuoco" da numerose piattaforme, con estrema precisione e sicurezza. I sistemi di intelligence connessi in rete consentono l'identificazione di obiettivi molto più vari e dettagliati, e la "fusione" tra sensore e sistema d'arma permette alle forze terrestri di condurre simultaneamente operazioni di intelligence e di attacco e, in aggiunta, di collegare sistemi manned e unmanned con modalità completamente nuove. L'Esercito, ad esempio, è in procinto di impiegare dei sistemi che permettono ai piloti di elicotteri da combattimento di controllare dalla loro cabina i velivoli unmanned, ma altresì di monitorare i feed video provenienti dai droni e vari mezzi dell'Aeronautica[27]. Infine, alcuni esperti del settore si domandano se le nuove capacità di comunicazione

[27] Paul McCleary, "US Army Presses Ahead on Manned-Unmanned Teaming", in *Defense News*, 30 April 2013, http://www.defensenews.com/article/20130430/DEFREG02/304300018.

satellitare a banda stretta possano offrire link di comando e controllo più resistenti, agevolando la capacità di fuoco a livello tattico da vari sistemi di artiglieria o missilistici[28].

Forse il risvolto più significativo dell'impiego delle ICT in tale campo si riflette nella possibilità che esse generino il potenziale per attacchi cinetici e non cinetici. Sebbene persistano barriere (molte delle quali culturali) alla piena integrazione delle capacità di fuoco non-cinetiche come la guerra elettronica, cyber, e le cosiddette "information operations", tali limitazioni sembrerebbero comunque venir meno. Ad esempio, si sta ricostituendo in seno all'Esercito una "community" dedicata alla guerra elettronica, il cui obiettivo è sviluppare un più ampio insieme di capacità che vada oltre a quelle sviluppate specificatamente per fronteggiare la minaccia degli ordigni esplosivi improvvisati (Improvised Explosive Devices – IEDs) in Iraq e Afghanistan. Entrambe le forze armate hanno sviluppato nuove organizzazioni (la Cyber and Electronic Warfare Coordination Cell, o CEWCC, per il Corpo dei Marines, e le Cyber Electromagnetic Activities, o CEMA, per l'Esercito) volte a coadiuvare gli sforzi per una migliore integrazione delle capacità di fuoco non-cinetiche sia al loro interno che con le capacità di fuoco cinetiche terrestri. Liberarne il potenziale richiede di mettere in rete alcune capacità già esistenti (per esempio i dispositivi jammer individuali), ma anche continuare ad evolvere in termini di struttura organizzativa e strumento dottrinale in modo tale che i comandanti apprezzino pienamente e utilizzino gli strumenti non cinetici a supporto del loro schema complessivo di manovra.

Movimento e manovra. Come accennato in precedenza, le capacità netcentriche hanno determinato un duplice effetto sulla funzione "movimento e manovra". I progressi in termini di precisione non hanno riguardato solo le forze armate americane ma anche quelle potenzialmente ostili, e ciò ha obbligato in particolare l'Esercito a rivedere il proprio concetto di massa. Gli stessi progressi hanno senza dubbio permesso all'Esercito e al Corpo dei Marines di considerare nuove modalità per disperdere e raggruppare le forze per sfruttare un vantaggio operativo.

Al di là dell'abilità delle unità di coordinare più efficacemente i propri movimenti, le ICT e le capacità netcentriche hanno prodotto effetti rilevanti sull'evoluzione dei veicoli da combattimento che supportano la capacità di manovra. Ognuna delle principali piattaforme ruotate o cingolate (per

[28] Patrick A. Schrafft, "Enhancing fires with next-generation narrowband SATCOM", in *Fires*, July-August 2014, http://www.readperiodicals.com/201407/3410820761.html.

esempio i carri armati) è stata sottoposta a molteplici programmi di aggiornamento volti a migliorarne la capacità di ricevere e trasferire dati, confrontandosi continuamente con i limiti imposti dalle dimensioni e dalla potenza. Tuttavia, un'ulteriore testimonianza di come le forze di terra americane ritengono essenziali le capacità netcentriche si può osservare nei requisiti stabiliti per i futuri veicoli terrestri, sia ruotati che cingolati. Ognuno di questi dispone di uno spazio dedicato alle capacità netcentriche, e specifici requisiti per massimizzare la possibilità di upgrade tramite continui aggiornamenti software, molti dei quali intesi a collegare ulteriormente i sistemi alle informazioni connesse in rete. Le forze di terra americane continuano inoltre a perseguire quelle capacità netcentriche che meglio sintetizzano le fonti di dati esistenti, dai display integrati e sistemi di puntamento per i comandanti di carri armati ai data link che permettono di vedere i video provenienti dai velivoli senza pilota[29].

La funzione "movimento e manovra" non si limita alle operazioni di combattimento high-end bensì si applica nondimeno all'addestramento e all'esercitazioni così come ad ulteriori attività che l'Esercito definisce come "shaping the security environment". Anche in questa prospettiva, le capacità netcentriche sono ugualmente rilevanti. Sempre a scopo illustrativo, il Corpo dei Marines ha recentemente deciso di rilasciare per le sue unità con compiti civili un'applicazione basata su Android che permette di raccogliere, elaborare e condividere elettronicamente le informazioni sulle condizioni delle infrastrutture locali – come acqua e reti fognarie, scuole o strade durante le operazioni di assistenza umanitaria – rendendo in questo modo l'erogazione di aiuti più efficiente ed efficace[30].

Protezione. La capacità di assicurare che le forze di terra americane abbiano sufficiente protezione è intrinsecamente legata alle altre funzioni di combattimento. La dottrina in materia prevede che le forze di terra utilizzino informazioni di intelligence e C2 per agevolare nuove modalità di manovra che evitino potenziali minacce, servendosi dei vantaggi dell'informazione – come il fuoco di precisione – per neutralizzarle. La crescente centralità del concetto di dispersione si riflette nuovamente nell'importanza conferita alle comunicazioni e alla connettività. Entrambe si affidano alle capacità netcentriche – es. reti di sensori attivi e passivi per fornire informazioni sulla minaccia – e si servono delle ICT per tra-

[29] US Marine Corps Systems Command, *Modern Day Marine: Report to Industry*, 25 September 2014.

[30] Barb Hamby, "Fielding decision made on new civil affairs app", *Marine Corps Systems Command Press Release*, 9 October 2014.

sformare quei dati in display visivi per il personale equipaggiato e non. Un esempio su tutti riguarda ciò che avviene a livello di singolo soldato; infatti, sia l'Esercito che la Marina stanno esaminando la fattibilità di alcuni sensori installati negli elmetti che potrebbero fornire informazioni sulla posizione e sulla gravità delle ferite alla testa, sulla presenza o meno di lesioni cerebrali traumatiche avvenute nell'ultimo decennio o più.

Oltre a proteggere loro stesse, le forze terrestri svolgono una funzione fondamentale nella protezione delle altre forze sul campo e della popolazione civile. Il sistema di difesa missilistica Patriot è stato uno degli assetti più richiesti negli ultimi anni; motivo per cui l'Esercito è alla ricerca di kit in grado di mettere in rete tale sistema ad una architettura di difesa missilistica[31]. E sia la versione della Marina che dell'Aeronautica del Joint Strike Fighter F-35 – che si basano tanto sul targeting e munizioni di precisione quanto sulla messa in rete di dati relativi alla posizione delle forze amiche – sono intese a fornire in futuro un maggiore supporto aereo ravvicinato a tutte le forze di terra.

Supporto logistico. L'esistenza di lunghe linee di comunicazione in Afghanistan e Iraq ha suscitato nuova enfasi su come ridurre i requisiti operativi relativi al supporto logistico (e.g. limitare la dipendenza da carburante e batterie) e sull'opportunità di nuovi metodi alternativi per condurre il supporto logistico. Prima dei due conflitti in Medio Oriente, l'interesse era di sviluppare capacità netcentriche che permettessero una maggiore efficienza e trasparenza nei processi logistici attraverso l'utilizzo di tecnologie quali i chip a radio-frequenza (Radio-frequency identification, RFID). Ora, sebbene sia Esercito che Marines rimangano determinati a migliorare la catena di supporto logistico, le due operazioni militari hanno indotto verso una ricerca molto più approfondita nel campo della robotica e dei sistemi unmanned volti a dare il loro contributo al funzione di supporto logistico. Entrambi i campi di ricerca e sperimentazione si servono delle capacità netcentriche.

Per esempio, nel 2011 il Corpo dei Marines ha impiegato in Afghanistan l'elicottero unmanned K-MAX per le operazioni di approvvigionamento e rifornimento. L'elicottero ha ottenuto un discreto successo tanto che sia il Corpo dei Marines che l'Esercito stanno valutando l'eventualità di formalizzarlo come programma delle due forze armate[32]. Per integra-

[31] Justin Doubleday, "Army seeks info on Patriot-interface kits for networked missile defense", in *Inside the Army*, 3 October 2014.

[32] Mike Hoffman, "Marines Work to Extend K-MAX in Afghanistan Through 2014", in *DefenseTech*, 25 September 2013, http://defensetech.org/2013/09/25/marines-work-

re ulteriormente i benefici della piattaforma, i Marines partecipano allo sviluppo di un sistema di controllo automatizzato basato su avanzati algoritmi e reti di sensori che permettono al K-MAX – o ad altre piattaforme aeree – di operare autonomamente e in ambienti complessi[33]. L'Esercito e l'Aeronautica hanno inoltre contribuito allo sviluppo di tecnologie volte a realizzare il Joint Precision Air Drop System (JPADS), un parafoil a guida GPS in grado di effettuare precise operazioni di approvvigionamento di carichi (payloads) variabili[34].

Key enablers. Come già accennato, è ampiamente riconosciuto che quasi ogni aspetto delle operazioni militari americane si basi sull'integrità delle reti e delle informazioni che viaggiano su di esse. Il mantenimento di questa integrità interessa diverse dimensioni, poiché essa richiede strumenti di difesa adeguati contro eventuali interruzioni, come ad esempio attacchi cyber, spettri elettromagnetici congestionati, e crescenti quantità di detriti spaziali. Per assicurare tali difese, all'interno delle forze armate americane le responsabilità sono condivise a vari livelli tra i cosiddetti "functional combatant commanders" – in particolare lo U.S. Strategic Command e lo U.S. Cyber Command – e tra le varie forze armate.

Due fenomeni in particolare hanno contribuito ad accrescere i timori americani per potenziali vulnerabilità causate dalle interruzioni di rete. Il primo di questi è la crescente dipendenza dalle capacità netcentriche, tema ricorrente in queste pagine. Ognuno dei domini militari riconosciuti nella dottrina interforze americana – aria, terra, mare, spazio e cyber – non solo si basa ma ricopre un ruolo fondamentale per agevolare l'impiego e l'utilizzo di capacità netcentriche. Considerando nello specifico uno di questi domini, un ufficiale del Dipartimento della Difesa americana ha recentemente fatto notare che

> negli ultimi 25 anni, le capacità spaziali sono divenute…una "commodity service" la cui presenza è data per scontata fino al momento in cui la sua disponibilità risulta essere interrotta. La nostra dipendenza dallo spazio è divenuta inestricabilmente collegata alle altre nostre capacità critiche[35].

---

to-extend-k-max-through-2014.

[33] Kris Osborn, "Marines fly helicopters with mini-tablet", in *DoD Buzz*, 5 April 2014, http://wp.me/pgSCu-8kt.

[34] "JPADS: Making precision air-drops a reality", in *Defense Industry Daily*, 27 April 2014, http://www.defenseindustrydaily.com/?p=678.

[35] US House of Representatives, Armed Service Committee, Subcommittee on Strate-

Questo vale più in generale anche per lo spettro elettromagnetico, che supporta la connettività wireless e la guerra elettronica, così come per le reti cablate. Non a caso recentemente, l'Army Science Board ha constatato che l'Esercito sarà chiamato a contrastare le "vulnerabilità digitali…dovute alla dipendenza degli Stati Uniti dai sistemi digitali", e che esso deve sviluppare un concetto di "contro-digitalizzazione" sia per fare fronte a tale realtà sia per sfruttare questa stessa dipendenza nei confronti degli avversari[36].

Il secondo fenomeno scaturisce anch'esso da una sorta di timore che i conflitti in Iraq e Afghanistan abbiano generato un'eccesiva fiducia e, in una certa misura, una falsa sicurezza al riguardo. In entrambi i conflitti le forze armate americane godevano di un dominio quasi totale, specialmente in ambito aereo e spaziale. Le attività in campo marittimo erano invece piuttosto limitate, mentre il dominio cyber era per lo più insicuro. In ogni caso, le sfide maggiori hanno avuto luogo nel dominio terrestre. Inoltre, sebbene le due operazioni avessero messo in evidenza alcune importanti criticità in termini di interoperabilità tra le forze americane e quelle dei Paesi partner, in alcuni casi esse hanno trovato spazio per una loro risoluzione[37]. È altrettanto vero però la mancanza di un avversario capace e altamente addestrato ha indotto le forze della coalizione a pensare di poter fare maggior affidamento sulla resilienza delle loro capacità netcentriche, rispetto a come sarebbe stato in caso di nemici e avversarsi più preparati sotto questo aspetto.

Per ovviare a quello che molti vedono come un falso – e pericoloso – senso di autocompiacimento, l'establishment militare americano torna a porre l'accento sull'addestramento e la preparazione del personale per ambienti operativi meno favorevoli, specialmente in ambito aereo, marittimo e cyber. Questo preoccupazione spiega, almeno parzialmente, l'emergere di un forte interesse per le minacce "anti-access, area denial", o A2/AD. Queste includono missili a lunga gittata, ma anche avversari altamente competenti e preparati in ambito cyber, possibili sfide all'accesso allo spazio, impulsi elettromagnetici, e ulteriori capacità avanzate che annullerebbero o renderebbero vani i vantaggi tecnologici americani.

---

gic Forces, *Statement of Gil I. Klinger*, 3 April 2014, http://docs.house.gov/meetings/AS/AS29/20140403/102037/HHRG-113-AS29-Wstate-KlingerG-20140403.pdf.

[36] Army Science Board, *Decisive Army Strategic and Expeditionary Maneuver*, 18 September 2014.

[37] Sydney J. Freedberg, "What the US, NATO must do to counter Russia: Breedlove, Gorenc & Odierno", in *Breaking Defense*, 22 September 2014, http://breakingdefense.com/?p=15930.

Con riferimento al dominio spaziale, i funzionari americani sembrano particolarmente preoccupati della cosiddetta "spazzatura spaziale" (space clutter) e delle capacità avversarie che minacciano l'uso di questo dominio (adversary counter-space capabilities). Entrambi gli aspetti tendono ad orientare lo sviluppo di una strategia americana basata su una maggiore resilienza in campo spaziale e che poggia su tre elementi principali. Il primo è quello di accrescere la cosiddetta "space situational awareness" attraverso la stipula di accordi di condivisione delle informazioni con aziende commerciali e altri governi che dispongono di capacità PNT, con l'obiettivo di agevolarne l'accesso da parte americana in caso di danneggiamento o compromissione[38]. Questi accordi richiedono la modifica delle apparecchiature in modo che esse possano ricevere i segnali da altri sistemi di navigazione spaziale[39]. Il secondo elemento della strategia consiste nel realizzare una maggiore diversificazione degli assetti spaziali americani (e.g. includere payloads inferiori su più veicoli spaziali sia commerciali che militari).

Infine, potenziare l'affidabilità delle piattaforme esistenti quali GPS, la suite di satelliti Wideband Global SATCOM (WGS), lo Space-Based Infrared System (SBIRS) – ovvero una costellazione di sei satelliti che supportano l'early warning e la difesa missilistica – e l'Advanced Extremely High Frequency (AEHF), anch'essa una costellazione di quattro satelliti che assicura solide capacità di comunicazione. Gli Stati Uniti continuano altresì a mettere a punto un apposito sistema dagli impulsi elettromagnetici (Electromagnetic Pulse, EMP), dopo che una lunga serie di commissioni di studio guidate dal Congresso e analisi interne al Dipartimento della Difesa ne hanno ripetutamente evidenziato il potenziale danno[40].

---

[38] Ad aprile 2014 gli Stati Uniti avevano stretto accordi in tal senso con Australia, Canada, Francia, Giappone e Italia, così come tutta una serie di intese con 41 operatori satellitari commerciali. US House of Representatives, Armed Service Committee, Subcommittee on Strategic Forces, *Statement of Douglas L. Loverro*, 3 April 2014, http://docs.house.gov/meetings/AS/AS29/20140403/102037/HHRG-113-AS29-Wstate-LoverroD-20140403.pdf.

Nell'agosto dello stesso anno, lo US Strategic Command aveva sottoscritto un ulteriore accordo di condivisione dei dati con l'European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT). Jordana Mishory, "Stratcom signs new space situational awareness data-sharing agreement", in *Inside the Pentagon*, 4 September 2014.

[39] U.S. House of Representatives, House Armed Service Committee, Subcommittee on Strategic Forces, *Statement of Douglas L. Loverro*, cit., p. 8.

[40] James Jay Carafano and Richard Weitz, "EMP attacks: What the U.S. must do now", in *Heritage Foundation Backgrounder*, n. 2491 (17 November 2010), http://www.heritage.

Oltre a puntare verso una capacità di comunicazione satellitare più diversificata e robusta, le forze armate americane sono intenzionate a rafforzare l'intera architettura delle comunicazioni per consentire una connettività continuata e duratura, anche nell'eventualità che un qualsiasi livello dell'architettura – ad esempio i satelliti – non sia più disponibile. Per esempio, uno dei dichiarati benefici delle comunicazioni attraverso velivoli senza pilota è che essi forniscono capacità di backup qualora le comunicazioni satellitari vengano meno[41]. Questa logica sta parzialmente orientando gli sforzi del Corpo dei Marines nel rafforzamento dell'interoperabilità digitale tra le sue piattaforme.

Come già constatato in precedenza, gli sforzi e gli investimenti per migliorare la cyber security delle forze armate americane sono piuttosto ingenti. Ad ulteriore conferma, lo U.S. Cyber Command ha istituito una Cyber Mission Force (CMF) formata da tre componenti: una National Mission Force per proteggere le reti nazionali; una Cyber Combat Mission Force allo scopo di provvedere al supporto in materia cibernetica dei comandi regionali; e infine la Cyber Protection Force per difendere le reti del Dipartimento della Difesa[42]. L'Esercito, la Marina e l'Aeronautica contribuiscono al progetto fornendo personale qualificato allo scopo di formare 133 squadre CMF. Per quanto riguarda specificatamente le forze terrestri, Esercito e Corpo dei Marines stanno formando operatori specializzati per supportare le unità al di sotto del livello di comando combattente.

Sul lato procurement, il Dipartimento della Difesa americano ha sviluppato il Joint Information Environment (JIE), un'architettura aperta e standard di reti, basata su un'infrastruttura comune e in grado di coadiuvare processi e specifiche politiche. Uno degli obiettivi chiave del JIE consiste nel sostenere una maggiore interoperabilità tra le forze armate americane e nel potenziare la cybersecurity[43]. Il JIE facilita lo sviluppo di "capacità unificate", uno sforzo intrapreso dalla Defense Information Systems Agency (DISA), l'Esercito e l'Aeronautica per arrivare ad ottenere "voice, video and data tools" che potrebbero essere utilizzati da tutto il sistema militare americano. L'Esercito è alla guida di tale sforzo, che si

org/research/reports/2010/11/emp-attacks-what-the-us-must-do-now.

[41] Army Science Board, *Decisive Army Strategic and Expeditionary Maneuver*, cit.

[42] Cheryl Pellerin, "Cybercom activates national mission force headquarters", in *DoD News*, 25 September 2013, http://www.defense.gov/news/newsarticle.aspx?id=120854.

[43] Jordana Mishory, "DoD eyes interoperability in next-gen host-based cybersecurity strategy", in *Inside the Pentagon*, 21 August 2014.

presume includerà l'estensione dei servizi chat – come quelli impiegati diffusamente in Iraq e Afghanistan – ad un insieme più ampio di utenti[44].

A livello di forza armata, l'EF 21 del Corpo dei Marines evidenzia che "la libertà di azione nel cyberspazio e nello spettro elettromagnetico è una key enabler per le operazioni militari del 21esimo secolo"[45]. Pur in maniera meno esplicita e diretta, l'Esercito condivide la stessa visione: non a caso negli ultimi anni la forza armata ha istituito un nuovo Cyber Center of Excellence – integrando la capacità di guerra elettronica all'interno di tale centro – e ha creato una nuova divisione militare per il personale cyber (la prima dalla creazione delle forze speciali alla fine degli anni '80). Mentre entrambe le forze armate rimangono ora impegnate a far evolvere le proprie strutture organizzative che regolano le responsabilità sia per il settore cyber sia per quello attinente all'EMS, la strada che sembra profilarsi prevede un incremento della loro rilevanza e incisività (sia difensiva che offensiva) nelle operazioni militari future.

1.3 I principali programmi di procurement

Ogni principale programma di procurement delle forze armate americane ha già incorporato al suo interno le capacità netcentriche. Alcuni di questi sono concepiti esplicitamente con l'obiettivo di fornire un sistema di reti interconnesso, mentre altri sfruttano indirettamente le capacità netcentriche per incrementare la loro performance complessiva. Sulla base delle sei "funzioni di combattimento" elencate in precedenza, il seguente paragrafo passa in rassegna alcuni dei principali programmi terrestri che riguardano più direttamente le capacità netcentriche.

Comando e controllo (C2). Sia l'Esercito che il Corpo dei Marines partecipano a vari livelli a diversi programmi interforze che mirano a fare leva sulle capacità netcentriche in un'ottica C2. Uno di questi è il Joint Battle Command-Platform (JBC-P), il principale strumento di comando e controllo e situational awareness predisposto per i livelli di brigata e inferiori. È un programma di sviluppo che vuole porre le basi per la futura situational awarness interforze; è guidato dal Software Engineering Directorate dell'Esercito ad Huntsville (Alabama) e vede altresì il coinvol-

[44] Justin Doubleday, "Solicitation eyed this fall for 'unified capabilities' networking tools," in *Inside the Army*, 19 September 2014.

[45] US Marine Corps, *Expeditionary Force 21*, cit., pp. 35-36.

gimento di varie aziende del settore tra cui DRS Technologies e General Dynamics. Sullo stesso piano si pone l'ambizioso, non solo tecnicamente, Joint Tactical Radio System (JTRS), meglio conosciuto ora come Family of Networked Tactical Radios. In origine l'obiettivo era sviluppare una famiglia di radio completamente interoperabili con lunghezze d'onda esportabili ma, a causa di numerose problematiche nelle tempistiche e nei costi, il programma fu definitivamente rivisto e riconfigurato nel 2011.

Con il nuovo tentativo di sviluppare una Family of Networked Tactical Radios – "famiglia di radio tattiche interconnesse" – si vuole realizzare dispositivi multi-banda e multi-modali attraverso l'utilizzo di tecnologie basate su protocolli IP (Internet Protocol[46]). Una componente del nuovo progetto è il programma Handheld, Manpack, and Small-Form Fit, per il quale concorrono General Dynamics, Rockwell Collins, Thales, e la Harris Corporation. Tra gli elementi chiave che costituiscono tale programma, la radio ManPack ha sperimentato diverse criticità: ad esempio, nel giugno 2014 l'Esercito ha sospeso l'utilizzo in teatro del modello proposto da General Dynamics per via di alcune riserve dal punto di vista tecnico in termini di peso, surriscaldamento, portata e consumo energetico.

Nonostante General Dynamics abbia poi replicato autofinanziando lo sviluppo di una versione migliorata del dispositivo, non è ancora chiaro se questa nuova opzione possa avere la meglio sui design concorrenti[47]. L'Esercito comunque prevede di formulare una "request for proposals" per la radio ManPack nella prima metà del 2015, sulla scia di quanto fatto a inizio dello stesso anno per la versione portatile (handheld radio version) conosciuta come Rifleman, e per la quale la forza armata sarebbe intenzionata per la fase di test a stipulare diversi contratti quanti sono i potenziali fornitori prima di compiere un'ulteriore selezione per l'avvio della produzione in serie. Nel frattempo, per affrontare i ritardi nelle programmazione del JTRS il Corpo dei Marines ha avviato un nuovo programma denominato Tactical Communications Networking (TCN), una

[46] IP (Internet Protocol) è il protocollo di comunicazione attualmente più usato, poiché costituisce il protocollo di base usato per le comunicazioni tramite Internet, compresa la posta elettronica, il Web e le applicazioni multimediali. Una delle ragioni della sua popolarità risiede nella sua scalabilità. Ciò significa, in altre parole, che questo protocollo può essere usato sia per le piccole installazioni che per quelle di dimensioni maggiori, perché è in grado di garantire prestazioni elevate, costi ridotti e un'ampia compatibilità con attrezzature e tecnologie consolidate.

[47] Sebastian Sprenger, "General Dynamics launches "Apollo" in bid to save its Army radio business", in *Inside the Army*, 3 October 2014.

famiglia di apparecchiature radio in grado di supportare le comunicazioni voce e dati per le forze dispiegate in teatro.

Oltre ai programmi congiunti, Esercito e Corpo dei Marines sono impegnati in specifici programmi a livello di singola forza armata aventi come obiettivo l'incremento delle rispettive capacità netcentriche. Ad esempio, una componente fondamentale della "network strategy" dell'Esercito è il programma Warfighter Information Network-Tactical (WIN-T), sistema sviluppato e prodotto da General Dynamics, che fornisce comunicazioni voce, video e dati sia via terra sia tramite collegamenti satellitari[48]. L'attuale upgrade (Increment 2) fornisce una capacità iniziale "On-The-Move", oltre a flussi di dati più ampi per i livelli superiori. Gli upgrades successivi sono destinati ad incrementare la sicurezza delle trasmissioni attraverso principalmente gli assetti aerei connessi all'architettura. Detto ciò, il Dipartimento della Difesa continua ad avere timori sull'instabilità, la complessità, l'affidabilità e la portata del sistema[49]. Timori peraltro condivisi in parte anche dall'Esercito, tant'è che si discute di una potenziale estensione o ristrutturazione del programma qualora tali criticità dovessero persistere[50]. Inoltre, le costanti pressioni sul budget contribuiscono non poco a rallentare l'effettivo impiego del programma WIN-T.

Un'altra importante iniziativa condotta dall'Esercito è il cosiddetto Nett Warrior, un sistema di comando di missione per il singolo soldato che fornisce comando, controllo e situational awareness a ciascun membro della squadra. Si tratta di un piccolo dispositivo commerciale che si connette alle rete tramite gli apparecchi radio e attraverso il quale l'Esercito cercherà di far convergere i dispositivi portatili in una singola tecnologia. La forza armata funge da integratore di sistema mentre varie aziende – tra cui Samsung, ADS-Inc. e General Dynamics – provvedono alla fornitura delle diverse componenti.

Oltre al già citato TCN, il Corpo dei Marines si trova impegnato nello sviluppo del Common Aviation Command and Control System (CAC2S). Il CAC2S è una combinazione di hardware, software e strutture fisiche che vuole supportare l'integrazione delle informazioni provenienti da piatta-

[48] "Bringing situational awareness to the battlefield", in *C4ISR & Networks*, 18 August 2014, http://www.c4isrnet.com/article/20140818/C4ISRNET06/308180005.

[49] US Dept of Defense, Director Operational Test and Evaluation, *Reasons behind program delays: 2014 update*, 26 August 2014, http://www.dote.osd.mil/pub/presentations/ProgramDelaysBriefing2014_8Aug_Final-77u.pdf.

[50] Sebastian Sprenger, "Army may break up major network program if results fall short", in *InsideDefense.com*, 14 October 2014.

forme aeree già esistenti (sia appartenenti al Corpo dei Marines che ad altre forze armate così come manned e unmanned) per agevolare la funzione di comando, controllo e coordinamento. I prime contractors sono in questo caso General Dynamics e Raytheon.

Ora, sebbene lo studio concentri la sua attenzione in particolare sulle forze terrestri americane, una visione completa e sufficientemente esaustiva del complesso mondo delle capacità netcentriche non può prescindere dal prendere in esame anche le iniziative della Marina e dell'Aeronautica, due forze armate che seguono e partecipano con uguale interesse a diversi programmi "network-enabled" per la funzione C2. Uno di questi è il Consolidated Afloat Networks and Enterprise Services (CANES) della U.S. Navy: trattasi della rete tattica di prossima generazione per le unità navali di superficie (incluse le navi d'assalto anfibie impiegate dai Marines) e sottomarini. Il programma vede inoltre il coinvolgimento di BAE, General Dynamics, Global Tactical Systems, Northrop Grummam e Serco. Al tempo stesso, attraverso il programma Navy Multiband Terminal sviluppato da Raytheon la Marina è alla ricerca di un accesso allo spazio più affidabile ed efficace. Sempre in un'ottica C2, l'Aeronautica punta al rinnovamento del suo Joint Surveillance and Target Attack Radar System (JSTARS) sostituendo la vecchia cellula del velivolo con un'altra già adottata su aeromobili commerciali. L'attuale piattaforma è realizzata da Northrop Grumman mentre in prospettiva del nuovo programma ci si aspetta una partecipazione più numerosa e variegata di più aziende concorrenti. La forza armata intende inoltre assicurare che il sistema sia capace di integrare facilmente nuovi sensori, computer, avionica e altri apparati elettronici non appena questi saranno sviluppati.

Intelligence. I principali programmi hanno lo scopo di incrementare l'abilità delle forze armate di sfruttare la molteplicità delle fonti d'intelligence. Ogni forza armata è coinvolta nello sviluppo e schieramento del Defense Common Ground System (DCGS); la configurazione adottata dall'Esercito è denominata DCGS-A mentre quella del Corpo dei Marines DCGS-MC. Il DCGS è un programma su larga scala con molteplici funzionalità, incluse l'elaborazione, lo sfruttamento, l'analisi e produzione di dati d'intelligence. La versione impiegata dall'Esercito (DCGS-A) è stata particolarmente criticata per essere eccessivamente "rigida", poco flessibile e difficile da utilizzare, sebbene i vertici della forza armata continuino a sostenere il programma e incoraggiare l'integrazione di nuove capacità[51]. Vari contractor della difesa partecipano al progetto, incluse

[51] A questo proposito l'Esercito è alla ricerca di informazioni (RFI) da parte di even-

Lockheed Martin, General Dynamics e Northrop Grumman, il cui costo totale – quando sarà terminato – dovrebbe aggirarsi intorno alle decine di miliardi di dollari.

Tutte le forze armate partecipano parimenti al programma Tactical Exploitation of National Capabilities, o TENCAP. Esso è incentrato sullo sviluppo di strumenti che permettano alle piccole unità sul terreno di attingere alle capacità di intelligence americane satellitari o di altra natura. TENCAP è una sorta di "programma ombrello" che include altrettanti progetti, iniziative e sistemi, con la partecipazione dei maggiori player della difesa americani.

L'Esercito prosegue congiuntamente con Boeing lo sviluppo del programma Enhanced Medium Altitude Reconnaissance and Surveillance System (EMARSS). I velivoli EMARSS sono progettati per rilevare, localizzare, identificare e seguire gli obiettivi di superficie, di giorno o di notte, in quasi tutte le condizioni atmosferiche. Essi forniranno capacità di intelligence, sorveglianza e ricognizione, nonché di comunicazione e di targeting. I miglioramenti previsti dal programma includono l'aggiunta di una suite di raccolta dati in tempo reale, multi-sensore e interconnessa, dedicata alle operazioni a livello di brigata e inferiore.

Fuoco. Ogni programma delle forze armate volto a supportare la capacità di produrre in maniera precisa "effetti" sul bersaglio, siano essi cinetici (fisici) o non-cinetici, si basa sullo sfruttamento dei vantaggi che l'interconnessione e le reti sono in grado di offrire. L'Esercito ad esempio cerca di fare leva sul programma WIN-T menzionato poc'anzi per facilitare una maggiore dispersione degli assetti di artiglieria, servendosi più recentemente delle comunicazioni satellitari per trasmettere dati in formato digitale e aumentare fino a dieci volte la velocità di esecuzione[52]. Inoltre, l'Esercito e il Corpo dei Marines collaborano congiuntamente all'interno dell'Advanced Field Artillery Tactical Data System (AFATDS) – realizzato da Raytheon – ossia un sistema automatizzato di comando e controllo di supporto al fuoco che si serve di connessioni dati digitali. Il sistema consente l'integrazione di artiglieria, missili, mortai, supporto di fuoco dagli assetti navali, e supporto aereo ravvicinato a molteplici livelli operativi.

---

tuali futuri fornitori su come migliorare il software e le capacità di visualizzazione del Defense Common Ground System Increment 2, il cui contratto verrà assegnato nel 2016. "Feedback Sought", in *Inside the Pentagon*, 21 August 2014.

[52] Kevin McCaney, "Mobile satellite network gives Army swift artillery support", in *DefenseSystems.com*, 2 December 2014, http://defensesystems.com/articles/2014/12/02/army-win-t-satellite-artillary-support.aspx.

L'Aeronautica e la Marina sono ugualmente interessate a sfruttare i vantaggi delle capacità netcentriche per le loro rispettive funzioni e capacità di ingaggio. Nonostante i dettagli a riguardo siano scarsi e frammentati perché classificati, il Long-Range Strike Bomber (LRS-B) dell'Aeronautica è candidato a sostituire l'attuale flotta di bombardieri. Il contratto verrà probabilmente assegnato al team Boeing-Lockheed Martin oppure a Northrop Grumman.

Si ipotizza che il progetto possa includere una sorta di "famiglia di sistemi" (family of systems) ma non è affatto chiaro quale forma e contenuto possa assumere. Alcuni esperti suggeriscono che possa trattarsi di un sistema integrato di missili e velivoli manned e unmanned[53], il che implicherebbe lo sviluppo di una notevole capacità netcentrica. In alternativa, questa "famiglia" potrebbe includere piattaforme "optionally manned" – ossia con o senza pilota – oppure di diversa grandezza. Dal momento che l'Aeronautica ha previsto il raggiungimento della capacità operativa iniziale (Initial Operating Capability, IOC) entro il 2025, ciò suggerisce che il programma cercherà di servirsi delle più avanzate tecnologie ICT disponibili nel breve periodo, ma altresì che farà affidamento su architetture aperte per integrare le repentine evoluzioni tecnologiche derivanti dallo sviluppo del mondo ICT. Dal canto suo la Marina si è piuttosto focalizzata su due innovazioni fondamentali in termini di capacità di fuoco: cannoni laser ed elettromagnetici a rotaia. Entrambi fanno leva sulle capacità netcentriche per acquisire il bersaglio e fare fuoco.

Movimento e manovra. Sebbene le restrizioni finanziarie abbiano in qualche modo ridimensionato le ambizioni delle due forze armate, Esercito e Corpo dei Marines proseguono nello sviluppo di nuove piattaforme sia terrestri che aeree. Pur non essendo motivate esplicitamente dalle potenzialità delle capacità netcentriche, ciascun programma vuole sfruttare al meglio l'evoluzione tecnologica nel campo dell'ICT. L'Esercito ad esempio è impegnato in diverse iniziative ritenute "significant priorities", incluso l'Armored Multi-Purpose Vehicle (AMPV) (sviluppato da BAE Systems), il programma Paladin Integrated Management (PIM) (BAE Systems) e il Joint Light Tactical Vehicle (JLTV) (AM General, OshKosh Defense, e Lockheed Martin)[54]. La forza armata sarebbe inoltre intenzionata a sviluppare un nuovo veicolo da combattimento per la fanteria per sosti-

[53] Stew Magnuson, "Top secret Air Force bomber program moves forward", in *National Defense*, September 2014, http://www.nationaldefensemagazine.org/archive/2014/September/Pages/TopSecretAirForceBomberProgramMovesForward.aspx.

[54] US Dept of the Army, *Army Equipment Program in Support of President's Budget 2015*, cit.

tuire i suoi ormai obsoleti carri armati Bradley, ma ha dovuto rimandare il progetto per mancanza di fondi.

Il Corpo dei Marines a sua volta partecipa al programma JLTV per rimpiazzare i suoi veicoli multipurpose Humvees e ritiene parimenti opportuno rivedere completamente la sua flotta di mezzi d'assalto anfibio, anch'essa in via di obsolescenza. A questo riguardo, la forza armata aveva originariamente optato per un veicolo ottimizzato per il trasporto nave-terra (con determinate capacità di combattimento terrestre) e per un altro mezzo con maggiore mobilità terrestre ma con limitate capacità di navigazione. Per ragioni finanziarie, ora la forza armata ha deciso di rimandare lo sviluppo di nuovo veicolo – capace di viaggiare ad alta velocità in acqua e per grandi distanze – preferendo invece l'Amphibious Combat Vehicle, o ACV. Su questo fronte, è stato adottato un approccio incrementale per l'acquisizione di diverse versioni del mezzo, la prima delle quali trarrà i maggiori benefici da tecnologie mature. Le aziende coinvolte nel programma non sono ancora state selezionate, sebbene il Corpo del Marines abbia esplorato alternative sia americane che straniere.

Per quanto riguarda le capacità aeree, nel 2014 l'Esercito ha reso noto un piano di riduzione delle capacità elicotteristiche da sette a quattro tipologie, rivedendo la loro distribuzione tra componenti attive e di riserva e migliorando l'attività addestrativa dei piloti. L'idea è quella di mantenere attivi gli aeromobili più moderni e dismettere quelli più obsoleti, o se non altro, meno netcentrici. Inoltre, proseguono gli upgrades alla versione E degli elicotteri d'attacco Apache AH-64 realizzati da Boeing.

Gli aggiornamenti prevedono l'integrazione di nuove tecnologie, fino ad includere dei sistemi di controllo di velivoli unmanned e un'architettura di sistemi aperti. Il Corpo dei Marines ha completato il dispiegamento del convertiplano Boeing-Bell V-22, impiegato anche dalle Special Operation Forces dell'Aeronautica. Il Corpo dei Marines è inoltre impegnato nella fase di test per il nuovo elicottero da trasporto pesante CH-53K (Sikorsky), il quale offre maggiori prestazioni in termini di potenza e una cabina di pilotaggio completamente digitalizzata.

Sul lato dei velivoli ad ala fissa, il Corpo dei Marines sono la prima forza armata ad impiegare una delle tre configurazioni dell'F-35 Joint Strike Fighter (JSF), programma in cui Lockheed Martin figura come prime contractor. La versione "B", a decollo corto e atterraggio verticale, si stima che possa raggiungere la capacità operativa iniziale nel 2015. La forza armata, insieme alla Marina, acquisirà inoltre un quantità limitata di velivoli versione "C" – per portaerei con catapulte – mentre l'Aeronautica ha optato

invece per la configurazione a decollo e atterraggio convenzionale. Tutte e tre le configurazioni fanno un abbondante uso delle ICT, utilizzando non solo le informazioni generate dai sensori di bordo e dai sistemi d'arma ma anche quelle originate da altri velivoli. I benefici che questi offrono in termini di interconnessione dei sensori sono visti come un vantaggio significativo rispetto ai velivoli attualmente in uso[55].

Protezione. Oltre a garantire una protezione intrinseca ai rispettivi veicoli, le forze terrestri degli Stati Uniti puntano ad estendere le capacità netcentriche anche ad altri programmi volti alla protezione delle forze. Al di là degli aggiornamenti per il semovente d'artiglieria Paladin, l'Esercito sta adottando alcune migliorie sul controllo del fuoco e sui sistemi di lancio del Multiple Launch Rocket System (MLRS) realizzato da Lockheed Martin. Nel frattempo, sta continuando ad acquistare radar Lockheed TPQ-53 per l'acquisizione di bersagli di controfuoco, il quale impiega le reti per supportare operazioni a distanza.

Il programma di punta del Corpo dei Marines volto ad aumentare la protezione da minacce aeree è il G/ATOR o Ground/Air Task Oriented Radar. Prodotto da Northrup Grumman Electronic Systems, il G/ATOR sarà costituito da due "blocchi". Il primo è focalizzato sulla difesa aerea a corto raggio, mentre il secondo sull'individuazione degli obiettivi per controfuoco. Inoltre, sebbene si prevedano dei "blocchi" aggiuntivi, questi non sono ancora stati pienamente/completamente definiti.

Oltre ai programmi d'artiglieria e di difesa aerea e missilistica, sia l'Esercito che i Marines stanno investendo somme ingenti nello sviluppo di contromisure a protezione da attacchi elettronici. Durante le guerre in Iraq e Afghanistan, buona parte di questi investimenti era atta a potenziare ed ampliare in tempi brevi il numero di dispositivi jammers (attivi e passivi) volti ad impedire la detonazione di IEDs. Tutte le forze armate, incluse quelle di terra, hanno dovuto riconoscere che gli avversari dispongono di ampie opportunità per sfruttare lo spettro elettro-magnetico, opportunità che trovano spesso la loro ragion d'essere nei costanti sviluppi commerciali delle ICT. Per fare fronte a questa sfida, l'Esercito intende aprire un nuovo laboratorio per testare nuove tecniche e modalità, tra cui diverse soluzioni per trattare tutta una serie di problematiche collegate alla frequenza dei dispositivi radio[56].

[55] US Marine Corps, *Concepts and Programs: Aviation, Joint Strike Fighter (JSF)*, https://marinecorpsconceptsandprograms.com/programs/aviation/joint-strike-fighter-jsf.

[56] Justin Doubleday, "Army aims to jump-start development of radio-frequency defenses", in *Inside the Army*, 29 December 2014.

Supporto logistico. Ogni singola forza armata è coinvolta nel programma Global Command Support System (GCSS), il cui prime contractor è Oracle, azienda basata in California. Trattasi di un sistema accessibile online che fornisce informazioni sullo stato logistico e finanziario delle unità schierate sia in territorio nazionale che all'estero, inteso a fornire una visibilità in tempo reale delle necessità di approvvigionamento e manutenzione delle forze. In modo analogo, l'Electronic Maintenance Support System del Corpo del Marines – sviluppato congiuntamente dalla Marina americana e dall'azienda GovWare LLC dell'Arizona – è un dispositivo portatile elettronico in grado di operare anche in rete, e permette agli operatori di interfacciarsi con il sistema e/o l'equipaggiamento in corso di manutenzione, avendo accesso ai dati tecnici e alla relativa documentazione.

Più in generale, Esercito, Aeronautica, Marina e Corpo dei Marines sono impegnati a fare leva sulle tecnologie ICT per migliorare il supporto anche a livello medico. In aggiunta agli investimenti del Dipartimento della Difesa per facilitare un maggiore accesso alle cartelle sanitarie elettroniche, alcune forze armate stanno investendo in capacità netcentriche per ottimizzare la logistica dei servizi medici e incrementare la quantità di informazioni mediche disponibili alle forze schierate sul terreno.

Key enablers. Lo spazio extra-atmosferico rimane uno dei domini fondamentali a supporto delle capacità netcentriche, ragion per cui le iniziative intraprese in questo campo ricevono spesso importanti finanziamenti. Come osservato in precedenza, gli Stati Uniti dispongono di varie costellazioni di satelliti, tra cui il sistema WGS (realizzato da Boeing), SBIRS (Lockheed Martin e Northrup Grumman) e AEHF (Lockheed Martin). Il Dipartimento della Difesa sta altresì incrementando l'impiego di satelliti commerciali e, simultaneamente, sta considerando l'eventualità che le forze armate siano chiamate ad accettare uno sviluppo più lento e graduale delle capacità di ogni nuovo satellite al fine di ridurre i rischi tecnici e così abbassare i relativi costi di sviluppo[57]. Tra le principali aziende coinvolte si annoverano Intelsat, Braxton Technologies, e DigitalGlobe (che si è recentemente fusa con GeoEye).

Infine, benché sottoposte a forti pressioni finanziarie, le forze armate hanno continuato ad investire notevoli risorse nei servizi ICT. Un recente

[57] Si veda ad esempio Marcus Weisgerber, "USAF General: DoD Must Change How it Buys Satellites", in *C4ISR & Networks*, 19 August 2014, http://www.c4isrnet.com/article/20140813/C4ISRNET06/308130001.

rapporto ha evidenziato che i contratti relativi al settore dei servizi in generale stipulati dall'Esercito sono diminuiti complessivamente del 15% tra il 2009 e il 2012. Tuttavia, i contratti per i servizi ICT sono diminuiti nello stesso periodo solo del 4%[58]. Le imprese maggiormente attive in questo campo includono Lockheed Martin, Northrop Grumman e General Dynamics.

1.4 Sfide e opportunità future

Le ICT e le capacità netcentriche, così come il loro impiego, sono chiaramente destinate a permeare il tessuto militare e industriale degli Stati Uniti. Oltretutto, molti ritengono che il loro potenziale sia ancora tutto da scoprire e che solo in parte sia stato adeguatamente sfruttato. Persistono però ancora diverse difficoltà – a livello tecnico e di interoperabilità – limiti finanziari, ostacoli istituzionali, giuridici e di policy.

Tecnologia. Malgrado il ritmo vertiginoso dell'innovazioni tecnologica, rimangono ancora irrisolte diverse incognite di natura tecnica legate alle capacità netcentriche. Probabilmente le criticità maggiori sono quelle poste da vincoli strettamente fisici; dimensione, peso e potenza continuano a limitare il pieno sfruttamento delle capacità sia a livello di sistemi d'arma sia a livello del singolo soldato. Le forze di terra americane rimangono molto attente nel soppesare i benefici che si trarrebbero dall'inserimento di nuovi dispositivi netcentrici rispetto a cosa comporterebbero e "costerebbero" in termini di capacità di carico e di alimentazione. A tal fine, la ricerca prosegue verso lo sviluppo di batterie con maggiore densità energetica e/o di minor peso.

Nonostante la cyberdefense costituisca un interesse crescente, le forze armate ancora mal sopportano le restrizioni o gli impedimenti necessari per rafforzare la sicurezza cibernetica. Il trade-off tra sicurezza e funzionalità coinvolge nondimeno i programmi a livello di singola forza armata. Per esempio, la versione dell'Esercito del DCGS è stata fortemente criticata, anche pubblicamente, per non aver sufficientemente sfruttato gli sviluppi tecnologici in campo commerciale. L'Esercito, dal canto suo, ha risposto affermando che alcuni sistemi commerciali non sono in grado di

[58] Jesse Ellman, Gregory Sanders and Rhys McCormick, U.S. Department of Defense Contract Spending and the Industrial Base, 2000-2013, in *CSIS Events*, 16 October 2014, http://csis.org/node/52055.

collegarsi adeguatamente o in maniera sicura alla totalità dei database di intelligence americani così come alle relative reti. Comunque, ci sono forti pressioni sia sulle forze armate sia al loro interno affinché da una parte si aumenti l'efficacia e l'efficienza, sfruttando gli sviluppi tecnologici avvenuti in campo commerciale, e dall'altra si minimizzino i rischi di una eventuale compromissione dei dati.

Interoperabilità. L'interoperabilità con le altre forze armate americane e con i principali partner internazionali è solo in parte un problema tecnico ed è soprattutto un problema politico. La strategia americana indica chiaramente che le future operazioni saranno a carattere interforze e internazionale. Detto questo, sebbene ogni amministrazione americana affermi e ribadisca il diritto sovrano di intraprendere iniziative unilaterali, è ormai generalmente riconosciuto che esse non siano più concepibili né realizzabili concretamente. L'interoperabilità continua quindi ad essere una priorità a vari livelli: all'interno di ogni singola forza armata, tra le forze armate, e con i maggiori partner internazionali.

Ma nonostante la retorica, a livello pratico c'è ancora molto da fare. Ne è un esempio l'esperienza in Iraq e Afghanistan dove l'Esercito ha schierato troppo rapidamente così tanti e diversi sistemi netcentrici da non disporre dei necessari procedimenti per assicurare che tali sistemi fossero interoperabili perfino tra le stesse formazioni dell'Esercito americano.

Alla luce di questa e altre esperienze, l'Esercito ha deciso così di istituire il Network Integration Evaluation (NIE), una sorta di evento che si tiene più volte l'anno volto a testare l'interoperabilità di un determinato sistema all'interno di una brigata, inserire nuove capacità all'interno dei programmi già avviati, e identificare tecnologie ritenute promettenti per un loro rapido dispiegamento in teatro[59]. Il valore e l'efficacia del NIE sono stati messi in discussione sia dalle aziende fornitrici della Difesa che dal Congresso[60], ma l'Esercito continua a sostenere la sua utilità nel coadiuvare la forza armata per valutare possibili nuovi sistemi e per verificare l'opportunità di intraprendere cambiamenti o modifiche atti ad incrementare l'efficacia degli equipaggiamenti esistenti[61]. I vertici dell'E-

[59] US Dept of Defense, Director Operational Test and Evaluation, Army Programs, *Network Integration Evaluation (NIE)*, 2011, http://www.dote.osd.mil/pub/reports/FY2011/pdf/army/2011nie.pdf.

[60] Si veda a titolo di esempio: Ellen Mitchell, "Shyu: Army to procure $25M in technologies tested at NIE 14.1", in *Inside the Army*, 8 September 2014.

[61] Ellen Mitchell, "Key Army official predicts growth of "Network Integration Evaluation" drills", in *Inside the Army*, 3 October 2014.

sercito difendono saldamente il NIE ma hanno parimenti riconosciuto che le critiche potrebbero minarne la reale fattibilità.

Motivo per cui si pensa di far evolvere il NIE in un più ampio Capabilities Integration Assessment (CIA), che possa estendere il suo mandato ben al di là delle tecnologie netcentriche. Gli stessi vertici della forza armata prevedono inoltre di associarlo più direttamente all'Army Warfighter Assessment, il quale diventerà la "sede" principale per le attività di sperimentazione e "concept development", mentre il CIA fungerebbe in sostanza per la verifica finale e la convalida prima dell'impiego in teatro. Inoltre, la forza armata sembra intenzionata a focalizzare le prossime esercitazioni (wargames) sull'interoperabilità sia in un'ottica interforze sia con altri importanti partner internazionali[62]. L'Esercito, insieme a tutte le altre forze americane, continuerà inoltre a partecipare al Joint Users Interoperability Coalition Exercise (JUICE), esercitazione annuale dedicata all'interoperabilità tra le forze armate, con altre agenzie governative e con principali Paesi alleati. Da un punto di vista tecnico, l'Esercito sta rivedendo alcune delle sue modalità di acquisizione per coinvolgere maggiormente l'industria e confrontarsi con essa su come strutturare più adeguatamente quelle architetture aperte concepite per specifici programmi – come i sistemi robotici e unmanned[63]; un passaggio, questo, che dovrebbe incrementare la funzionalità man mano che i programmi evolvono.

Le forti pressioni sul bilancio sembrano però incoraggiare ognuna delle forze armate a "start at home", ossia ad attribuire priorità al miglioramento dell'interoperabilità a livello interno, poi in un'ottica joint e solo in seguito in prospettiva multinazionale. Al tempo stesso ognuna di esse sembra voler confermare, per quanto possibile, la propria partecipazione alle esercitazioni internazionali (sia per ragioni militari che diplomatiche), che rimarranno probabilmente nei prossimi anni la principale occasione per lavorare sulle questioni dell'interoperabilità multinazionale.

A livello di policy in materia di acquisizioni, la Difesa stabilisce che l'equipaggiamento sarà interoperabile nel suo complesso, e che quello

[62] Questi "war games" potrebbero agevolare il processo di allineamento tra capacità e obiettivi ma è improbabile che essi forniscano utili spunti o suggerimenti in merito alle capacità tecniche attuali. Joe Gould, "New war game to focus on tech, partnerships," in *Defense News*, 13 October 2014, http://www.defensenews.com/article/20141013/SHOWSCOUT04/310130030.

[63] Mary-Louise Hoffman, "Heidi Shyu: Army eyes interoperability, open standards for ground robotic system", in *Executive Gov*, 15 August 2014, http://www.executivegov.com/?p=62462.

specificatamente acquisito per determinate operazioni sarà interoperabile con tutti i partner della coalizione[64]. Assunto, questo, che trova ulteriore riscontro nell'indicazione secondo la quale l'information technology utilizzata da ogni altra organizzazione all'interno del Dipartimento deve essere interoperabile con i sistemi esistenti e futuri "nella misura più ampia possibile" e con l'equipaggiamento delle altre forze armate (anche internazionali)[65]. Tuttavia, allineare gli investimenti e gli standard tra i principali Paesi rimane una questione da affrontare. Come ha fatto notare un ufficiale dell'Esercito americano di base in Europa, i Paesi NATO sono ancora incapaci di dispiegare dei dispositivi radio capaci di fornire comunicazioni dirette[66], in parte perché l'aspetto dell'interoperabilità a livello NATO non sembra costituire un fattore sufficiente rilevante nelle scelte di procurement adottate a livello nazionale.

Da un punto di vista operativo, nonostante le tecnologie permettano la condivisione dei dati, l'approvazione di tale condivisione richiede spesso negoziazioni bilaterali alquanto dettagliate che tuttavia non possono prevedere ogni circostanza che si può verificare a livello tattico, causando continue frizioni e contrasti durante l'effettiva condotta delle operazioni. Alcuni funzionari della difesa americana stanno tentando di colmare il suddetto gap, identificando quelle tipologie contrattuali che potrebbero essere negoziate prima dell'effettivo inizio della missione, ma il risultato resta ancora tutto da verificare. Certamente, un aspetto ancora irrisolto a livello internazionale è rappresentato dalla legislazione americana. L'oltre un decennio di operazioni intraprese con diversi partner internazionali ha portato senza dubbio ad una maggiore condivisione rispetto al passato, ma la sua evoluzione è stata comunque più lenta di quanto ritenuto necessario. Capacità come l'Afghan Mission Network – che attinge e condivide dati provenienti dalle reti nazionali – hanno notevolmente agevolato la condivisione dei dati a livello multinazionale, ma le soluzioni rimangono tuttora disomogenee, pensate su misura e quindi piuttosto customizzate.

---

[64] US Dept of Defense, *Instruction 2010.06*: Materiel Interoperability and Standardization with Allies and Coalition Partners, 29 July 2009, http://dtic.mil/whs/directives/corres/pdf/201006p.pdf.

[65] US Dept of Defense, Instruction 8330.01, *Interoperability of Information Technology (IT), including National Security Systems (NSS)*, 21 May 2014, http://dtic.mil/whs/directives/corres/pdf/833001p.pdf.

[66] Walter Piatt, "The Future of European Collective Defense", in *CSIS Events*, 16 October 2014, http://csis.org/node/52206.

Risorse e bilancio. Sebbene il bilancio della difesa americano sia notevolmente superiore rispetto a quello di molti altri Paesi, ciò non impedisce l'articolazione di un vivace dibattito interno sulle questioni fiscali e, in particolare, sullo stesso budget della difesa. Malgrado gli Stati Uniti abbiano registrato frequenti altalene di aumento e riduzione di tale bilancio, molti esperti si attendevano una riduzione della spesa militare in seguito al ritiro dei contingenti in Iraq e Afghanistan. Tuttavia, altri hanno fatto notare che alcuni cambiamenti strutturali avvenuti all'interno della struttura di bilancio rendono tali riduzioni più difficili da realizzare rispetto a quanto fatto in precedenza. Infatti, rispetto agli aumenti verificatisi in passato, gran parte delle spese aggiuntive osservate negli anni 2000 non era dovuta all'impiego massiccio di personale aggiuntivo.

Ciò significa che i consueti interventi di riduzione quantitativa della forza non rendono lo stesso livello di risparmio che generavano in precedenza. C'è da dire inoltre che le numerose crisi internazionali scoppiate nel 2014 – dalle incursioni russe in Ucraina, all'epidemia di Ebola in Africa, fino all'avanzamento dello Stato Islamico in Iraq – hanno indotto molti a rivedere le proprie considerazioni in merito al cosiddetto "dividendo della pace"[67]. Mentre le capacità militari americane sono sottoposte a continue sollecitazioni e pressioni, l'attuale legge approvata nel 2011 richiede di imporre un tetto alla spesa pubblica (inclusa la difesa) a livelli inferiori rispetto al passato. Ne consegue quindi che qualora l'Esecutivo presenti delle proposte di budget superiori ai tetti di spesa prefissati, le risorse di ogni Dipartimento – incluso quello della Difesa – sarebbero soggetti a tagli lineari.

La legge è stata lungamente dibattuta, e sia il Congresso che l'Esecutivo sono stati coinvolti in vari scontri a livello politico nel tentativo di addossarsi l'un l'altro la colpa dei suddetti tagli. Per le forze armate, la reale conseguenza si è tradotta non solo in un ammontare di risorse inferiore rispetto a quanto ritenuto indispensabile, ma altresì in una forte incertezza sulle future condizioni finanziarie[68]. Esercito e Corpo dei Marines,

[67] Un caso particolarmente noto è l'editoriale di un influente quotidiano americano che sosteneva la necessità di riportare la spesa per la difesa ai livelli previsti e pianificati in precedenza. "Paying for wars against the Islamic State, Ebola, and more", in *The Washington Post*, 5 October 2014, http://wpo.st/S9aG0.

[68] Questo perché il ramo esecutivo ha rifiutato di sottoporre proposte di bilancio conformi ai limiti massimi stabiliti per legge, nella speranza di un loro possibile allentamento da parte del Congresso. Una strategia che nel 2013 ottenne un parziale successo in seguito all'approvazione di una proposta di legge che ne concedeva un allentamento temporaneo

oltre a ridurre il personale nella misura in cui ritenevano possibile pur mantenendo un appropriato mix di esperienza, hanno dovuto cancellare un certo numero di programmi già pianificati.

L'Esercito nello specifico ha adottato una "strategia di impiego incrementale" delle capacità ritenute essenziali – come il WIN-T – che in certa misura accentua le sfide in termini di interoperabilità poiché le unità si trovano ad utilizzare differenti versioni di vari equipaggiamenti. Seppur il Corpo dei Marines tragga beneficio dalle sue dimensioni più ridotte, anch'esso è stato costretto a dare priorità alla messa in campo degli equipaggiamenti ritenuti indispensabili. Ed entrambe le forze armate hanno dovuto rallentare lo sviluppo e l'acquisizione di altre ICT e NEC. Entrambe ritengono inoltre che ulteriori riduzioni potrebbero essere necessarie in mancanza del consenso politico di ripristinare il finanziamento alle spese della difesa[69].

Ambito istituzionale. È ampiamente riconosciuto che le procedure di acquisizione di servizi e prodotti per la difesa siano piuttosto problematiche. È altrettanto e forse più complesso definire quale sia il modo migliore per cambiare l'attuale sistema. Ci sono stati decine di rapporti, commissioni e studi sulla riforma del processo di acquisizione (acquisition reform), ma i progressi a riguardo sono stati altrettanto limitati e circoscritti. Il Dipartimento della Difesa e il Congresso sono attualmente impegnati in un'ulteriore spinta riformatrice. Uno dei punti cardine emersi durante l'ultimo dibattito sulla riforma è costituito dalla necessità della Difesa di adoperare un approccio più sfumato – meno "one-size-fits-all" – circa l'acquisizione di diverse tipologie di capacità militari. In ambito NEC, alcuni hanno suggerito che il sistema tradizionale può essere adatto nel caso di reti fisse ma – per altri sistemi e servizi ICT – è necessario un sistema più rapido, meno rigido e quindi più flessibile[70].

L'idea non è nuova e sono state proposte varie soluzioni. In generale, quando applicate al settore ICT, le procedure esistenti sono ritenute

per soli due anni. La strada da percorrere rimane però tuttora incerta: l'Esecutivo sembra essere ancora riluttante a presentare proposte di bilancio nei limiti prestabiliti mentre il Congresso appare poco intenzionato a concedere maggiori risorse. In assenza di un ulteriore accordo bipartisan, le risorse del Dipartimento della Difesa saranno ancora soggette a progressive riduzioni negli anni a venire.

[69] Jason Sherman, "In event of sequester, entire modernization portfolio to be 'stretched out'", in *InsideDefense.com*, 14 October 2014.

[70] Justin Doubleday, "Army crafting career field, occupational specialty for cyber forces", in *Inside the Army*, 19 September 2014.

responsabili di numerosi ritardi nella tabella di marcia e di generare un aumento significativo dei costi. In un rapporto del 2009, l'autorevole Defense Science Board (DSB) ha evidenziato che

> [i]l problema fondamentale [che deve affrontare il Dipartimento della Difesa] è che il processo attraverso il quale vengono acquisiti i sistemi d'arma e l'information technology non corrisponde alla velocità con cui le nuove capacità IT vengono introdotte nell'odierna era dell'informazione. Di conseguenza [...] la Difesa necessita di un nuovo sistema di acquisizione nel campo dell'IT[71].

Altri invece sostengono che il sistema attuale sia praticabile se attuato in modo diverso: per esempio, alcuni centri di ricerca hanno pubblicato delle sorta di linee guida volte ad assistere il Pentagono a migliorare il suo processo di acquisizione[72].

Prendendo atto delle sfide da affrontare, la Difesa ha preferito adottare quest'ultimo approccio, impegnandosi a utilizzare al meglio le procedure esistenti piuttosto che rielaborarle in toto. A tal fine, lo Stato Maggiore ha recentemente modificato il sistema ufficiale di acquisizione per creare una nuova "categoria" riferita ai programmi IT, consentendo una maggiore delega del potere decisionale. Inoltre, il Pentagono sta tentando di reclutare nuovi professionisti con una preparazione specifica dei sistemi IT[73]. Ciononostante, ancora una volta, quanto questi sforzi avranno davvero successo non è dato sapersi, e alcuni esperti del settore continuano a ritenere che alla fine si renderà necessario rivedere l'intera architettura di acquisizione. In tutto questo, il Congresso deve ancora meditare sulla sua posizione mentre l'industria vigila attentamente per controllare se e come le riforme legislative promesse nel 2015 affronteranno questo argomento. Se così fosse, non è ancora chiaro se il Congresso proporrà un nuovo sistema, delle modifiche su quello esistente, oppure una via di mezzo tra le due opzioni.

Uno dei motivi per cui il Dipartimento della Difesa ha riscontrato di-

---

[71] US Dept of Defense, *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology*, March 2009, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf.

[72] Pete Modigliani and Su Chang, *Defense Agile Acquisition Guide. Tailoring DoD IT Acquisition Program Structures and Processes to Rapidly Deliver Capabilities*, Mitre Corporation, March 2014, http://www.mitre.org/node/18951.

[73] US Senate, Committee on Armed Services, *Testimony of Frank Kendall*, 30 April 2014, http://www.armed-services.senate.gov/imo/media/doc/Kendall_04-30-14.pdf.

verse difficoltà nell'affidarsi agli sviluppi commerciali nel campo delle ICT può attribuirsi al fatto che esso ha agito per molto tempo come "market driver" piuttosto che "market taker". I funzionari della Difesa tradizionalmente chiedevano alle aziende di adattarsi ai cambiamenti per soddisfare le esigenze militari, per esempio in termini di maggior sicurezza oppure incrementando la capacità di un dato componente di resistere a temperature o ad altri eventi meteorologici estremi. Per molti fornitori di prodotti ICT tuttavia, il mercato della difesa è così piccolo e relativamente poco remunerativo rispetto all'alternativa commerciale che non vale la pena né di investire né di tentare di penetrarlo. Tale compito ricade quindi sulle aziende della difesa più tradizionali, richiedendo loro più tempo e spese significative o comportando la rinuncia a funzionalità chiave; due aspetti che contrastano con alcune logiche fondamentali dell'acquisto di prodotti commerciali.

I diritti di proprietà intellettuale sono un ulteriore elemento di criticità. Il Dipartimento della Difesa, sostenuto dal Congresso, è stato sempre più esplicito circa la sua intenzione di evitare l'acquisizione di sistemi con interfacce hardware e software brevettate[74]. Tuttavia, le aziende con modelli di business strutturati su diritti di proprietà di lunga data sono restie a muoversi verso architetture più aperte, specialmente quando percepiscono che il tempo è dalla loro parte. Le aziende che hanno sviluppato componenti chiave di sistemi più complessi – i quali stanno divenendo obsoleti e necessitano di sostituzioni o aggiornamenti – devono decidere se vogliono continuare a competere per un ruolo che forse potrebbe essere minoritario col passare del tempo.

Alcune delle aziende stanno optando per questa soluzione mentre altre – consapevoli che trovare una soluzione alternativa in grado di fornire livelli equivalenti di interoperabilità o prestazioni avrebbe costi proibitivi per le forze armate – continuano a commercializzare soluzioni brevettate. Un ulteriore ostacolo è rappresentato dal tempo necessario per sviluppare standard sufficientemente in grado di supportare un approccio basato sull'architettura aperta. Nei casi in cui questi non siano ancora stati definiti, i vertici aziendali sono stati costretti a rinunciare ai requisiti legali per le soluzioni non brevettate affinché potessero proseguire con le necessarie acquisizioni[75].

[74] Ad esempio, il National Defense Authorization Act per l'anno fiscale 2013 includeva un provvedimento che proibisce al Dipartimento della Difesa Americano di acquisire "proprietary or undocumented waveforms or interfaces".

[75] Jordana Mishory, "DoD waives data link requirement so Navy can obtain eight sy-

Benché la strada da fare sia ancora piuttosto lunga, le forze armate continuano a fare progressi per sfruttare meglio gli sviluppi tecnologici in campo commerciale. Il successo o meno di queste iniziative può dipendere da "piccoli" dettagli circa la proprietà intellettuale e la contrattualistica, ma anche dalla pianificazione e dal budget. Ad esempio, al momento il Dipartimento della Difesa sta esaminando come modificare le modalità di valutazione delle proprie necessità future circa il supporto fornito da satelliti commerciali con l'obiettivo di definire dei procedimenti d'acquisizione più efficienti[76].

Concettuale. Come discusso poc'anzi, sia le forze armate che più in generale il Dipartimento della Difesa riconoscono sia le opportunità che le vulnerabilità associate ad una forte dipendenza dalle reti. Ciononostante non sembra emergere al momento una visione condivisa su come affrontare soprattutto le seconde, ossia le vulnerabilità. La naturale propensione delle forze armate è stata quella di difendersi, specialmente in campo cyber – aumentando la spesa per le capacità di difesa e quelle per l'infrastruttura e la progettazione di reti. In campo spaziale, tale approccio si è tradotto piuttosto in un'attenzione più bilanciata verso l'incremento sia delle capacità di difesa sia della resilienza, in termini di payloads, satelliti e costellazioni. Nell'ambito relativo allo spettro elettromagnetico, il tradizionale filone di studi e ricerca sulla guerra elettronica ha accentuato l'attenzione sulle capacità di difesa.

Alcuni di questi approcci sono basati sull'evoluzione della minaccia, e hanno radici sia culturali che burocratiche, mentre altri ne riflettono la natura attuale, così come i costi (finanziari e non) di soluzioni alternative. In ogni caso, solo in seguito ad un vero dibattito a livello nazionale si potrà definire la migliore strategia relativa a ciascun aspetto delle capacità netcentriche e valutare, di conseguenza, la necessità di cambiamenti. Ad esempio, il comandante del US Army Cyber Command ha affermato che disporre di una capacità totale di cyber defense non sia possibile, e che l'Esercito "[deve] essere in grado di operare anche qualora venisse compromesso."[77] La capacità delle forze di terra americane di addestrarsi in tal senso è ostacolata da una serie di fattori, dalla legislazione nazionale

stems", in *Inside the Pentagon*, 14 August 2014.

[76] Scott Maucione, "Pentagon eyes reforms in commercial SATCOM acquisition practices", in *Inside the Pentagon*, 9 October 2014.

[77] Edward C. Cardon, *Keynote Address*, Brookings Fifth Annual Military and Federal Research Symposium: "Securing America's Future in the New 'Interwar Years'", 12 March 2014, http://brook.gs/1F8BpAi.

che limita alcuni tipi di attività cyber all'interno degli Stati Uniti fino alla carenza di risorse volte a sostenere tale addestramento. Ma questo potrebbe anche essere un indizio della volontà che il problema non si ponga; è molto meno complicato presupporre che le reti, in qualche modo, saranno comunque funzionali.

Questioni politiche/regolatorie. Infine, come spesso accade, gli sviluppi nel campo dell'ICT evolvono in molti casi più velocemente di quanto non facciano gli "impianti" politici e regolatori che dovrebbero permettere la loro piena applicazione. Il tema dell'interoperabilità è già stato in parte discusso, ma le criticità si annidano e si estendono anche ad altri campi. Ad esempio, le policies americane che regolano l'utilizzo delle tecnologie cloud da parte delle forze armate riflettono alcune tensioni tra i timori circa la sicurezza, l'accessibilità economica e, appunto, l'interoperabilità. Il Chief Information Officer della Difesa ha recentemente riconosciuto che il suo dipartimento è stato eccessivamente lento a fornire le dovute indicazioni su come ciascuna delle forze armate debba acquisire servizi e prodotti cloud. Alla fine il Dipartimento della Difesa si è orientato verso un approccio decentralizzato affinché ciascuna delle forze armate possa procurarsi autonomamente sistemi cloud digitalizzati se conformi agli standard comuni. Questa decisione ha però subito sollevato forti preoccupazioni sul fatto che l'interoperabilità potrebbe essere compromessa, ora o in futuro, man mano che i fornitori sono in grado di perfezionare le loro offerte commerciali[78]. Mentre queste incertezze potrebbero rivelarsi ingiustificate, esse sono comunque rappresentative delle sfide che persistono nell'ottenere sistemi e servizi che permettano di raggiungere una vera interoperabilità tra le varie organizzazioni, americane e non.

Un altro settore in cui i progressi tecnologici mettono a dura prova l'impianto giuridico esistente è quello relativo alle attività militari nello spettro elettromagnetico. Via via che si sviluppano nuove capacità, molti cercano di integrare le informazioni di intelligence con l'abilità di produrre effetti. Ciò crea una tensione intrinseca tra il Titolo 50 del Codice della legislazione federale degli Stati Uniti (US Code[79]), che disciplina le

[78] Scott Maucione, "Upcoming DoD CIO cloud policy leaves questions over interoperability", in *Inside the Pentagon*, 9 October 2014.

[79] Lo US Code è composto da cinquanta titoli, a ciascuno dei quali corrisponde una materia oggetto di legislazione. Il titolo 10 (Armed Forces) fornisce la base legale in merito ai ruoli, alle missioni e all'organizzazione di ciascuna delle forze armate americane e del Dipartimento della Difesa. Il titolo 50 (War and National Defense) è suddiviso in ulteriori 43 capitoli.

attività di intelligence, con il Titolo 10 che regolamenta le operazioni militari[80]. Le operazioni di guerra elettronica sono state condotte nell'ambito del Titolo 10 ma, ad esempio, la volontà di coniugare le attività di guerra elettronica (che cercano di interrompere i segnali) con operazioni cyber (che potrebbero cercare di influenzare le informazioni all'interno di tali segnali) presenta nuove sfide di tipo giuridico che non sono ancora state pienamente esaminate, né tanto meno risolte[81]. Si tratta di una problematica complessa, resa ulteriormente spinosa dall'esistenza di leggi che limitano ciò che può essere fatto negli Stati Uniti, influendo di fatto sulle modalità attraverso le quali le forze armate addestrano il proprio personale all'impiego di tali strumenti.

1.5 Conclusioni

In conclusione, le forze armate americane sono e saranno in futuro completamente dipendenti dalle capacità netcentriche, in ogni funzione e dominio di combattimento: aria, terra, mare, spazio e cyber. Il grado con cui le capacità netcentriche sono impiegate per scopi offensivi e difensivi varia in ogni dominio e funzione, così come il bilanciamento tra un approccio difensivo rispetto ad quello "dispersivo" per mitigare le vulnerabilità loro associate. E sebbene le ICT e le capacità netcentriche abbiano trasformato le modalità di condotta, odierne e future, della guerra da parte degli Stati Uniti, rimangono ancora irrisolti molti ostacoli circa il loro potenziale sfruttamento. Detto questo, il momento è propizio; la sfida, per l'Esercito americano e il Corpo dei Marines, sarà quella di massimizzarne i benefici minimizzando i rischi.

[80] Sydney J. Freedberg, "STRATCOM lacks authority, $$ on electronic warfare", in *Breaking Defense*, 7 October 2014, http://breakingdefense.com/?p=16291.

[81] Maren Leed, *Offensive Cyber Capabilities at the Operational Level. The Way Ahead*, Washington, Center for Strategic and International Studies (CSIS), September 2013, http://csis.org/node/46679.

2.
Il percorso d'avvicinamento alle NEC: Francia, Germania e Regno Unito

Nick Brown[1]

2.1 Introduzione

Francia, Germania e Regno Unito hanno già da tempo intrapreso il cammino verso la digitalizzazione delle proprie forze armate per mettere in campo adeguate NEC.

A livello nazionale, ognuno di questi tre Paesi sembra aver iniziato percorsi differenti e, in un certo senso, l'esperienza di ognuna di queste nazioni con i programmi di digitalizzazione degli equipaggiamenti del singolo soldato costituisce una cartina tornasole della loro più ampia esperienza con le NEC. La precoce adozione e l'impegno da parte francese nel programma Fantassin à Équipementet Liaisons Intégrés (FELIN) – soldato di fanteria con equipaggiamenti e collegamenti integrati – ed il dispiegamento relativamente tardivo della Francia in Afghanistan hanno permesso al Paese di elaborare un pacchetto coeso di sistemi, che funzionano a livello di singolo soldato e costituiscono la base di partenza per costruire una rete costituita da altre piattaforme dispiegate in teatro operativo.

Se messi a confronto, sempre a livello di digitalizzazione degli equipaggiamenti del singolo soldato, i tentativi britannici legati al programma Future Infantry Soldier Technology (FIST) hanno garantito qualche successo iniziale. Tuttavia, l'adozione da parte di Londra di Urgent Operational Requirements, (UOR) – ovvero acquisizioni urgenti di sistemi quali radio, visori ottico-elettronici ed altri equipaggiamenti off the shelf per fornirli rapidamente alle truppe dispiegate in teatro operativo – hanno causato involontariamente dei problemi, che alla fine hanno fatto naufragare tanto il FIST quanto altri progetti di digitalizzazione. Infatti, un tale processo di acquisti off the shelf ha impedito al Ministero della Difesa di

[1] La traduzione dall'inglese all'italiano è stata curata da Leonardo Tiengo.

acquisire o sviluppare elementi e moduli che avrebbero potuto operare meglio assieme all'interno di un sistema coeso.

Similmente, i piani dell'Esercito britannico per un lancio su larga scala degli ammodernamenti progettati per il sistema di comunicazioni Bowman sono naufragati. Ciò è avvenuto a causa della necessità di bilanciare due necessità confliggenti: da un lato l'esigenza di disporre il prima possibile in teatro degli standard più avanzati di equipaggiamenti; dall'altro, quella di assicurare che anche i soldati in fase di addestramento per il successivo avvicendamento in missione avessero accesso a quei sistemi e fossero in grado di usarli adeguatamente. In tempo di pace questo bilanciamento non avrebbe costituito un problema: standard più avanzati avrebbero potuto essere introdotti in servizio da una compagnia o da un reggimento nel momento in cui fossero stati disponibili. Invece, le rotazioni degli operativi in Afghanistan e Iraq si sono dimostrate una complicazione troppo difficile da gestire per il procurement militare. Le Forze Armate britanniche hanno imparato da questa esperienza e vi sono già ora tentativi volti a impedire che tali problematiche si ripetano nuovamente, in particolar modo adesso che il nuovo sistema che sostituirà il Bowman – il cosiddetto Morpheus – è in fase di sviluppo.

L'esperienza dell'Esercito britannico con un singolo prime contractor – General Dynamics – durante il programma Bowman ha altresì spinto la forza armata ad adottare un approccio completamente diverso con il Progetto Morpheus. Invece di siglare un contratto "big bang" con un fornitore unico, l'attuale programma dell'Esercito punta ad indire una serie di gare che incarichino industrie diverse di fornire componenti differenti, anche se in modo coerente tra loro. Quantunque questo obblighi l'Esercito a generare e sostenere un nuovo livello di expertise al proprio interno per la gestione dei vari programmi, lo lascia comunque meno dipendente dalla volontà e dai vincoli di un singolo prime contractor.

L'esperienza tedesca con il programma di digitalizzazione degli equipaggiamenti del singolo soldato "Fante del Futuro" (Infanterist der Zukunft, IdZ) si colloca a metà strada tra l'esperienza francese e britannica. L'IdZ è rimasto ancorato ai suoi piani e concetti originali, a differenza di quanto accaduto nel Regno Unito, ma si è dimostrato più flessibile del sistema sviluppato dalla Francia in quanto l'Esercito tedesco non ha avuto timore nell'eliminare gli elementi che non funzionavano come sperato per cercare nuove soluzioni.

In linea generale, malgrado i tre Paesi condividano l'esperienza delle realtà operative dell'ultimo ventennio – grazie ai combattimenti fianco

a fianco in Afghanistan ed in altri teatri – ognuno di essi rimane concentrato nello sfruttare al meglio i benefici potenziali offerti da NEC a livello nazionale, sia esso di singola forza armata o interforze. Si può sostenere che questo approccio sia il più sensato, poiché ha poco senso creare piattaforme sicure per l'interconnessione con gli alleati internazionali se, a livello nazionale, i singoli equipaggiamenti della squadra o della task force interforze non comunicano fra di loro. Ma rimane il fatto che una delle più grandi sfide con cui ci si è dovuti misurare nel corso delle missioni internazionali in Afghanistan, Iraq, Libia e altrove, sia stata quella posta dalla difficoltà di armonizzare l'operato di forze armate di diversi Paesi che adottavano interpretazioni indipendenti dei concetti e dei sistemi NEC.

La compatibilità rappresentava, e tuttora rappresenta, un problema a livello nazionale. Francia, Germania e Regno Unito stanno operando per rimuovere gli ostacoli ai rispettivi sistemi netcentrici. Tuttavia, per quanto concerne la possibilità di far dialogare tra loro i rispettivi sistemi NEC al di là dei confini nazionali, si è rimasti alle dichiarazioni di buone intenzioni. Buona parte della connettività raggiunta ad oggi nelle operazioni ed esercitazioni è rimasta ad un livello di "swivel chair", "sedia girevole": i singoli sistemi possono essere resi interoperabili aggiungendo l'elemento umano nel processo, ovvero del personale che usi di volta in volta sistemi diversi facendo esso stesso da tramite.

In assenza di standard ed architetture condivisi, i Paesi europei corrono il rischio serio e reale di procedere comunque in modo isolato a livello nazionale, sebbene operino per garantire la connettività fra di loro. Se così fosse, è possibile che future operazioni condotte nell'ambito di coalizioni multinazionali incorrano nuovamente nell'ormai nota carenza di interoperabilità, impedendo di fatto di sfruttare tutti i benefici delle capacità netcentriche. Ciò malgrado la crescente importanza di laboratori commerciali "di integrazione", utilizzabili per testare le capacità dei sistemi di interfacciarsi agevolmente in vista del dispiegamento in teatro. In un'epoca in cui le operazioni militari unilaterali stanno diventando difficili anche solo da immaginare, ciò costituisce un nodo importante e difficile da sciogliere.

Le recenti operazioni aeree hanno fornito una "foglia di fico" rispetto al livello raggiunto dalla netcentricità multinazionale. Infatti, la quasi universalità di accesso dei velivoli da combattimento al sistema Link 16, assieme a tecnologie e procedure radio unificate, hanno consentito alle forze armate di dare almeno l'impressione di operare congiuntamente e in modo uniforme. In effetti, ad un livello operativo base, vi sono molti dati che testimoniano come le forze aeree NATO possano operare insieme nel bom-

bardare gli obiettivi designati. La domanda è se ogni ingaggio del bersaglio sia stato reso possibile e veramente ottimizzato dalle capacità netcentriche, o se queste abbiano fornito semplicemente un quadro entro cui agire. Le operazioni nei cieli libici tenderebbero a suffragare quest'ultima ipotesi. La mancanza di un targeting veramente netcentrico, multinazionale e tempestivo, ha fatto sì che alcuni obiettivi di terra fossero attaccati più volte malgrado fossero stati già messi fuori combattimento ore prima – o in alcuni casi da diversi giorni. La Marina francese è stata così frustrata da questa situazione da iniziare a utilizzare un proprio sistema di ingaggio time-sensitive[2]: sistema che ha permesso di mettere rapidamente in rete i risultati della ricognizione effettuata dai pods Damocles a bordo dei velivoli Rafale e Super Etendard, che una volta tornati sulla portaerei sono stati valutati da una squadra di militari che ha trasmesso le coordinate degli obiettivi ai velivoli in uscita. Per quanto questo sforzo sia stato notevole a livello nazionale, esso ha verosimilmente accresciuto il problema dell'efficienza complessiva dell'operazione, in quanto le forze francesi hanno agito all'interno della loro rete isolandosi dagli altri Paesi attivi nella missione in Libia: in parecchie occasioni, la Royal Air Force (RAF) britannica ed anche gli stessi Mirage dell'Aeronautica francese hanno finito per effettuare sortite inutili.

Vi è comunque del potenziale che fa ben sperare per il futuro. L'apprezzamento e il sostegno verso architetture aperte e a standard di interfaccia condivisi tra Francia, Germania e Regno Unito volti all'attuazione di tali architetture sta aumentando. Ad esempio, il programma britannico denominato Generic Vehicle Architecture (GVA) verrà probabilmente adottato come standard a livello europeo e NATO. Malgrado ciò, non sembra che la volontà di cooperazione multinazionale in programmi di procurement sia così forte, e la storia dei tentativi europei di sviluppare e ottenere qualcosa congiuntamente, dai fucili ai velivoli da combattimento, è stata segnata più da fallimenti che da successi. Le comunicazioni satellitari mostrano anch'esse un grande potenziale, ma lo sfruttamento di tale opportunità si dimostra nei fatti non attuabile nel quadro dei rapporti tra Francia, Germania e Regno Unito.

La natura sconfinata dell'ambito cibernetico potrebbe essere foriera di una qualche collaborazione internazionale, certamente a livello di condivisione di informazioni e contrasto alle attività criminali. Tuttavia,

[2] Il cosiddetto "time-sensitive targeting" rappresenta un ingaggio estremamente tempestivo di bersagli mobili che in una determinata circostanza presentano l'opportunità di essere colpiti e al tempo stesso costituiscono una priorità operativa oppure una minaccia immediata.

al momento sembra che Francia, Germania e Regno Unito preferiscano mantenere un alto grado di controllo ed indipendenza a livello nazionale. Inoltre, la mancanza di coerenza circa le interfacce radio e dati si sta rivelando un problema, nel momento in cui i tre Paesi in esame devono soppesare le rispettive esigenze per il decennio a venire.

Nel complesso, l'intento cooperativo parrebbe forte in linea di principio, ma di fatto poco realizzato.

2.2 Lo spazio cibernetico

2.2.1 Regno Unito

L'approccio dell'establishment della difesa britannica al mondo cibernetico è stato definito con la Strategic Defence and Security Review (SDSR) del 2010, nel corso degli ultimi cinque anni ha compiuto alcuni progressi in sintonia con le aspirazioni ivi delineate. Nello specifico, la SDSR del 2010 affermava:

> attueremo un programma nazionale di trasformazione per proteggerci nel cyberspazio. Nel decennio appena trascorso, le minacce alla sicurezza e prosperità nazionali poste dagli attacchi cibernetici sono aumentate esponenzialmente. Nel prossimo futuro questo trend potrebbe continuare ad aumentare per entità e sofisticazione, con enormi implicazioni sulla natura dei conflitti moderni[3].

Il nuovo documento strategico sulla difesa che verrà realizzato nel corso del 2015 potrebbe mutare leggermente l'enfasi posta dalla SDSR, anche se ci si attende che esso sia strutturato in linea con quanto stabilito nel 2010.

All'interno di tale concetto omnicomprensivo, il Ministero della Difesa ha siglato contratti con una serie di compagnie commerciali per garantire la sicurezza delle proprie capacità netcentriche e, per estensione, delle guarnigioni e delle forze dispiegate. Uno sviluppo questo di notevole interesse, soprattutto visto che fino ad ora le forze armate britanniche, così come molte altre, si erano vantate – quanto meno in pubblico – della

[3] UK Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 19 October 2010, https://www.gov.uk/government/publications/the-strategic-defence-and-security-review-securing-britain-in-an-age-of-uncertainty.

sicurezza intrinseca tanto delle proprie infrastrutture di comunicazione quanto dei propri sistemi informatici. Sistemi che però erano stati sviluppati per contrastare la minaccia della guerra elettronica, lievemente diversa da quella cibernetica.

Con l'attuazione di questi contratti si può raggiungere una certa sicurezza cibernetica dei sistemi a livello tattico. Tuttavia, il Ministero della Difesa ha compreso che l'utilizzo pervasivo dei computer portatili – ad uso personale e lavorativo – di reti wifi, di apparecchi radio software-defined, di chiavette USB di altre interfacce standard, nonché l'adozione sempre più frequente di sistemi operativi provenienti dal settore commerciale, si stanno tramutando in realtà impossibili da sorvegliare in modo classico, e costituiscono quindi elevatissimi fattori di vulnerabilità. A partire dal 2010, il concetto di difesa cibernetica è diventato quindi predominante ed è stato generalmente accettato come necessario, anche se di natura intrinsecamente difensiva rispetto ad operazioni offensive imputate a stati "canaglia", gruppi hacker non-statuali, e organizzazioni criminali.

Con una chiara inversione di tendenza, il Regno Unito è stato tra i primi ad ammettere tacitamente di possedere capacità cibernetiche offensive quando, nel settembre 2013, il Segretario alla Difesa Philip Hammond affermò che il Regno Unito stava "sviluppando un ampio spettro di capacità cibernetiche militari, ivi comprese quelle offensive"[4]. Uno dei passi più significativi compiuti in tal senso è stata la creazione, nel maggio 2013, del Joint Forces Cyber Group. Nel settembre dello stesso anno, Hammond dichiarò altresì che tale forza sarebbe stata ampliata con l'attivazione di una nuova task force di riservisti – essenzialmente una sezione del Territorial Army – che si immagina formata da "parecchie centinaia" di professionisti IT e hacker, per contrastare le offensive cibernetiche. All'inizio del 2015, non è ancora chiaro quale sia l'esito della nuova campagna di reclutamento. Il Ministero della Difesa tuttora evita di fornire i dettagli sulle capacità cibernetiche del dicastero e, malgrado la schiettezza di Hammond, la Difesa rimane sempre attenta a non rivelare elementi al riguardo. In altre parole, tali capacità rimangono coperte da un velo di segretezza.

Parimenti, la Government Communications Headquarters organisation (GCHQ) parrebbe disporre di notevoli capacità cibernetiche, ma i dettagli non sono pubblici in quanto capacità, esigenze e tecnologie im-

[4] UK Ministry of Defence Joint Forces Command and Philip Hammond, *New cyber reserve unit created*, 29 September 2013, https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit.

piegate sono considerate molto sensibili e coperte dal segreto di stato. Tuttavia, la GCHQ balza periodicamente allo scoperto nel dominio cibernetico. Ad esempio, nell'agosto 2014, ha accreditato sei istituti universitari per impartire insegnamenti di livello di laurea magistrale sulla sicurezza cibernetica. Successivamente, nel corso dello stesso mese ha lanciato un gioco online per testare l'abilità dei giocatori nel proteggere una finta compagnia aerospaziale: quest'ultimo è stato più che altro uno strumento di reclutamento e valutazione, ed ha fornito poche indicazioni sulle effettive capacità dell'organizzazione.

Leggermente meno sensibili, ma ancora non ampiamente discussi pubblicamente, sono i dettagli delle disposizioni predisposte nel Defence Cyber Protection Partnership (DCPP). Questo programma ha visto il Ministero della Difesa e la GCHQ cooperare con BAe Systems, il gigante delle comunicazioni British Telecom, Cassidian (ora parte di Airbus Defence and Security) e Lockheed Martin al fine di condividere criticità e soluzioni rispetto agli attacchi cibernetici. L'ex Cassidian svolge un ruolo di rilievo, fornendo servizi per la sicurezza delle reti del Ministero della Difesa, incluse da poco tempo quelle delle forze dispiegate in operazioni, attraverso le proprie strutture nel Galles. Quest'ultimo aspetto era incluso in un UOR del 2014 rispetto ad un accesso internet sicuro e senza restrizioni ai nodi del TACIP dispiegati dalla Gran Bretagna nel Golfo Persico. Secondo Steve Whitby, Strategic Accounts Director di Airbus Defence and Security, gli operatori TACIP in precedenza avevano avuto accesso limitato ai trasmettitori di comunicazioni militari, ma possono ora accedere ad internet attraverso il Defence Information Infrastructure Portal del Ministero della Difesa con un collegamento diretto alle strutture Airbus site in Galles[5].

In teoria da parte del Regno Unito vi è ampia disponibilità a cooperare in ambito internazionale nel controverso terreno della difesa cibernetica, in special modo attraverso le strutture della NATO. Tuttavia, vi è ben poco di pubblico dominio che può fornire una qualche concreta indicazione che Londra stia guardando attivamente oltre le proprie capacità militari nazionali. Come per altri aspetti fondamentali per il settore della difesa nazionale, Londra mostra una forte propensione a mantenere una forte sovranità sulle capacità militari. Infatti, forse più che in altre aree dove la costruzione di "grandi muraglie cinesi" fornisce sufficiente sicurezza, l'insidiosa e pervasiva natura delle reti informatiche fa sì che la

[5] Nick Brown, "Airbus adds internet freedom to UK TACIP", in *Jane's International Defence Review*, 26 November 2014.

sicurezza cibernetica sia spesso trattata in modo simile allo spionaggio.

Per quanto riguarda il comparto industriale, molte delle grandi imprese attive in Gran Bretagna nel settore della difesa – Airbus, BAe System, Thales, Lockheed Martin, Northrop Grumman e Raytheon-Systems – sono già impegnate sul versante cibernetico. Tutti questi attori vantano vari livelli di capacità trans-nazionali. Ad esempio, il cuore delle capacità nel campo cibernetico di Airbus sono i Cyber Security Customer Solutions Centres siti in Francia, Germania e Regno Unito.

2.2.2 Francia

Come la Germania ed il Regno Unito, la Francia ha preso la minaccia cibernetica molto seriamente ed ha confermato esplicitamente la propria capacità di condurre operazioni cibernetiche di tipo offensivo. Le risorse destinate al campo cibernetico sono aumentate costantemente e, a inizio 2015, il Ministro della Difesa Jean-Yves Le Drian ha annunciato che il suo Ministero ha allocato 1 miliardo di euro appositamente per incrementare il livello di sicurezza cibernetica del Paese. Tale somma verrà destinata al Centro Analisi Informazioni della Difesa (Centre d'analyses en lutte informatique défensive CALID) e alla Direzione Generale Armamenti (Délégation Générale pour l'Armement, DGA). Entrambi gli enti progettano una considerevole espansione delle attività in campo cibernetico. Il CALID rimarrà di dimensioni relativamente contenute, ma punta ad accrescere il proprio personale dai 20 effettivi del 2011 a 120 nel 2019; mentre per il cyber team della DGA presso l'information superiority centre di Bruz si prevede un ampiamento d'organico dagli attuali 250 a 450 "nel corso dei prossimi anni". I nuovi stanziamenti consentiranno inoltre di stabilire un centro di eccellenza per le operazioni cibernetiche a Rennes, di triplicare il numero di studi "a monte" per la difesa cibernetica ed ampliare l'attuale rete di 80 riservisti cibernetici inaugurata nel 2012 – l'equivalente francese della Joint Force Cyber Reserve britannica. Le Drian ha altresì precisato di voler creare una forza operativa di specialisti della difesa cibernetica, la quale sarebbe presumibilmente di carattere più proattivo.

La difesa cibernetica ha rappresentato un elemento fondamentale del pensiero strategico francese a partire dal Libro Bianco sulla Difesa nel 2013. Ma un cambio di passo si è verificato a gennaio 2014 quando Le Drian ha affermato – di fronte all'International Forum on Cyber Security, tenutosi a Lille – che le operazioni cibernetiche sono diventate una "pri-

orità nazionale". Secondo il Maggiore Arnaud Le Dez, vicedirettore del ramo "prontezza operativa" del CALID, il Ministero della Difesa ha subìto nel 2013 circa 700 attacchi cibernetici – che vanno dai virus relativamente innocui a seri tentativi di mettere fuori uso le reti del dicastero – un numero quattro volte superiore rispetto a quello del 2011[6].

Come il Regno Unito, la Francia ha messo sotto contratto Airbus Defence and Space per ricevere i suoi servizi quanto a sicurezza informatica. Alla luce anche dell'interesse francese, la compagnia ha acquisito il tool di monitoraggio reti Cymerius. Questo tool, utilizzato presso il Ministero, permette di effettuare una scansione delle reti per ricercare anomalie ed attività sospette, ma è uno strumento di decision-assistance piuttosto che un pacchetto difensivo completo. Altre sue versioni sono state impiegate sulle navi dell'Aeronautica francese come parte integrante del loro aggiornamento al sistema di comunicazioni basato sul Rifan 2 IP.

Sebbene non di carattere militare, un altro elemento di interesse nell'ambito cibernetico è emerso nell'ottobre 2014, quando l'associazione delle imprese francesi della difesa GICAT ha siglato un accordo con il Gruppo Hexatrust, specialista nella sicurezza cibernetica, per sviluppare la struttura del mercato nazionale della sicurezza cibernetica. Hexatrust è una sorta di gruppo commerciale che raccoglie 18 imprese informatiche e di sicurezza cibernetica. La strategia dell'accordo con GICAT è di promuovere, sia a livello nazionale che internazionale, soluzioni cibernetiche sviluppate in Francia ad esclusione di altre opzioni europee. In tal senso, quantunque vi possa essere margine di collaborazione, la Francia non sembra essere così aperta al business internazionale o, qualora lo fosse, le aziende internazionali dovrebbero attendersi una concorrenza serrata da parte dalle imprese locali. Una significativa capacità cibernetica risulta altresì presente nel quadro del più ampio contesto industriale francese, nazionale e multinazionale. Nell'ottobre 2014, uno dei maggiori sviluppi industriali ha portato all'acquisizione da parte di Thales del settore sicurezza cibernetica e comunicazioni di Alcatel-Lucent.

2.2.3 Germania

Rispetto a Francia e Regno Unito, la Germania si è rivelata un po' più lenta nell'affrontare la minaccia cibernetica, probabilmente in virtù della resi-

[6] Nadia Deseilligny, "France earmarks EUR1 billion in spending on cyber defence", in *Jane's Defence Industry*, Vol. 31, No. 2 (1 February 2014).

stenza istituzionale al monitoraggio delle comunicazioni dopo anni di spionaggio da parte della Stasi, e a causa di un generale desiderio a livello nazionale di riconciliare la trasparenza governativa con la privacy personale.

Nonostante questi presupposti, nel 2010 la Germania ha istituito un National Cyberdefence Centre, al fine di coordinare le risorse e riunire i vari stakeholders militari e governativi nell'ambito della sicurezza cibernetica. Il suo sviluppo ha subito un'importante accelerazione nel corso degli ultimi due anni, sviluppo che ha consentito a Berlino di unirsi alle fila di coloro che affermano di possedere capacità cibernetiche offensive. Tale politica appare insolitamente schietta per un Paese che solo di recente ha dispiegato le proprie forze in missioni internazionali – per lo più per compiti di peacekeeping – e che, rispetto alla maggior parte degli altri stati, ha imposto controlli più restrittivi alle esportazioni di armi.

La preoccupazione per l'aumento di attacchi cibernetici si è fatta più concreta negli ultimi anni. Episodi come i numerosi tentativi di hackeraggio del telefono di Angela Merkel nel 2014, seguiti, all'inizio del 2015, dagli attacchi a siti governativi da parte di hacker filo-russi che contestavano la posizione tedesca in Ucraina, hanno accresciuto l'attenzione di Berlino verso la difesa dello spazio cibernetico. Nello specifico, la Germania sta lavorando alla definizione di capacità di prevenzione atte a prevenire, sventare e preparare in caso di attacco cibernetico grazie al Bundesnachrichtendienst (BND), l'iniziativa tecnologica strategica del servizio di intelligence per le minacce provenienti dall'estero. Tale iniziativa ha fatto sì che venissero allocati 300 milioni di euro di finanziamenti per il quinquennio 2015-2020 per la sicurezza cibernetica – cifre che, anche se ingenti, impallidiscono al confronto con le somme allocate da Francia e Regno Unito. Dato che il BND si concentra sulla sicurezza esterna, sembrerebbe che il nuovo sistema si limiti a cercare tracce di minacce esterne.

La coalizione politica di centrodestra al governo del Paese ha adottato per il momento una posizione formale secondo cui non assumerà un approccio globale alla sorveglianza elettronica, anche se tale posizione potrebbe subire delle modifiche in seguito alle prossime elezioni. Nel frattempo, alla fine del 2014 Stephan Meyer, un portavoce della coalizione, ha dichiarato che "esiste una visione generale negli USA secondo cui tutto ciò che è tecnologicamente possibile può essere fatto. Non condividiamo tale impostazione. Ma non dovremmo nemmeno affrontare tali scenari con miopia"[7]. La

[7] Stefan Wagstyl, "Germany plans early-warning defence against cyber attacks", in *Financial Times*, 10 November 2014, http://on.ft.com/1uXsbBS.

sorveglianza interna da parte dello stato è strettamente regolata da principi costituzionali, limitando di fatto le capacità tedesche nel settore cibernetico. Ciò nonostante, il Bundesministerium des Innern (BMI), il Ministero dell'Interno, ha definito una strategia per la sicurezza cibernetica nel cui quadro poter operare. La strategia dichiara che "garantire la sicurezza cibernetica è diventata una sfida cruciale per lo stato, il mondo dell'impresa e la società, a livello tanto nazionale quanto internazionale", ma riconoscendo come la portata della sfida sia imponente sottolinea anche che "considerati i malware tecnologicamente sofisticati, le possibilità di rispondere e rintracciare la provenienza di un attacco rimangono piuttosto limitate."

È altresì chiaro come la strategia per la sicurezza cibernetica del BMI sia incentrata principalmente su approcci e misure civili. Essi sono completati da misure prese dalla Bundeswehr, l'Esercito tedesco, atte a proteggere le proprie capacità, e da altre misure volte a fare della sicurezza cibernetica una parte della strategia di sicurezza della Germania. Data la natura globale dell'ICT, il coordinamento internazionale e quadri di riferimento appropriati che si preoccupino degli aspetti riguardanti la politica estera e di sicurezza appaiono indispensabili. Ciò include la cooperazione non solo in seno alle Nazioni Unite, ma anche in altri ambiti quali l'UE, il Consiglio d'Europa, la NATO, il G8, l'OSCE e le altre organizzazioni internazionali"[8]. Non è chiaro esattamente quali misure la Bundeswehr voglia sollecitare, ma essa dispone di un team di hacker in grado di eseguire operazioni cibernetiche, inquadrati all'interno dello Strategic Reconnaissance Command di recente costituzione.

Dalla dichiarazione di cui sopra, emerge comunque chiaramente come la Germania sia una fervida sostenitrice della cooperazione internazionale a livello governativo. Ciò risulta però in qualche modo in disaccordo con l'approccio di Berlino alla politica industriale nella difesa, il quale è più affine a quello francese o britannico ed incline più che altro a favorire l'industria nazionale.

2.2.4 I contesti EDA e NATO

L'EDA ha ripetutamente esortato i propri membri a cooperare in materia di sicurezza cibernetica (ed in altri settori), ma ha faticato nel dare il giu-

[8] German Ministry of the Interior, *Cyber Security Strategy for Germany*, February 2011, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf.

sto impulso, ritrovandosi con quasi nulla di tangibile da presentare come risultato dei propri sforzi.

La NATO ha guadagnato più terreno, ma Jamie Shea – Vice Assistente del Segretario Generale per le nuove sfide alla sicurezza, in sostanza il più alto funzionario NATO in tema di sicurezza informatica – ha affermato, in occasione di una conferenza sulla cyber-intelligence tenutasi a Bruxelles nel settembre 2014, che resta ancora molto da fare. Egli ha sostenuto che, ancorché il NATO Computer Incident Response Centre (NCIRC) abbia acquisito piena capacità operativa all'inizio del 2014, gli stati membri NATO hanno bisogno di semplificare le proprie reti per minimizzare il rischio di intrusioni cibernetiche: "abbiamo ora bisogno di semplificare le nostre strutture informatiche. Con il tempo si sono sommati così tanti strati al sistema legacy da dover ora fronteggiare vari livelli di attacco"[9]. Quale indicatore dell'entità del problema, Shea ha affermato che nel 2013 il NCIRC ha rilevato quotidianamente 200 milioni di incidenti sulle reti NATO e 2.500 attacchi significativi. Ma i progetti messi in campo da Francia, Germania e Regno Unito dimostrano per lo meno come il numero e la complessità delle reti e delle comunicazioni stia crescendo.

2.3 COMANDO E CONTROLLO (C2)

2.3.1 Regno Unito

Il Regno Unito vanta una ampia gamma di sistemi C2. Si possono senz'altro riscontrare una certa coerenza e logica, anche se permangono ancora anomalie in ambito interforze che danneggiano il potenziale di connessione.

Ad esempio, l'esercitazione NATO denominata ARRCade Fusion, svoltasi nel novembre 2014, ha visto l'Esercito britannico adottare l'infrastruttura Magpie che ha costituito la spina dorsale di una serie di attori NATO ivi compresi operatori tedeschi e francesi. Tale infrastruttura ha fornito connettività satellitare all'Italia con un distaccamento del Skylark (composto da due terminal UK/TSC 729 Rockwell Collins CCT 120 operanti su Skynet 5). I Joint Terminal Attack Controllers (JTAC) hanno partecipato all'esercitazione con la capacità Magpie della RAF cablata nel com-

[9] Brooks Tigner, "NATO urged to embed cyber defence into mission planning", in *Jane's Defence Weekly*, 23 September 2014.

plesso High Wycombe della RAF. La Royal Navy è stata però lasciata fuori da tale esercitazione. Per l'ARRCade Fusion 14, parte della rete interna nel quartier generale è stata fornita usando le infrastrutture del nuovo sistema Falcon.

Il passo successivo alla Magpie è rappresentato dal programma Jackdaw, il quale introdurrà un'architettura che integrerà il Magpie. Nel frattempo, per le operazioni in Afghanistan il Regno Unito si è affidato alla rete OverTask e alla Defence Information Infrastructure – Land Deployable (DII – LD), che ha fornito i Functional Area Services (FAS) della NATO, e un Enterprise Services Bus (ESB) come piattaforma ed applicazioni comuni. Questo è un sistema "mission-configurable" che soddisfa le necessità del Federated Mission Network (FMN) NATO, il quale gestirà le reti dell'Alleanza Atlantica in futuro. Il programma Jackdaw dovrebbe entrare in servizio quest'anno. La principale applicazione C2 usata nel quartier generale è il tool integrato di Comando e Controllo: questo fornisce la COP e può altresì essere usato per visualizzare la Recognised Air Picture (RAP, rappresentazione dei velivoli che stanno volando in un certo spazio aereo) e la Recognised Maritime Picture (RMP).

La struttura JCHAT rappresenta anch'essa uno strumento fondamentale, disponibile per tutti i componenti in grado di connettersi. Questa è in grado di operare egregiamente tra le forze di terra ed aria, ma l'integrazione navale risulta ancora assente. In generale, le piattaforme marittime in grado di effettuare comunicazioni satellitari usano la Wide Area Network (rete di grandi dimensioni) segreta della NATO e hanno accesso al software Integrated Command and Control (ICC), consentendo quindi agli equipaggi navali di unirsi alla struttura JCHAT. Tuttavia, le esigenze operative implicano contesti in cui la connettività con le navi sarà limitata alle comunicazioni radio in High Frequency (HF), con una larghezza di banda ridotta tra terra e navi. Le forze navali continuano di conseguenza a puntare su comunicazioni basate su protocolli di traffico messaggi di base. Tuttavia, l'introduzione di sistemi ben più evoluti a terra, subito adottati dall'Esercito, hanno come conseguenza una comunicazione interforze non efficace e sono quindi fonte di frustrazione. Sebbene le trasmissioni in HF possano trasmettere e-mail, formalmente non sono riconosciute come traffico registrato e la consegna non viene garantita. Esse non dispongono pertanto dello stesso status di "non ripudio" della messaggistica formale, o anche della struttura JCHAT, dove tutti gli scambi di comunicazioni sono registrate sul server di rete. A livello di singola forza armata, ciò rappresenta naturalmente un problema di minore entità, ma

complica indubbiamente la definizione di una COP e crea una stridente disconnessione con le forze navali.

Rimanendo nell'ambito commando e controllo terra-aria, nel dicembre 2014 le forze armate britanniche hanno certificato come operativo il proprio sistema Land Environment Air Picture Provision (LEAPP), sviluppato da Lockheed Martin. Questo fornisce una Common Air Picture (CAP) usando il radar Saab Giraffe ed il collegamento dati Link 16. Quest'ultimo rende naturalmente più facile la connettività delle forze aeree, in quanto la maggior parte di quelle NATO (inclusi i caccia francesi, tedeschi e britannici) sono ora adeguatamente attrezzati. Le forze armate britanniche stanno già cercando di aggiornare alcuni elementi del LEAPP e di aggiungere nuove capacità mediante il contratto di assistenza siglato con Lockheed Martin UK.

Per ciò che concerne il sistema di comunicazioni militari britannico, il più grande progetto riguarda l'imminente sostituzione dell'architettura di comunicazione tattica Bowman, sviluppata da General Dynamics UK (GDUK). Seppure il sistema stesso sia relativamente nuovo, poiché a disposizione delle forze armate britanniche solo dal 2008, esso dovrà essere comunque rivisto in alcuni dei suoi aspetti in quanto l'esperienza concreta ha rafforzato la volontà di sostituirlo. Il Bowman rappresenta il primo tentativo delle forze armate britanniche di imbastire un sistema di comunicazioni digitali e – come ci si potrebbe attendere dall'applicazione di tali pioneristiche tecnologie – ha palesato significativi e perduranti problemi nella fase di lancio. Alcuni di questi erano relativi alle tecnologie impiegate, altri erano legati più alla struttura stessa del programma. Ciononostante, nelle ultime configurazioni Bowman and ComBAT and Information and Platform (BCIP) – versione 5.5, realizzata nel 2013 e la cui definitiva messa in campo è programmata per aprile 2015 – e vari Battlefield Information Systems Applications (BISA) si sono evoluti in un sistema veramente efficiente.

Anche se coordinato da GDUK, alla realizzazione del sistema hanno partecipato BAe Systems, Blazepoint, Cogent Defence Systems (ora facente parte di Airbus Defence & Space), DRS Tactical Systems, Harris, ITT (ora Exelis), L-3 Communications, Finmeccanica-Selex ES e Thales. L'aspetto importante su cui porre l'accento è il carattere in buona parte britannico del sistema: nonostante molte delle compagnie coinvolte fossero multinazionali, la progettazione di stampo britannico ha dato l'impronta e la base del programma. Diverse versioni possono ora essere impiegate dalla fanteria a piedi ed essere integrate in tutte le piattaforme, dal semplice

Land Rover sino al principale tank da battaglia Challenger 2, assieme agli elicotteri Chinook, Merlin, Lynx and Apache in dotazione all'Esercito e alla RAF. Tali dotazioni sono state fornite anche alla Royal Navy. Gli equipaggiamenti associati al sistema Bowman variano a seconda del ruolo, ma le capacità di base offerte comprendono: voce e dati criptati mediante radio software-defined che trasmettono dati variando casualmente le frequenze radio in modo da non essere intercettati (frequency-hopping), sia UHF che VHF; parte della dotazione del singolo soldato o dei veicoli, con una radio MANET di tipo UHF High Capacity Data Radio (HCDR) che garantisce un potente e autonomo accesso internet sia modem che mobile.

Uno dei primi componenti che finì per essere acquisito separatamente dal programma Bowman (al fine di renderlo disponibile in tempi rapidi) è stata la UHF H4855 Personal Role Radio (PRR) di Finmeccanica-Selex ES, che ha costituito la base per tutti i successivi pacchetti di digitalizzazione futuri a livello di singolo soldato. Sebbene fosse un pacchetto semplice ad uso esclusivamente vocale, ha consentito per la prima volta di connettere tra loro i soldati, con metodi di comunicazione decisamente migliori rispetto a grida e segnali con le mani. Essa si è rivelata di per sé un'acquisizione molto importante, perché ha rappresentato un cambio di paradigma per quanto concerne la connettività a livello di squadra e ha consentito alle forze armate britanniche di rivoluzionare la propria strategia basata su unità di piccole dimensioni. Altre forze armate hanno potuto apprezzarne i benefici ed hanno rapidamente seguito l'esempio dei britannici.

Il Regno Unito punta a continuare ad usare il sistema Bowman nel corso dei prossimi anni, ma intende altresì imprimere un cambio di passo in termini di capacità a partire all'incirca dal 2018, con una nuova architettura generale che verrà sviluppata nell'ambito del programma Land Environment Tactical Communications and Information System (LETacCIS), altresì noto come Morpheus, e con una potenziale transizione ad altra denominazione: Battlefield Tactical Communications and Information System (BatCIS). Il programma LETacCIS prevede il supporto al Bowman ed in futuro la sua sostituzione, e questo rende chiaro come il Regno Unito punti a qualcosa di più di una semplice transizione indolore rispetto a quanto avvenuto con il lancio del Bowman. Tale processo mira ad unire tutti gli elementi del sistema Bowman in maniera più coerentemente integrata, e ad aggiungere alcune nuove capacità basate su tecnologie più moderne. Nello specifico, la forma d'onda e l'architettura del Bowman non sono state pensate per essere interoperabili con i sistemi di comunicazione di altri Paesi: dato che le forze armate del Regno Unito si stanno

riducendo in termini quantitativi e che la probabilità che esse operino assieme ad altre Nazioni risulta sempre maggiore, ciò rappresenta un elemento quanto mai importante.

Nei propositi del Ministero della Difesa, tale sistema dovrebbe essere più flessibile e in grado di rimanere al passo con gli aggiornamenti tecnologici non appena questi vengano resi disponibili. Attualmente è prevista una fase di sviluppo in tre passaggi. Quello iniziale è stato avviato nel 2013 con un finanziamento di circa 50 milioni di sterline, ed è attualmente in corso lo studio di fattibilità che prevede la definizione dei miglioramenti da apportare rispetto a determinate esigenze. Essendo impiegato da tutte e tre le forze armate, la concezione del programma è di responsabilità dello UK Joint Forces Command, sebbene a guida dell'Esercito in quanto utente principale.

Com'era prevedibile, il programma ha come base di sviluppo le lezioni apprese in Iraq ed Afghanistan, e punta a valutare se queste si potranno applicare ad eventuali conflitti futuri o se quanto appreso in teatro fosse invece specifico di quei contesti. Ad esempio, il dominio pressoché completo da parte della missione ISAF del contesto comunicativo ha reso possibile un accesso relativamente agevole e sicuro alla possibilità di trasmissione ad alta velocità, cosa che non risulterebbe possibile in un teatro meno permissivo. Potrà perciò verificarsi che il flusso dati per i sistemi futuri sia ridotto e comunque in grado di soddisfare tutti i requisiti. Le forze dispiegate in Afghanistan risultano ben addestrate all'uso di video full-motion – collegati direttamente a velivoli, siano essi dotati o meno di pilota, o condivisi da unità schierate in teatro – ed il Ministero della Difesa sta valutando il loro valore, e su dove possa essere applicato al meglio, soprattutto qualora la capacità di trasferimento dati fosse limitata. Il presupposto è che non tutti i soldati al fronte ed ogni ufficiale di Stato Maggiore presso il quartier generale ne abbiano necessariamente bisogno.

Nel frattempo, uno dei primi passi concreti in tal senso prevede lo sviluppo del BCIP5.6+, la cui entrata in servizio è prevista per il 2017. Secondo il Colonnello Richard Spencer, capo del BATCIS delivery team del Ministero della Difesa, queste capacità potrebbero migliorare tanto da garantire un superamento del Bowman. In un modo o nell'altro, l'attuale versione del Bowman sarà probabilmente l'ultima; pertanto, i successivi upgrade dei velivoli legacy saranno determinati dalla direzione che prenderà il programma LETacCIS/Morpheus. Tra le altre migliorie, ciò consentirà lo sfruttamento delle capacità di "positioning" che era potenzialmente fornibile dalla radio Harris PRC-153, che permetterà a coloro che utilizzeranno il network BCIP di "vedere" la radio e vice versa. Questo

significa che il sistema potrebbe finalmente essere utilizzato come sistema di tracciamento delle forze amiche – il sistema legacy dispone di un sistema incorporato di posizionamento, ma solo a livello di singolo soldato e come aiuto alla localizzazione.

Questo verrà probabilmente inserito all'interno di un sub-programma distinto nell'ambito del programma LETacCIS: la Dismounted Situational Awareness che garantirà piena visibilità a Esercito, RAF e Royal Navy. "Desideriamo arrivare ad un punto" ha affermato a metà 2014 il Colonnello Spencer "in cui, invece di una situazione dove il Combat fa tutto, si possono avere una serie di applicazioni più piccole che svolgono compiti specifici, supportate da alcuni servizi comuni quali il Geographic Information System (GIS)"[10].

Tre sono le opzioni prese in considerazione dal LETacCIS su come finanziare e mettere in campo queste capacità. La prima consiste nel continuare a far funzionare il sistema legacy il più a lungo possibile, riadattandolo per aggiungere capacità. Tuttavia, le tecnologie radio fulcro del sistema sono essenzialmente d'inizio secolo e diventeranno sempre più obsolete, con il rischio che, per la fine dell'attuale decennio, esse risultino inutilizzabili. La seconda opzione è un approccio ibrido, e prevede che si stabilisca quali elementi possano essere mantenuti, e quali si debbano sostituire tramite nuovi acquisizioni per contrastare l'obsolescenza del sistema. La terza opzione è la più costosa: acquisire un'architettura totalmente nuova. L'aspetto positivo di quest'ultima soluzione è che la nuova architettura sarebbe più flessibile e moderna, e potrebbe essere meno costosa nel lungo termine.

Qualunque opzione verrà scelta, è chiaro che le forze armate non desiderano replicare una situazione in cui l'Esercito non possieda gli standard dei dati impiegati dal Bowman. Secondo il Colonnello Giles Ebbutt, direttore di IHS Jane's C4I (Command, Control, Communications, Computers and Intelligence),

> ciò ha implicazioni sulle risorse. Non vi è alcuna capacità interna nell'ambito dell'Esercito britannico quanto a risorse umane che possa attualmente svolgere tali mansioni; sarebbe necessaria assistenza per consentire l'integrazione di prodotti di parti terze in un network. Sarebbero necessarie le risorse sia per acquisire tali competenze che per coltivarle al proprio interno[11].

[10] Giles Ebbutt, "Beyond Bowman", in *Jane's Defence Weekly*, Vol. 51, No. 26 (25 June 2014), pp. 28-31.

[11] Ibid.

Per come stanno le cose, l'Esercito preferirebbe idealmente adottare solo standard concordati a livello internazionale (applicando, naturalmente, crittografia e criteri di sicurezza propri) che sarebbero più facili da utilizzare, aprire il mercato a nuovi software in formato "app", ridurre i costi attraverso la competizione e facilitare l'interoperabilità con le forze di altri Paesi.

La sfida consiste nel fatto che le opzioni disponibili sono ancora un azzardo, in quanto gli attuali standard del Multilateral Interoperability Programme (MIP) variano tra i diversi operatori. Ad esempio, il MIP Block 2 è usato da Francia e Stati Uniti, il che sembrerebbe renderlo un problema di facile soluzione. Tuttavia, il livello successivo – il MIP Block 3 – è usato dalla Germania e non è retro-compatibile con il MIP Block 2. A complicare ulteriormente le cose concorrono le diverse versioni del MIP Block 3. Allo stesso modo, il Regno Unito potrebbe intraprendere un percorso autonomo o creare un altro MIP Block. Ma quest'ultima opzione appare pericolosa, in quanto potrebbe portare di nuovo il Regno Unito alla situazione in cui si trova attualmente. Un raggruppamento industriale verrà messo sotto contratto per studiare queste opzioni produrre qualche risultato verso la fine del 2015. Il completamento della prima fase è programmato per l'inizio del 2016, imprimendo un'impronta significata alla connettività in teatro del Regno Unito per il prossimo decennio.

Il team a capo del programma Morpheus deve altresì rimanere consapevole dell'importanza di un altro livello di compatibilità: assicurarsi che il sistema possa operare nell'ambito della Land Open Systems Architecture (LOSA), la quale definisce gli standard d'interfaccia netcentrici aperti sotto le nomenclature Generic Soldier Architecture (GSA), Generic Vehicle Architecture (GVA) e Generic Base Architecture (GBA). Il GVA è probabilmente il più avanzato, perché installato nel veicolo Foxhound, e programmato per il Warrior, lo Specialist Vehicle Scout ed il Challenger. Ha sinora ottenuto risultati positivi, ed ha fornito agli sviluppatori standard formalizzati e concordati per la condivisione dati e per facilitare la connettività, nei e tra i veicoli. Il programma di modernizzazione dei veicoli portato avanti dalle forze armate del Regno Unito appare ben strutturato, con un chiaro percorso pensato per l'aggiornamento delle piattaforme legacy e con la GVA quale punto di riferimento e cardine per facilitare l'integrazione. Nel medio-lungo termine, il Morpheus sarà senza dubbio il chiaro fattore determinante, ma, fino a quando tale direttrice non sarà pienamente definita, vi sono ancora tre progetti in ballo.

Sinora, l'introduzione del Bowman ha assicurato che tutti i veicoli da

battaglia disponessero di un livello di connettività con gli equipaggiamenti specializzati della BCIP. L'introduzione del nuovo veicolo Scout a partire dal 2017 rappresenterà però un nuovo termine di riferimento per l'integrazione. Thales cura lo sviluppo della sua nuova dotazione di sensori nell'ambito GVA, per trasferire le immagini ed i video raccolti intorno al veicolo, e trasmetterli ad altri mezzi sul campo di battaglia. Se venissero adeguatamente ridimensionate, simili capacità si possono prefigurare per la flotta Warrior. Tale progetto però appare costantemente mal programmato e soggetto a continui rinvii. Lockheed Martin UK costituisce il principale integratore del progetto ed anche il fornitore della torretta del nuovo Scout, ed ha superato con successo una serie di importanti test nel 2014, ma attende il Critical Design Review (CDR). A quel punto, il Ministero della difesa potrebbe decidere l'ordine di produzione per rispettare le scadenze di consegna, attualmente previste per il 2018, ma dato che il CDR coinciderà con le elezioni politiche nel Regno Unito esso potrebbe subire un ulteriore rinvio.

L'altro principale progetto di aggiornamento degli assetti legacy è rappresentato dalla permanenza in servizio del carro armato da battaglia Challenger 2, che vedrà probabilmente i propri esemplari spogliati diparte delle protezioni metalliche per essere rivestiti con un serie di strumenti digitalizzati compatibili con la GVA. L'aggiornamento è però già stato posticipato e rivisto nei suoi obiettivi una volta, e la decisione su cosa esattamente dovrebbe prevedere il programma è stata posticipata a dopo le elezioni britanniche.

La flotta di veicoli da pattugliamento dell'Esercito comprendente tutti i rimanenti tipi di veicoli anti-mina e anti-imboscata è oggi sottoposta ad un processo di riconfigurazione al fine di renderli maggiormente adatti (e legalmente conformi) ad essere operativi in Europa. Tuttavia, per quanto concerne la loro connettività, i piani dell'Esercito si basano attualmente sul mantenimento dei propri sistemi Bowman.

Un altro livello di comunicazione sul campo di battaglia è fornito dalla rete di teatro Cormorant, la quale fornisce strutture di comunicazione di teatro interforze ed è stata dichiarata operativa nel dicembre 2004, anche se ha raggiunto la piena capacità solo dal 2007. Dopo solo due anni, essa è stata dichiarata inadatta a fornire le capacità richieste dalle forze armate britanniche in Afghanistan, ed un sistema sostitutivo – il Radwin 2000 israeliano – è stato pertanto urgentemente acquisito off-the-shelf. Il Radwin 2000 ha dato risultati positivi, ma è stato a sua volta sostituito in teatro dal sistema Falcon. Sebbene la rete Cormorant rimanga ancora in servizio, allo stato attuale il Falcon rappresenta la principale rete di

comunicazioni in teatro del Regno Unito. A seguito di un contratto siglato nel 2006 con BAe Systems, è giunto l'ordine di rimpiazzare una grande quantità di sistemi, inclusi il Ptarmigan ed il RAF Transportable Telecommunications System. In origine tale sostituzione sarebbe dovuto essere operativa dal 2010, ma i test sul campo non sono stati completati prima del 2012, e le forniture sono state completate ed i sistemi resi operativi sia per l'Esercito che per l'Aeronautica solo nel 2014. Si tratta di una scelta che all'inizio, con la decisione di adottare una soluzione all-IP, poteva apparire ambiziosa. Tuttavia la bontà della decisione è stata confermata dal fatto che anche la maggior parte degli altri sistemi hanno successivamente intrapreso tale percorso. Un miglioramento precedentemente pianificato prevedeva l'inserimento del Falcon a bordo delle navi da guerra, ma non è chiaro se ciò sia ancora in agenda o se vi sia una tempistica concordata per la una sua adozione in tal senso.

2.3.2 Francia

La Francia conta su una serie di programmi, tuttora in corso, volti a modernizzare la propria capacità di connessione netcentrica. Per quanto riguarda l'Esercito, il programma Synergie du COntact Renforcé par la Polyvalence et l'InfovalorisatiON (SCORPION), iniziato nel 2010, costituisce la cornice principale all'interno della quale vanno a posizionarsi diverse iniziative. A differenza dei britannici e dei tedeschi, i quali hanno tentato di portare avanti programmi tra loro separati di acquisizione di equipaggiamenti per poi integrare i rispettivi sistemi, lo SCORPION ha adottato un approccio olistico, concepito per potenziare le forze di terra francesi con nuovi veicoli, sistemi d'arma ed equipaggiamenti netcentrici in un insieme integrato e coeso.

Le stime dei costi possano apparire quindi piuttosto elevate, circa 5 miliardi di euro, ma ciò è dovuto al fatto che vengono combinate tutta una serie di nuove acquisizioni. La spesa più consistente copre l'acquisto di circa 2.500 nuovi veicoli blindati VBMR ed EBRC e l'ammodernamento del carro armato da battaglia Leclerc. Ogni piattaforma verrà interconnessa dal nuovo sistema di comunicazioni integrate conosciuto come Système d'Information et de Combat SCORPION (SICS), che collegherà altresì i mezzi corazzati sia ai velivoli senza pilota sia a quelli ad ala rotante, con l'obiettivo di ottenere un miglior coordinamento. Quest'ultimo sviluppo è in parte il risultato della "lesson learned" circa l'integrazione terra/aria appresa nel corso delle operazioni in Afghanistan, durante le

quali le forze terrestri hanno avuto difficoltà nel richiedere il supporto aereo ravvicinato.

L'architettura SCORPION mira a consentire ai battaglioni Groupements Tactiques Interarmes (GTIA) – tra 500 e i 1.500 soldati provenienti da fanteria, artiglieria, unità corazzate e genio – di essere dispiegati in gruppi integrati e netcentrici. La tabella di marcia è piuttosto stretta e dovrà probabilmente essere rivista, in quanto i primi 18 GTIA verranno auspicalmente digitalizzati tra il 2014 ed il 2020, ed un secondo gruppo tra il 2018 ed il 2023. I tagli previsti al bilancio della difesa sembravano aver imposto un rinvio di tali scadenze ma, a seguito degli attacchi terroristici a Parigi nel gennaio 2015 e dell'apparente ascesa della minaccia islamista, il governo sta riconsiderando la spesa militare.

Nello specifico, il SICS sostituirà con una singola architettura l'ormai antiquato Système d'Information pour le Commandement des Forces (SICF), costituito invece da una serie di sistemi diversi tra loro. Il SICS prevede una serie di aggiornamenti da applicare a quei veicoli che non saranno sostituiti o ammodernati dal progetto SCORPION. Lo sviluppo della prima versione del sistema è stato assegnato a Bull Systems – tra lo stupore di molti, compresi Airbus e Thales – con un contratto da 40 milioni di euro siglato con la DGA nel giugno 2013. Le prime consegne dovrebbe avvenire ad inizio 2016.

Malgrado le limitate informazioni pubblicamente disponibili circa l'equipaggiamento e la struttura SICS, Bull Systems afferma che sarà ampiamente autonomo, sicuro e fornirà connettività a tutti i livelli di comando. In aggiunta, l'azienda ha fatto sapere che la sua proposta "prende in prestito metodologie e tecnologie dalla sfera civile, migliorandole alla luce dei requisiti militari" e "l'uso di tecnologie aperte dovrebbe ridurre il costo complessivo di sistemi informatici per le operazioni tattiche ed offrire maggiori opportunità affinché il sistema si evolva e rimanga al passo con le esigenze future."[12]

La DGA ha intrapreso un ampio programma di ammodernamento delle comunicazioni noto come Communications Numériques TACtiques et de Théâtre (CONTACT), finalizzato ad introdurre delle nuove software-defined radio per rimpiazzare i sistemi legacy, quali i dispositivi PR4G di Thales, ma comunque retrocompatibili per facilitarne l'integrazione. La

[12] Bull, *French Defense Procurement Agency (Direction Générale de l'Armement, DGA) Turns to Bull to Develop Initial Version of Its Scorpion Combat Information System*, 17 June 2013, http://www.wcm.bull.com/internet/pr/new_rend.jsp?DocId=812919.

prima fase è datata giugno 2012 con un contratto da 1,06 miliardi di euro siglato con Thales per la fornitura di 2.400 apparecchi radio (circa 2.000 dei quali veicolari, i restanti portatili) per equipaggiare due brigate anfibie entro il 2018. Al tempo stesso, nel 2014 Thales ha iniziato le consegne dei nuovi sistemi di comunicazione per il quartier generale interforze a livello di battaglione. Ad esempio, il Réseau Intégré des Transmissions Automatiques (RITA) N4 è un sistema IP che consente l'accesso alle comunicazioni satellitari Syracuse, al Link 16, alle radio VHF e HF, come parte del sistema di comunicazioni in teatro Astride usato dall'Esercito francese. Thales fornirà un totale di 60 nodi: 20 consegnati nel 2014, altri 20 dovrebbero seguire nel 2015 e i restanti nel 2016, con un aggiornamento di 150 nodi legacy RITA NG allo standard di Astride. L'Aeronautica francese potrebbe inoltre acquisire un certo numero di sistemi per equipaggiare le proprie basi aeree avanzate con il Link 16 ed altri sistemi di connessione.

Questi contratti sono in qualche modo il frutto di uno studio, conosciuto come ETO AGORA, affidato nel gennaio 2014 dalla DGA a Thales, volto a definire l'architettura di sistema complessiva per le future operazioni interforze netcentriche francesi tra il 2020 e il 2025. Ciò ha consentito a sua volta di specificare le modalità attraverso le quali i servizi forniti da Astride e da altre reti possano essere distribuiti in modo coerente attraverso altri sistemi – come ad esempio COMSAT NG, COMCEPT, il sistema RIFAN per la flotta navale – in aggiunta alle nuove tecnologie quali la LTE/4G. I risultati di questo studio non sono ancora stati resi pubblici.

La Francia è altresì pronta ad introdurre una versione aggiornata del proprio FELIN. Sotto molti punti di vista, il FELIN costituisce il più avanzato tra tutti i sistemi di digitalizzazione del soldato, grazie anche all'esperienza acquisita in Afghanistan, Ciad, Mali e in altre operazioni delle forze armate francesi. L'utilizzo del sistema di gestione del campo di battaglia Système d'information terminal du Combattant Débarqué (SitCom-Dé) avvenuto durante l'esperienza in questi teatri operativi conferma la buona resa del FELIN. Tuttavia, una delle criticità che dovranno essere affrontate a partire dal 2016 è insita nel fatto che, analogamente all'architettura dell'IdZ tedesco, la Francia impiega attualmente tre sistemi C2 forniti da tre imprese diverse per coprire i diversi livelli di comando, a partire da quello del singolo soldato fino ai comandi superiori. Rispetto a quanto realizzato in Germania, l'Esercito francese è stato in grado di integrare con successo i vari sistemi ma, quando la nuova versione del FELIN diverrà operativa, la forza armata dovrà avviare la transizione verso una singola architettura di C2. Le altre modifiche relative al FELIN

riguardano l'ergonomia, con nuovi cavi, display più moderni e così via. La versione 2.0 del FELIN punterà a razionalizzare le capacità e le componenti hardware del sistema. Mentre Sagem, l'azienda incaricata per lo sviluppo del sistema, ha cercato di esportare il FELIN come sistema off-the-shelf, in Francia si è dibattuto circa la possibilità di condividere con il Regno Unito lo sviluppo di future versioni del sistema. Allo stato attuale appare però altamente improbabile che la Francia acquisisca una soluzione "chiavi in mano" così come è altresì discutibile quanto Parigi possa realisticamente condividere lo sviluppo di un tale sistema con Londra o Berlino, in quanto ogni forza arma rimane particolarmente ancorata ai suoi specifici equipaggiamenti, costumizzati in base a concetti operativi tra loro diversi. All'inizio del 2015 alcuni elementi dell'Aviazione dell'Esercito francese (Aviation légère de l'armée de terre – ALAT) avevano aggiunto un nuovo importante elemento di connettività attraverso un aggiornamento al Système d'Information Terminal de l'ALAT (SIT-ALAT), collegandolo insieme al Système d'Information Régimentaire (SIR) e al sistema di simulazione Helicopter Mission Trainer (HMT). Ciò ha consentito a 18 vecchi elicotteri Gazelle e Puma ed ai loro rispettivi equipaggi di compiere un'esercitazione – nota come Aozou – insieme ad altri 12 elicotteri virtuali pilotati attraverso il simulatore HMT. Si è trattato di un test chiave per il software C2 che l'azienda Miccavionics ha sviluppato per Bull Systems, come elemento essenziale del SIC-S e che si integrerà con il sistema SIT-ALAT. La prima versione operativa del SIC-S verrà schierata nel 2016 e l'esito positivo dell'esercitazione Aozou fa ben sperare per il suo impiego poiché ha dimostrato un'agevole integrazione di diverse piattaforme.

2.3.3 Germania

Gli addetti alle comunicazioni militari tedeschi hanno dovuto misurarsi con gli stessi problemi affrontati dagli omologhi britannici e francesi, in particolare nel campo dell'interconnessione a livello interforze e di coalizione. In ogni caso la Germania ha riscontrato probabilmente un problema ben maggiore rispetto ai primi due Paesi, dato che ha dovuto riconoscere che la sua digitalizzazione, frammentaria e sporadica, non era così integrata come Berlino inizialmente sperava.

La più grande spinta alla digitalizzazione e alle comunicazioni degli assetti nel campo di battaglia è strettamente legata al destino del programma per dotare il soldato semplice di un kit netcentrico di equipag-

giamenti, denominato Infanterist der Zukunft Erweitertes (IdZ-ES). La Bundeswehr aveva ordinato i primi kit IdZ, sviluppati prima da Airbus ed in seguito da Rheinmetall Detec, nel 2004 con l'obiettivo di impiegare il sistema in teatro afghano e assicurare così un primo feedback operativo. Dopo una serie di evoluzioni e valutazioni, un primo lotto di 30 IdZ è stato consegnato all'Esercito tedesco solo nel dicembre 2012. Sono poi seguiti altri, lotti in proporzioni tali da rispondere alle esigenze dei vari Einsatzverband (battaglioni) tedeschi in Afghanistan, fino a marzo 2014 quando l'ultimo dei 900 kit ordinati è stato consegnato.

Al momento sono state destinate ulteriori risorse alla digitalizzazione, all'interno della pianificazione finanziaria della Bundeswehr, ragion per cui Rheinmetall è in attesa di nuovi ordini. L'azienda tuttavia ha fatto notare che alcune componenti risultano ormai superate dal punto di vista tecnologico. Ad esempio, i display sono alimentati da computer portatili con sistema operativo Windows – ormai obsoleti – dato che erano stati sviluppati prima del massiccio avvento degli smartphone. Una versione dell'IdZ fornita al Canada era basata sul sistema operativo Android e ciò costituirà la nuova architettura informatica dei prossimi IdZ. Rheinmetall sta altresì lavorando allo sviluppo di un'interfaccia dati affinché la prima generazione del IdZ-Basissystem (BS) possa dialogare con l'ultima generazione IdZ-Es, al fine di garantire per quanto possibile un certo grado di continuità e riutilizzo. I sistemi si sono dimostrati efficaci ed hanno riscosso l'approvazione dei soldati dispiegati in Afghanistan, ma la mancanza di connettività aldisopra del livello di squadra ne forse ha compromesso l'efficacia e l'utilità.

Il dispositivo radio Thales SOLAR 400EG-E ha fornito dati e comunicazioni voce sicure a livello intra-team e squadra, mentre la versione SOLAR 400V montata sul veicolo militare corazzato multiruolo Boxer ha offerto un'estesa capacità di connessione con altri elementi. Tuttavia, il fatto che il sistema non disponesse di connettività dati con il Führungsinformationssystem Heer (FüInfoSys-Heer/FIS-H) sviluppato da Airbus, ha spinto i capisquadra a tornare sui propri passi e optare per le meno sicure radio a frequenza fissa ThalesSEM 52SL VHF per collegarsi con le altre unità (plotone o compagnia) tramite esclusivamente la comunicazione vocale.

Nel frattempo, la Bundeswehr è riuscita a garantire l'interoperabilità tra i sistemi IdZ-BS e FIS-H – entrambi sviluppati da Airbus – utilizzando una simbologia brevettata e sviluppata dalla stessa azienda. Questa differiva però dallo standard MIP-DEM adottato per l'IdZ-ES. Quanto accaduto

ha reso evidenti i rischi che possono manifestarsi anche in occasione di una corretta selezione di standard condivisi, e rappresenta un insegnamento importante per il prossimo futuro considerando che gli standard "aperti" stanno via via diventando prassi comune.

Nel 2012, Rheinmetall ed Airbus sono state selezionate congiuntamente per sviluppare un meccanismo per l'interfaccia dati. L'Esercito ha poi sperimentato la soluzione proposta, aggiungendo un traduttore ATM KommServer modificato e connesso ad un apparecchio radio Thales SEM 93 16 kbit/secondo, impiegato insieme al nuovo veicolo blindato Puma. Nonostante sembri funzionare, il sistema non costituisce una soluzione definitiva, in quanto la capacità di trasmissione dati del più vecchio dispositivo radio VHF SEM rimane quanto mai indietro rispetto a quella raggiunta dai sistemi SOLAR 400 UHF utilizzati a livello tattico. Nel 2014, Thales ha consegnato l'ultimo lotto di radio a banda larga SEM 600A V/UHF. La fornitura è avvenuta appena in tempo, dal momento che i nuovi equipaggi del Puma e i comandanti di battaglione avevano programmato l'inizio della fase addestrativa per metà 2015.

La Bundeswehr prevede infine di impostare l'architettura di comunicazione dei futuri veicoli su un sistema di software-defined radio interforze, attualmente in via di sviluppo e denominato StreitkräftegemeinsameVerbundfähigeFunkgeräteausstattung (SVFFuA), conforme alla Software Communications Architecture (SCA). La radio Harris AN/PRC-117G, utilizzata dalle forze speciali tedesche in Afghanistan, è stata adattata sia per i nuovi carri armati Leopard 2A7 – consegnati nel 2014 – sia per i veicoli Puma. Il modello radio PRC-117G è anch'esso conforme alla SCA e potrebbe essere adattato al programma SVFFuA, ma finora è stato selezionato esplicitamente per assicurare la connessione SATCOM. In aggiunta, l'Esercito è intenzionato a introdurre rapidamente una nuova radio portatile dotata di maggiori capacità, integrata con il sistema IdZ-ES, che faccia parte dell'equipaggiamento del caposquadra per fornire connettività con i livelli più alti nonché aggirare il problema della sola comunicazione vocale. Il piano della Bundeswehr presume che tutte e tre le forze armate selezionino un'opzione idonea per tale requisito ma, dato che la mancanza di connessione rappresenta una criticità da affrontare urgentemente, l'Esercito potrebbe adottare rapidamente una decisione che le altre forze armate in seguito potrebbero – o meno – condividere.

Ulteriori upgrade riguardano la rete a banda larga di comunicazioni integrate posto-comando BIGSTAF (Breitbandiges IntegriertesGefechts-

STAndFernmeldenetz) di Thales. Nel 2013, le aziende Steep GmbH e Blackned GmbH sono state selezionate per sostituire gli elementi in fibra ottica del FuInfoSysH con un nuovo sistema di comunicazioni vocale basato su protocolli IP Mobile Unified Platform.

In un certo senso, si potrebbe affermare che la Germania goda di un ottima base di partenza quanto ad hardware, in quanto le sue flotte di veicoli sono relativamente nuove o stanno per essere sostituite. Questi veicoli sono stati progettati con moderni sistemi C3 e verranno sottoposti solo a qualche aggiornamento di routine quando i sistemi verranno introdotti o aggiornati nel prossimo futuro. Tuttavia, sulla falsariga delle criticità riscontrate con i dispositivi radio, i veicoli impiegati in Afghanistan dovevano essere aggiornati in base alle necessità del teatro operativo ma l'Esercito sta rivedendo completamente il suo operato con lo scopo di definire un parco veicoli più omogeneo.

Nondimeno, la questione della connettività riscontra diverse problematiche. Le nuove versioni che a breve entreranno in servizio assorbono risorse ingenti e il governo appare riluttante a spendere ulteriormente per veicoli ormai datati e che nel giro di poco tempo verranno rimpiazzati. Sembrerebbe inevitabile pertanto che emergano alcuni disallineamenti a livello di capacità. Dopo alcuni ritardi, la flotta di veicoli da combattimento si sta riposizionando sui Puma, dato che i Marders sono stati dismessi e i nuovi Boxer stanno gradualmente sostituendo la flotta Fuchs. I mezzi Dingo e gli Eagle V sono sostanzialmente nuovi, dotati di elettronica ed interfacce moderne. È però singolare – una sorta di passo indietro che mette in dubbio l'impegno tedesco verso l'adozione su ampia scala di moderni sistemi di comunicazioni – la sorprendente determinazione di Berlino nel proseguire ad utilizzare un telefono "wired" sul retro dei propri Leopard 2 MBT per assicurare un collegamento con il singolo soldato.

2.4 COMUNICAZIONI SATELLITARI (SATELLITE COMMUNICATION, SATCOM)

2.4.1 Regno Unito

Le telecomunicazioni satellitari militari del Regno Unito sono fornite dalla costellazione di satelliti Skynet e dai relativi segmenti di terra. Tale sistema è stato oggetto di aggiornamenti periodici fino ad arrivare all'attuale

Skynet 5, di cui il quarto ed ultimo satellite – lo Skynet 5D – è operativo dall'aprile del 2013. La costellazione dei satelliti al momento non vede in programma cambiamenti significativi. Tuttavia, quello dei lanciatori e della produzione di satelliti è un mercato contraddistinto da cicli di stasi a cui seguono dei picchi di attività in concomitanza del lancio di nuovi assetti, per poi assistere ad una riduzione delle risorse che si limitano a contratti di supporto. Ne consegue che entro i prossimi cinque anni il Regno Unito dovrà necessariamente impostare il processo di sostituzione dei vecchi Skynet 5A-C.

Nel complesso, il programma Skynet fu il risultato di un'innovativa Private Finance Initiative (PFI) con Paradigm Services – gruppo Airbus – del valore di circa 2,5 miliardi di sterline, l'investimento più corposo che il Ministero della Difesa britannico avesse mai sostenuto in campo spaziale fino a quel momento. Secondo l'accordo, Paradigm avrebbe fornito al Regno Unito una accesso sicuro alle comunicazioni satellitari tramite una larghezza di banda concordata, garantendosi al tempo stesso la possibilità di utilizzare la rimanente capacità degli assetti per altri fini. L'accordo sembra abbia pienamente soddisfatto le aspettative del Ministero della Difesa, tanto che Paradigm continuerà ad assicurare il servizio sino al 2022.

L'intesa franco-britannica di cooperazione in materia di difesa siglata nel 2012 definisce misure specifiche per le comunicazioni satellitari: "la Francia ed il Regno Unito confermano la rispettiva intenzione di adottare un approccio cooperativo al fine di soddisfare le rispettive necessità nel campo delle SATCOM, che costituiranno l'asse portante per ogni capacità futura di Beyond Line of Sight."[13] Tre anni dopo, l'accordo deve ancora generare dei risultati concreti, almeno per quanto riguarda l'infrastruttura satellitare. La decisione della Francia, nel gennaio 2015, di procedere con il lancio dei propri satelliti sembrer evidenziare che una eventuale cooperazione anglo-britannica potrebbe essere finalizzata solo alla condivisione della lunghezza di banda e non allo sviluppo e alla cooperazione multinazionale, come invece nel caso degli accordi esistenti tra Italia e Francia.

Dal momento che i satelliti britannici Skynet sono già soggetti ad un insolito accordo di proprietà con un'entità commerciale, è possibile che il Regno Unito consenta in futuro ulteriori condivisioni di capacità con i propri partner europei. In effetti, le capacità di Skynet sono già state uti-

[13] UK Prime Minister's Office, *UK-France declaration on security and defence*, 17 February 2012, https://www.gov.uk/government/news/uk-france-declaration-on-security-and-defence12.

lizzate da Australia, Canada, Francia, Germania, Paesi Bassi, Portogallo e Stati Uniti. Sebbene rimanga ancora da valutare se tale approccio si estenderà anche allo sviluppo congiunto di futuri satelliti, il Regno Unito vorrà probabilmente mantenere la sua sovranità in materia. Ad oggi infatti, i programmi di sviluppo congiunto non hanno dato alcun frutto.

Nel frattempo, il Ministero della Difesa britannico ha dimostrato ancora una volta un approccio pragmatico nel garantire una adeguata ampiezza di banda satellitare. Nel marzo 2015 ha infatti siglato un contratto di 12 mesi con Airbus Defence and Space allo scopo di supportare l'identificazione delle forze alleate. Secondo l'accordo, si utilizzerà l'Iridium Short Burst Data e l'Iridium Rudics Data Minutes per sostenere il Ground Asset Tracking System (GrATS) e l'Helicopter Asset Tracking System (HeATS), con un reporting in tempo reale dei dati GPS provenienti da tutti i devices opportunamente configurati ed equipaggiati.

2.4.2 Francia

La Francia sembra aver perso fiducia nei programmi di cooperazione multinazionale in ambito EDA/ESA (vedi paragrafo 4.4). Infatti, sembrerebbe ormai certa la volontà di Parigi di proseguire in modo autonomo per assicurarsi il mantenimento delle proprie capacità satellitari. Ne sono un esempio i due nuovi satelliti per le comunicazioni militari che la Francia intende acquisire da Airbus Defence and Space e Thales Alenia Space. Questi satelliti fanno parte di Comsat Next Generation (NG) e, insieme alle nuove infrastrutture di terra, avrebbero un costo stimato di 800 milioni di euro. L'obiettivo è quello di far entrare in servizio il primo satellite entro il 2021 per sostituire una coppia di satelliti Syracuse 3.

Diversamente dal Regno Unito, dal momento che la Francia non è stata in grado di accordarsi per una PFI il programma dovrà essere interamente finanziato con il bilancio per la difesa. Se tale scelta comporti dei costi inferiori rispetto a quelli che il Regno Unito sostiene per i servizi garantiti da Airbus per Skynet è ancora oggetto di dibattito. C'è da dire inoltre che le informazioni circa le proiezioni francesi sul programma non sono state rese pubbliche, rendendo alquanto difficile qualsiasi valutazione comparativa. Tuttavia, non si può dire che Parigi non abbia tentato di esternalizzare le proprie capacità: nel 2010 la DGA aveva pianificato di rivendere alle imprese i satelliti Syracuse 3 per poi firmare un contratto di leasing per una determinata cifra annuale, sulla falsariga dell'accordo Skynet in Regno Unito. I satelliti a quel tempo avevano un eccesso di ca-

pacità latente di circa il 10%, situazione che ha indotto la DGA a supporre che i nuovi proprietari avrebbero semplicemente dato in leasing i satelliti a qualcun altro. L'intero piano tuttavia è stato cancellato nel marzo 2012. Da un lato, l'accordo non era infatti sufficientemente allettante per l'industria, e dall'altro l'atteggiamento ondivago e incerto del governo aveva di fatto eroso il ciclo di vita operativo – stabilito in 15 anni – dei satelliti, riducendo così il loro valore di permuta per le casse del Tesoro.

In ogni caso la Francia è stata in grado di negoziare un accordo sulla condivisione delle partecipazioni azionarie e dei carichi utili (payloads) con l'Italia, attraverso il quale è stato possibile lanciare il satellite ATHENA-FIDUS all'inizio del 2014, caricando i sistemi franco-italiani sugli stessi asset. Un successivo satellite SICRAL 2 (anche questo payloads franco-italiani) si prevede venga lanciato a metà del 2015. Se da un lato adottando tale approccio vi sono benefici di condivisione dei costi tra i due Paesi, dall'altro questo determina effetti negativi in quanto i due payloads sono sulla stessa orbita e ciò riduce i potenziali benefici in termini di copertura che si potrebbero ottenere qualora non fossero ospitati nello stesso satellite.

Considerando i tre Paesi analizzati, la Francia gode della più ampia varietà di satelliti militari, con diversi e importanti programmi in corso, a dispetto dei molti anni di vita operativa e della loro ormai prossima obsolescenza. La più vecchia delle attuali generazioni di satelliti è quella dei Syracuse 3A (lanciati nel 2005) e dei 3B (2006), i quali forniscono connessioni dati e voce sicure a livello globale. Inoltre, essi sono impiegati per la funzione di C2, per la condivisione di informazioni di intelligence e logistica.

I Syracuse 1 e 2 sono stati "inseriti" all'interno di un'architettura di satelliti civili per le telecomunicazioni francesi, mentre la terza generazione di Syracuse è costituta da piattaforme specificamente militari, rafforzate contro attacchi nucleari ed elettromagnetici. L'esatta capacità di trasmissione dei satelliti non è un dato di pubblico dominio, ma sembra che sia nell'ordine di parecchie centinaia di megabit/secondo, sufficiente per sostenere video conferenze e un certo livello di cloud computing. Tale capacità tuttavia comporta dei costi. Thales Alenia Space e Thales Communications (responsabile del segmento di terra) valutano l'attuale Syracuse nell'ordine dei 2,3 miliardi di euro. Inoltre, la DGA ha accesso a circa 600 stazioni di rete fisse e mobili, insieme ad una serie di ripetitori SATCOM-On-The-Move originariamente acquistati per la missione in Afghanistan, ma che non hanno trovato impiego durante le operazioni in Africa.

L'accesso ai satelliti è una questione fortemente interforze. I soldati appiedati, così come i mezzi, i velivoli, i sottomarini e le navi da guerra dispongono dell'accesso al sistema, ed i satelliti sono ritenuti in linea con gli standard di sicurezza NATO STANAG 4606. I canali di comunicazione avvengono tramite banda SHF/X e EHF. Quest'ultima però non è compatibile con i sistemi statunitensi, poiché l'elaborazione del segnale EHF non è condotta a bordo del satellite.

La Francia ha definito un piano di sostituzione parziale dei suoi attuali satelliti con i programmi SICRAL 2 ed ATHENA-FIDUS, entrambi in collaborazione con l'Italia. ATHENA-FIDUS, lanciato in un'orbita geostazionaria nel 2014, è un sistema con caratteristiche meno militari del Syracuse, utilizza standard di comunicazioni civili a prestazioni elevate (DVB-RCS e DBV-S2), e dovrebbe rimanere operativo per oltre 15 anni. Non vanta elevate capacità anti-jamming, ma dispone di alte velocità di trasmissione dati, oltre 3 Gbits/secondo. Il SICRAL 2 punta a combinare elementi dell'italiano SICRAL 1 con quelli del francese Syracuse 3, ed il suo lancio è previsto a metà 2015. Andrà a posizionarsi in orbita geostazionaria, con payloads UHF/SHF ed un'aspettativa di vita fino al 2029. Ciò consentirebbe alla Francia di mantenere una capacità che copra il gap tra il de-orbit o il ritiro del Syracuse 3 prima della fine di questo decennio e l'introduzione del Comsat NG. Recentemente, Thales Alenia Space ha annunciato di aver siglato un contratto con la DGA volto a fornire supporto operativo a tutti i tre principali sistemi di comunicazioni satellitari (Syracuse 3, SICRAL 2, ATHENA-FIDUS) fino al 20131. Pertanto Parigi sembra aver soddisfatto le proprie necessità per il prossimo futuro.

Il segmento finale delle comunicazioni satellitari francesi verrà completato grazie al programma COMCEPT (COMplément de Capacités en Elongation, Projection et Théâtre). Nel 2010 Thales ha condotto uno studio per la DGA, ed il successivo contratto è stato affidato nel 2013 ad Airbus Defence e Space Services, assieme ad ActiaSodielec. In breve, l'appalto è volto a fornire un segmento di terra Ka-band per l'Esercito, l'Aeronautica e la Marina francesi, garantendo loro comunicazioni sicure su banda larga veloce (10 Mb/s). Questa sarà poi utilizzabile per lo scambio di dati e video full-IP per sistemi mobili e fissi. Gli elementi saranno integrati in velivoli manned e unmanned, navi e mezzi terrestri. Airbus ha completato il suo primo COMCEPT end-to-end per il collegamento ATHENA-FIDUS nel 2014 e, secondo l'accordo, la relativa assistenza durerà 17 anni.

2.4.3 Germania

Le comunicazioni satellitari militari della Germania sono supportate dai satelliti COMSATBw sviluppati da Astrium. Il COMSATBw-1 è stato lanciato in orbita nel 2009 ed il COMSATBw-2 nel 2010. Entrambi hanno un'aspettativa di vita di 15 anni. Ciò significa che, anche considerando un periodo di gestazione durato anni necessario per realizzare e lanciare i satelliti, la Germania non necessita al momento di sviluppare una nuova generazione di sistemi, tant'è che non è stato individuato alcun successore né ci sono sul tavolo piani al riguardo. Entrambi i satelliti COMSATBw sono in orbita geostazionaria, uno sopra l'Oceano indiano e l'altro sopra il continente africano. Essi garantiscono comunicazioni voce e dati sicure tramite quattro transponder SHF e cinque UHF, e ripetitori terrestri che forniscono un collegamento nell'ordine di 6 Mb/s.

I sistemi sono stati sviluppati da Thales Alenia Space e affidati ad Airbus. La Germania ha esternalizzato gran parte del funzionamento dei suoi satelliti, gestiti da Milsat Services – sussidiaria di Astrium/Airbus – con i segmenti di terra gestiti invece da LSE Space, lasciando alla Bundeswehr l'utilizzo delle comunicazioni satellitari a mo' di cliente, senza l'incombenza di dover gestire la rete – e, viceversa, senza la possibilità di prendere in mano direttamente la gestione del sistema nel caso fosse necessario.

Oltre ai COMSATBw, la Germania ha stipulato degli accordi di leasing per acquisire larghezza di banda dal gruppo privato Intelsat. Allo stesso modo, quando il Paese ha avuto bisogno di capacità aggiuntive oltre a quelle offerte dalla Bundeswehr a livello nazionale, ne ha prese in prestito dalla costellazione britannica Skynet e da analoghe strutture statunitensi. La Germania ha però riscontrato diverse difficoltà nella condivisione delle proprie capacità satellitari con i Paesi partner a causa delle leggi federali, le quali proibiscono che la banda venga distribuita senza alcuna compensazione. Ciò ha rappresentato un elemento quanto mai problematico per le forze tedesche dispiegate nell'ambito della missione ISAF, la cui politica era orientata ad una condivisione ad hoc delle strutture allo scopo di garantire la massima flessibilità. In futuro Berlino potrebbe essere chiamata a rivedere tali vincoli legali. In aggiunta, con operazioni che richiedono un uso sempre più massiccio di dati e la crescente propensione da parte tedesca per operazioni out-of-area – compresi i dispiegamenti navali nel Corno d'Africa, le operazioni condotte dall'Esercito e dell'Aeronautica in Afghanistan, così come quelle di peacekeeping in Ruanda e

Georgia – potrebbero costringere la Bundeswehr a individuare capacità aggiuntive. Ciononostante, al momento non sembra vi siano piani concreti per aggiungere un terzo COMSATBw.

2.4.4 L'ambito EDA

Francia, Germania e Regno Unito sono membri, insieme a Italia e Spagna, di un "gruppo di utenti" (user group) per le comunicazioni satellitari creato nel 2014 dall'EDA. Il gruppo vuole esplorare il potenziale derivante dalla condivisione di SATCOM governative non "rafforzate", ma comunque sicure. A questo proposito, nel 2014 è stato concluso uno studio finalizzato ad identificare le necessità operative, e nel 2015 tale studio è poi transitato in un più ampio progetto di gap analysis volto a favorire l'allocazione di risorse per la ricerca e sviluppo e a stabilire una roadmap a livello europeo. L'EDA ha stimato che la condivisione di capacità da parte di questi cinque Paesi potrebbe portare ad un risparmio di circa 2,5 miliardi di euro. Tuttavia l'Agenzia non sembra essere particolarmente credibile nel fornire risultati tangibili, poiché è dalla metà degli anni 2000 che cerca con scarso successo, di mettere a fattore comune le rispettive capacità nazionali aumentanto l'efficienza della spesa militare. È improbabile quindi che tale iniziativa possa guadagnare forza nell'immediato futuro, mentre nell'ambito spaziale commerciale l'ESA ha invece saputo costruirsi una solida reputazione.

Lo scoglio principale è dato dal fatto che la durata del ciclo di vita dei satelliti militari legacy nei tre Paesi non sembra coincidere del tutto: la Germania ha ancora almeno dieci anni a disposizione prima di sostituire i satelliti di comunicazione COMSATBw; il Regno Unito inizierà a pianificare la sostituzione dello Skynet 5 solo tra qualche anno; per la Francia, al contrario, il tempo a disposizione è limitato e avrebbe teoricamente dovuto iniziare a lavorare per acquisire i nuovi assetti già nel 2014. Parigi ha avuto maggior fortuna lavorando con l'Italia, la quale ha simili scadenze temporali. In ogni caso l'EDA ha ottenuto anche qualche successo, benché di minor portata, con lo European Satellite Communication Procurement Cell (ESCPC), istituito dall'Agenzia e da Astrium/Airbus nel 2012. In sintesi, la ESCPC mette insieme i requisiti di più utenti ed usa questa maggiore capacità negoziale per garantire un accesso a tassi più bassi ai satelliti commerciali.

Nel 2014, l'EDA ha annunciato di aver

agevolato il raggiungimento di ordinativi per un valore di oltre 1 milione di euro. Altri stati UE (Belgio, Finlandia e Lussemburgo) si sono uniti ai cinque Paesi fondatori (Francia, Italia, Polonia, Romania e Regno Unito), mentre altri hanno manifestato il proprio interesse allo schema pay-per-use[14].

L'EDA ha poi affermato di aver ridotto del 20% i costi per gli utenti che utilizzano il suddetto schema. Nel corso dello stesso anno la Francia ha tratto vantaggio dalla partnership con l'Agenzia, acquisendo capacità satellitari per sostenere le proprie operazioni in Mali con breve preavviso. Non sussistono statistiche recenti sull'utilizzo effettivo al riguardo e, sebbene non si debba sottostimare l'aver conseguito un risparmio del 20%, nel più ampio contesto dei costi satellitari a livello nazionale l'utilità dell'ESCPC non sembra generare grandi risparmi.

2.5 La connettività in campo navale

Da una prospettiva navale, tutti e tre i Paesi sono attivamente coinvolti in diversi programmi con l'obiettivo di connettere digitalmente le unità delle proprie flotte. Tali sforzi tuttavia risultano piuttosto marginali rispetto a quanto realizzato dalla US Navy. Ad esempio, nessuno di questi Paesi partecipa allo US Cooperative Engagement Capability (CEC). In sostanza, il CEC è un sistema di fusione dei dati che mette insieme e combina i dati di diversi radar e sistemi di combattimento (principalmente il radar APY-9 e SPY, quest'ultimi componenti del sistema Aegis), permettendo alle navi e ai velivoli di avere accesso ad un quadro condiviso della situazione aerea. Questo strumento è altamente automatizzato e fornisce dettagli anche di singole rotte, consentendo agli operatori di distribuire agevolmente i compiti d'ingaggio agli assetti più appropriati. La US Navy è così soddisfatta di tale concetto che sta esaminando la possibilità di estenderlo nell'ambito del programma denominato Distributed Lethality, il quale potrebbe prevedere l'inserimento di unità di lancio missilistiche su una quantità maggiore di navi di superficie – incluse quelle di supporto ed i mezzi anfibi – ponendole teoricamente in

[14] European Defence Agency (EDA), *Progress for European Satellite Communication Procurement Cell (ESCPC)*, 5 February 2014, http://www.eda.europa.eu/info-hub/news/article/2014/02/05/progress-for-european-satellite-communication-procurement-cell-%28escpc%29.

grado di ingaggiare obiettivi aerei e di superficie individuati da sensori offboard.

Ciò costituisce un progetto ben più avanzato rispetto a quanto mai tentato di realizzare da Francia, Germania o Regno Unito. Quest'ultimo Paese in particolare aveva pianificato di adottare il CEC, tant'è che la Royal Navy aveva condotto una serie di esercitazioni durante lo scorso decennio con l'obiettivo di acquisire i sistemi CEC per le fregate classe Type 23 Duke e per il cacciatorpediniere classe Type 45 Daring. Il progetto era stimato attorno ai 400 milioni di sterline. Tuttavia, nel 2005 una serie di ostacoli finanziari e l'impegno crescente nelle operazioni in Iraq e Afghanistan hanno indotto il Ministero della Difesa a congelare il programma, sostituendolo con un altrettanto – ma piuttosto inglorioso – Operational Capability Demonstrator. Nel frattempo il Regno Unito ha continuato a stanziare una quota relativamente esigua per il CEC americano. Tale impegno però non ha mai prodotto un vero programma di procurement e nel 2012 il Ministero della Difesa ha formalmente lasciato cadere il programma di acquisizione, adducendo come motivazione le restrizioni di bilancio. Anche la Germania ha manifestato a metà degli anni 2000 un certo interesse nei riguardi del CEC ma, ancora una volta, a ciò non è seguito nessun impegno formale.

In Francia, la DGA e la Marina hanno condotto un programma interforze con DCNS e Thales noto come Tenue de Situation Multi Plates-Formes (TSMPF) o Multi-Platform Tracking Capability, una piattaforma dimostrativa per una Capacité d'Engagement Multi Plates-Formes (CEMP), quasi analoga al CEC. I dettagli del programma furono rivelati alla conferenza MAST di Cadice nel 2008; il progetto avrebbe dovuto iniziare nel 2009 ma in seguito non se ne ebbe più traccia. In sostanza, sembrerebbe essersi trattato solo un programma di simulazione volto ad esplorare architetture volte a far funzionare una rete cooperativa di ingaggio, suggerendo che tale rete sarebbe possibile acquisendo alcuni nuovi elementi ed unendoli a sistemi legacy di comunicazione in una forma ibrida.

Apparentemente, l'unico Paese ad essersi unito al CEC è l'Australia, e Canberra sta acquisendo nuove capacità per i suoi cacciatorpedinieri classe Hobart. Anche il Giappone potrebbe in futuro prendere parte al CEC. A livello europeo, la maggior parte della connettività netcentrica è limitata alle comunicazioni e ai datalink, in particolare attraverso i Link 16 e 22 della NATO.

2.6 La connettività in campo aereo

La Francia vuole estendere all'Aeronautica il time-sensitive targeting loop testato dalla Marina a bordo della portaerei Charles de Gaulle durante le operazioni del 2011 in Libia. Il cuore del sistema è puramente netcentrico ed utilizza un datalink digitale TDH 6000 sviluppato da Thales per trasmettere le immagini ad alta risoluzione (a livelli maggiori di 100Mb/secondo) generate dal pod da ricognizione Thales Reco-NG su distanze fino a 350 km.

L'aspetto innovativo dell'approccio della Marina francese consisteva nel collocare in posizione avanzata una cellula di targeting dotata di sistemi multisensore SAIM-NG (Systèmed'Aide à l'Interprétation Mmulti-capteurs) per l'interpretazione e la diffusione delle immagini, allo scopo di consentire rapidi cambiamenti nell'ingaggio del bersaglio. L'Aeronautica è in procinto di adottare un approccio simile. Per le sue operazioni in Mali, la forza armata ha dispiegato la sua targeting cell presso la base aerea ospitante, ma nel 2015 prevede di installare il sistema SAIM-NG a bordo del tanker C-135 a supporto dei velivoli da combattimento, riducendo così drasticamente il processo che va dal sensore all'attuatore. La trasmissione costante dell'analisi dati verrà eseguita attraverso connessioni voce o dati standardizzate NATO, il che apre la possibilità di cooperare con le forze alleate, ma si affida tuttora a velivoli francesi dotati di pod Reco-NG, i quali non sono ancora così diffusi. Curiosamente, sebbene il Regno Unito guardi con attenzione a tali sviluppi, non sembra sussistere un simile piano per accelerare le capacità di ingaggio britanniche e, a onor del vero, Londra non guarda nemmeno positivamente all'esperienza americana circa il dispiegamento di controllori aerei avanzati aviotrasportati (Forward Air Controller, FAC).

2.7 Conclusioni

I casi di Francia, Germania e Regno Unito hanno diversi aspetti in comune: i tre Paesi si trovano di fronte a sfide simili in termini di digitalizzazione e connessione delle rispettive forze armate, sebbene ognuna stia cercando di seguire il proprio percorso. L'essere tutti membri dell'Alleanza Atlantica assicurerà un certo livello di interoperabilità tra i vari sistemi nazionali, ed iniziative come la NATO Future Mission Network contribuiranno a tale sforzo standardizzando le interfacce di base. Ciò consentirà

semplicemente ai vari sistemi netcentrici nazionali di interfacciarsi ai più alti livelli di comando ma, nel breve periodo, non permetterà ad esempio a soldati francesi con equipaggiamento FELIN di operare in modo uniforme con i propri omologhi tedeschi dotati di kit IdZ. L'interconnessione per lo meno ai livelli superiori è un elemento determinante, ma essa non produce quelle capacità capillari che, al contrario, vengono generate da un insieme di forze operanti in modo uniforme all'interno dello stesso network.

Rispetto ai tre Paesi considerati, la Francia è forse quella più impegnata nello sviluppo di una vera forza netcentrica, con il FELIN già in corso d'opera e lo SCORPION volto ad ammodernare le forze di terra.

Il Regno Unito si trova in una buona situazione, poco dietro i francesi: il programma LETacCIS dovrebbe sviluppare delle capacità altrettanto interconnesse, soprattutto ora che i funzionari del Ministero della Difesa hanno il tempo e la disponibilità di elaborare un percorso coerente piuttosto che rispondere in tempi brevi agli UOR a supporto delle truppe dispiegate in teatro operativo. Anche la Germania vuole mettere a frutto i suoi piani di integrazione dei diversi sistemi e applicare le lessons learned emerse durante l'esperienza operativa, ma le pressioni finanziarie a cui la Bundeswehr deve far fronte e la mancanza di un percorso coerente potrebbero continuare a minare le ambizioni di Berlino. Ad onor del vero, ciò potrebbe valere per tutti e tre i Paesi.

Sebbene il numero e la serietà degli attacchi cibernetici continuano a crescere ad un livello allarmante, finora sono stati condotti contro infrastrutture civili o i media, oppure finalizzati a negare l'accesso a siti web militari, con un impatto limitato a livello tattico o perfino operativo. Di conseguenza, le forze armate francesi, tedesche e britanniche non sono ancora sollecitate a livello nazionale per far fronte a tale minaccia – contrariamente agli imperativi di carattere finanziario, organizzativo e strategico – né tanto meno sentono la necessità di operare congiuntamente a livello operativo, al di là della semplice condivisione di informazioni. Paradossalmente questo è uno degli elementi di forza di un approccio multinazionale non coordinato alla netcentricità, alle comunicazioni, alla cyber security e alle comunicazioni satellitari: se gli utenti e i proprietari delle varie reti e capacità nazionali faticano a trovare la quadra nell'integrazione dei propri sistemi, allora probabilmente ciò costituisce un'intrinseca difesa contro un attacco cibernetico coordinato.

3.
L'Italia e il programma Forza NEC

Tommaso De Zan

Questo capitolo fornisce una panoramica di Forza NEC, il programma di procurement guidato dall'Esercito Italiano (EI) ed iniziato nel 2007, che mira alla creazione di un'architettura netcentrica in grado di fornire una condizione di "superiorità dell'informazione" attraverso la digitalizzazione della forza armata. Forza NEC mira a soddisfare le esigenze operative dell'Esercito attraverso l'acquisizione di determinati assetti e/o l'ammodernamento di quelli già in suo possesso, adottando un approccio molto mirato: infatti, ha intrapreso una significativa fase di sviluppo e sperimentazione – fase in cui Forza NEC si trova tuttora – per validare soluzioni tecnologiche ai requisiti operativi man mano dettagliati, anche tramite un dialogo tra forza armata ed industria. Rispetto all'idea iniziale del 2006, l'acquisizione degli assetti digitali e/o la digitalizzazione dell'asset legacy non si concretizzerà in un unico grande programma di produzione, ma avverrà, ed in parte sta già avvenendo attraverso i cosiddetti programmi "spin off", per quelle soluzioni tecnologiche ritenute più mature ed adatte a soddisfare i requisiti dell'Esercito. Ciò alla luce non solo delle suddette sfide tecnologiche poste dall'applicazione dell'ICT al mondo militare, ma anche delle limitazioni di bilancio e dell'incertezza degli stanziamenti per la Difesa sperimentata negli ultimi anni. Al tempo stesso, si punta a far sì che i risultati della fase di sviluppo e sperimentazione di Forza NEC influenzino positivamente l'ammodernamento complessivo della forza armata, interagendo con altri programmi di procurement esistenti o futuri.

Il capitolo è organizzato in cinque paragrafi. Il primo descrive il ruolo dell'Esercito nel perseguimento degli obbiettivi della politica di difesa italiana, le sue principali esperienze operative dalla fine della Guerra Fredda ad oggi e i possibili scenari futuri d'impiego. Lo scopo di questo primo paragrafo è definire i requisiti operativi che hanno spinto le forze armate a puntare verso la tecnologia netcentrica. Il secondo paragrafo spiega in cosa consiste questa tecnologia e la sua importanza in ambito militare, per poi analizzare i vantaggi che l'Esercito ne potrà ricavare. Questo pa-

ragrafo tratta anche della trasformazione a cui sarà sottoposta la forza armata nel processo di digitalizzazione previsto dal programma. Il terzo paragrafo delinea gli aspetti industriali del programma quali il quadro finanziario, l'organizzazione della controparte industriale, la struttura di governance, i principi di management, e infine fasi e tempistiche di Forza NEC. Il quarto paragrafo valuta le sfide e le opportunità che il programma implica, sia in ottica attuale per il suo sviluppo, sia in chiave futura per eventuali altre acquisizioni. Il quinto paragrafo conclude il capitolo ed offre alcune riflessioni sul ruolo della tecnologia in chiave militare ed industriale.

3.1 La politica di difesa italiana e il ruolo dell'Esercito

3.1.1 La politica di difesa italiana

Secondo il "Libro Bianco per la sicurezza internazionale e la difesa", l'obiettivo primario della politica di sicurezza e difesa nazionale consiste nella "protezione degli interessi vitali e strategici dell'Italia"[1]. Sempre secondo il documento del 2015, "tale obiettivo richiede che sia assicurata la difesa dello Stato e della sua sovranità, che sia perseguita la costruzione di una stabile cornice di sicurezza regionale e che si operi per facilitare la creazione di un ambiente internazionale favorevole"[2]. In tale prospettiva, secondo il Libro Bianco, "la 'funzione Difesa' e il suo strumento operativo rappresentato dallo Strumento militare, costituiscono

[1] Ministero della Difesa, *Libro bianco per la sicurezza internazionale e la difesa. La nostra Difesa*, p. 15, http://www.difesa.it/Primo_Piano/Pagine/20150429Libro_Bianco.aspx. Gli interessi vitali sono "quell'insieme di elementi che costituiscono i bisogni primari e non derogabili del Paese, includendo l'autoconservazione, l'integrità territoriale, e la sicurezza economica". Gli interessi strategici sono invece "rappresentati dall'insieme di utilità, vantaggi, convenienze di grande importanza per una Nazione. La mancata tutela di un Interesse Strategico, pur non compromettendo l'esistenza stessa della Nazione, mina lo sviluppo sociale, economico, tecnologico e culturale futuro, quale previsto essere se l'interesse non fosse compromesso". Ministero della Difesa, *Linee guida del Libro bianco per la sicurezza internazionale e la difesa*, giugno 2014, p. 15, http://www.difesa.it/Primo_Piano/Pagine/LibroBianco.aspx.

[2] Ministero della Difesa, *Libro bianco per la sicurezza internazionale e la difesa. La nostra Difesa*, cit., p. 15.

un elemento imprescindibile del sistema nazionale posto a tutela e garanzia delle nostre libertà"[3].

Dal secondo dopoguerra in poi, il contesto di sicurezza regionale ha portato i vari governi che si sono succeduti ad investire nei rapporti con le principali organizzazioni internazionali di sicurezza collettiva – l'ONU, l'UE, la NATO e l'OSCE – per assicurare che gli interessi vitali nazionali fossero tutelati in maniera più efficace di quanto l'Italia avrebbe potuto garantire autonomamente, oltre che per agire in un contesto di un sempre più ricercato "consenso condiviso". A sua volta, la natura multilaterale di tale "architettura" non solo permette all'Italia di essere beneficiario e fruitore di garanzie internazionali in caso di minaccia, ma richiede altresì di partecipare attivamente alla "produzione di sicurezza" quando le crisi internazionali lo richiedono. Oltre quindi alla funzione classica dello strumento militare, ovvero la salvaguardia e la protezione del territorio nazionale da attacchi esterni, le forze armate italiane hanno assunto dei compiti che sono andati al di là della sola protezione dell'integrità territoriale dello stato, soprattutto dalla fine della Guerra Fredda in poi.

Dall'insieme degli interessi nazionali derivano delle specifiche missioni per le forze armate nel perseguimento degli obbiettivi della politica di difesa nazionale, così specificati dal Libro Bianco[4]:

a) la difesa dello Stato contro ogni possibile aggressione per salvaguardare la propria integrità territoriale, gli interessi vitali nazionali, la sicurezza delle aree di sovranità nazionale e dei connazionali all'estero e in ultimo la sicurezza e l'integrità delle vie di comunicazione per l'accesso al Paese;
b) la difesa degli spazi euro-atlantici ed euro-mediterranei attraverso il contributo alla difesa collettiva della NATO e il mantenimento della stabilità delle aree incidenti al Mar Mediterraneo;
c) contributo alla realizzazione della pace e della sicurezza internazionali attraverso la partecipazione a operazioni di prevenzione e gestione di crisi nello spirito della Carta delle Nazioni Unite;
d) concorso alla salvaguardia delle libere istituzioni e nello svolgimento di compiti specifici in caso di calamità o urgenza.

[3] Ibid., p. 3.
[4] Ibid., p. 20.

3.1.2 Il ruolo dell'Esercito

In un'ottica interforze e di singola forza armata, l'Esercito ha un ruolo fondamentale nel raggiungimento degli obbiettivi della politica di difesa. L'EI è attualmente costituito da 103.000 militari e 9.800 civili, e conta su 3.800 mezzi da combattimento e 7.300 di supporto, tra cui 226 elicotteri, il tutto dislocato in 3.900 strutture sul territorio nazionale[5]. Queste cifre sono destinate a diminuire in virtù del processo di razionalizzazione delle risorse della Difesa cominciato nel dicembre 2012 con la legge 244/2012[6] e proseguito nel gennaio 2014 con il relativo decreto attuativo[7]. Al termine di tale processo, l'EI sarà composto da 9 brigate in luogo delle 11 attuali – e scenderà quindi a 90.000 soldati e 9.000 civili – e un complesso infrastrutturale ridotto del 40%[8].

Nelle ultime due decadi, l'Esercito ha impiegato mediamente 9.000 unità in missioni internazionali e 4.000 in operazioni nazionali, con punte di 19.000 soldati contemporaneamente impiegati in operazioni nazionali e internazionali. L'EI è dal punto di vista quantitativo la forza armata maggiormente dispiegata in operazioni, fornendo circa il 75% dei militari italiani complessivamente impiegati in teatro[9]. Nel 2014, l'Esercito è stato

[5] Ibid, p. 17.

[6] Legge n° 244/2012 "Delega al Governo per la revisione dello strumento militare nazionale e norme sulla medesima materia". La riforma si fonda su quattro pilastri fondamentali: 1) un nuovo limite per le dotazioni organiche di Esercito, Marina e Aeronautica che nel complesso non dovranno superare le 150 mila unità; 2) il personale dirigente delle tre forze armate dovrà essere di 310 unità; 3) una riduzione strutturale complessiva non inferiore al 30%; 4) l'attuazione della riforma non potrà comportare nuovi o maggiori oneri per la finanza pubblica, e tutti i risparmi ottenuti dovranno essere reinvestititi nel bilancio della Difesa. Alessandro Marrone, "I quattro pilastri della riforma della Difesa", in *AffariInternazionali*, 17 dicembre 2012, http://www.affarinternazionali.it/articolo.asp?ID=2208.

[7] Decreto legislativo 28 gennaio 2014, n°7-8. Il decreto legislativo dà attuazione alla legge n° 244/12 con un taglio dell'organico che dovrà essere di 13.400 unità per l'Esercito, 8.575 per l'Aeronautica e 4.325 per la Marina entro il 2024. Tuttavia, secondo alcuni analisti, la ricomposizione del personale militare attraverso un trasferimento ad altre amministrazioni del personale in esubero "previo consenso dell'interessato" rischia di far deragliare il processo di riforma. Per un ulteriore approfondimento si veda Alessandro Marrone, "La non riforma della Difesa", in *AffariInternazionali*, 24 febbraio 2012, http://www.affarinternazionali.it/articolo.asp?ID=2544.

[8] Stato Maggiore dell'Esercito, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre – PROSPECTA*, 2015, pp. 6-7.

[9] Ibid., p. 16.

impiegato in due operazioni sul territorio nazionale e in dodici missioni all'estero, con un totale di 10.361 soldati coinvolti nei diversi teatri operativi. Quella che segue è una breve sintesi dell'impegno operativo dell'Esercito nelle principali operazioni degli ultimi due decenni. Questo al fine sia di evidenziare l'impegno profuso dalla forza armata nel contesto della politica di difesa italiana, sia di spiegare come tali operazioni abbiano poi concorso a definire i requisiti di strumenti, assetti e piattaforme che l'Esercito andrà ad acquisire negli anni a venire[10]. A tal fine, ci si concentrerà maggiormente sulle operazioni in Kosovo, Iraq, Afghanistan e Libano. Infatti, benché vi siano state indubbiamente altre operazioni importanti, in primis in Somalia e in Bosnia, questi quattro casi hanno maggiormente concorso ad identificare le mancanze capacitive esistenti e quindi a delineare le nuove esigenze operative della componente terrestre.

Dopo la campagna aerea NATO contro la Serbia e la conseguente firma degli accordi tra le parti nel giugno del 1999, l'EI è presente in Kosovo dal 1999 in quanto parte della missione di peace-keeping "Kosovo Force" (KFOR) nel quadro della risoluzione 1244 del Consiglio di Sicurezza dell'ONU. La presenza militare in teatro, un contingente iniziale di 6.000 soldati, secondo solo a quello degli Stati Uniti, testimonia il decisivo impegno della forza armata in un'area geografica di interesse strategico per l'Italia[11]. A partire dal 2004 le autorità NATO decisero di raggruppare in un unico contesto operativo tutte le operazioni dell'Alleanza Atlantica dispiegate nei Balcani, dando inizio nell'aprile 2005 all'operazione "Joint Enterprise" che includeva la missione KFOR, i rapporti con le missioni dell'Unione europea, e i NATO HQ di Skopje, Tirana e Sarajevo[12]. Dal maggio 2006 la forza militare internazionale subì una riconfigurazione, passando da quattro Multinational Brigades a cinque Multinational Task Forces, divenute poi Multinational Battle Groups su base reggimento nel 2010[13]. Dal maggio 2011, le forze permanentemente stanziate in Kosovo che costituiscono KFOR sono due Multinational Battle Groups (uno a comando italiano), un reggimento carabinieri Multinational Specialized Unit (MSU) di cui fanno parte esclusivamente i carabinieri italiani, tre unità multinazionali denominate Joint Regional Detachment (JRD) di cui uno a guida

[10] Intervista, 10 febbraio 2015.

[11] Fabrizio Coticchia, Qualco*sa è cambiato? L'evoluzione della politica di difesa italiana dall'Iraq alla Libia (1991-2011)*, Pisa, Pisa University Press, 2013, pp. 158-171.

[12] Ministero della Difesa, *Kosovo - KFOR - Joint Enterprise*, http://www.difesa.it/OperazioniMilitari/op_intern_corso/KFOR/Pagine/default.aspx.

[13] Ibid.

italiana e, infine, un reggimento multinazionale con funzioni di riserva tattica[14]. Dal 2011 operano in Kosovo complessivamente 550 militari italiani appartenenti a tutte le forze armate, ma in particolare all'Esercito. Dal settembre 2013 l'Italia ha assunto la guida dell'intera operazione a cui partecipano 31 nazioni, di cui 23 Stati membri della NATO e 8 Paesi partner[15]. Attualmente, tra i compiti assegnati ai soldati italiani sono compresi la tutela delle condizioni di sicurezza e libertà di movimento, la supervisione dell'attuazione del Military Technical Agreement stipulato fra Serbia e NATO, l'assistenza allo sviluppo delle istituzioni locali e il supporto alle organizzazioni internazionali presenti sul territorio[16].

Nel marzo 2003 una coalizione internazionale a guida americana intraprendeva l'operazione "Iraqi Freedom" in Iraq[17]. In seguito alla vittoria sul campo della coalizione e alla risoluzione ONU 1483 del 22 maggio del 2003, iniziò una seconda fase delle operazioni, la quale si poneva come obiettivo la stabilità economica, sociale e politica dell'Iraq[18]. A partire dall'agosto 2003 un contingente italiano di 3.000 soldati – salito poi a 3.300 unità nella primavera del 2005 – veniva impiegato per quella che si sarebbe chiamata operazione "Antica Babilonia", a garanzia del ripristino delle condizioni di sicurezza, delle infrastrutture e dei servizi essenziali del Paese iracheno. I militari italiani furono dislocati a Nassiriyah, Baghdad e Bassora, così come nei comandi in Kuwait e a Tampa (USA). All'Esercito venne affidato il settore della provincia di Dhi Qar, sotto la Divisione Multinazionale nella parte sud-orientale (Multi-National Division South-East – MND-SE) guidata dal Regno Unito[19]. I militari italiani furono impegnati in attività quali: l'addestramento e l'equipaggiamento delle forze di sicurezza irachene, il mantenimento della condizioni di sicurezza sul terreno, il ripristino delle infrastrutture e dei servizi essenziali, il rilevamento di minacce NBC, senza dimenticare le attività di carattere umanitario e la realizzazione di progetti per il miglioramento della qualità della vita, l'educazione e l'assistenza

[14] Ibid.

[15] Ministero della Difesa, *Kosovo - KFOR - Joint Enterprise. Contributo nazionale*, http://www.difesa.it/OperazioniMilitari/op_intern_corso/KFOR/Pagine/ContributoNazionale.aspx.

[16] Ibid.

[17] L'Italia non partecipò a questa fase delle operazioni militari.

[18] Ministero della Difesa, *Iraq - Antica Babilonia*, http://www.difesa.it/OperazioniMilitari/op_int_concluse/Iraq_AnticaBabilonia/Pagine/default.aspx.

[19] Ministero della Difesa, *Iraq - Antica Babilonia. Forze impegnate*, http://www.difesa.it/OperazioniMilitari/op_int_concluse/Iraq_AnticaBabilonia/Pagine/Forzeimpegnate.aspx.

sanitaria alla popolazione[20]. L'operazione è stata a detta di molti "onerosa, complessa a drammatica", con un totale di 33 caduti, il dato più alto dopo l'Afghanistan in operazioni militari dopo la seconda guerra mondiale[21]. I soldati italiani si trovarono ad operare in un contesto altamente conflittuale, che spesso limitò le attività di ricostruzione o di supporto alla pace. A titolo di esempio, si può ricordare l'attacco suicida contro la base "Maestrale" organizzato da Al-Qaeda nel novembre del 2003 che costò la vita a 17 militari, due civili italiani e nove iracheni. I soldati italiani furono anche coinvolti in una serie di scontri a fuoco ad alta intensità, nonostante una generale carenza dei mezzi a disposizione in teatro e di regole di ingaggio fortemente limitanti rispetto ad una situazione di conflittualità superiore ad una operazione di mero peace-keeping[22]. Si ricordano, ad esempio, le tre "battaglie dei ponti" che contrapposero le forze armate italiane all'Esercito del Mahdi' costituito dalle unità di Muqtada al-Sadr. L'operazione italiana si concluse nel dicembre 2006 con l'ammainabandiera a Nassiriyah.

I militari italiani hanno operato in Afghanistan nel quadro dell'operazione "Enduring Freedom" da marzo a settembre 2003 e nella cornice dell'International Security Assistance Force (ISAF) da agosto 2003 fino a dicembre 2014. L'operazione "Enduring Freedom" si colloca anch'essa nell'ottica della lotta contro il terrorismo internazionale da parte degli Stati Uniti a seguito dei drammatici attacchi del 2001. L'obiettivo della missione era creare le condizioni per un Afghanistan stabile e sicuro attraverso l'eliminazione della resistenza talebana e la minaccia di Al-Qaeda, in particolare nelle zone geografiche al confine con il Pakistan nella provincia di Paktia. La missione italiana "Nibbio", composta da un contingente di 1.000 soldati, ha assunto i compiti di controllo del territorio e lotta alla minaccia proveniente dai gruppi terroristici, inclusa la distruzione di basi logistiche e centri di reclutamento. La missione può verosimilmente considerarsi una delle più rischiose condotte dalla forza armata[23] nel secondo dopoguerra, avvenuta in un teatro operativo collocato su un confine "poroso" come quello afgano e pakistano, ma anche e innanzitutto per

[20] Ministero della Difesa, *Iraq - Antica Babilonia. Missione*, http://www.difesa.it/OperazioniMilitari/op_int_concluse/Iraq_AnticaBabilonia/Pagine/Missione.aspx.

[21] Fabrizio Coticchia, *Qualcosa è cambiato?*, cit., pp. 198-204.

[22] Ibid., pp. 204-213.

[23] Per quanto riguarda il contributo della componente aero-navale alle operazioni in Afghanistan si veda Vincenzo Camporini et al., *Il ruolo dei velivoli da combattimento italiani nelle missioni internazionali: trend e necessità*, Roma, Nuova Cultura, 2014 (Quaderni IAI n. 10), http://www.iai.it/it/node/1851.

il tipo di minaccia asimmetrica a cui le truppe hanno dovuto fare fronte (lanci di bombe a mano, raffiche di armi leggere, ordigni esplosivi)[24].

Per quello che riguarda ISAF, la missione fu attivata a seguito della risoluzione 1386/2001 del Consiglio di Sicurezza ONU e nel quadro degli accordi di Bonn del dicembre 2001. Fu a partire dall'agosto del 2003, dopo l'assunzione delle responsabilità di ISAF da parte della NATO, che iniziò l'operazione italiana nel quadro degli accordi sopracitati[25]. Lo scopo della missione ISAF era quello di sostenere il Governo afghano nel mantenimento delle condizioni di sicurezza all'interno del Paese, favorire lo sviluppo delle strutture amministrative, estendere il controllo del governo e, in ultima analisi, assistere gli sforzi umanitari e di ricostruzione del Paese[26]. In particolare, le truppe italiane si occuparono della formazione dell'Esercito afghano e delle sue forze di polizia, della somministrazione di aiuti umanitari e della ricostruzione di infrastrutture[27]. Il personale presente a Kabul fu impegnato soprattutto presso il Comando ISAF (ISAF HQ), l'ISAF Joint Command HQ (ISAF JC HQ), il Comando Special Operation Forces (ISAF SOF HQ) e il NATO Training Mission – Afghanistan (NTM-A). Le forze armate italiane del Train Advise Assist Command-West (TAAC-W) operarono in un'ampia regione dell'Afghanistan occidentale, comprendente le provincie di Herat, Badghis, Ghowr e Farah. Negli anni, con l'intensificarsi della guerriglia talebana, l'EI è stato coinvolto in una serie di scontri contro gli insorti talebani, soprattutto nella zona di Bala Murghab[28], zona dove operarono anche le forze speciali della Task Force 45, impegnate prevalentemente nella provincia di Helmand e sul confine con il Pakistan per bloccare le iniziative talebane, oltre che ad essere impegnate sul confine con l'Iran dove condussero l'operazione "Sarissa"[29].

---

[24] Stato Maggiore della Difesa, *Task Force Nibbio*, ottobre 2013, http://www.difesa.it/OperazioniMilitari/op_int_concluse/Afghanistan_Nibbio/Documents/92952_SchedaNIBBIO131003.pdf.

[25] Esercito, *ISAF. Contributo nazionale*, http://www.esercito.difesa.it/operazioni/operazioni_oltremare/Pagine/ISAF-Contributo-Nazionale.aspx.

[26] Ibid.; NATO, *ISAF's mission in Afghanistan (2001-2014)*, last update 13 January 2015, http://www.nato.int/cps/en/natohq/topics_69366.htm.

[27] Ministero della Difesa, *Afghanistan - ISAF. Missione*, http://www.difesa.it/OperazioniMilitari/op_int_concluse/ISAF/Pagine/Missione.aspx.

[28] "Afghanistan: l'inferno di Bala Murghab", in *L'Espresso*, 21 luglio 2010, http://espresso.repubblica.it/internazionale/2010/07/21/news/l-inferno-di-bala-murghab-1.22554.

[29] "I soldati invisibili della Task Force 45", in *Il Sole 24 Ore*, 18 settembre 2010, http://www.ilsole24ore.com/art/notizie/2010-09-18/soldati-invisibili-task-force-105713.shtml; Fabrizio Coticchia, *Qualcosa è cambiato?*, cit., pp. 188-195.

Nel corso degli anni, quindi, l'Italia ha messo a disposizione un numero rilevante di uomini e mezzi, rispondendo adeguatamente alle esigenze della forza multinazionale specialmente nel momento del cosiddetto "surge" deciso dall'amministrazione americana nel 2009. A sostegno della nuova strategia del Presidente americano, da raggiungere attraverso un aumento sostanziale delle truppe sul terreno, l'Italia arrivò a schierare fino a 4.000 uomini nel 2011, ovvero il 50-60% di tutti gli uomini – così come delle risorse economiche – dedicati alle operazioni all'estero in quel determinato anno[30]. Tra i mezzi utilizzati, l'Esercito ebbe a disposizione elicotteri CH-47, A-129 e NH-90, i veicoli ruotati VBM "Freccia" e VTLM "Lince", velivoli C-130 e unmanned. Durante gli undici anni di missione, le forze armate italiane hanno subito centinaia di attacchi che hanno provocato la morte di oltre cinquanta soldati, il dato più alto di caduti registrati in operazioni militari dalla seconda guerra mondiale in poi[31]. Terminata la missione ISAF nel dicembre 2014, da gennaio 2015 è partita, sempre in Afghanistan, la missione "Resolute Support" dove l'Esercito schiera 500 militari su base annua, a fronte di un numero iniziale di 750 unità. Lo scopo della missione è addestrare e fornire assistenza alla forze di sicurezza e istituzioni del Paese. Rispetto all'operazione precedente, "Resolute Support" non si caratterizza per essere una missione "combat" e conta un numero di unità sul terreno ben più limitato. Secondo gli attuali piani NATO, la prima fase dell'operazione si concluderà nel luglio del 2015, quando comincerà a rientrare gran parte del contingente italiano, mentre verso la fine del 2015 rimarranno in teatro circa una settantina di militari. L'Esercito è la forza armata più consistente all'interno della missione, in particolare con i militari della Brigata bersaglieri "Garibaldi" per compiti di Force Protection e Quick Reaction Force, più una componente del genio guastatori "Timavo" specializzata nella gestione di materiale esplosivo e mine[32].

L'Esercito è impegnato in Libano nel quadro delle risoluzioni del Consiglio di Sicurezza delle Nazioni Unite n. 425 (1978), 1701 (2006) e 1832 (2008)[33], le ultime due adottate in seguito agli scontri e alle tensioni fra le forze armate israeliane e quelle di Hezbollah. L'Italia, e in particolare l'Esercito, fa parte della forza multinazionale United Nations Interim Force In

[30] Il dato si riferisce all'insieme delle forze armate italiane schierate nell'operazione.

[31] Fabrizio Coticchia, *Qualcosa è cambiato?*, cit., p. 188.

[32] Esercito, *RS: Contributo Nazionale*, http://www.esercito.difesa.it/operazioni/operazioni_oltremare/Pagine/RS-Contributo-Nazionale.aspx.

[33] Ministero della Difesa, *Operazioni Militari/Libano*, http://www.difesa.it/OperazioniMilitari/Pagine/scheda_ops_libano.aspx.

Lebanon (UNIFIL) sotto l'egida ONU che dal 1978 controlla la linea armistiziale Blue Line tra Libano ed Israele. Dopo la guerra del 2006, al compito di verificare il ritiro delle truppe israeliane dai territori libanesi si sono aggiunti anche il sostegno al governo libanese per la protezione dei suoi confini e il compito di assistenza umanitaria alla popolazione civile[34]. All'inizio dell'operazione nazionale "Leonte", l'Italia è stata tra i Paesi che più ha contribuito alla missione con ben 2.500 uomini[35]. Oltre al ruolo di mantenimento della pace tramite la presenza stessa di un significativo contingente militare multinazionale in un contesto altrimenti instabile, l'Esercito ha fatto leva principalmente sulla cooperazione civile-militare, concentrandosi ad esempio sulle attività di bonifica da ordigni esplosivi e corsi di prevenzione presso le scuole. A dimostrazione della qualità del lavoro svolto dall'Esercito, l'Italia ha assunto il comando dell'intera operazione ONU per sei degli ultimi otto anni di missione[36] (l'ultima volta dall'ottobre 2014) in un teatro regionale sempre più pericoloso a causa delle tensioni e dell'instabilità generate dal conflitto civile in Siria[37] e della sanguinosa avanzata dello Stato Islamico in Iraq e Siria[38]. Il contributo italiano ad aprile 2015 è pari a 1.100 uomini[39].

Le operazioni che hanno visto e vedono tuttora impegnato l'Esercito hanno messo alla prova i soldati italiani in una serie di compiti richiedenti abilità e capacità differenti proprio per la diversità delle mansioni svolte. L'ambiente operativo si è dimostrato[40]:

a) complesso, interforze e multidimensionale;
b) con una prevalenza di conflitti asimmetrici rispetto a quelli di natura tradizionale e/o ibridi;
c) dilatato negli spazi e nei settori di intervento;
d) caratterizzato dalla copresenza di più attori (governativi e non), insorgenti e popolazione civile;
e) interconnesso quanto a piattaforme, sensori e attuatori.

---

[34] Ibid.

[35] Fabrizio Coticchia, *Qualcosa è cambiato?*, cit., p. 220.

[36] Ministero della Difesa, *Operazioni Militari: Libano*, http://www.difesa.it/OperazioniMilitari/Pagine/scheda_ops_libano.aspx.

[37] "Lebanon under fire: Two years of spillover from the Syrian civil war", in *The Daily Star*, 16 January 2015, http://bit.ly/1JSUCaw.

[38] Carol Malouf e Ruth Sherlock, "ISIS Is Building Strength On Lebanon's Doorstep", in *BusinessInsider*, 20 January 2015, http://read.bi/15thyfi.

[39] Esercito, *UNIFIL: Contributo Nazionale*, http://www.esercito.difesa.it/operazioni/operazioni_oltremare/Pagine/UNIFIL-Contributo-Nazionale.aspx.

[40] Intervista, 10 febbraio 2015.

Se si volesse generalizzare in estrema sintesi quelle che sono state, e sono attualmente, le necessità principali dell'Esercito, le missioni in teatro hanno evidenziato che in futuro sarà auspicabile sviluppare un'architettura C2[41] in grado di convogliare le informazioni a supporto di un processo decisionale più tempestivo ed efficace; ampliare la capacità di aggiornamento in tempo reale della situazione in teatro attraverso sofisticate capacità di intelligence; e in ultimo potenziare tutte le nuove piattaforme con sistemi di protezione attiva e passiva[42].

3.1.3 I possibili scenari d'impiego

Anche se questa possibilità appare obiettivamente remota, un primo possibile scenario d'impiego in cui la forza armata di terra potrebbe essere chiamata ad operare è quello della difesa del territorio nazionale in un classico conflitto convenzionale fra attori statuali, in cui le forze in battaglia sono ben definite e tendenzialmente cercano di evitare di coinvolgere la popolazione civile[43].

Legato indissolubilmente al primo, anche se forse più probabile, il secondo possibile scenario presuppone che l'EI partecipi alla difesa dell'area euro-atlantica in caso di attacco ad uno dei Paesi membri della NATO. Tale attacco attiverebbe l'articolo 5 del trattato di Washington e il principio della difesa collettiva[44]. Ad esempio, è ipotizzabile che l'Esercito intervenga

[41] Comando e Controllo è "l'esercizio dell'autorità e della direzione su determinate unità da parte di un comandante nel conseguimento di una missione". Carl H. Builder, Steven C. Bankes, Richard Nordin, *Command Concepts. A Theory Derived from the Practice of Command and Control*, Santa Monica, RAND, 1999, http://www.rand.org/pubs/monograph_reports/MR775.html.

[42] A titolo esaustivo, oltre a quelle già citate, i teatri operativi hanno evidenziato anche le seguenti esigenze: migliorare il supporto aereo ravvicinato e di artiglieria terrestre; favorire una migliore e maggiore integrazione delle dimensioni civile e militare attraverso capacità duali; aumentare la capacità di identificazione della minaccia; migliorare le procedure di evacuazione medica d'urgenza; incrementare l'autonomia operativa e logistica. Stato Maggiore dell'Esercito, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit., p. 35.

[43] Ibid., p. 35.

[44] L'articolo 5 del Trattato di Washington recita: "Le parti convengono che un attacco armato contro una o più di esse in Europa o nell'America settentrionale sarà considerato come un attacco diretto contro tutte le parti, e di conseguenza convengono che se un tale attacco si producesse, ciascuna di esse, nell'esercizio del diritto di legittima difesa, individuale o collettiva, riconosciuto dall'art. 51 dello Statuto delle Nazioni Unite, assisterà

a seguito di una profonda crisi politica generatasi all'interno di uno stato membro dell'Allenza, ulteriormente aggravata da tensioni alimentate da minoranze etniche al suo interno e ostili al quadro politico in essere. Alcune potenze regionali potrebbero esacerbare la conflittualità interna per aumentare la loro influenza, facendo leva sulle minoranze etniche presenti. Un intervento potrebbe configurarsi nella mobilitazione delle forze armate a scopo di deterrenza, la messa in sicurezza delle infrastrutture critiche (principali vie di comunicazione, aeroporti, ecc.) e dell'area a garanzia di una certa libertà di movimento. In casi estremi le forze terrestri potrebbero essere chiamate all'ingaggio con le truppe ostili per ripristinare l'integrità territoriale del Paese alleato nel caso esso fosse stato occupato[45].

La terza opzione prevede il possibile impiego dell'EI in missioni di prevenzione, gestione e stabilizzazione di crisi all'interno di Paesi al di fuori dei confini italiani o del perimetro dei Paesi NATO[46]. Nella fattispecie, è possibile che uno Stato in una di queste zone venga fortemente destabilizzato da una serie di rivolte di natura socio-politica oppure etnico-religiosa e che queste sfocino in una guerra civile fra un governo centrale debole e uno o più gruppi ribelli armati. A seguito di una risoluzione del Consiglio di Sicurezza, le forze armate potrebbero intervenire prima in attività di peace-enforcement[47], per impedire nuovi scontri fra i belligeranti e/o a protezione della popolazione civile, e poi in attività di peace-building[48],

---

la parte o le parti così attaccate intraprendendo immediatamente, individualmente e di concerto con le altre parti, l'azione che giudicherà necessaria, ivi compreso l'uso della forza armata, per ristabilire e mantenere la sicurezza nella regione dell'Atlantico settentrionale. Ogni attacco armato di questo genere e tutte le misure prese in conseguenza di esso saranno immediatamente portate a conoscenza del Consiglio di Sicurezza. Queste misure termineranno allorché il Consiglio di Sicurezza avrà preso le misure necessarie per ristabilire e mantenere la pace e la sicurezza internazionali".

[45] Stato Maggiore dell'Esercito, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit., pp. 35-37.

[46] Ibid., pp. 44-45. Esempi di queste missioni sono citati nel paragrafo precedente.

[47] "Peace enforcement involves the application of a range of coercive measures, including the use of military force. It requires the explicit authorization of the Security Council. It is used to restore international peace and security in situations where the Security Council has decided to act in the face of a threat to the peace, breach of the peace or act of aggression. The Council may utilize, where appropriate, regional organizations and agencies for enforcement action under its authority and in accordance with the UN Charter". United Nations Peacekeeping, *Peace and Security*, http://www.un.org/en/peacekeeping/operations/peace.shtml.

[48] "Peacebuilding aims to reduce the risk of lapsing or relapsing into conflict by strengthening national capacities at all levels for conflict management, and to lay the founda-

a sostegno delle condizioni per una pace durevole. Durante queste operazioni l'Esercito si potrebbe trovare di fronte ad una minaccia irregolare o ibrida[49]. A compiti di natura prettamente militare, come quelli di difesa e deterrenza, si affiancherebbero anche altre mansioni come le missioni di pattugliamento e di supporto all'ordine pubblico. L'EI potrebbe essere chiamato ad intervenire anche in un "Failed o Fragile State" (Stato fallito o fragile), qualora il governo del suddetto Paese richiedesse aiuto nel rafforzamento delle proprie capacità di difesa e di controllo del territorio, o consulenza in attività di riforma del settore della sicurezza (Security Sector Reform) e consolidamento istituzionale.

La quarta e ultima opzione strategica consiste nel supporto alle attività della Protezione Civile e ad altri attori istituzionali in caso di calamità o più in generale di pubblica necessità sul territorio nazionale, sulla scorta di quanto fatto, per esempio, a L'Aquila dopo il terremoto del 2009 o più recentemente in Emilia o in Toscana. L'EI potrebbe essere impiegato in seguito ad un terremoto con magnitudo elevata, anche con conseguente onda anomala, se questo si originasse in una zona costiera. In una prima fase, la forza armata sarebbe impegnata in attività di soccorso e supporto alle popolazioni colpite, mentre successivamente si concentrerebbe sulla messa in sicurezza dell'area in generale, a prevenzione di fenomeni di sciacallaggio e saccheggio.

In futuro l'Esercito continuerà ad avere un ruolo fondamentale a sostegno della politica di difesa nazionale, a maggior ragione a fronte del deterioramento del contesto di sicurezza in cui si trova l'Italia poiché, come gli eventi degli ultimi anni hanno dimostrato, l'imprevedibilità del quadro strategico è diventata un tratto caratterizzante del mondo in cui viviamo, insieme alla rapidità stessa dei cambiamenti.

Il ruolo fondamentale dell'Esercito rimane quello della protezione dell'integrità del territorio nazionale, anche se le possibilità di un attacco

---

tion for sustainable peace and development. It is a complex, long-term process of creating the necessary conditions for sustainable peace. Peacebuilding measures address core issues that effect the functioning of society and the State, and seek to enhance the capacity of the State to effectively and legitimately carry out its core functions". Ibid.

[49] Per minaccia irregolare s'intende l'uso della forza tipico di attori non statali come ad esempio gruppi terroristici o di ribelli che fanno ampio ricorso alla strategia del terrore. Per minaccia ibrida s'intende quella derivante da nemici di natura difficilmente identificabile che non necessariamente conducono la loro azione sulla base di vincoli giuridici o etici delle forze statuali. Essi si affidano a pratiche di "logoramento", attraverso tattiche regolari ed irregolari in maniera concertata e combinata, e sono in grado di portare avanti anche un conflitto "mediatico" in maniera efficace. Stato Maggiore dell'Esercito, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit., p. 50.

diretto all'Italia appaiono lontane, per lo meno da parte di attori statuali. Nonostante sia improbabile, la possibilità che esso sia coinvolto in uno scontro convenzionale non può essere esclusa a priori e ciò impone all'Italia di dotarsi degli strumenti necessari affinché sia pronta ad affrontare una minaccia che potrebbe diventare incombente.

Tutt'altro discorso merita l'analisi in merito alla seconda opzione strategica, ovvero quella della protezione dello spazio euro-atlantico. La crisi in Ucraina del 2014 sembra aver riproposto lo spettro della contrapposizione fra Occidente e Russia, con molti a dubitare sulle capacità di tenuta del sistema di sicurezza europeo post-Guerra Fredda[50]. A questo proposito, le conseguenze della crisi si sono già manifestate in alcune recenti dichiarazioni e decisioni assunte a livello militare da parte dei Paesi baltici e scandinavi, i Paesi maggiormente allarmati dai risvolti della crisi in corso e dal crescente attivismo russo sui propri confini[51]. Anche la NATO ha preso importanti decisioni in seguito alla crisi. Al vertice del settembre 2014 in Galles, i Paesi membri hanno deciso per un aumento delle esercitazioni alleate in Europa orientale, approvando al tempo stesso un Readiness Action Plan volto a mantenere alta la prontezza delle forze armate alleate. Prontezza frequentemente testata di recente dalle missioni russe in prossimità dello spazio aereo e/o marittimo di Gran Bretagna, Repubbliche Baltiche, Svezia e altri Paesi nord europei[52]. In un tale contesto, non è da escludere che un intervento della NATO possa rivelarsi necessario qualora uno dei suoi Stati membri sia vittima delle stesse tattiche usate dalla Russia per destabilizzare l'Ucraina, arrivando fino alla possibilità di ingaggio di tipo convenzionale con truppe nemiche[53].

---

[50] Mikhail Gorbachev, "A New Cold War Order", in *Project Sindicate*, 5 January 2015, http://po.st/QpXoPk; Robert H. Legvold, "Managing the New Cold War", in *Foreign Affairs*, Vol. 93, No. 4 (July/August 2014), pp. 74-84, https://www.foreignaffairs.com/node/1113241; Stephen Walt, "The Bad Old Days Are Back", in *Foreign Policy*, 2 May 2014, http://foreignpolicy.com/2014/05/02/the-bad-old-days-are-back. Per maggiori informazioni sulla crisi ucraina si veda il sito del Center for Strategic and International Studies (CSIS): *The Ukraine Crisis Timeline*, http://csis.org/ukraine.

[51] Giovanna De Maio, "Nel Baltico col fiato sul collo", in *AffariInternazionali*, 29 gennaio 2015, http://www.affarinternazionali.it/articolo.asp?ID=2951; Andrius Sytas, "Worried about Russia? Lithuania says 'Keep calm and read the war manual'", in *Reuters*, 15 January 2015, http://reut.rs/1E2ALjq.

[52] Giovanna De Maio, "Nel Baltico col fiato sul collo", cit.

[53] Peter Apps, "Ambiguous warfare' providing NATO with new challenge", in *Reuters*, 21 August 2014, http://reut.rs/1wdWRzi; Alistair Scrutton e Sabina Zawadzky, "EU must prepare for Russia's 'hybrid warfare': Danish formin", in *Reuters*, 27 October 2014, http://

Sembra più probabile tuttavia che in futuro l'Esercito sarà impiegato in situazioni simili alla terza opzione strategica, ovvero in missioni internazionali in contesti operativi affini a quelli dove la forza armata ha operato negli ultimi 25 anni. Le aree situate nell'immediato vicinato dell'Italia – Nord Africa e Africa sub-sahariana, Medio Oriente, Europa Orientale, Balcani e Caucaso – sembrano particolarmente inclini a questo tipo di situazioni, aree dove prevalgono ancora regimi non pienamente democratici e dove sono tuttora presenti "conflitti congelati"[54]. Questa opzione sembra ancora più probabile rispetto a quella della protezione dello spazio atlantico viste le condizioni attuali in cui versa la Libia, caduta nel caos più totale a causa della lotta fra milizie e governi rivali in seguito all'intervento NATO nel 2011. Uno scenario di questo tipo appare di grande attualità, a maggior ragione alla luce dell'intensificarsi degli scontri fra miliziani, all'avanzata dello Stato Islamico nel Paese nordafricano e alle dichiarazioni di importanti esponenti del governo italiano che hanno proposto un intervento di peacekeeping in Libia nel quadro di una risoluzione delle Nazioni Unite[55]. In tali contesti, il conflitto terrestre si caratterizzerà per la molteplicità delle sue dimensioni, a cui si aggiungeranno oltre a quelle classiche le "nuove" dimensioni dell'arena mediatica e dello spazio cibernetico. I combattimenti si svolgeranno in aree congestionate dove sarà complesso discriminare fra forze amiche e nemiche, e sarà necessario valutare in ogni circostanza se utilizzare la forza o meno[56].

3.2 L'Esercito Italiano e la capacità netcentrica

I recenti piani d'ammodernamento dello strumento militare di diversi Paesi NATO, volti alla digitalizzazione e alla messa in rete dei propri assetti militari, rappresentano l'esempio più recente del costante tentativo di incorporare nuove tecnologie nel modus operandi delle forze armate. Nel caso della capacità netcentrica, come è accaduto di frequente dalla seconda metà del '900 in poi nel campo della tecnologia militare, l'impulso iniziale si è originato dagli Stati Uniti – oltre due decenni fa – con il concetto

reut.rs/1wvAhyU.

[54] Stato Maggiore dell'Esercito, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit., pp. 26-27.

[55] Laurence Figa'-Talamanca, "L'Isis avanza in Libia. Gentiloni, pronti a combattere con Onu", in *Ansa*, 16 febbario 2015, http://ow.ly/2UGRdr.

[56] Intervista, 4 febbraio 2015.

di Network Centric Warfare[57]. I Paesi NATO presero alcune importanti iniziative in tal senso al summit di Praga del 2002, quando si impegnarono ad acquisire una serie di capacità giudicate irrinunciabili per l'attuazione del processo di trasformazione in senso digitale delle forze armate alleate. Con l'acronimo NEC, la NATO esprimeva l'idea di "abilitare la capacità" (Enable Capability) di combinare in un'unica rete (Network) elementi tra loro diversi – dottrinali, procedurali, tecnologici, organizzativi ed umani – in modo da ottenere la loro interazione per raggiungere e mantenere una marcata superiorità strategica nella condotta delle operazioni militari – anche alla luce dell'esperienza operativa del periodo post-Guerra Fredda. Si trattava di una scelta meno radicale rispetto all'iniziale proposito americano ma altrettanto efficace, preferita dalla NATO, ed in particolare da Paesi quali Francia, Germania e Gran Bretagna.

I primi segnali dell'interesse italiano verso la capacità netcentrica vennero espressi nel Concetto Strategico del capo di Stato Maggiore della Difesa nel 2005. Il rapporto sottolineava l'importanza della "capacità di raccogliere, gestire e condividere l'informazione acquisita, mediante un robusto sistema di C4I[58] a carattere netcentrico" per rendere le forze armate "più idonee ad affrontare le operazioni future"[59]. Nel 2006, lo Stato Maggiore della Difesa (SMD) pubblicava il documento "La trasformazione netcentrica: il futuro dell'interoperabilità multinazionale e interdisciplinare", in cui l'allora Capo di Stato Maggiore della Difesa, l'Ammiraglio Giampaolo Di Paola, non poneva più la domanda se l'Italia avesse dovuto o no acquisire una capacità netcentrica, bensì quando e in quale misura, ritenendola oramai un'esigenza prioritaria e assolutamente ineludibile. Alla luce anche della rapida evoluzione dei processi di ammodernamento dello strumento terrestre negli altri Paesi NATO, nel gennaio 2007 prendeva avvio lo studio del programma Forza NEC, che si delineava come programma interforze a guida dell'Esercito[60].

---

[57] Per una trattazione del tema si veda Michele Nones e Marrone Alessandro (a cura di), *La trasformazione delle Forze Armate: il programma Forza Nec*, Roma, Nuova Cultura, 2011 (Quaderni IAI n. 2), pp. 31-40, http://www.iai.it/it/node/1149.

[58] Comando, Controllo, Comunicazioni, Computer e Intelligence (C4I) costituisce l'evoluzione del concetto di Comando e Controllo "analogico" a seguito dell'introduzione della componente Comunicazioni (TLC), Computer e Intelligence.

[59] Stato Maggiore della Difesa, *Il Concetto strategico del Capo di Stato Maggiore della Difesa*, 2005, http://www.aeronautica.difesa.it/Missione/Documents/libroconcettostrategico.pdf.

[60] Si veda Michele Nones e Marrone Alessandro (a cura di), *La trasformazione delle Forze Armate*, cit., p. 48.

La precedente analisi dei possibili scenari di impiego suggerisce che l'Esercito continuerà in futuro ad operare prevalentemente e verosimilmente in operazioni di pace nel contesto di operazioni multinazionali, come verificatosi nella recente esperienza operativa. L'esperienza nei teatri kosovaro, iracheno, afgano e libanese è stata utile nell'elaborare una serie di apposite TTP (Tactics, Techniques & Procedures) e SOP (Standing Operating Procedures) per la conduzione di operazioni future in cui il grado di interoperabilità fra forze armate nazionali rappresenterà la discriminante di successo oppure no. È in questo contesto che va letta la volontà dell'EI di acquisire la NEC.

Per le forze armate italiane la trasformazione netcentrica significa

> riuscire ad interconnettere in rete sensori, le apparecchiature o i soldati che percepiscono e rilevano attività naturali e umane, i decisori, ovvero coloro i quali, sulla base delle informazioni disponibili, assumono una decisione, e gli attuatori, cioè i sistemi che mettono in pratica una decisione siano essi armi o soldati, formando una struttura unica, complessa ed integrata. In questo modo è possibile sfruttare sinergicamente informazioni e capacità operative allo scopo di conseguire gli effetti desiderati[61].

In questo senso, la digitalizzazione delle forze armate rappresenta il primo passo verso la realizzazione di un sistema netcentrico, ovvero l'integrazione in un sistema C4I[62] di sistemi e tecnologie per acquisire, scambiare, mettere in correlazione e utilizzare nel momento appropriato le informazioni ottenute durante le varie fasi di un'operazione. Questo processo di raccolta delle informazioni permette di acquisire una Shared Situational Awareness, ossia "la conoscenza della situazione operativa tra le forze"[63]. È attraverso la Shared Situational Awareness che è possibile acquisire la cosiddetta "Information Superiority" – la superiorità delle informazioni – la quale rappresenta un moltiplicatore di forza, un elemento chiave nel raggiungimento del successo, soprattutto nel quadro di operazioni interforze e internazionali[64]. In sostanza, la tecnologia netcentrica offre la possibilità di integrare i dati che provengono dal campo in un'unica COP e fornire una visione globale di quello che succede sul campo ai vari livelli di coman-

[61] Ibid., p. 51.
[62] Ibid., p. 52.
[63] Ibid., p. 96.
[64] Ibid., p. 41.

do. Come è facilmente intuibile, conoscere il corso degli eventi in tempo reale costituisce un vantaggio notevole poiché consente ai comandanti di prendere decisioni coerenti e adeguate agli sviluppi che si materializzano sul terreno, nonché adottare le contromisure ed i correttivi più opportuni. Grazie ai vari sensori e alla fusione delle informazioni, quindi, l'"Information Superiority" favorisce una migliore gestione delle operazioni da parte dei comandanti: una più efficace capacità di identificazione classificazione ed ingaggio dell'obiettivo, una maggiore localizzazione delle forze alleate e protezione del soldato dal fuoco amico, una efficace integrazione delle piattaforme aeree e terrestri e infine una logistica migliorata e pianificata a seconda dei pericoli e delle minacce che provengono dal terreno. In riferimento all'ipotesi di impiego in caso di calamità, la filosofia netcentrica consentirà alla forza armata un miglioramento delle comunicazioni in ambito urbano, della capacità di individuazione dei feriti e delle attività di evacuazione[65]. Digitalizzare significa anche connettere in un'unica rete e mettere in comunicazione i differenti sistemi di C2 adoperati dalle forze armate, e, per quanto possibile, i vari assetti e piattaforme utilizzate dalla Marina, dall'Aeronautica e dall'Esercito.

Ma il grande vantaggio della filosofia netcentrica si concretizza in ambito multinazionale, con la possibilità di permettere a sistemi e assetti di diversi Paesi di comunicare tra loro in maniera automatica o semi-automatica, con l'indubbio beneficio dell'interoperabilità tra truppe operanti nell'ambito di una coalizione internazionale. L'interoperabilità è sempre maggiormente richiesta nel caso di condotta di operazioni in contesti multilaterali (NATO, UE e ONU) e chiaramente – laddove raggiunta – si traduce in una maggiore visibilità dell'apporto italiano al mantenimento della sicurezza internazionale, e possibilmente anche nell'assunzione diretta della leadership in specifiche missioni dove l'interesse italiano risulta maggiormente in gioco.

Forza NEC è alla base di una forza terrestre moderna che sia "expeditionary", ovvero in grado di proiettarsi all'esterno, "network capable", vale a dire di operare in maniera netcentrica, e "effect based operations oriented", capace di eseguire missioni che raggiungano l'intero raggio di "effetti" desiderati attraverso l'applicazione di strumenti militari, diplomatici, psicologici ed economici[66]. Esso mira a connettere tutti i livelli della catena di comando e controllo di un'operazione, dal sensore (livello T0),

[65] Ibid., pp. 96-99.

[66] Ibid., p. 60.

al soldato (livello T1), passando per tutti i livelli intermedi quali squadra (T2), plotone (T3), compagnia/squadrone (T4), battaglione/gruppo/reggimento (T5), fino alla brigata (T6). L'evoluzione netcentrica presuppone che tutti i sistemi vengano digitalizzati, ossia dotati di sistemi informatici per l'invio e la ricezione delle informazioni di nuova generazione, siano messi in rete e possano comunicare fra di loro in relazione ad una ben precisa politica di information management, ovvero gestione dell'informazione. Forza NEC, nell'indicare "la via" per la digitalizzazione dei sistemi, si pone come catalizzatore di altri programmi in essere, andando ad intervenire sia sugli aggiornamenti di programmi consolidati già avviati sia sulla definizione delle specifiche tecniche per quelli non ancora avviati. Anche per questo, il programma Forza NEC è un programma di procurement sui generis, in quanto i suoi esiti andranno a influire e confluire nell'ambito più generale dell'ammodernamento dell'EI. A dimostrazione di ciò, esso coinvolge e fa convergere al suo interno altri programmi come il SIACCON, il SICCONA, il BFSA e Soldato Futuro.

Il SIACCON-2 (SIstema Automatizzato di Comando e CONtrollo ver. 2) è il sistema di C2, evoluzione del SIACCON 1AW, utilizzato dall'Esercito a supporto di operazioni militari di diverso tipo per i posti comando fissi (normalmente dal livello battaglione/reggimento a salire).

In modo analogo, il SICCONA (SIstema di Comando COntrollo e NAvigazione) è il sistema di C2 impiegato sulle piattaforme terrestri dotate di sistema d'arma (es. VBM "Freccia", VCC "Dardo", Centauro, ecc.) in grado di fornire le funzionalità di comando e controllo, nonché gestire dati legati al sistema d'arma ospitato, o dati logistici (carburante, manutenzione, ricambi, munizioni, ecc.) e di navigazione[67].

Il BFSA (Blue Force Situational Awareness) è un sistema che serve all'identificazione delle forze amiche in teatro a livello tattico e alla navigazione, che, a differenza del SICCONA, andrà ad equipaggiare la maggior parte delle piattaforme non dotate di armamento e quindi impiegate per attività di combat support, combat service support e le piattaforme logistiche.

Il programma Soldato Futuro ha come obiettivo quello di dotare il singolo soldato delle tecnologie in grado di migliorare la sua performance e trasformarlo allo stesso tempo in un "nodo" della rete. Il nuovo concetto alla base dello studio del sistema Soldato Futuro si basa sulla capacità

[67] Da un punto di vista tecnico-ingegneristico, la compatibilità fra sistemi C2 e piattaforme NEC viene garantita attualmente da una soluzione legacy denominata "Information Dissemination Mechanism". Per il futuro si prevede di adottare una sorta di mediatore di servizi detto "Service Bus". Intervista, 10 febbraio 2015.

di elevare in termini assoluti la protezione del soldato, agendo sulla protezione relativa delle singole componenti dell'equipaggiamento; evitare il blue-on-blue (c.d. fuoco amico); e infine di aumentare l'efficacia complessiva del soldato/uomo. Il programma, oltre a prevedere le dotazioni classiche non-NEC di nuova generazione (elmetto, giubbetto antiproiettile, fucile, zaino modulare, congegni di puntamento, individual safety kit, una nuova tuta da combattimento, ecc.) prevede di dotare il soldato – con livelli diversi di complessità in relazione al compito/ruolo da svolgere – di radio a larga banda e minicomputer per poter dialogare con gli altri nodi della rete, a seconda delle diverse configurazioni[68].

Ad ulteriore titolo di esempio, si possono citare alcuni mezzi che verranno aggiornati alla capacità netcentrica: il veicolo da combattimento blindato Centauro, l'elicottero d'attacco A-129 Mangusta, il veicolo da combattimento corazzato Dardo, il veicolo blindato da trasporto truppe Freccia, i velivoli a pilotaggio remoto (Remotely Piloted Aerial Systems, RPAS) e i veicoli terrestri senza pilota utilizzati sia per attacco che ricognizione (Unmanned Gound Vehicles, UGV), il Veicolo Tattico Leggero Multiruolo (VTLM) "Lince" e il Veicolo Tattico Medio Multiruolo (VTMM)"Orso".

3.3 Il programma Forza NEC e i suoi aspetti industriali

3.3.1 Il programma Forza NEC

Forza NEC è un programma complesso poiché riguarda la digitalizzazione di veicoli, piattaforme dotate di sistema di armamento, equipaggiamenti del soldato, sistemi informatici, e quelli di telecomunicazioni. Da qui la necessità che più industrie specializzate siano parte del progetto. Data la

[68] Uno degli aspetti più importanti del programma riguarda la definizione del "carico" delle differenti configurazioni, determinato dalle componenti aggiuntive che può portare un singolo soldato: radio, visore notturno, minicomputer, relativi cavi e batterie. L'insieme della componente "elettronica" della dotazione pesa 4-5 kg, ovvero circa il 15% del carico che può mediamente sostenere un soldato, che dovrebbe corrispondere – in configurazione massima – ad un terzo del suo peso corporeo. Sebbene la gran parte del peso dipenda invece da protezioni balistiche, razioni, arma e munizioni, anche la componente elettronica dovrebbe tendere verso la massima leggerezza consentita per favorire la mobilità del singolo. Inoltre, unità come le forze speciali disporranno di configurazioni parzialmente diverse, ad esempio con maggiori strumenti per l'identificazione del bersaglio.

natura di Forza NEC, che prevede l'integrazione di vari assetti e piattaforme in un'unica rete digitale, fare affidamento su più industrie che operano "slegate" fra di loro significherebbe rischiare di generare un processo inefficiente, e nel caso più probabile assetti che alla fine del programma non sarebbero in grado di connettersi e comunicare efficacemente fra di loro. Un assetto industriale di aziende che operano in completa autonomia creerebbe inoltre ulteriori insidie a livello amministrativo-contabile, con la Difesa chiamata a stipulare tanti contratti quanti sono i fornitori. Per mitigare questi rischi, il programma Forza NEC ha introdotto un'interessante novità, unendo in un'unica entità – la società Finmeccanica-SES – le figure del "system integrator" e del "prime contractor". In quanto "system integrator", Finmeccanica-SES è incaricata di assicurare l'integrazione delle componenti prodotte dalle altre industrie coinvolte nel programma, svincolando dunque la Difesa da questo compito, ed evitando che complicazioni di natura tecnica dovute all'assemblaggio delle varie parti possano impedire la funzionalità della rete netcentrica. Lo scopo del "system integrator" è quindi quello di assicurare lo sviluppo coerente di un "sistema di sistemi", ovvero un'architettura onnicomprensiva che integri sistemi di C2, piattaforme e sensori. Oltre a ciò, Finmeccanica-SES è anche il "prime contractor", sostanzialmente l'unico interlocutore con il quale la Difesa si interfaccia a livello economico-amministrativo, e che svolge la funzione di coordinatore fra le altre aziende all'interno del raggruppamento. La Difesa può quindi interagire con una sola entità – piuttosto che tante e diversificate – con chiari benefici in termini di linearità del processo gestionale.

Tabella 1. Imprese coinvolte nel programma Forza NEC e loro competenza

Impresa	Competenza
Finmeccanica SES (Prime Contractor)	Architettura, sistemistica, sistema C2, sistemi di navigazione, sensoristica, UAV, sistemi di comunicazione e sicurezza
MBDA Italia	Sottosistema artiglieria contraerea
Oto Melara	Sistemi di digitalizzazione veicolare e di C2 e navigazione, UGV
AgustaWestland	Integrazione piattaforme aeromobili
Elettronica	Sistemi di guerra elettronica
Iveco DV	Sistemi di digitalizzazione veicolare e di C2 e navigazione
Engineering	Sistemi di data fusion
CIO, Consorzio Iveco-Oto Melara	Sistemi di digitalizzazione veicolare, C2 e navigazione
RTI "Soldato Futuro" (Finmeccanica SES, Beretta, Sistemi Compositi, Areosekur)	Sistema "Soldato futuro"

Forza NEC è un programma innovativo anche per la sua struttura di governance e per i principi di management che si è scelto di adottare nell'ambito prettamente militare. L'organizzazione di governance ha subito durante il suo corso delle variazioni a dimostrazione della sua estrema complessità. Ad oggi la governance di Forza NEC prevede[69]:

- Il Comitato Direttivo, presieduto dal Comandante Logistico dell'EI, su delega del Capo di Stato Maggiore dell'Esercito (SME), che riporta gli esiti degli sviluppi del programma direttamente al Capo di SMD. Ne fanno parte i Capi Reparto dello SMD, i capi dei III Reparti di F.A. e il Segreteriato Generale della Difesa/Direzione Nazionale degli Armamenti (SEGREDIFESA/DNA), attraverso il Direttore di Programma Forza NEC. Il Comitato Direttivo ha il compito di fornire le linee guida strategiche inerenti allo sviluppo del programma e di verificare il conseguimento degli obbiettivi sulla base delle indicazioni fornite dal Capo di SMD;
- Il Project Office, presieduto dal Capo Dipartimento per la Trasformazione Terrestre, si concentra sugli aspetti tecnico-esecutivi di medio profilo del programma. Grazie ad incontri periodici, il Project Office verifica la coerenza tecnico-capacitiva del programma ed elabora le proposte dei programmi da sviluppare in relazione allo stato di maturità tecnologica dichiarato dall'industria.

Per quel che riguarda gli aspetti di management, si è scelto di seguire tre principi di base[70]. In primo luogo, il cosiddetto "approccio capacitivo". Già assunto a livello NATO, presuppone l'identificazione dei vari assetti in relazione a specifiche esigenze d'impiego. Ciò presuppone, quindi, che un sistema di procurement preveda di arrivare all'identificazione dei mezzi e dei sistemi d'arma che siano in grado di svolgere determinate funzioni in base alle esigenze operative passate, ma anche agli scenari d'impiego futuri. Secondariamente, il principio "transforming while operating", ovvero di trasformazione mentre si sta operando: prevede che i sistemi ammodernati debbano essere perfettamente interoperabili con i sistemi non ancora digitalizzati. Infine, il principio cardine di Forza NEC, "evolution throughout production", cioè "evoluzione durante la produzione". Esso si basa su forme flessibili di approvvigionamento tali da poter tenere costantemente aggiornati i sistemi e le piattaforme ai repentini cambia-

[69] Intervista, 28 gennaio 2014.

[70] Michele Nones e Marrone Alessandro (a cura di), *La trasformazione delle Forze Armate*, cit., pp. 76-78.

menti della tecnologia. In questo senso, i sistemi da ammodernare sono configurati con una "architettura aperta", cioè la loro struttura è concepita in maniera tale da poter essere ulteriormente aggiornata in futuro. In breve, la tecnologia netcentrica dovrebbe permettere che le varie piattaforme vengano riconfigurate con l'avanzare della tecnologia.

3.3.2 Tempistica e costi del programma Forza NEC

Inizialmente la durata prevista del programma era stata stimata in 25 anni, dal 2007 al 2031. Tuttavia la natura stessa dei finanziamenti, che ha visto l'approvazione degli stanziamenti solo per la cosiddetta fase di Concept Development & Experimentation (CD&E), unita ad una serie di complicazioni di natura tecnico-tecnologica hanno successivamente condizionato in maniera significativa lo sviluppo e l'attuazione del programma. Originariamente le tempistiche di Forza NEC erano state così articolate[71]:

1. Studio di fattibilità (2007);
2. Fase di Project Definition (PD), (2007-2010);
3. Fase di CD&E, (2010-2013);
4. Prima fase di implementazione (entro il 2018): la digitalizzazione della prima Brigata, della Landing Force Digitalizzata (LFD) e del 50% degli enablers; il completamento dell'Integration Test Bed (ITB) e la fase di sperimentazione tramite Modeling and Simulation (M&S);
5. Seconda fase di implementazione (entro il 2026): la digitalizzazione della seconda Brigata Integrata Terrestre (BIT) e del 25% degli enablers;
6. Terza fase di implementazione (entro il 2031): la digitalizzazione della terza BIT e dell'ultimo quarto (25%) di enablers.

Ad oggi invece le varie fasi del programma possono essere così schematizzate[72]:

7. Studio di fattibilità (2008);
8. PD (2009);
9. CD&E (2010-2020)[73].

[71] Ibid., pp. 69-70.

[72] Intervista, 4 febbraio 2015.

[73] Ad oggi questa rappresenta la stima più attendibile circa la fine della fase di CD&E. Sebbene da un punto di vista finanziario (la stipula dei contratti) tale fase si potrebbe chiudere già nel 2018, da un punto di vista pratico, la produzione e sperimentazione di

Dopo lo studio di fattibilità di Forza NEC, in cui si sono gettate le basi concettuali per la realizzazione del programma, è iniziata la fase di PD con l'obiettivo di: selezionare le unità da digitalizzare e le relative modalità di trasformazione in senso netcentrico; preparare la documentazione per l'avvio della fase di CD&E e, in ultimo, consolidare la documentazione finora prodotta.

Contrariamente a quello che accade in programmi di procurement classici, tra la fase di PD e la produzione è stata inserita la fase di CD&E, la fase in cui si trova attualmente il programma. Data la presumibile complessità del programma, si è preferito inserire questa fase con l'obiettivo di mitigare i rischi di una eventuale produzione di sistemi tecnologicamente non ancora accertati e collaudati, mediante realizzazione e test di un'architettura completa NEC su scala ridotta. Lo scopo primario della CD&E è dunque di effettuare una serie di test per valutare attentamente quelle tecnologie che saranno alla base della digitalizzazione dell'Esercito. In altre parole, la fase di CD&E mira a fornire le capacità necessarie per "testare e validare l'architettura della forza digitalizzata attraverso la realizzazione su piccola scala di tutti i principali elementi componenti l'architettura NEC"[74]. Questa fase si è resa in qualche modo necessaria per le caratteristiche stesse del programma che deve digitalizzare assetti vetusti e integrarli con quelli di nuova generazione e per i quali è già stato avviato il processo di digitalizzazione. Esercito e Industria hanno collaborato fin dall'inizio del programma con la convinzione che la fase di CD&E fosse funzionale anche per realizzare sistemi che poi sarebbero stati "validati" in teatro. In sostanza con la CD&E si punta a realizzare cinque macro capacità:

1. C2 digitale: posto comando di Task Force (Brigata) di una forza media digitalizzata comprensiva di Comando Controllo e Navigazione (Command Control and Navigation-C2N)/BFSA su piattaforma VTLM; C2N di terza dimensione (3D) sviluppo e aggiornamento di SIACCON e SICCONA;
2. Sensori: micro e mini RPAS, UGV in differenti configurazioni; sistemi per la guerra elettronica, Force Protection e Reconnaissance Surveillance and Target Acquisition (RSTA);
3. Attuatori: sviluppo di sistemi per la parte Soldato Futuro;
4. Comunication e Information Systems (CIS): realizzazione di apparati per la trasmissione di dati tattici e cifranti; sistemi satellitari di

assetti e piattaforme stipulati dovrebbe protrarsi per almeno due anni.

[74] Intervista, 28 gennaio 2014.

nuova generazione; gateway[75] per connessioni bidirezionali di rete di computer di diversa classifica e per la LFD; e infine le Software Defined Radio (SDR)[76] e il sistema Battlefield Target Identification Device (BTID)[77];

5. Integration Test Bed (ITB): l'ITB è la realizzazione pratica – o meglio fisica – del M&S, inteso come l'insieme di attività che cercano di replicare fedelmente in un ambiente sintetico (virtuale) gli scenari e le caratteristiche delle unità, dei mezzi e dei sistemi d'arma con capacità netcentriche. In pratica, l'ITB è una infostruttura, composta da hardware, software e fabbricati – collegata con altri ITB – che permette di testare tutti gli elementi della tecnologia netcentrica. I vari ambienti virtuali, costituiti all'interno di siti collegati fra di loro, impiegheranno una serie di strumenti, detti tool di simulazione, per garantire la comunicazione tra i centri e con network analoghi. Data la natura interforze del programma, queste infostrutture non sono costituite esclusivamente in seno all'Esercito, ma anche presso la Marina e l'Aeronautica. Nondimeno, essendo l'Esercito l'attore principale del programma, l'ITB "centrale" è il Centro di Simulazione e Valutazione dell'Esercito (Ce.Si.Va.). Il Ce.Si.Va. e gli altri ITB di Aeronautica e Marina sono quindi connessi fra loro per testare la tecnologia netcentrica e consentire lo scambio costante di dati. L'ITB comporterà dei cambiamenti non solo nella fase di sperimentazione della tecnologia netcentrica, ma anche nella fase di addestramento con la possibilità di unire all'approccio reale anche l'aspetto virtuale, con sistemi e persone simulati. L'ITB ha permesso una significativa riduzione del rischio generale del programma, ed ha introdotto una nuova modalità di lavoro che ha affiancato personale dell'industria e dell'Amministrazione Difesa (AD), modalità rivelatasi vincente in un contesto di continua evoluzione tecnologica e dei requisiti operativi dell'Esercito. L'effetto immediato è stato quello di garantire un'interazione maggiore fra le due parti e quindi uno sviluppo della tecnologia realistico rispetto alle vere esigenze operative. Detto ciò, ad oggi il sistema M&S può verosimilmente essere considerato uno degli elementi di successo del programma,

[75] Nel linguaggio delle telecomunicazioni un gateway è il nodo di una rete utilizzato per far comunicare tra loro reti che usano diversi protocolli.

[76] Sistema di comunicazioni radio i cui componenti vengono aggiornati tramite software piuttosto che hardware.

[77] Sistema di identificazione amico/nemico.

da tenere in considerazione per programmi futuri, in particolare quando sarà necessaria la sperimentazione di strumenti, assetti e piattaforme pre-serie e tecnologie emergenti[78].

In conclusione si può affermare che lo sviluppo e la sperimentazione condotti nell'ambito della CD&E di Forza NEC permettono di:

- dotare mezzi legacy (es. Centauro, Dardo, Ariete) di nuove capacità net-centriche grazie alle quali collegare questi stessi mezzi alla "rete";
- aggiornare e garantire l'evoluzione di componenti dei mezzi di nuova introduzione ma già in linea di produzione (es. VBM Freccia);
- concepire le configurazioni dei futuri mezzi e sistemi (Nuova Centauro, VTLM 2, VTMM, ecc.) con un design già net-centrico.

Ciò nonostante, la natura stessa della fase CD&E – sperimentazione e sviluppo concetti – ha comportato alcune problematiche da un punto di vista amministrativo e tecnico che hanno prodotto un allungamento dei tempi del programma, giudicato però prevedibile sia dalla Difesa che dalla controparte industriale. Per questo motivo la sua fine è oggi fissata indicativamente al 2020[79].

In primis, alcune procedure amministrativo/burocratiche, volte al controllo della piena corrispondenza dei prototipi ai requisiti operativi iniziali dell'Esercito, non hanno permesso di arrivare in tempi rapidi alla sperimentazione dei prototipi come in altri programmi di procurement[80]. La natura stessa di una fase concepita per lo sviluppo di strumenti e la loro sperimentazione ha implicato quasi inevitabilmente una dilatazione dei tempi, soprattutto nel momento in cui un oggetto o un sistema, che prima era stato concepito solo "su carta", avrebbe dovuto rispettare alcuni standard ben definiti prima di essere testato sul terreno. Senza dimenticare, tra l'altro, dell'integrazione sotto l'ombrello di Forza NEC di una serie di programmi e contratti già avviati, che ha generato un numero complessivo di obblighi contrattuali intermedi – le cosiddette "milestones" – molto elevato[81]. Inoltre, i principi stessi di management su cui si basa il programma, "transforming while operating" e "evolution through production" sono talvolta risultati in una sovrapposizione di fasi di stu-

[78] Intervista, 10 febbraio, 2015.

[79] Ibid.

[80] Intervista, 4 febbraio 2015.

[81] Ibid.

dio, sperimentazione e valutazione, e quindi in cambiamenti del requisito operativo iniziale, che hanno portato nei fatti ad un inevitabile rallentamento della fase di CD&E. In particolar modo, il principio "evolution through production" – per cui da contratto dovrebbe essere possibile cambiare "in corso d'opera" i requisiti operativi a cui dovrebbero rispondere gli strumenti, assetti e piattaforme – sembra aver sollecitato non poco i ritmi e le procedure della filiera industriale[82]. Questo per via degli adeguamenti di apposite TTP e SOP avvenute in teatro e per il ritmo con cui si sono susseguiti cambiamenti e sviluppi della tecnologia in ambito militare, che in qualche modo dovevano essere integrati nelle produzioni pre-serie.

Ai limiti di carattere amministrativo burocratico si sono unite delle ragioni di natura tecnico-operativa. In alcuni casi si sono notati dei limiti strutturali di carattere fisico/tecnologico che non hanno permesso l'evoluzione sperata dei prototipi. Un esempio è dato dalle piattaforme VTLM e VTMM, la cui digitalizzazione comporterebbe un aumento dei pesi e degli apparati installati a bordo molto maggiore di quello che in realtà queste piattaforme possono sostenere[83]. Similmente, i primi prototipi di mini RPAS si sono dimostrati resistenti, ma allo stesso tempo troppo grandi e pesanti. In altre occasioni le soluzioni tecnologiche proposte non sono risultate completamente in linea con i requisiti operativi richiesti dalle forze armate, mentre in altre la tempistica dello sviluppo sembra abbia impedito di offrire soluzioni immediate in grado di essere sperimentate in tempi contenuti. In generale, si può affermare che si siano verificati i tipici problemi del passaggio da un requisito astratto ad una soluzione realizzativa concreta, i quali hanno richiesto cambiamenti in corso d'opera per passare dalla teoria alla pratica. La generazione del software di C2, ad esempio, ha evidenziato le criticità di cui sopra, quando per ragioni commerciali Microsoft ha deciso di passare dal sistema operativo Windows XP a Windows 7, rendendo di fatto il software di C2 sino ad allora sviluppato e strutturato non più supportabile – in termini di sicurezza – dalla casa produttrice[84]. Anche in tale ottica e per prevenire situazioni simili nel futuro, SELEX-ES ha stipulato un accordo quadro con Microsoft per avere indicazioni tempestive sulle linee di sviluppo tecnologico del software.

[82] Ibid.

[83] Intervista, 10 febbraio 2015.

[84] Ibid.

Dall'altra parte, invece, due note positive della fase di CD&E si sono registrate nel rapporto venutosi a creare fra l'Industria e la Difesa e nell'identificazione di un primo insieme di sistemi e strumenti maturi per un'eventuale loro produzione.

Per quel che riguarda la prima, il rapporto Difesa-Industria ha permesso un proficuo scambio di informazioni fra le parti sul campo e nelle attività di sperimentazione condotte dalla brigata Pinerolo in Italia. Nel complesso, sin dagli albori del programma vi è stato un flusso costante di informazioni al fine di comprenderne gli ostacoli principali che ha giovato sia alle parti che allo sviluppo del programma stesso. A titolo di esempio, l'adozione da parte dell'Industria della nuova metodologia Agile Scrum, che prevede lo sviluppo di un software secondo una modalità iterativa ed incrementale con il diretto coinvolgimento dell'Esercito, il. c.d. "customer in the loop", ha consentito di ridurre in maniera drastica le possibilità di fallimento nello sviluppo di alcuni prototipi pre-serie.

Grazie agli ultimi sviluppi di prototipi e sistemi di pre-serie, la fase di CD&E ha già permesso di identificare quelle capacità e quei sistemi abbastanza maturi per una eventuale produzione di serie, fermo restando che il livello di maturità complessivo delle capacità – inteso come abilità di tutti i nodi di interconnettersi e scambiare informazioni – potrà essere verificato solamente una volta portata a termine la CD&E. Nel merito, possono oramai ritenersi consolidati la maggior parte delle componenti costituenti, ovvero il sistema Soldato Futuro, il SICCONA, le cifranti dual stack IPv4/v6 e i Posti Comando (PC) digitalizzati[85]. Con un ragionevole grado di confidenza, si può prevedere che nel breve termine potranno essere considerati maturi anche alcuni sistemi sensoriali (UAV, UGV e RSTA), e nel corso del 2015 altre componenti del sistema C2 digitalizzato, come il PC di artiglieria digitalizzato e il sistema LOGBOX per il supporto logistico integrato, nonché alcune importanti CIS – su tutti il Satcom On-The-Move (SOTM), il Gateway LFD e gli apparati radio SDR[86]. Per ottenere un primo apprezzamento generale di quelle che possano essere le potenzialità della nuova tecnologia, alcuni dei prodotti della fase di CD&E sono stati testati con la partecipazione italiana all'esercitazione NATO Joint Eagle – Eagle Joker, che ha visto l'interazione di mezzi terrestri, RPAS e uni-

[85] Nel linguaggio delle telecomunicazioni e dell'informatica il Dual Stack permette il passaggio dal protocollo di versione 4 a quello più moderno versione 6 nella rete globale Internet.

[86] Intervista, 12 settembre 2014.

tà meccanizzate in ambito interforze e multinazionale[87]. Inoltre, alcune delle capacità ritenute mature verranno schierate in Spagna durante l'esercitazione Trident Juncture nel settembre 2015, nel quadro dalla NATO Connected Force Initiative (CFI), per testare in ambito multinazionale alcune capacità del programma finora sviluppate[88].

Nel 2006 il costo totale del programma Forza NEC era stato stimato dal comparto industriale attorno ai 22 miliardi di euro[89]. Tale stima era da considerarsi puramente indicativa perché antecedente alla fase stessa di CD&E, e quindi volta a definire l'ordine di grandezza economica dell'intero programma di ammodernamento. In seguito, l'evoluzione peculiare di Forza NEC ha portato a superare un simile approccio, per tre motivi. In primo luogo, il fatto che alcune tecnologie sviluppate e testate nella CD&E siano utilizzate in programmi di procurement già in corso e con un loro proprio finanziamento. In secondo luogo, l'avvio di programmi "spin off" finanziariamente autonomi per acquisire le soluzioni tecnologiche maturate in Forza NEC. Infine, l'obiettivo di utilizzare i risultati della CD&E per influenzare in senso netcentrico l'ammodernamento complessivo dell'EI. L'insieme di questi elementi cambia il modo stesso di stimare il costo della produzione di assetti digitali o dell'ammodernamento netcentrico dell'asset legacy in vario modo frutto di Forza NEC – tanto più che la fase di CD&E è ancora in corso. Ad oggi, il costo complessivo del programma Forza NEC per le finanze pubbliche ammonta quindi a 815 milioni di euro, considerando i 15 milioni per la fase di PD e i circa 800 milioni per la fase di CD&E[90].

Dati i risvolti tecnologici e di ricerca in chiave industriale, i costi del programma sinora sostenuti sono ricaduti quasi esclusivamente (tranne i 15 milioni per la PD) sul Ministero dello Sviluppo Economico (MiSE), che ha finanziato l'intero investimento della fase di CD&E[91]. L'intervento del MiSE, giudicato fondamentale in ragione dell'elevato contenuto tecnologico dell'impresa e del coinvolgimento dell'industria nazionale, ha consentito da un lato di non gravare ulteriormente sul già esiguo bilancio ordinario della difesa e dall'altro di permettere al comparto industriale

[87] Intervista, 4 febbraio 2015.

[88] Intervista, 10 febbraio 2015.

[89] Michele Nones e Alessandro Marrone (a cura di), *La trasformazione delle Forze Armate*, cit., pp. 69-70.

[90] I costi dello studio di fattibilità sono stati sostenuti dalla sola industria.

[91] Degli 800 milioni previsti finora per la fase di CD&E solo 554 sono stati effettivamente finanziati. Intervista, 10 febbraio 2015.

nazionale di investire in ricerca e sviluppo[92]. I finanziamenti del MiSE hanno ricoperto i costi non ricorrenti legati alle attività di ricerca e sviluppo dei nuovi sistemi; pertanto, in un eventuale fase di produzione in serie delle capacità finora sviluppate, essa sarà esente da tali costi e comprenderà solo quelli ricorrenti, ovvero i costi legati alla mera produzione dei sistemi e degli assetti validati.

3.4 Le prospettive di Forza NEC: sfide e opportunità

Come ipotizzabile il programma Forza NEC presenta molte sfide che, se affrontate positivamente, possono tramutarsi in opportunità da sfruttare sia in questo che in futuri programmi di procurement. Fra queste sfide/opportunità le maggiori sono:

1. produzione degli assetti frutto della CD&E;
2. formazione e addestramento delle forze armate;
3. asset legacy;
4. interoperabilità interforze;
5. gestione dei dati in teatro;
6. sicurezza cibernetica.

Produzione degli assetti frutto della CD&E. La produzione degli assetti frutto della CD&E rappresenta la vera incognita del programma per via delle importanti decisioni che si dovranno assumere rispetto alla produzione – e quindi all'acquisto – dei sistemi, assetti e piattaforme sviluppati da Forza NEC entro il 2020. Le risorse limitate di cui dispone attualmente la Difesa impediscono di poter pianificare con estrema certezza in che modalità, e in quali quantità, si passerà dallo sviluppo e produzione di modelli pre-serie alla fase di produzione di modelli in serie di determinati assetti. Ciononostante, da un punto di vista operativo, ma anche finanziario e industriale, appare evidente quanto sia necessario dare seguito alla fase di ricerca e sperimentazione con un piano di industrializzazione, per soddisfare le esigenze delle forze armate e non rendere la fase di CD&E un esercizio fine a se stesso[93].

L'acquisizione di quanto sviluppato e testato nel corso della CD&E andrà inquadrata nel piano complessivo di ammodernamento dello stru-

[92] Intervista, 18 marzo 2015.

[93] Intervista, 10 febbraio 2015.

mento militare, attraverso nuove produzioni e l'adeguamento alla tecnologia netcentrica degli assetti "legacy" (si veda sezione successiva). Un obiettivo minimo potrebbe essere rappresentato dall'acquisizione solamente di quei prodotti considerati abbastanza maturi per poter far fronte alle esigenze minime delle forze armate, in pratica solo quei sistemi, assetti e piattaforme che vengono ritenuti indispensabili per rispondere alle esigenze operative essenziali. Un risultato a cui forse si dovrebbe puntare, invece, sarebbe la graduale digitalizzazione dell'Esercito attraverso la produzione di "pacchetti completi" a livello di brigata, che includano comando e controllo digitali, sistemi attuatori e sensori, piattaforme e mezzi, equipaggiamento del soldato. Come accennato in precedenza, ciò dovrebbe comportare il congelamento dei requisiti e delle relative soluzioni tecnologiche raggiunte nella fase di CD&E, la produzione di lotti sufficientemente grandi di assetti per equipaggiare una brigata, che includano, ad esempio, kit per il soldato appiedato o veicoli da trasporto. Nel frattempo, la campagna di sperimentazione e validazione dovrebbe continuare, ad un costo inferiore rispetto a quello dell'attuale CD&E, perché si concentrerebbe solo sulle aree dove maggiore è l'innovazione tecnologica in corso, poggiando comunque sul lavoro svolto in precedenza, per preparare i successivi lotti ad un livello tecnologico più avanzato. In questo modo si potrebbe conciliare, da un lato, la necessità di acquisire assetti al passo con l'innovazione tecnologica in campo ICT, e dall'altro, quella di portare l'attività di CD&E a tradursi in una produzione in serie di dimensioni adeguate. Questo consentirebbe di fornire all'EI gli assetti necessari e all'industria un ritorno adeguato dell'investimento. In futuro sarebbe quindi opportuno che siano "congelati" dei requisiti di base per un periodo iniziale deciso fra le parti in fase di negoziazione, evitando così che i requisiti operativi cambino in fase di sperimentazione e validazione[94].

Poiché i costi esatti della produzione si rivelerebbero unicamente agli albori della fase successiva alla CD&E, prima di procedere all'acquisto si dovrà necessariamente tener conto della delicata situazione economica in cui si trova l'Italia, ma anche dell'importanza di fornire all'Esercito gli strumenti per poter operare e gli impegni presi in ambito NATO. Al di là quindi di dover dotare i soldati italiani degli strumenti necessari per poter operare in ambienti ostili, non ci si potrà nemmeno dimenticare degli impegni minimi di spesa ribaditi da Roma (e dagli altri Paesi alleati) nel vertice NATO del 2014 – ovvero di arrivare a spendere il 2% del PIL per

[94] Intervista, 4 febbraio 2015.

la difesa entro il 2024 – ed il gap pregresso di risorse destinate alla difesa rispetto agli altri grandi Paesi europei[95]. In pratica, sarà necessario senza dubbio considerare le limitate possibilità economiche mentre si discuterà su quello di cui si intende dotare l'EI, ma anche ricordarsi del deterioramento delle condizioni di sicurezza regionali e di far parte di un'Alleanza la cui efficacia è sottesa anche dalla natura, e quantità, dell'investimento per la difesa a livello di Paesi membri.

Formazione e addestramento delle forze armate. La digitalizzazione dell'EI e la sfida netcentrica coinvolgono l'organizzazione dell'Esercito in tutte le sue parti, e questo non esclusivamente da un punto di vista di scelte legate all'acquisto di nuove tecnologie, ma anche riguardo a modifiche sostanziali nella formazione e nell'addestramento del personale[96]. La tecnologia – e in particolar modo gli strumenti digitalizzati – permettono di ottenere informazioni che necessitano di una capacità decisionale individuale rapida e pensiero critico. La formazione militare dovrà quindi continuare ad essere rigorosa, articolata su esercitazioni realistiche e complesse, in grado di addestrare i comandanti ai vari livelli a decidere e operare in condizioni e situazioni il più possibile realistiche ed in linea con gli eventi dei teatri[97]. La formazione dovrà essere tale da insegnare la gestione di grosse quantità di informazioni, e la gestione dello stress che spesso si concretizza di fronte a dilemmi che riguardano anche la sfera emotiva. L'addestramento dovrà per forza di cose riprodurre nella maniera più realistica possibile gli scenari di impiego più probabili e preparare il soldato ad affrontate le complesse minacce future, anche considerando il venire meno dell'impegno in un teatro operativo come quello afgano. In quest'ottica, il Sistema Integrato di Addestramento Terrestre (SIAT) ha un grande potenziale di sinergie con l'ITB, per assicurare un adeguato training dell'EI rispetto alla tecnologia netcentrica[98].

[95] Nel 2012 l'Italia spendeva lo 0,87% del PIL per la "funzione difesa" rispetto al 2,08% inglese, 1,49% francese, e 1,2% tedesco. Alessandro Marrone, Paola Sartori, Alessandro R. Ungaro, *Bilanci e industria della difesa: tabelle e grafici*, luglio 2014, http://www.iai.it/it/node/702.

[96] Intervista, 10 febbraio 2015.

[97] Ibid.

[98] Per un'analisi approfondita sul training delle forze armate italiane si veda: Alessandro Ungaro, Alessandro Marrone e Michele Nones, "Sfide e opportunità dell'innovazione tecnologica nell'addestramento delle Forze armate italiane", in *Documenti IAI*, n. 15|02, gennaio 2015, http://www.iai.it/it/node/3247.

Asset legacy. Forza NEC pone delle problematicità legate ad alcune questioni "strutturali" del programma stesso, quali la notevole durata e la complessità tecnologica del processo di digitalizzazione. In termini procedurali, per rendere netcentrici i mezzi e i sistemi dell'EI si è deciso di aggiornare alcuni dei mezzi attualmente a disposizione dell'EI, la cosiddetta "asset legacy", agli standard netcentrici, in attesa che questi siano successivamente sostituiti da nuovi assetti che incorporino sin dalla fase di design la tecnologia netecentrica[99]. In pratica, si è optato per digitalizzare quanto è stato acquisito dalle forze armate prima di Forza NEC e adattarlo alla nuova architettura netcentrica, in attesa di essere sostituito attraverso future acquisizioni. Questo procedimento porterà ad una implementazione graduale della netcentricità, ossia in fasi differenti, e non in un'unica tranche, così come definito all'epoca dal "Concetto Operativo 2010-2030 dell'Esercito" e dal "Piano di Ammodernamento 2013-2030". Questo processo è stato adottato anche alla luce delle esperienze maturate da altri Paesi che prima dell'Italia si sono incamminati sulla strada NEC, come gli Stati Uniti, dove gli altissimi costi di programmi eccessivamente ambiziosi come il Future Combat System (FCS) hanno costretto il Pentagono a rivedere il programma in chiave riduttiva e a virate su progetti più fattibili ed inseriti poi nel Army Brigade Combat Team Program[100]. Di conseguenza, nella fase di CD&E di Forza NEC saranno presenti all'interno dell'EI sia sistemi aggiornati che verranno poi sostituiti alla fine del loro ciclo di vita operativo, sia nuovi sistemi con tecnologie netcentriche già incluse[101]. Almeno nell'attuale fase di CD&E, la questione dell'asset legacy non sembra preoccupare eccessivamente il comparto industriale proprio per l'intenso processo di prototipizzazione verso la tecnologia netcentrica che i principali strumenti, assetti e piattaforme hanno subito in precedenza e che sembra permetterà agli assetti legacy di reggere il confronto con le nuove acquisizioni fino al momento della loro sostituzione[102].

Qualche timore in più desta la gestione dell'obsolescenza dei nuovi sistemi portati alla luce dell'attuale CD&E, data la rapidità con cui successive innovazioni tecnologiche renderanno non più allo stato dell'arte sistemi che comunque sono stati prodotti relativamente di recente. Per ovviare al problema, durante la fase di sperimentazione e prototipazione

[99] Michele Nones e Alessandro Marrone (a cura di), *La trasformazione delle Forze Armate*, cit., pp. 66-67.

[100] Ibid.

[101] Ibid, pp. 76-78.

[102] Intervista, 4 febbraio 2015.

i sistemi dovrebbero essere configurati secondo una "architettura aperta", in grado cioè di recepire le repentine evoluzioni tecnologiche derivanti dallo sviluppo del mondo ICT[103]. Per quanto riguarda l'hardware ciò include anche, ad esempio, la progettazione delle piattaforme lasciando lo spazio fisico, la capacità di carico e di alimentazione elettrica per ulteriori sistemi elettronici, che potrebbero venire sviluppati e aggiunti nei suoi 30-40 anni di vita. Se si rispettasse il principio del "evolution throughout production" si riuscirebbe a fare in modo che strumenti, assetti e piattaforme che si stanno sperimentando attualmente non siano poi da sostituire integralmente con il sopraggiungere di nuove evoluzioni tecnologiche, come può essere il passaggio da un sistema operativo all'altro. Da questo punto di vista, appare verosimile che per far fronte alla costante innovazione tecnologica sarà necessaria in futuro una fase di sperimentazione continua che permetta di verificare preventivamente la fattibilità tecnica della resa netcentrica di apparati che hanno subito differenti processi di digitalizzazione[104]. In tale contesto, è presumibile che un ruolo importante sarà assunto da "lotti di integrazione" in grado di "livellare" le tecnologie dei differenti strumenti, assetti e piattaforme e di avere, grazie anche agli strumenti resi disponibili dall'ITB, una continua "Campagna di Sperimentazione e Validazione delle Capacità" acquisite dall'evoluzione di Forza NEC[105].

Interoperabilità interforze multinazionale. Un'altra sfida di carattere tecnico è rappresentata dalla necessità di garantire l'interoperabilità fra le forze armate italiane alla fine del processo di digitalizzazione dell'Esercito, ovvero che le piattaforme e gli assetti utilizzati da quest'ultimo, dalla Marina e dall'Aeronautica siano messi nelle condizioni di comunicare e interagire fra di loro e con quelli di altri stati. Questo non è un compito facile visto che le diverse forze armate utilizzano non solo differenti strumenti, ma anche diversi sistemi C2. Ad esempio, la Marina dispone di due diversi sistemi di C2, uno a livello strategico (Maritime Command and Control Information System, MCCIS) e uno a livello tattico (Command and Control Personal Computer, C2PC), mentre l'Esercito utilizza il SIACCON ed il SICCONA. Il contesto netcentrico presuppone che i vari sistemi C2 interagiscano fra di loro, consentendo il passaggio delle informazioni da

[103] Intervista, 10 febbraio 2015.

[104] Ibid.

[105] Ibid.

un punto all'altro della rete, sia esso una nave o un soldato in missione. Il design e lo sviluppo dell'architettura netcentrica ha prefigurato la definizione di componenti specifici con il fine di supportare l'interoperabilità fra forze armate nazionali ed internazionali: a livello strategico interforze l'interoperabilità è garantita attraverso il collegamento del SIACCON con il Command, Control, Intelligence (C2I) della Difesa; a livello tattico, invece, l'interoperabilità con la Marina è garantita con la messaggistica VMF e in futuro con Gateway della Landing Force Digitalizzata (GTWL-FD) che dovrebbe garantire la piena interoperabilità fra i vari sistemi di C2 (SIACCON-MCCIS e SICCONA-C2PC)[106]. Con l'Aeronautica si otterrà una maggiore comunicazione attraverso l'adozione del cosiddetto CID Server (Combat Identification Server), un sistema in grado di integrare e collezionare dati sulle coordinate di truppe amiche sul terreno[107]. A sua volta il CID server potrà essere interrogato dal sistema di comunicazioni a livello tattico dell'Aeronautica, il Link 16, il quale permette alle unità in teatro di diverse forze armate di scambiarsi dati in tempo reale.

In ambito NATO, l'interoperabilità a livello strategico-operativo è assicurata dal MIP, un programma multinazionale finalizzato alla definizione di uno standard comune per lo scambio dati tra diversi sistemi di C2, costantemente verificato durante esercitazioni interforze in ambito internazionale e meeting periodici che periodicamente si incontrano per la standardizzazione di tecniche e procedure.

Gestione dei dati in teatro. La possibilità di mettere in rete e far comunicare fra di loro una quantità ingente di nodi costituisce un'altra importante problematica da affrontare. Questo problema è intrinseco al programma stesso, che mira a connettere in uno spazio virtuale migliaia di elementi. Una situazione molto diversa da Marina e Aeronautica che, oltre ad aver avviato un processo di digitalizzazione da più tempo rispetto all'Esercito, devono al massimo connettere alcune centinaia di navi o velivoli. Di fatto, le flotte navali sono collegate già tempo via data link, mentre l'Aeronautica già compie operazioni utilizzando a pieno il sistema di scambio dati Link-16[108], in linea con gli standard NATO. L'Esercito deve quindi affrontare un doppio problema: da una parte partire da un livello di digitalizzazione più basso rispetto alle altre due forze armate, dall'altra rendere

[106] Intervista, 4 febbraio 2015.

[107] Intervista, 18 marzo 2015.

[108] Michele Nones e Alessandro Marrone (a cura di), *La trasformazione delle Forze Armate*, cit., pp. 50-51.

netcentrici una quantità di elementi di molto superiore rispetto a Marina e Aeronautica[109]. Affrontata l'incognita della messa in rete di migliaia di sensori, si pone l'ulteriore quesito di come elaborare l'ingente quantità di dati che da essi giungeranno. È sicuramente vero che maggiore è la raccolta di informazioni, maggiore sarà anche la possibilità di raggiungere l'Information Superiority. Ma bisogna ricordare che una grande quantità di dati necessita di una capacità di calcolo ed elaborazione che permetta una fruizione effettiva di tutte le informazioni raccolte. Per questo tavoli ad hoc con la presenza di tecnici della Difesa e dell'industria stanno lavorando a soluzioni specifiche per ovviare a questo problema. Attualmente il sistema netcentrico prevede che ci siano alcuni centri intermedi, che grazie all'intervento manuale da parte di operatori, siano in grado di filtrare le informazioni rilevanti da inviare ai livelli superiori (Reggimento e Brigata). Questa appare però una soluzione temporanea. In questo momento sono in fase di sperimentazione alcuni software in grado di elaborare i dati provenienti sul terreno in maniera "intelligente", ovvero di raccogliere le informazioni provenienti da punti critici, evitando di intasare la catena di comando con informazioni non totalmente rilevanti. Sembra chiaro che l'attenzione e gli sforzi su questa tematica si concentreranno maggiormente sui livelli alti della catena di comando, perché qui la probabilità di subire le conseguenze di una sovrabbondanza di dati è ovviamente più alta, data la gerarchizzazione dell'architettura militare, che tende a centralizzare i flussi nei nodi di comando[110].

Sicurezza cibernetica. Il programma Forza NEC nasce in un contesto fortemente influenzato dagli sviluppi dell'ICT. Se attraverso la tecnologia netcentrica si mira a raggiungere l'Information Superiority tramite la comunicazione dei dati fra i vari nodi della rete, bisogna porsi il problema di come intervenire qualora queste informazioni vengano intercettate o la rete venga manomessa da nemici. In un sistema con migliaia di sensori, ogni "nodo" può diventare un elemento di vulnerabilità. Similmente, qualora non si avessero dei mezzi avanzati per contrastare efficacemente i pericoli derivanti dalla guerra elettronica si rischierebbe di rendere più vulnerabile una forza armata. Per questo l'approccio "Information Security Engineering" ha avuto l'obiettivo di rendere i sistemi più robusti e sicuri di fronte a possibili minacce informatiche. Oltretutto, la sicurezza

[109] Ibid.

[110] Intervista,18 marzo, 2015.

è ulteriormente incrementata grazie ad attività di "security hardening" successive a valutazioni dei sistemi di sicurezza informatica in teatro. Si è voluto promuovere alcune componenti tecnologiche innovative (Multiple Independent Levels of Security, MILS, Gateway) atte a gestire l'interconnessione tra domini a seconda del diverso livello di classificazione dell'informazione. Durante le varie simulazioni con l'ITB si è cercato di analizzare e validare i sistemi e le piattaforme digitalizzate anche sotto l'aspetto della sicurezza cibernetica. Infine sono state sviluppati e realizzati dei protocolli internet cifranti, abilitati alla trattazione di dati classificati capaci di operare con apparati che poggiano su differenti versioni di protocollo.

3.5 Conclusioni

L'analisi condotta sulle interrelazioni fra difesa, industria e innovazione tecnologica consente di formulare una serie di valutazioni finali, utili a contestualizzare il programma Forza NEC in un ambito più ampio.

Investire in tecnologia per la difesa è fondamentale per assicurare la superiorità strategica che ha contraddistinto i Paesi NATO negli ultimi 25 anni, sia nei vari teatri internazionali nella gestione di crisi di varia natura, sia in termini di deterrenza contro minacce di natura convenzionale. La tecnologia netcentrica permetterebbe di continuare ad avere un alto livello di interoperabilità con gli Stati Uniti ed i maggiori Paesi europei in caso di operazioni multinazionali come quelle degli ultimi anni, ma anche di far fronte all'emergere di un mondo multipolare dove potenze come la Cina e la Russia potrebbero fare ricorso a tattiche "ibride" – o in alcuni casi all'uso convenzionale della forza vera e propria – per raggiungere i propri obiettivi di sicurezza. Avere successo nell'evoluzione netcentrica consentirebbe quindi di rimanere al passo con gli eserciti dei principali alleati dell'Italia e non trovarsi impreparati di fronte a minacce che si potrebbero configurare rapidamente. Nelle recenti missioni internazionali la superiorità tecnologica dimostrata in missioni navali e aeree ha consentito il raggiungimento degli obiettivi minimizzando le perdite tra le forze armate alleate e la popolazione civile. Questa superiorità tecnologica è stata raggiunta tramite un percorso durato decenni, in cui all'esigenza operativa nei teatri operativi si è associato un insieme di investimenti e ricerche che hanno permesso al comparto industriale di soddisfare efficacemente il requisito militare. A differenza dalla dimensione aerea e navale, dove le

forze occidentali potranno contare ancora nel medio periodo su una certa superiorità strategica e tecnologica, nell'immediato futuro la componente terrestre potrebbe trovarsi in situazioni non così favorevoli[111].

Un'altra non meno rilevante considerazione riguarda le ricadute che programmi tecnologicamente avanzati come Forza NEC hanno sull'industria italiana. La tecnologia non genera effetti positivi unicamente da un punto di vista militare-strategico, ma possiede una valenza straordinaria anche in ambito industriale. Lo sviluppo di sistemi avanzati ha spesso delle ricadute in campi diversi da quello militare, basti pensare alle tecnologie dual-use presenti in Forza NEC, come ad esempio posti di comando o UAV. Allo stesso tempo, sistemi all'avanguardia sviluppati per l'EI possono essere esportati in Paesi alleati e amici con un importante ritorno economico per l'industria italiana, ritorno ormai fondamentale per mantenere una base industriale competitiva e solida nonostante la stagnazione della spesa italiana per la difesa. Nella fattispecie, alcuni positivi effetti concreti del programma sono già maturati, ad esempio rispetto agli UGV di OtoMelara, oppure i VTLM-2 di Iveco, o le radio SDR di Finmeccanica-SES[112]. Forza NEC è un programma sicuramente complesso, la cui sperimentazione di tecnologie innovative permette un salto di qualità dell'industria, che si trova a dover ricercare, proporre e sperimentare sistemi che inevitabilmente portano ad un'evoluzione e rinnovamento della stessa. Oltretutto, la capacità di elaborare soluzioni nuove, e la possibilità di confrontarsi a livello internazionale con le realtà di altri Paesi, sono elementi che permettono di sviluppare un vantaggio comparato di nicchia ragguardevole, favorendo l'export verso mercati emergenti e la diffusione di un marchio italiano di qualità. Lo sviluppo tecnologico deve, però, essere sostenuto attraverso un piano di investimenti coerente, che consenta di non perdere il vantaggio tecnologico e industriale accumulato con anni di ricerca e sviluppo. Avere un'industria che sappia sviluppare tecnologia avanzata risponde anche all'esigenza di mantenere una propria sovranità su sistemi, piattaforme e infrastrutture, aspetto che risulterà non di poco conto in un possibile – ed auspicabile – processo di integrazione della difesa europea, dove l'apporto che ogni Paese sarà in grado di fornire sarà determinato anche dal livello di competitività tecnologica che sarà messo in condivisione con i partner[113].

---

[111] Stato Maggiore dell'Esercito, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit.

[112] Interviste, 4 febbraio 2015.

[113] Stato Maggiore dell'Esercito, *Linee di sviluppo evolutivo e innovativo dello strumento*

Alla luce dell'attuale linea politica che ha più volte rivendicato l'esigenza di "fare di più con meno"[114], l'ammodernamento della componente terrestre diventa quindi una necessità imprescindibile. L'Esercito, come le altre forze armate, è sotto pressione a causa del logoramento degli equipaggiamenti avvenuto in teatro negli ultimi vent'anni e della mancanza di risorse economiche dedicate. La scarsità di finanziamenti sta intaccando non solo il rinnovamento degli strumenti di difesa, ma anche l'adeguamento delle tecnologie, l'addestramento del personale, e la manutenzione dei mezzi. Succede così che nell'ultimo decennio l'EI ha potuto contare solamente sul 60% dei fondi che sarebbero stati necessari per l'ammodernamento della forza armata al nuovo contesto di sicurezza[115]. Se favoriti e promossi, gli investimenti in tecnologia permetterebbero la sostituzione dei materiali logorati dalle operazioni in teatro operativo, una razionalizzazione delle risorse e una protezione maggiore del soldato[116]. Non investire in tecnologia sarebbe, dunque, un errore da non commettere per salvaguardare le forze armate ed il Paese dalle evoluzioni di un contesto internazionale di sicurezza in continuo mutamento. Di conseguenza, quella che oggi è una realtà – ossia una stretta collaborazione che vede industria e Difesa lavorare fianco a fianco sin dalla fase di analisi delle esigenze e di concezione dei discendenti sistemi – si spera si consoliderà sempre più in futuro per consentire allo strumento militare di essere in linea con i progressi tecnologici delle altre forze armate, mantenendo i costi su un binario sostenibile, in un'ottica di condivisione degli sforzi in ambito europeo e NATO.

militare terrestre, cit., p. 65.

[114] Ministero della Difesa, *Tecnologia e innovazione per la difesa europea. Pinotti: fare di più con meno la nuova sfida globale*, 11 luglio 2014, http://www.difesa.it/Primo_Piano/Pagine/20140711_ConvegnoAvioAero.aspx.

[115] Stato Maggiore dell'Esercito, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit., p. 16.

[116] Ibid., p. 17.

4.
Le sfide delle capacità netcentriche

Alessandro Marrone, Michele Nones
e Alessandro R. Ungaro

Appare oggi banale ricordare quanto l'ICT abbia radicalmente trasformato l'economia e le stesse società nei Paesi occidentali, ed in una certa misura in tutto il mondo. Appare oggi banale perché ormai ci si è abituati al flusso costante di informazioni, attraverso la rete, tra una quantità impressionante di dispositivi diversi e fisicamente lontani tra loro – computer, televisori, tablet, smartphone, ecc. – e alla loro crescente rapidità di elaborazione ed integrazione dei dati abbattendo le barriere tra i formati testuale, video e audio. Il tutto ad una velocità di connessione che cresce a ritmo esponenziale, mentre i dispositivi si miniaturizzano e le interfacce diventano sempre più personalizzate rispecchiando bisogni e desideri di ogni singolo utente.

Meno banale è cogliere la direzione ed il ritmo della trasformazione portata dall'ICT. In ambito accademico, e non solo, ormai non si parla più solo di "terza rivoluzione industriale", quella avvenuta negli anni '80 e '90 con l'ICT appunto, ma di "quarta rivoluzione industriale" o meglio di "Industry 4.0"[1]. La nuova frontiera è l'Internet of Everything (IoE), un ulteriore passo in avanti del cosiddetto Internet of Things: l'IoE si basa su una nuova infrastruttura tecnologica che combina reti di sensori per l'uso personale e/o incorporati in oggetti, prodotti e cose con la connettività wireless, resi intelligenti come sorgenti di nuovi dati e informazioni e messi a disposizione per lo sviluppo di un nuovo ecosistema di sistemi e servizi[2]. Poiché si stima che il numero di dispositivi connessi nella rete mondiale passerà dai circa 13 miliardi del 2015 a circa 50 miliardi nel 2019[3], risulta evidente la portata rivoluzionaria del fenomeno. Fenomeno

[1] Si veda Andrea Renda (a cura di), *Global Outlook 2015: rapporto finale*, Roma, IAI, 29 aprile 2015, pp. 92-100, http://www.iai.it/it/node/4141.

[2] Per una visione d'insieme del tema si veda, tra gli altri, Camilla Bellini e Elena Vaciago (a cura di), *Internet of Everything: stato dell'arte, trend evolutivi*, Milano, The Innovation Group, giugno 2014, http://www.theinnovationgroup.it/?p=21936.

[3] Andrea Renda (a cura di), *Global Outlook 2015: rapporto finale*, cit., p. 92.

che poggia sui progressi nel cloud, nella robotica, nei sensori, nella gestione dei big data, nelle comunicazioni satellitari, nei microprocessori, ecc[4].

È una rivoluzione non solo tecnologica ma anche della forma mentis e del modus operandi di chi impiega l'ICT nella propria realtà lavorativa e non solo, sia essa pubblica o privata: si tratta infatti di ragionare in modo più orizzontale e meno verticale, più esponenziale e meno lineare, considerando il passato non un fardello, ma un patrimonio da ricostruire su nuove fondamenta. Nell'epoca odierna delle "disruptive technologies"[5] si prevede che entro il 2027 il 75% delle 500 grandi aziende della classifica Fortune sarà sostituito da nuove realtà oggi non presenti in classifica: in breve, per una grande azienda – e non solo – l'alternativa è essere "disrupting" oppure "disrupted"[6].

Queste brevi riflessioni indicano chiaramente che il progresso tecnologico, industriale ed economico punta verso la digitalizzazione e la connessione, con un impatto a cascata su tutti gli aspetti della vita sociale, incluso l'ambito militare che non può in alcun modo esimersi dal fare i conti con l'ICT.

Di fronte ad una tale rivoluzione, in parte già avvenuta ed in parte in divenire, occorre perciò valutare se, come e quanto le forze armate italiane, e dei principali Paesi NATO considerati in questo studio, stiano riuscendo a cogliere le opportunità offerte dall'ICT e a gestirne i rischi connessi. Nel fare ciò, è necessaria una buona dose di realismo e di comprensione delle specificità del mondo militare.

---

[4] Per una trattazione del tema si veda, tra gli altri, il fascicolo "Essere umani con i robot", in *Aspenia*, n. 68, marzo 2015.

[5] Nel loro articolo del 1995, divenuto ormai molto noto ("Disruptive Technologies: Catching the Wave", in *Harvard Business Review*), Joseph L. Bower e Clayton M. Christensen parlano di mutamenti tecnologici "disruptive". Per "disruptive technologies" intendono specifiche tecnologie che inizialmente affiancano quelle ampiamente collaudate e largamente diffuse senza apparentemente minacciarne l'esistenza, ma si indirizzano a nuove categorie di clienti ridefinendo radicalmente l'ecosistema e il ruolo nell'ecosistema produttivo delle imprese, finendo così con il costringere gli attori industriali consolidati a rivedere anche consistentemente i propri piani e modelli di business. Ad esempio, Umberto Bertelè del Politecnico di Milano riflette sul fatto che si acquistano sempre meno macchine fotografiche digitali compatte "non perché qualcuno voglia prendere il posto di Canon e Nikon, ma perché gli smartphone offrono la stessa funzionalità a un costo percepito come nullo e a un livello qualitativo che continua a crescere come conseguenza della guerra fra i produttori degli smartphone stessi." Cfr. Umberto Bertelè, "Le opportunità della disruptive innovation", in *ICT4Executive*, 10 aprile 2014, http://t.co/pQaNigcrix.

[6] Seminario IAI nel ciclo Global Outlook, Roma, 26 marzo 2015.

In generale, le pubbliche amministrazioni, incluse quindi le forze armate, sono meno flessibili, innovative e agili rispetto ai soggetti appartenenti al settore privato, non a causa di una minore qualità delle proprie risorse umane, ma per una loro diversa impostazione, struttura e modo di operare. Il settore pubblico ha, infatti, l'obbligo di prendere decisioni ed agire attraverso procedure estremamente formalizzate, spesso complesse e raramente rapide. Una condizione che tende a ridurre il margine di manovra per la dirigenza nel recepire l'innovazione – tecnologica ed organizzativa – aumentando viceversa il tempo e le risorse dedicate agli aspetti procedurali di ogni attività. Ciò è particolarmente vero per gli appalti pubblici, categoria nella quale rientra anche il procurement militare. Inoltre, il sistema di incentivi e disincentivi nella pubblica amministrazione in genere sfavorisce l'assunzione del rischio, che è tendenzialmente legata ad un processo di innovazione, ed incoraggia in modo più o meno indiretto la conservazione dello status quo – non a caso si parla di "inerzia burocratica".

In questo contesto, le forze armate non fanno eccezione, ed anzi scontano ulteriori limiti nell'approcciarsi all'ICT, dovuti alla loro peculiarità. In primo luogo, lo strumento militare da sempre e per sua stessa natura, è volto ad utilizzare la forza per costringere il nemico ad accettare la propria volontà politica[7]. Vi è quindi un nemico che si oppone in tutti i modi possibili, simmetrici e asimmetrici, all'azione delle forze armate, e ciò concorre a generare quella sorta di "attrito" che in un conflitto rende ogni operazione più difficile, rischiosa, complicata, e a rischio fallimento. Non a caso nelle operazioni militari che includono l'eventualità del combattimento, dalla controguerriglia alle missioni di peace-enforcing e peace-making, dalle attività di contro-terrorismo alla guerra ibrida, fino ovviamente all'ipotesi di una guerra inter-statuale[8], persiste l'incertezza e l'alea sulla condotta e sull'esito delle operazioni – la cosiddetta "fog of war"[9]. Parimenti si può affermare che anche le aziende si scontrano con la volontà dei propri competitori di prevalere sul mercato, e che anche il set-

[7] La definizione è di Karl Von Clausewitz, e si abbina all'altra ben nota definizione clausewitziana di guerra come "prosecuzione della politica con l'aggiunta di altri mezzi". Si veda al riguardo, Karl Von Clausewitz, *Della Guerra*, Milano, Mondadori, 2013.

[8] Ipotesi niente affatto remota neanche per lo strumento militare italiano, che ha combattuto le Forze Armate irachene nel 1991, quelle serbe nel 1999 e quelle libiche nel 2011, nell'ambito di missioni internazionali a fianco degli alleati occidentali, ma sempre in sostanza in una guerra inter-statuale.

[9] Si veda al riguardo, Karl Von Clausewitz, *Della Guerra*, cit.

tore privato è normalmente esposto ad attacchi informatici di varia natura[10]. Tuttavia i due ambiti non sono comparabili. L'intelligence economica, oggi ampiamente praticata anche attraverso intrusioni informatiche, può portare all'acquisizione di know-how del concorrente e quindi ad un vantaggio relativo in termini industriali, ma nessun soggetto privato cerca di eliminare completamente il sistema di comunicazione interno di un concorrente per poi annientare fisicamente i suoi assetti resi in questo modo inermi – cosa accaduta nel 1991 e 2003 alle forze armate irachene, e nel 2011 a quelle libiche, dopo la distruzione dei propri sistemi di comando e controllo da parte delle coalizioni occidentali. In ambito militare è direttamente in gioco la vita delle persone in uniforme, e ciò comporta necessità e requisiti particolari per l'ICT: se in ambito civile può essere accettabile disporre di uno smartphone estremamente performante, ma la cui batteria si scarica nel giro di poche ore – perché si avrà tempo e modo di metterlo tranquillamente in carica ogni giorno – lo stesso non si può dire per un plotone in missione di pattugliamento o per un commando di forze speciali in azione in Afghanistan: entrambi non possono permettersi di perdere il contatto radio a causa dell'esaurimento delle proprie batterie in dotazione. I dispositivi digitalizzati devono rispettare i massimi standard non solo in termini di sicurezza cibernetica, ma anche in termini di contromisure per la guerra elettronica, e allo stesso tempo dovranno disporre di hardware e software in grado di operare in condizioni ambientali e operative avverse.

Le forze armate si trovano, quindi, in una situazione unica ed estremamente difficile. Da un lato la rivoluzione tecnologica dell'ICT ha cambiato e continuerà a cambiare radicalmente l'economia e le società a livello mondiale, e quindi il quadro di riferimento in cui operano nemici ed alleati[11]. Dall'altro, le forze armate scontano una serie di limiti strutturali, in quanto pubblica amministrazione ed in quanto soggetto parte attiva di un conflitto, nel cogliere le opportunità offerte dall'ICT e gestirne i rischi.

[10] Essenziale e quanto mai efficace è l'affermazione del presidente e amministratore delegato di Cisco John Chambers: "Le aziende oggi si dividono in due categorie: quelle che hanno subito un attacco informatico, e quelle che lo hanno subito e non se ne sono ancora accorte". John Chambers, "What does the Internet of Everything mean for security?", in *World Economic Forum* blog, 21 January 2015, http://wef.ch/1C8yELC.

[11] Google Earth offre oggi a qualsiasi gruppo di insorti connesso ad internet la possibilità di avere un'idea della geografia del teatro operativo migliore di quella che aveva lo stato maggiore alleato nel 1944 al momento di pianificare lo sbarco in Normandia, o l'esercito israeliano quando nella Guerra del Kippur del 1973 varcò il Canale di Suez.

Poste di fronte allo stesso problema di fondo, le forze armate americane ed europee hanno cercato soluzioni in parte simili, ed in parte differenti sulla base della specifica realtà nazionale.

Negli Stati Uniti l'ICT e le capacità netcentriche sono divenute profondamente e irrevocabilmente radicate nelle operazioni militari, soprattutto alla luce delle cosiddette "lessons learned" emerse durante le guerre in Iraq e Afghanistan. Ciò che sembra contraddistinguere l'approccio americano, rispetto a quello di altri Paesi tecnologicamente e militarmente avanzati, è la duplice constatazione delle enormi potenzialità e delle altrettanto significative vulnerabilità di un crescente affidamento ad un complesso sistema di reti alla base delle capacità netcentriche. La volontà di sviluppare l'utilizzo di tali capacità in ognuna delle sei "funzioni di combattimento" – "C2", "Intelligence", "Fuoco", "Movimento e manovra", "Protezione" e "Supporto" – dimostra come l'establishment della Difesa americano sia profondamente consapevole della necessità di proseguire verso una completa "messa in rete" degli assetti fisici e umani che danno forma alle forze armate. Al tempo stesso però, assicurare l'integrità delle reti e delle informazioni che viaggiano su di esse costituisce un tema sempre più centrale nel dibattito statunitense. Ogni singolo dominio nella dottrina interforze americana – aria, terra, mare, spazio e cyber – ricopre un ruolo fondamentale per agevolare l'impiego e l'utilizzo di capacità netcentriche, capacità a loro volta necessarie perché le forze armate operino efficacemente in ciascuno dei cinque ambienti. Motivo per cui l'interesse e gli sforzi – soprattutto economici – profusi dalla Difesa americana si orientano in modo particolare verso la neutralizzazione o la mitigazione delle principali minacce che potrebbero causare un'eventuale interruzione nell'utilizzo delle reti – quali ad esempio attacchi cyber, spettri elettromagnetici "congestionati" e crescenti quantità di detriti spaziali – dalle quali dipendono le capacità strategiche militari, e non solo, degli Stati Uniti. In particolare, lo spettro elettromagnetico e lo spazio extra-atmosferico preoccupano non poco le forze armate americane. A titolo di esempio si potrebbero menzionare i continui tentativi per mettere a punto un apposito sistema di difesa dagli impulsi elettromagnetici. Oppure, gli accordi di condivisione delle informazioni stipulati da Washington con aziende commerciali e altri governi che dispongono di capacità di PNT per agevolarne l'accesso da parte americana in caso di danneggiamento o compromissione dei propri.

Come ogni grande rivoluzione tecnologica che deve trovare la sua applicazione in campo militare, anche la strada verso le capacità netcentri-

che non è esente da ostacoli e difficoltà, sia a livello tecnico-ingegneristico sia a livello politico-strategico. Al di là di alcune specificità legate alla realtà americana – come ad esempio determinate problematiche istituzionali, legali e finanziarie – le forze armate degli Stati Uniti sono come le altre di fronte alla necessità di superare quei limiti fisici che inibiscono la reale portata delle capacità netcentriche. In particolare, ci si riferisce a quelle limitazioni attualmente imposte dalla tecnologia, ad esempio in termini di peso, dimensioni e potenza dei sistemi con cui dotare i soldati, e che sono all'attenzione di specifici programmi di R&D volti proprio a ricercare nuove soluzioni per "liberare" le potenzialità, finora rimaste in parte inespresse e non sfruttate, delle capacità netcentriche. Allo stesso tempo, negli Stati Uniti l'interoperabilità interforze e soprattutto con i principali Paesi alleati rimane tuttora un aspetto che – al di là della retorica e di qualche isolato esempio – sembra mancare di vera concretezza operativa, forse a causa della mancanza di una reale volontà politica di istaurare una solida e strutturata cooperazione a riguardo. Le incertezze sull'ammontare del bilancio della difesa e le restrizioni finanziarie già sperimentate negli anni scorsi hanno forse spinto le forze armate americane a prediligere in prima battuta un approccio più "domestico", dando priorità alla risoluzione di problematiche interne, e solo dopo aver raggiunto un adeguato livello di interoperabilità interforze è possibile un orientamento verso una prospettiva multinazionale e di integrazione netcentrica con gli altri assetti e piattaforme appartenenti alle forze armate dei principali partner.

Nel Vecchio Continente il punto di partenza e le ambizioni in fatto di capacità netcentriche sono parzialmente diversi. Francia, Germania e Regno Unito hanno intrapreso un proprio percorso per la trasformazione netcentrica delle rispettive forze armate, che è stato influenzato anche dall'esperienza nelle missioni internazionali dell'ultimo quindicennio.

Ad esempio, la Francia ha intrapreso rapidamente la digitalizzazione del livello del singolo soldato – con il programma FELIN – e ha potuto sviluppare il processo in senso verticale senza la pressione di impegni operativi quali quello in Iraq ed in Afghanistan – dove ha assunto un ruolo relativamente piccolo e per un tempo limitato. Viceversa, il Regno Unito ha dovuto ricorrere agli UOR per equipaggiare le proprie brigate impegnate massicciamente nei teatri iracheno ed afgano, acquisendo spesso equipaggiamenti off-the-shelf da diversi fornitori e complicando così la messa in rete degli assetti e la costruzione di una architettura netcentrica – senza contare il drenaggio di risorse dai programmi di procurement ordinari verso il sostegno gli UOR. La Germania si è collocata in una posizio-

ne mediana rispetto ai due estremi francese e britannico, con una certa coerenza nell'impegno per la digitalizzazione delle proprie forze armate e al tempo stesso uno sforzo militare significativo e prolungato in Afghanistan (ma non in Iraq).

Quanto alla minaccia alle reti che costituiscono il sistema nervoso delle capacità netcentriche, la sicurezza cibernetica ha acquisito sempre maggiore importanza nella concezione sia britannica che francese. Entrambe le forze armate stanno sviluppando capacità non solo di difesa cibernetica ma anche di offesa, come compensazione per la riconosciuta vulnerabilità intrinseca al processo di digitalizzazione delle rispettive forze armate. A tale impegno corrisponde altresì un certo attivismo dell'industria della difesa nei due Paesi. Anche la Germania si è mossa in questa direzione, anche in seguito alla recente crisi in Ucraina, in particolare quanto a capacità di early warning ed interdizione rispetto ad attacchi cibernetici.

In termini di C2, la vicenda britannica dell'architettura di comunicazione a livello tattico Bowman è un buon esempio della difficoltà per le forze armate di tenere il passo con l'innovazione tecnologica nel campo dell'ICT. Il sistema Bowman è entrato in servizio nel 2008, dopo una lunga fase di gestazione a causa delle difficoltà di digitalizzare e mettere in rete gli assetti dell'Esercito, e nel 2015 è in via di introduzione la sua versione più aggiornata. Eppure già nel 2018 è prevista la sostituzione del Bowman con un nuovo sistema, anche noto come Morpheus, che si spera sia più facilmente aggiornabile nel tempo per restare al passo con gli sviluppi dell'ICT. In Francia, il programma SCORPION adotta un approccio centralizzato all'acquisizione di veicoli, sistemi d'arma e di comunicazione in modo integrato per ottenere capacità netcentriche. In parallelo, tuttavia, viene finanziato l'upgrade dell'attuale architettura di comunicazione, il SICS, per mantenere operativi i veicoli che non saranno riconfigurati in ambito SCORPION. Il combinato dei due programmi cerca sostanzialmente di bilanciare il bisogno di tenere il passo con l'ICT con l'impossibilità di poter rimpiazzare tout court l'asset legacy dell'Esercito francese. Anche la Germania ha dovuto affrontare problemi simili. Il programma IdZ di digitalizzazione degli equipaggiamenti del singolo soldato – l'equivalente del FELIN francese – è iniziato nel 2004 ma ha visto la consegna del primo lotto di prodotti solo nel 2012, lotto che si è rivelato per certi versi obsoleto a causa, ad esempio, del rapido avvento dei dispositivi smartphone. Il fatto che i veicoli dell'Esercito tedesco siano nuovi o in fase di acquisizione è un fattore positivo nella misura in cui sono già disegnati per soddisfare le esigenze netcentriche.

In generale, in tutti e tre i Paesi si è adottato un approccio più cauto rispetto agli Stati Uniti nella digitalizzazione delle forze terrestri, anche a causa dei limiti di bilancio e/o delle esigenze di breve periodo legate alle operazioni in corso. Tuttavia, gli stessi hanno riconosciuto l'importanza delle capacità netcentriche, in particolare del dominio cyber, investendo ingenti risorse economiche nell'affrontare le difficoltà che la trasformazione netcentrica comporta, in termini di asset legacy, interoperabilità, e obsolescenza dei sistemi acquisiti anche a causa della lentezza del processo di sviluppo, produzione ed entrata in servizio.

È in questo contesto che va valutata l'esperienza italiana. L'approccio altrettanto cauto e graduale alla trasformazione netcentrica dell'Esercito, concretizzatosi anche nell'introduzione di una lunga ed economicamente significativa fase di CD&E, serve anche ad affrontare le intrinseche difficoltà delle forze armate nello sfruttare le opportunità dell'ICT e mitigarne i rischi. Non a caso, come avvenuto ad esempio in Francia, l'Italia ha optato per aggiornare parte dell'asset legacy agli standard netcentrici e mantenerla ancora a lungo in servizio, in attesa che gli equipaggiamenti vengano man mano sostituiti dai nuovi assetti che incorporino la tecnologia netcentrica già dalla fase di design. Il problema delle brigate "a tecnologia differente" è quindi una realtà con cui bisognerà convivere, perché l'innovazione nel campo ICT continuerà ad un ritmo serrato mentre procederà la digitalizzazione degli assetti dell'Esercito. L'unica strada da percorrere verso le capacità netcentriche, per quanto difficile, consiste nel prevedere e gestire un ciclo continuo di immissione in servizio di nuove piattaforme, più vicine allo stato dell'arte quanto ad ICT, in sostituzione di una parte dell'asset legacy, e al tempo stesso di aggiornamento netcentrico della parte di asset legacy che è conveniente ammodernare.

Questa strada è estremamente tortuosa e difficile, come un sentiero alpino, perché ai lati si pongono due precipizi, ovvero due rischi da evitare. Da un lato vi è la tentazione di inseguire costantemente l'innovazione tecnologica con attività di CD&E, rimandando il momento di mettere la parola fine alla sperimentazione di prototipi e passare alla produzione dei sistemi ormai maturi. In questo caso, per inseguire una soluzione tecnologicamente più avanzata, si lasciano in realtà le forze armate ad utilizzare equipaggiamenti maggiormente obsoleti, mentre quello che viene sviluppato non vedrebbe mai la luce in teatro perché sottoposto ad ulteriori aggiornamenti. Tale rischio è strettamente connesso al principio dell'"evolution through production", e può essere evitato da un approccio realistico che preferisca una soluzione utilizzabile in tempi brevi sebbe-

ne non perfettamente allo stato dell'arte, combinato con l'utilizzo della "architettura aperta" per poter aggiornare successivamente i sistemi man mano introdotti. L'altro rischio della strada verso le capacità netcentriche, speculare al primo, è quello di arrendersi – di fatto, se non formalmente – di fronte alle suddette difficoltà nello sfruttare le potenzialità dell'ICT: ovvero accontentarsi di soluzioni al ribasso, non sforzarsi di sviluppare tecnologie all'avanguardia, restare ancorati a procedure di procurement burocratizzate, poco efficienti ed efficaci (peraltro inadatte ad una CD&E). La strada più idonea e conveniente da percorrere è invece quella che, proprio grazie ai risultati delle attività di sviluppo e sperimentazione, preveda di "fissare" i nuovi sistemi/sensori/dispositivi validati da prove tecnico-tattiche sui prototipi operativi ed iniziare la produzione di serie volta ad equipaggiare tanto il singolo combattente quanto intere unità. Così procedendo si raccoglierebbero i frutti maturi della ricerca e sviluppo e si condurrebbe il rinnovamento di almeno una parte delle componenti delle forze armate, procedendo in futuro per step successivi ed incrementali in termini di innovazione tecnologica con approccio evolutivo e modulare.

Dopo i naturali e fisiologici problemi e ritardi (insiti in tutte le fasi di ricerca, sviluppo e sperimentazione), i risultati prodotti durante la fase di CD&E di Forza NEC consentono ora lo svolgimento di test tecnici e prove tattiche di integrazione su più livelli e in ambito interforze. Le campagne di verifica in svolgimento nel 2015 presso la Brigata Pinerolo e l'Unità Sperimentale di Digitalizzazione svolte congiuntamente con l'industria confermano la possibilità di raggiungere obiettivi concreti e comparabili con quelli dei grandi Paesi europei con cui l'Italia si confronta e coopera a livello politico, militare e industriale.

In quest'ottica vanno considerate le questioni dell'interoperabilità interforze, della gestione dei dati in teatro e della sicurezza cibernetica. L'attenzione eccessiva di ciascuna forza armata per la sua specificità è un altro di quegli elementi peculiari del mondo militare che rendono difficoltosa la trasformazione netcentrica, in particolare limitando e ostacolando l'interoperabilità interforze a livello tattico, operativo e strategico.

La gestione di un flusso di dati molto ingente, come quello risultante dalla messa in rete di migliaia di sensori delle varie unità dell'Esercito, è un'attività particolarmente complessa per la forza armata. Infatti, in una struttura gerarchica come quella militare è necessario che le informazioni siano condivise a livello verticale, ma ciò pone il duplice problema di non intasare la catena di comando con una mole di dati non rilevanti, e di evitare il rischio di micro-management una volta che i livelli superio-

ri sono in grado di accedere in tempo reale alle stesse informazioni di quelli inferiori e di comunicare altrettanto rapidamente i propri ordini. Un problema niente affatto nuovo per le forze armate, nei suoi termini di base, ma non per questo meno cruciale per una condotta efficace delle operazioni militari[12].

Quanto alla sicurezza cibernetica, è ormai una priorità nell'ambito della trasformazione netcentrica non solo per gli Stati Uniti ma anche per i maggiori Paesi europei. Sono quindi più che giustificati gli sforzi del programma Forza NEC al riguardo, dalle attività di "security hardening" alle simulazioni condotte tramite l'ITB. Occorre tuttavia essere consapevoli che nel dominio cibernetico la competizione tra "offesa" e "difesa" procede ad una velocità esponenziale rispetto a quella sperimentata nel corso dei secoli in ambito militare, la cosiddetta dinamica "spada-scudo" o "corazza-cannone" per cui a fronte di capacità offensive più performanti le capacità difensive vengono ulteriormente rafforzate, e viceversa. Tale competizione senza fine richiede, quindi, attenzione ed investimenti costanti, per mantenere a livelli accettabili la vulnerabilità di uno strumento militare reso inevitabilmente più esposto del passato ad attacchi cibernetici proprio dal processo di digitalizzazione.

Rispetto alla sicurezza cibernetica, ed in generale alle capacità netcentriche, vale una riflessione di fondo sull'importanza delle tecnologia in ambito militare. Più volte nel corso della storia moderna e contemporanea l'innovazione tecnologica ha dato l'impressione di poter fornire l'arma "strategica" o "definitiva", risolutiva di ogni conflitto, come nel caso del potere aereo teorizzato da Giulio Douhet[13] a cavallo della Grande guerra o dell'avvento dell'arma atomica nel secondo dopoguerra. Tuttavia, ogni volta, il combinato disposto della stessa innovazione tecnologica e soprattutto dei cambiamenti nelle modalità di condotta delle operazioni militari a livello tattico, operativo e strategico, hanno compensato il vantaggio re-

[12] Quando il telegrafo ha accelerato in maniera esponenziale le comunicazioni attraverso la catena C2 degli eserciti europei, le forze armate tedesche e francesi hanno sfruttato in modo molto diverso le potenzialità offerte dalla nuova tecnologia alla vigilia della Seconda Guerra Mondiale: mentre la Germania ha lasciato amplia autonomia ai comandanti delle divisioni impegnate nel teatro operativo, secondo la dottrina del Blitzkrieg, la Francia ha mantenuto una stretta dipendenza delle forze dispiegate lungo la Linea Maginot dal comando di Parigi, e ciò ha contribuito in maniera non marginale alla disfatta francese nel 1940.

[13] Prima nell'articolo "I problemi della aeronavigazione", pubblicato sulla rivista *La Preparazione* nel 1910, e poi nella sua opera più famosa del 1921, *Il dominio dell'aria*.

lativo fornito in un primo tempo dalla nuova tecnologia utilizzata a scopi bellici[14]. Anche l'ICT non fa eccezione al riguardo, e quindi il vantaggio assicurato dalle capacità netcentriche va commisurato con l'abilità dell'avversario di modificare la propria strategia per compensare la condizione di svantaggio in cui si viene a trovare: attrito ed alea non possono essere eliminati neppure da una piena "information superiority" e dalla migliore "situational awareness".

In altre parole, la tecnologia non è e non può diventare la soluzione a tutti i dilemmi di sicurezza, in quanto il futuro ambiente operativo sarà ancora caratterizzato dalla dimensione umana che alberga in ogni conflitto. Sebbene siano innegabili i miglioramenti ottenuti in ambito militare grazie all'innovazione tecnologica, ed in particolare all'ICT, bisogna essere coscienti dei limiti di un eccessivo affidamento su sistemi avanzati. Ad esempio, consapevoli dell'attenzione dei governi occidentali all'opinione pubblica interna, gli avversari hanno spesso impiegato tattiche asimmetriche contro la superiorità tecnologica dei Paesi NATO, facendo ricorso a propaganda o pratiche terroristiche, e utilizzando la popolazione come scudo agli attacchi di forze armate più avanzate al fine di indebolire il consenso interno per l'intervento militare. Anche diverse realtà statuarie fanno ampio ricorso a strumenti di disinformazione e intimidazione, nonché ad attori non-statuali, per perseguire i propri obiettivi in quella che oggi viene chiamata "guerra ibrida". La tecnologia da sola difficilmente può prevalere sull'aspetto umano del conflitto nel momento in cui non si prendono delle misure adatte per affrontarlo. In quest'ottica l'Italia, ed in generale i Paesi occidentali, dovranno assicurarsi di saper condurre battaglie militari ma anche politiche, e di saper integrare i propri assetti militari e civili in maniera più coerente e sinergica.

Se è vero che la tecnologia non è di per sé sufficiente per raggiungere gli obiettivi militari di un Paese come l'Italia, è altrettanto vero che è assolutamente necessaria – una vera e propria conditio sine qua non. In particolare, oggi e nel prossimo futuro la trasformazione netcentrica delle capacità militari rappresenta un passaggio irrinunciabile per mantenere l'operatività e l'efficacia delle forze armate, soprattutto dell'Esercito italiano.

[14] Si veda al riguardo Edward N. Luttwak, *Strategia. La logica della guerra e della pace*, Milano, Rizzoli, 2013.

Bibliografia

Army Science Board, *Decisive Army Strategic and Expeditionary Maneuver*, 18 September 2014.

Camilla Bellini e Elena Vaciago (a cura di), *Internet of Everything: stato dell'arte, trend evolutivi*, Milano, The Innovation Group, giugno 2014, http://www.theinnovationgroup.it/?p=21936.

Umberto Bertelè, "Le opportunità della disruptive innovation", in *ICT4Executive*, 10 aprile 2014, http://t.co/pQaNigcrix.

Joseph L. Bower e Clayton M. Christensen, "Disruptive Technologies: Catching the Wave", in *Harvard Business Review*, Vol. 73, No. 1 (January-February 1995), pp. 43-53.

Bob Brewin, "Army Eyes 4G Cellular Tech for Combat Communications", in *Nextgov*, 10 September 2014, http://www.nextgov.com/defense/2014/09/army-eyes-4g-cellular-tech-combat-communications/93689.

Bob Brewin, "The Navy wants a tactical cloud", in *Defense One*, 25 September 2014, http://www.defenseone.com/technology/2014/09/navy-wants-tactical-cloud/95129.

Nick Brown, "Airbus adds internet freedom to UK TACIP", in *Jane's International Defence Review*, 26 November 2014.

Carl H. Builder, Steven C. Bankes, Richard Nordin, *Command Concepts. A Theory Derived from the Practice of Command and Control*, Santa Monica, RAND, 1999, http://www.rand.org/pubs/monograph_reports/MR775.html.

Amy Butler, "USMC to outfit Ospreys with comms node", in *Aviation Week & Space Technology*, 14 October 2013, http://aviationweek.com/node/ 4026.

Vincenzo Camporini et al., *Il ruolo dei velivoli da combattimento italiani nelle missioni internazionali: trend e necessità*, Roma, Nuova Cultura, 2014 (Quaderni IAI n. 10), http://www.iai.it/it/node/1851.

James Jay Carafano and Richard Weitz, "EMP attacks: What the U.S. must do now", in *Heritage Foundation Backgrounder*, n. 2491 (17 November 2010), http://www.heritage.org/research/reports/2010/11/emp-attacks-what-the-us-must-do-now.

Edward C. Cardon, *Keynote Address*, Brookings Fifth Annual Military and Federal Research Symposium: "Securing America's Future in the New 'Interwar Years'", 12 March 2014, http://brook.gs/1F8BpAi.

John Chambers, "What does the Internet of Everything mean for security?", in *World Economic Forum* blog, 21 January 2015, http://wef.ch/1C8yELC.

Karl Von Clausewitz, *Della Guerra, Milano, Mondadori, 2013.*

Fabrizio Coticchia, *Qualcosa è cambiato? L'evoluzione della politica di difesa italiana dall'Iraq alla Libia (1991-2011)*, Pisa, Pisa University Press, 2013.

Defense Advanced Research Projects Agency (DARPA), *Adaptable Navigation Systems (ANS)*, http://www.darpa.mil/Our_Work/STO/Programs/Adaptable_Navigation_Systems_(ANS).aspx.

Defense Advanced Research Projects Agency (DARPA), *Micro-Technology for Positioning, Navigation and Timing (Micro-PNT)*, http://www.darpa.mil/Our_Work/MTO/Programs/Micro-Technology_for_Positioning,_Navigation_and_Timing_(Micro-PNT).aspx.

Giovanna De Maio, "Nel Baltico col fiato sul collo", in *AffariInternazionali, 29 gennaio 2015, http://www.affarinternazionali.it/articolo.asp?ID=2951.*

Nadia Deseilligny, "France earmarks EUR1 billion in spending on cyber defence", in *Jane's Defence Industry*, Vol. 31, No. 2 (1 February 2014).

Justin Doubleday, "Army aims to jump-start development of radio-frequency defenses", in *Inside the Army*, 29 December 2014.

Justin Doubleday, "Army crafting career field, occupational specialty for cyber forces", in *Inside the Army*, 19 September 2014.

Justin Doubleday, "Army seeks info on Patriot-interface kits for networked missile defense", in *Inside the Army*, 3 October 2014.

Justin Doubleday, "Congress approves Army funding for 'assured' navigation technology", in *InsideDefense.com*, 10 October 2014.

Justin Doubleday, "Solicitation eyed this fall for 'unified capabilities' networking tools," in Inside the Army, 19 September 2014.

Giulio Douhet, *Il dominio dell'aria*, Roma, Ufficio Storico dell'Aeronautica Militare, 2002, http://www.liberliber.it/mediateca/libri/d/douhet/il_dominio_dell_aria/pdf/il_dom_p.pdf.

Giles Ebbutt, "Beyond Bowman", in *Jane's Defence Weekly*, Vol. 51, No. 26 (25 June 2014), pp. 28-31.

Jesse Ellman, Gregory Sanders and Rhys McCormick, *U.S. Department of Defense Contract Spending and the Industrial Base, 2000-2013*, in CSIS Events, 16 October 2014, http://csis.org/node/52055.

Sydney J. Freedberg, "The Army gropes toward a cultural revolution", in

Breaking Defense, 22 October 2014, http://breakingdefense.com/?p=16597.

Sydney J. Freedberg, "STRATCOM lacks authority, $$ on electronic warfare", in *Breaking Defense*, 7 October 2014, http://breakingdefense.com/?p=16291.

Sydney J. Freedberg, "What the US, NATO must do to counter Russia: Breedlove, Gorenc & Odierno", in *Breaking Defense*, 22 September 2014, http://breakingdefense.com/?p=15930.

German Ministry of the Interior, *Cyber Security Strategy for Germany*, February 2011, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf.

Matthew Glavy, "The Flight MAP: The Marine Aviation Plan Through 2040", in *CSIS Events*, 28 April 2014, http://csis.org/node/48793.

Mikhail Gorbachev, "A New Cold War Order", in *Project Sindicate*, 5 January 2015, http://po.st/QpXoPk.

Joe Gould, "New war game to focus on tech, partnerships", in *Defense News*, 13 October 2014, http://www.defensenews.com/article/20141013/SHOWSCOUT04/310130030.

Mary-Louise Hoffman, "Heidi Shyu: Army eyes interoperability, open standards for ground robotic system", in *Executive Gov*, 15 August 2014, http://www.executivegov.com/?p=62462.

Mike Hoffman, "Marines Work to Extend K-MAX in Afghanistan Through 2014", in *DefenseTech*, 25 September 2013, http://defensetech.org/2013/09/25/marines-work-to-extend-k-max-through-2014.

Henry Kenyon, "Navy views network infrastructure as a vital combat component," in *DefenseSystems.com*, 9 June 2011, http://defensesystems.com/articles/2011/06/09/naval-it-day-greenert-network-as-combat-system.aspx.

Maren Leed, *Offensive Cyber Capabilities at the Operational Level. The Way Ahead*, Washington, Center for Strategic and International Studies (CSIS), September 2013, http://csis.org/node/46679.

Robert H. Legvold, "Managing the New Cold War", in *Foreign Affairs*, Vol. 93, No. 4 (July/August 2014), pp. 74-84, https://www.foreignaffairs.com/node/1113241.

Edward N. Luttwak, *Strategia. La logica della guerra e della pace, Milano, Rizzoli, 2013.*

Stew Magnuson, "Top secret Air Force bomber program moves forward", in *National Defense*, September 2014, http://www.nationaldefensemagazine.org/archive/2014/September/Pages/TopSecretAirForceBomberProgramMovesForward.aspx.

Carol Malouf e Ruth Sherlock, "ISIS Is Building Strength On Lebanon's Doorstep", in *BusinessInsider*, 20 January 2015, http://read.bi/15thyfi.

Alessandro Marrone, "La non riforma della Difesa", in *AffaiInternazionali*, 24 febbraio 2012, http://www.affarinternazionali.it/articolo.asp?ID=2544.

Alessandro Marrone, "I quattro pilastri della riforma della Difesa", in *AffariInternazionali*, 17 dicembre 2012, http://www.affarinternazionali.it/articolo.asp?ID=2208.

Alessandro Marrone, Paola Sartori, Alessandro R. Ungaro, *Bilanci e industria della difesa: tabelle e grafici*, luglio 2014, http://www.iai.it/it/node/702.

Scott Maucione, "DARPA wants white papers on 'Squad X' dismounted info-sharing", in *InsideDefense.com*, 31 July 2014.

Scott Maucione, "Pentagon eyes reforms in commercial SATCOM acquisition practices", in *Inside the Pentagon*, 9 October 2014.

Scott Maucione, "Upcoming DoD CIO cloud policy leaves questions over interoperability", in *Inside the Pentagon*, 9 October 2014.

Kevin McCaney, "Mobile satellite network gives Army swift artillery support", in *DefenseSystems.com*, 2 December 2014, http://defensesystems.com/articles/2014/12/02/army-win-t-satellite-artillary-support.aspx.

Paul McCleary, "US Army Presses Ahead on Manned-Unmanned Teaming", in *Defense News*, 30 April 2013, http://www.defensenews.com/article/20130430/DEFREG02/304300018.

Ministero della Difesa, *Libro bianco per la sicurezza internazionale e la difesa. La nostra Difesa*, http://www.difesa.it/Primo_Piano/Pagine/20150429Libro_Bianco.aspx.

Ministero della Difesa, *Linee guida del Libro bianco per la sicurezza internazionale e la difesa*, giugno 2014, http://www.difesa.it/Primo_Piano/Pagine/LibroBianco.aspx.

Jordana Mishory, "DoD eyes interoperability in next-gen host-based cybersecurity strategy", in *Inside the Pentagon*, 21 August 2014.

Jordana Mishory, "DoD waives data link requirement so Navy can obtain eight systems", in *Inside the Pentagon*, 14 August 2014.

Jordana Mishory, "Official: DoD needs to better coordinate, oversee electronic warfare efforts", in *InsideDefense.com*, 15 October 2014.

Jordana Mishory, "Stratcom signs new space situational awareness data-sharing agreement", in *Inside the Pentagon*, 4 September 2014.

Ellen Mitchell, "Key Army official predicts growth of "Network Integration Evaluation" drills", in *Inside the Army*, 3 October 2014.

Ellen Mitchell, "Shyu: Army to procure $25M in technologies tested at NIE 14.1", in *Inside the Army*, 8 September 2014.

Pete Modigliani and Su Chang, *Defense Agile Acquisition Guide. Tailoring DoD IT Acquisition Program Structures and Processes to Rapidly Deliver Capabilities*, Mitre Corporation, March 2014, http://www.mitre.org/node/18951.

Michele Nones e Marrone Alessandro (a cura di), *La trasformazione delle Forze Armate: il programma Forza Nec*, Roma, Nuova Cultura, 2011 (Quaderni IAI n. 2), http://www.iai.it/it/node/1149.

Kris Osborn, "Marines fly helicopters with mini-tablet", in *DoD Buzz*, 5 April 2014, http://wp.me/pgSCu-8kt.

Cheryl Pellerin, "Cybercom activates national mission force headquarters", in *DoD News*, 25 September 2013, http://www.defense.gov/news/newsarticle.aspx?id=120854.

Walter Piatt, "The Future of European Collective Defense", in *CSIS Events*, 16 October 2014, http://csis.org/node/52206.

Andrea Renda (a cura di), *Global Outlook 2015: rapporto finale,* Roma, IAI, 29 aprile 2015, pp. 92-100, http://www.iai.it/it/node/4141.

Patrick A. Schrafft, "Enhancing fires with next-generation narrowband SATCOM", in *Fires*, July-August 2014, http://www.readperiodicals.com/201407/3410820761.html.

Jason Sherman, "In event of sequester, entire modernization portfolio to be 'stretched out'", in *InsideDefense.com*, 14 October 2014.

Sebastian Sprenger, "Army may break up major network program if results fall short", in *InsideDefense.com*, 14 October 2014.

Sebastian Sprenger, "General Dynamics launches "Apollo" in bid to save its Army radio business", in *Inside the Army*, 3 October 2014.

Stato Maggiore della Difesa, *Il Concetto strategico del Capo di Stato Maggiore della Difesa, 2005*, http://www.aeronautica.difesa.it/Missione/Documents/libroconcettostrategico.pdf.

Stato Maggiore dell'Esercito, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre - PROSPECTA,* 2015.

Brooks Tigner, "NATO urged to embed cyber defence into mission planning", in *Jane's Defence Weekly*, 23 September 2014.

UK Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 19 October 2010, https://www.gov.uk/government/publications/the-strategic-defence-and-security-review-securing-britain-in-an-age-of-uncertainty.

UK Ministry of Defence Joint Forces Command and Philip Hammond, *New*

cyber reserve unit created, 29 September 2013, https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit.

UK Prime Minister's Office, *UK-France declaration on security and defence*, 17 February 2012, https://www.gov.uk/government/news/uk-france-declaration-on-security-and-defence12.

Alessandro Ungaro, Alessandro Marrone e Michele Nones, "Sfide e opportunità dell'innovazione tecnologica nell'addestramento delle Forze armate italiane", in *Documenti IAI*, n. 15|02, gennaio 2015, http://www.iai.it/it/node/3247.

US Army Combined Arms Center, *U.S. Army Mission Command Strategy, FY13-16*, June 2013, http://usacac.army.mil/cac2/Repository/Army_Mission_Command_Strategy_dtd_12June%202013.pdf.

US Army Training and Doctrine Command (TRADOC), *The United States Army Operating Concept, 2016-2028*, TRADOC Pamphlet No. 525-3-1, 19 August 2010, https://fas.org/irp/doddir/army/opcon.pdf.

US Army Training and Doctrine Command (TRADOC), *The U.S. Army Operating Concept: Win in a Complex World*, 2020-2040, 31 October 2014, TRADOC Pamphlet No. 525-3-1, 31 October 2014, http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf.

US Dept of the Army, *Army Equipment Program in Support of President's Budget 2015*, May 2014, http://usarmy.vo.llnwd.net/e2/c/downloads/348286.pdf.

US Dept of Defense, *Instruction 2010.06: Materiel Interoperability and Standardization with Allies and Coalition Partners*, 29 July 2009, http://dtic.mil/whs/directives/corres/pdf/201006p.pdf.

US Dept of Defense, *Instruction 8330.01, Interoperability of Information Technology (IT), including National Security Systems (NSS)*, 21 May 2014, http://dtic.mil/whs/directives/corres/pdf/833001p.pdf.

US Dept of Defense, *Quadrennial Defense Review 2014*, March 2014, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

US Dept of Defense, *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology*, March 2009, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf.

US Dept of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2012, http://www.defense.gov/news/ Defense_Strategic_Guidance.pdf.

US Dept of Defense, Chairman of the Joint Chiefs of Staff, *Joint Publication*

3-0: Joint Operations, 11 August 2011, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

US Dept of Defense, Director Operational Test and Evaluation, *Army Programs, Network Integration Evaluation (NIE)*, 2011, http://www.dote.osd.mil/pub/reports/FY2011/pdf/army/2011nie.pdf.

US Dept of Defense, Director Operational Test and Evaluation, *Reasons behind program delays: 2014 update*, 26 August 2014, http://www.dote.osd.mil/pub/presentations/ProgramDelaysBriefing2014_8Aug_Final-77u.pdf.

US House of Representatives, Armed Service Committee, Subcommittee on Strategic Forces, *Statement of Gil I. Klinger*, 3 April 2014, http://docs.house.gov/meetings/AS/AS29/20140403/102037/HHRG-113-AS29-Wstate-KlingerG-20140403.pdf.

US House of Representatives, Armed Service Committee, Subcommittee on Strategic Forces, *Statement of Douglas L. Loverro*, 3 April 2014, http://docs.house.gov/meetings/AS/AS29/20140403/102037/HHRG-113-AS29-Wstate-LoverroD-20140403.pdf.

US Marine Corps, *Expeditionary Force 21. Forward and Ready: Now and in the Future*, 4 March 2014, http://www.mccdc.marines.mil/Portals/172/Docs/MCCDC/EF21/EF21_USMC_Capstone_Concept.pdf.

US Marine Corps, *Service Campaign Plan for 2014-2022*, 21 May 2014, https://marinecorpsconceptsandprograms.com/sites/default/files/files/United%20States%20Marine%20Corps%20Service%20Campaign%20Plan%202014-2022.pdf.

US Marine Corps, *USMC Concepts and Programs 2013*, http://www.hqmc.marines.mil/pandr/ConceptsandPrograms/ConceptsandPrograms2013.aspx.

US Marine Corps Systems Command, *Modern Day Marine: Report to Industry*, 25 September 2014.

US Senate, Committee on Armed Services, *Testimony of Frank Kendall*, 30 April 2014, http://www.armed-services.senate.gov/imo/media/doc/Kendall_04-30-14.pdf.

US Senate, Committee on Armed Services, Subcommittee on AirLand, *Statement of Gen. John F. Campbell, Vice Chief of Staff, United States Army, on Fiscal Year 2015 Ground Force modernization and individual equipment modernization programs*, 9 April 2014, http://www.armed-services.senate.gov/imo/media/doc/Campbell-Barclay-Williamson_04-09-14.pdf.

Stefan Wagstyl, "Germany plans early-warning defence against cyber attacks", in *Financial Times*, 10 November 2014, http://on.ft.com/1uXsbBS.

Stephen Walt, "The Bad Old Days Are Back", in *Foreign Policy*, 2 May 2014, http://foreignpolicy.com/2014/05/02/the-bad-old-days-are-back.
Marcus Weisgerber, "USAF General: DoD Must Change How it Buys Satellites", in *C4ISR & Networks*, 19 August 2014, http://www.c4isrnet.com/article/20140813/C4ISRNET06/308130001.

Finito di stampare nel mese di maggio 2015
con la tecnologia *print on demand*
presso il Centro Stampa "Nuova Cultura"
p.le Aldo Moro n. 5, 00185 Rome
www.nuovacultura.it
per ordini: ordini@nuovacultura.it

[Int_9788868125066_17x24bn_LM03]

Innovazione tecnologica e mondo militare sono da sempre in costante interazione – dinamica accelerata nel periodo post-Guerra Fredda. In questo contesto, lo studio si concentra sul rapporto tra l'Information Communication Technology (ICT) e le forze armate di Italia, Stati Uniti, Gran Bretagna, Francia e Germania. Sì intende così analizzare nel quadro euro-atlantico il percorso intrapreso dall'Esercito Italiano per sviluppare delle capacità militari netcentriche (Network Enabled Capabilities, NEC) attraverso il programma Forza NEC. Con l'acronimo NEC ci si riferisce all'interconnessione di diversi elementi delle forze armate in un'unica rete, in modo da ottenere la loro interazione per raggiungere una marcata superiorità strategica.
Il Quaderno si articola in tre capitoli, che offrono rispettivamente un'analisi del caso americano, una panoramica degli sviluppi in Francia, Germania e Gran Bretagna, ed infine una disamina della situazione italiana. Il volume mira – a quattro anni di distanza dallo studio *La trasformazione delle Forze Armate: il programma Forza NEC* – a fare il punto rispetto ad una relazione tra innovazione tecnologica e difesa in piena evoluzione. Evoluzione segnata dal fatto che gli sforzi per digitalizzare ed interconnettere gli equipaggiamenti delle forze terrestri, sfruttando le potenzialità dell'ICT, si scontrano con realtà operative e di bilancio che rendono particolarmente difficile per le forze armate dei paesi analizzati percorrere la propria strada verso capacità netcentriche.

Alessandro Marrone è responsabile di ricerca presso il Programma Sicurezza e Difesa dell'Istituto Affari Internazionali (IAI).
Michele Nones è direttore del Programma Sicurezza e Difesa dello IAI.
Alessandro R. Ungaro è ricercatore presso il Programma Sicurezza e Difesa dello IAI.

13.30 EURO

ISBN 978-88-6812-506-6
9 788868 125066
9788868125066_166_LM_4