EVOLUZIONE DEGLI SCENARI E RUOLO DELLE NUOVE SMART TECHNOLOGIES

di
Francesco Tosato

Lo scenario che l'Alleanza Atlantica si troverà ad affrontare nei prossimi anni è ricco di sfide determinate dalla molteplice presenza di **fattori di instabilità sia a carattere regionale sia di natura terroristica.**
L'evoluzione della cosiddetta Primavera Araba è ancora tutta da scrivere e attualmente, a seguito della caduta dei vecchi regimi e del conseguente vuoto di potere creatosi, **ha comportato la deflagrazione di una serie di conflitti etnici e religiosi, di antica data, in tutta l'area del Sahel.** Contemporaneamente, in Siria, quella che inizialmente si era caratterizzata come una rivoluzione popolare contro il regime di Bashar Assad, s**i è lentamente trasformata in una guerra civile dalle forti connotazioni settarie, capace di degenerare in un conflitto in grado di coinvolgere diversi attori regionali.**

La contemporanea modifica della natura dell'impegno dell'Alleanza nel contesto afghano, con un sostanziale ritiro di uomini e mezzi nel corso del 2014, metterà la NATO nella migliore posizione per riorganizzare le proprie priorità e focalizzarsi nel contrasto di una **minaccia che, sempre più spesso, prenderà connotati ibridi assumendo sembianze di volta in volta terroristiche, cibernetiche, o convenzionali .**

Per quanto riguarda il primo aspetto, è importante sottolineare che il saccheggio degli arsenali libici nel 2011 e di quelli siriani, ancora in corso, **ha permesso a diversi gruppi di matrice salafita e qaedista di venire in possesso di grandi quantità di armi leggere e pesanti** e di disporre anche di sistemi d'arma più sofisticati e pericolosi, dal punto di vista della proliferazione, come **i Manpads e i missili anticarro.** Se a questo, si aggiunge anche la circostanza che tali formazioni rappresentano la componente più motivata ed addestrata tra le varie milizie dell'area, si intuisce come **sia imperativo disporre di adeguati sistemi ISR al fine di evitare per quanto possibile, in futuro, sorprese strategiche** come, ad esempio, l'attacco di Bengasi costato la morte dell'ambasciatore Stevens (nel settembre 2012) o l'offensiva islamista in Mali che, senza l'intervento francese (Operazione Serval gennaio 2013), avrebbe condotto al collasso di un Paese chiave dell'area del Sahel. Infine, ll monitoraggio delle attività delle formazioni terroristiche nelle aree di crisi,

rappresenta la principale tutela per prevenire attentati terroristici sul suolo dei Paesi NATO visto e considerato che, proprio questa settimana, il Ministro degli Interni britannico Theresa May ha ricordato come la guerra civile siriana si stia trasformando in una palestra di allenamento per potenziali terroristi britannici e, per estensione, europei. A questo proposito un grande passo in avanti sarà compiuto con il completamento del programma AGS Alliance Ground Surveillance basato sui 5 droni RQ-4 Global Hawk in fase di acquisizione da parte dell'Alleanza e basati a Sigonella. Infatti, l'AGS consentirà, finalmente, agli Alleati di disporre di una piattaforma in grado di concorrere specificatamente alla creazione di una J-ISR capability nel quadro dei dettami del nuovo concetto strategico dell'Alleanza, espressi a Lisbona nel 2010, **che comprendono tre pilastri fondamentali: Sicurezza Cooperativa, Gestione delle Crisi e Difesa Collettiva.**

Per quanto concerne invece la minaccia cibernetica, va rimarcato come, lo scenario post-2020 vedrà il dominio cyber quale sicuro campo di confronto per qualunque genere di operazione militare. Dalla comparsa del famigerato malware Stuxnet, prima arma cyber offensiva conosciuta della storia, nel 2010, **gli attacchi cibernetici alle reti di comando e controllo, alle reti di distribuzione dell'energia e ai network della difesa aerea rientreranno nel normale spettro delle minacce da affrontare.** E' altresì noto che diversi attori statuali stiano dedicando ingenti risorse umane ed economiche allo sviluppo di capacità cyber offensive sempre più sofisticate. I progetti NATO di Smart Defence prevedono un approccio collettivo alla problematica della cyberdefence, tuttavia è sempre più evidente che l'aspetto "difensivo" costituisce solo una faccia della medaglia. Infatti, la predisposizione di un'arma d'attacco cyber ha costi decisamente inferiori rispetto alla creazione di un sistema difensivo in grado di proteggere tutti i possibili target. **Di conseguenza, diversi Paesi occidentali si stanno apertamente preparando ad affiancare capacità cibernetiche offensive di "deterrenza" quale ulteriore misura di dissuasione nei confronti di potenziali attaccanti.** Tale approccio è stato annunciato pubblicamente dalla Francia nel suo Libro Bianco della Difesa 2013 (in cui si cita testualmente la possibilità di risposta cibernetica proporzionale all'attacco subito) e, più recentemente, dal Segretario alla Difesa britannico Philip Hammond. Se, per il momento, sembra che le capacità offensive in ambito cyber saranno sviluppate secondo direttive ed esigenze prettamente nazionali, è auspicabile che la NATO, seguendo lo stesso approccio adottato per il programma AGS, possa in futuro sviluppare proprie capacità di ricognizione cibernetica magari mettendo a sistema l'expertise esistente presso il Centro di Eccellenza di Tallin.

Infine, per quanto riguarda la minaccia convenzionale è opportuno rimarcare come, a fronte di un **generalizzato calo delle risorse destinate alla Difesa in gran parte dei Paesi NATO (certificato dal rapporto SIPRI 2013), fa da contraltare un forte aumento degli investimenti nei Paesi del Golfo, del Nord Africa e dell'Asia.** Il trend dei Paesi dell'Alleanza vede un continuo ridimensionamento quantitativo degli strumenti militari ed è quindi auspicabile che parte delle risorse risparmiate per esigenze di bilancio, possa essere reinvestita nel miglioramento qualitativo dei mezzi in servizio e nello sviluppo dei cosiddetti moltiplicatori di forze. **In tale contesto, un ruolo primario spetterà ai sistemi ISR per migliorare la "situation awareness" delle forze alleate** e consentire loro di mantenere e, se possibile, incrementare il vantaggio competitivo attuale disponendo di informazioni sempre più accurate, tempestive e decisive per lo svolgimento dell'azione. Questo risultato, potrà essere ottenuto non solo grazie all'introduzione di sistemi ISR sempre più performanti, ma anche lavorando sull'interoperabilità delle piattaforme stesse al fine di costruire una picture derivante dalla "sensor fusion" di più sistemi. La necessità di mantenere la supremazia tecnologica nel campo di battaglia networkcentrico è un'esigenza ben presente anche al di fuori del contesto NATO nell'ambito delle Forze Armate dei Paesi più avanzati tecnologicamente. Infatti, un simile approccio è in fase di implementazione a partire dall'anno in corso anche da parte delle Forze Armate Israeliane che, a causa dei limiti di bilancio, ritireranno i mezzi pesanti ora in riserva ed anche i velivoli e i mezzi navali più anziani, reinvestendo tutte le risorse disponibili **sull'ammodernamento della vetronica e della sensoristica delle piattaforme più recenti oltre che sulle capacità C4I e sui droni.**

La capacità di disporre della migliore situation awareness e, di converso, di poterla negare all'avversario, rappresentano uno degli obiettivi primari nella conduzione di operazioni militari nel contesto di questo che viene definito come il "secolo dell'informazione". Tuttavia l'evoluzione delle smart technologies e il progressivo accesso a tali tecnologie anche nelle aree di crisi **ha generato un potenziale di comunicazione e di capacità di mobilitazione impossibile da ignorare e fino ad oggi praticamente sconosciuto in quelle zone del mondo. La rete internet e i social network hanno avuto un ruolo fondamentale nello sviluppo della cosiddetta Primavera Araba rappresentando un potentissimo veicolo di diffusione di idee, desideri e aspirazioni sociali. Tuttavia, tali tecnologie stanno anche consentendo ai gruppi terroristici di disporre di affidabili e spesso anonime reti di comunicazione e applicazioni da utilizzare per i loro fini.** Il trend

evolutivo si sta modificando rispetto ad un pur elaborato utilizzo in termini propagandistici e di controinformazione di vari accout sui più popolari social network come Facebook, Twitter e Youtube. Secondo i primi report disponibili sull'attacco terroristico al WestGate mall di Nairobi, pare infatti **che alcuni degli attentatori (membri del gruppo Al Shabab) potessero comunicare in tempo reale attraverso Twitter con i vertici dell'organizzazione ricevendo ulteriori istruzioni e aggiornamenti in diretta sulla situazione intorno a loro.** Inoltre, la diffusione di smartphone e tablet dotati di fotocamere e perennemente collegati alla rete renderà le operazioni in ambiente urbano sempre più facilmente monitorabili. **Le attività al WestGate di Nairobi, sono state seguite minuto per minuto sui social network con aggiornamenti costanti sulla natura del dispositivo di reazione keniota diffondendo informazioni potenzialmente molto sensibili per lo svolgimento del blitz volto a liberare gli ostaggi.** Anche il fronte siriano sta vedendo un massiccio utilizzo di tecnologie commerciali ai fini più disparati. Le normali applicazioni cartografiche, sono utilizzate dalle varie forze in campo per costruire mappe della situazione quartiere per quartiere relative al proprio schieramento e a quello nemico da condividere con le proprie unità. Inoltre, svariate applicazioni per tablet sono state proficuamente riadattate per agevolare il puntamento di mortai o remotizzare artigianalmente postazioni per sniper. Tali utilizzi imprevisti di tecnologie commerciali a fini militari si aggiungono a quelli già sperimentati dai talebani afgani che, ad esempio, utilizzano normali telecamere e fotocamere civili in modalità "notte" per individuare le emissioni IR degli apparati di visione notturna delle Forze NATO acquisendo così una rudimentale capacità di targeting notturno.

Ulteriori elementi di criticità vengono portati da tutti i software free che garantiscono l'anonimità all'utente e la crittazione dei dati scambiati. Il più famoso rappresentante di questa tipologia di applicativi è sicuramente **"Tor"** citato anche recentemente per essere entrato nell'obiettivo dell'NSA americana. E' evidente come sistemi simili, oltre ad un utilizzo perfettamente legale e volto a tutelare il bene supremo della privacy dell'individuo (segreti industriali, dati personali ecc) **possono essere ampiamente utilizzati per ogni tipologia di scambio illecito di informazioni o di pianificazione di attività criminose o terroristiche e, per questo motivo, diventano un target per le agenzie di intelligence.**
Il monitoraggio della rete, dei social network e delle attività che in essa si svolgono già oggi rappresenta una sfida per le istituzioni dedicate alla sicurezza e alla difesa dei Paesi e ancora di più lo sarà in futuro. Per quanto queste attività siano di enorme importanza per la sicurezza nazionale esse, come il recente caso dell'NSA americana

insegna, si scontrano con le esigenze di rispetto della privacy degli individui che sono fortemente sentite nell'ambito delle democrazie occidentali. E' quindi necessario individuare un compromesso che risulti sufficientemente soddisfacente tanto per le agenzie di intelligence quanto per le opinioni pubbliche. Per quanto poi i social network possano rappresentare un obiettivo di legittimo interesse per le organizzazioni militari e quindi anche per la NATO, è opportuno considerare che alcuni Paesi demandano le attività di intelligence ad organismi esclusivamente civili. Se consideriamo il caso dell'Italia ad esempio, i servizi di intelligence (DIS, AISE e AISI) sono appunto di esclusiva natura civile e rispondono direttamente alla Presidenza del Consiglio. **E' quindi evidente che eventuali future iniziative comuni della NATO nel settore ISR cibernetico dovranno tenere conto della necessità, in alcuni Paesi, di relazionarsi con entità non militari**.

In conclusione, è importante sottolineare che, secondo le stime degli operatori di settore, il mercato C4ISR **nel periodo 2013-2023 si quantificherà a livello mondiale in un valore prossimo ai 94,4 miliardi di dollari rappresentando uno dei comparti più dinamici dell'industria mondiale della difesa.**
Il mantenimento, quindi, della supremazia nelle tecnologie informative anche negli scenari post 2020, determinerà in modo sostanziale il vantaggio competitivo della NATO rispetto a tutte le potenziali minacce, siano esse statuali o terroristiche, e consentirà di compensare la diminuzione quantitativa degli strumenti militari dei Paesi membri causata dalla scaristà di risorse economiche in questa fase storica. **A parere del Ce.S.I. è importante che lo sviluppo delle componenti ISR più tecnologicamente avanzate e costose avvenga in un'ottica Joint NATO al fine di garantire il migliore utilizzo possibile delle scarse risorse economiche disponibili.** Tale percorso, se sarà ulteriormente coordinato con futuribili sviluppi della dimensione militare dell'Unione Europea, consentirà anche di evitare costose duplicazioni e problemi di interoperabilità tra Alleati determinati da scelte esclusivamente nazionali di corto respiro. Il framework, **da utilizzare con convinzione, è quello appena sviluppato con il programma AGS possibilmente replicandolo per analoghe iniziative a livello di cyberwarfare e comunicazione strategica.**