Dai network informatici alla guerra nello spazio elettromagnetico e cibernetico: il cambio delle dinamiche del campo di battaglia nell'era digitale

di Mario SECHI

Lo spazio cibernetico è stato globalmente riconosciuto come la quinta dimensione del campo di battaglia in aggiunta alla dimensione terrestre, navale, aerea e spaziale

Nell'ultimo summit della NATO tenutosi recentemente in Galles i Capi di Stato e di Governo delle nazioni dell'Alleanza Atlantica hanno riconosciuto che la difesa cibernetica (*cyber defence*) deve essere parte del processo decisionale e che la pianificazione di operazioni militari deve, d'ora in poi, affrontare le problematiche ad essa connessa. Tuttavia, ad oggi, la dottrina della NATO rimane in prospettiva puramente difensiva mirando alla protezione tecnica dei soli network appartenenti alla propria struttura, ovvero il *NATO classified network* ed il *NATO unclassified network*. Inoltre, la suddetta protezione si basa solo su misure difensive passive inerenti le reti, tralasciando al momento

azioni difensive attive o azioni offensive, ovvero attacchi cibernetici contro potenziali aggressori. In verità, le singole nazioni della NATO non negano l'utilità della difesa attiva e dell'attacco, ma al momento le ritengono prerogativa del NAC (*North Atlantic Council*), ovvero il livello decisionale più alto. Muovendosi a livello operativo e tattico ci si rende facilmente conto di come un Comando a livello *Joint* o *Component (Land, Air, Maritime o Special Operations)*, specialmente se schierato in area di operazioni, non disponga né di una *policy* adeguata né tantomeno degli strumenti necessari ad affrontare una realtà così particolarmente articolata, dove la corsa ad individuare le soluzioni idonee ad affrontare l'evoluzione delle minacce e dei relativi rischi ha ritmi elevatissimi, nettamente accelerati rispetto ai normali tempi decisionali di strutture complesse quali l'organizzazione politico/militare della NATO.

A tal proposito è opportuno ricordare che il concetto di difesa cibernetica va decisamente oltre la semplice protezione delle reti informatiche (attività di difesa passiva prettamente tecnica, cd. *INFOSEC*) che ha lo scopo di garantire *'confidentiality, integrity e availability'* delle reti informatiche. A livello NATO tale funzione viene principalmente assicurata dalla *NATO Communications and Information Agency* (NCIA).

Lo spazio cibernetico è stato globalmente riconosciuto come la quinta dimensione del campo di battaglia in aggiunta alla dimen-

sione terrestre, navale, aerea e spaziale, conseguentemente, come per le altre dimensioni, anche la *cyber* deve essere strutturata e gestita con una visione olistica e omnicomprensiva.

Appare evidente che se si tiene conto della specificità dello spazio cibernetico, ovvero la peculiarità dei suoi mezzi di trasporto (reti informatiche e spettro elettromagnetico), delle tattiche e degli armamenti (*social engineering*, *malware*, e via dicendo) e dell'addestramento delle forze, risulta evidente che esso debba essere gestito da un altrettanto specifico Comando - CYBERCOM - così come avviene per le altre dimensioni (LANDCOM, MARCOM, AIRCOM, SPACECOM), soluzione peraltro già adottata dalle forze armate degli Stati Uniti. A tale entità verrebbe devoluto il Comando e Controllo di tutte le capacità inerenti la quinta dimensione secondo la metodologia del DOTMLPF (*Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities).*

La minaccia cibernetica, in passato area di interesse per soli esperti, è oggi nota anche all'opinione pubblica, almeno nella percezione dell'esistenza del rischio. A titolo di esempio, e per evidenziarne lo sviluppo quale vera e propria Linea Operativa di un progetto terroristico, si riporta l'estratto di un articolo proveniente da un sito jihadista dove vengono dettagliate le attività cibernetiche di supporto ai *mujahiddin* sul terreno e da effettuare contro una coalizione militare internazionale:

- disabilitare e paralizzare le reti di comunicazione, comando e controllo sul campo di battaglia, attraverso attacchi verso le reti GPS, GSM, GPRS;
- distruggere le attività informatiche di banche, oleodotti e sistemi di navigazione;
- attaccare i sistemi di scambio di dati del nemico e paralizzare la vita nei loro paesi;
- disturbare gli attacchi missilistici e le attività nemiche dei droni e re-indirizzare i missili da dove sono partiti.

Il Comando del Corpo di Armata di Reazione Rapida della Nato (NRDC ITA HQ) ha riconosciuto questa esigenza dando vita ad un progetto di individuazione ed organizzazione della capacità di *Cyber Defence* (CD) che al momento è unico nell'ambito della *NATO Force Structure*.

Pur riconoscendo la specificità della *cyber defence*, la trasversalità delle minacce che la contraddistinguono e l'influenza che tali minacce hanno ai vari livelli (dallo strategico al sub-tattico), non si può non tenere in considerazione l'attuale scarsità di risorse, almeno nel breve termine. Per tale motivo NRDC ITA, durante la fase di validazione quale *Joint HQ*, ha optato per un approccio multidisciplinare con la creazione di un *Cyber Defence Working Group* (CDWG), con elementi di staff provenienti dall'area J2, J3 e J6, che hanno sopperito alla mancanza di una struttura e di personale dedicato garantendo una funzione attiva nel *core process* decisionale di gestione di una crisi.

Da un punto di vista concettuale, durante l'esercitazione NATO Trident Jaguar 2015, il Comando NRDC ITA ha affrontato la prospettiva *Cyber Defence*, operando lungo 2 linee di azione distinte:

1. Consapevolezza della minaccia: briefing informativi sulle minacce cibernetiche verso le reti militari e civili,

le minacce provenienti dai social media, misure pratiche di riduzione del rischio e distribuzione di opuscoli informativi a tutto lo staff.

2. Costituzione di un core team di difesa cibernetica: con esperti provenienti dalle aree J2, J3, J6 e attraverso il *CD Working Group*, al fine di supportare, coordinare e deconflittuare le attività dello staff nelle aree connesse con la *cyber defence*, il *cyber incident handling*, la *business continuity* e il *disaster recovery*.

Inoltre grazie alle risorse fornite dalla nazione è stato possibile formare un numero adeguato di personale con specifiche *expertise* nelle aree del *vulnerability assessment*, nella *cyber security* e *security* in generale, *cyber incident handling* e *disaster recovery*, tale da offrire alla *host nation*, qualora necessario, il supporto per la protezione delle infrastrutture critiche del settore pubblico e privato che hanno, direttamente o indirettamente, effetti sulle operazioni militari.

Dopo questa fase transitoria ci sono all'orizzonte diverse alternative, ancora peraltro a livello di studio. Una delle opzioni all'esame, al fine d'inserire la capacità di *cyber defence* nel giusto contesto, è quella che vedrebbe la trasformazione dell'attuale SEWOC (SIGINT *and Electronic Warfare Operations Centre*) in un CEMOC (*Cyber and Electro-Magnetic Operation Centre*). Questo tipo di soluzione è in parte simile a quella già adottata dalle forze armate statunitensi che, con l'introduzione del concetto di *Cyber and Electro-Magnetic Activities* (CEMA[1]), hanno creato l'area funzionale di convergenza delle *cyberspace*

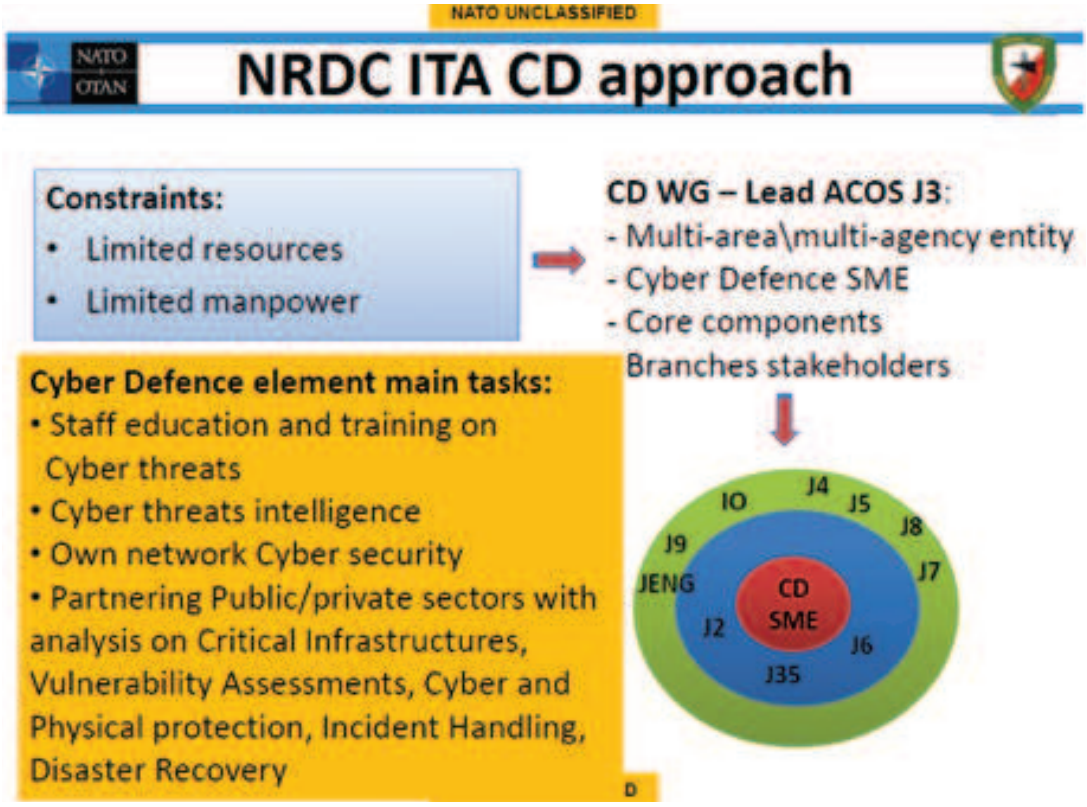
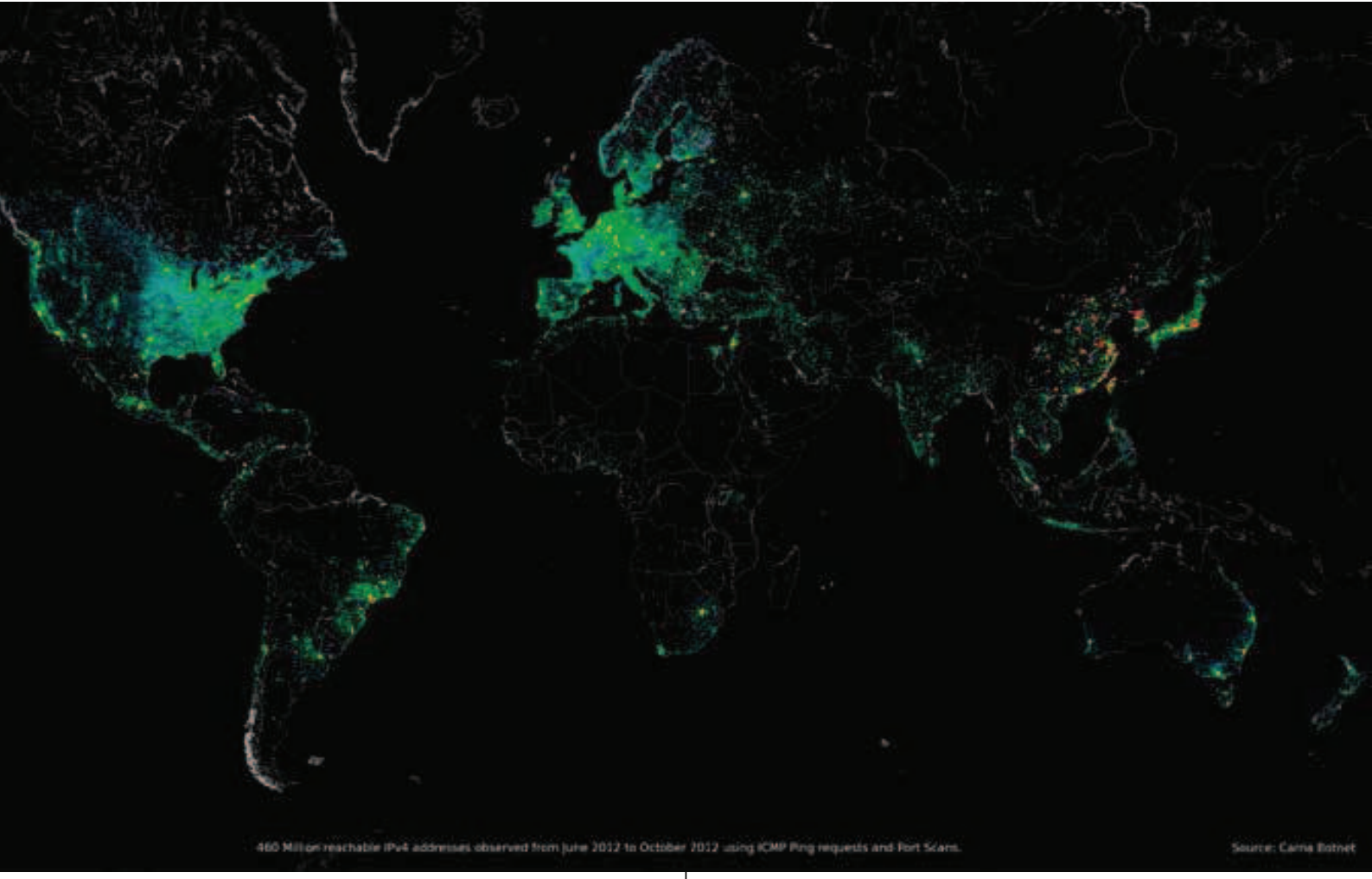


Tavola 1 - Il contesto e lo scopo del Cyber Defence Working Group

1 *FM 3-38 Cyber Electromagnetic Activities – Ed. Febbraio 2014.*



operations, l'*electronic warfare* e le *spectrum management operations*. Questa scelta è dettata principalmente dalle analogie presenti tra la *EW* (*electronic warfare*) e la *cyberwarfare* in termini di fattori tecnologici ed operativi all'interno del comune spettro elettromagnetico. A titolo di esempio si possono citare le reti wireless o i sistemi di navigazione GPS, realtà sempre più presenti anche nell'ambito militare e che già oggi rappresentano il *core element* del progetto Soldato Futuro.

Di fatto, la scelta del CEMOC ottimizzerebbe le capacità già acquisite nell'area della guerra elettronica (con attività appartenenti al J2 e J3) e il già esistente coordinamento con lo *spectrum management* (J6), ampliando il quadro delle capacità esprimibili con l'aggiunta della *cyber defence*. Si tratta di una soluzione ibrida che presenta margini di miglioramento ma che comunque va a colmare una lacuna normativa e procedurale nella capacità di difesa cibernetica a livello operativo.

Tale soluzione si attaglia alle esigenze del livello *Joint HQ*. Infatti, è a livello operativo che la *cyber defence* supera la semplice esigenza di protezione del network militare per ampliare il campo di azione alle entità esterne all'organizzazione militare stessa ma aventi comunque un impatto sulle operazioni militari e il successo della missione (*End State)*. Si introduce dunque il concetto di network dei networks, ovvero l'insieme delle reti riguardanti tutte le organizzazioni che supportano o che comunque vanno a influenzare una missione militare quali per esempio: le infrastrutture critiche della *host nation*, le reti delle varie nazioni partecipanti alla missione, le reti su cui operano i fornitori locali e internazionali, e tutto ciò per il

quale non esiste uno standard comune di protezione e sicurezza, ma che necessariamente sono in qualche modo parte del *mission confederated network* contribuendo ad aumentare le criticità nei confronti della minaccia cibernetica.

A queste aree si dedica la cyber defence del Comando JTF, supportata dal *Cyber Defence Working Group*, con compiti che variano da:

- supporto alle forze della coalizione, *host nation* e le altre agenzie esterne, nell'identificazione delle vulnerabilità e l'implementazione di misure di protezione al fine di mitigare il danno e l'impatto di attacchi cibernetici contro quelle infrastrutture critiche che risultano vitali per il successo della missione stessa;
- identificazione e prioritarizzazione delle infrastrutture critiche da difendere (CPDAL, *Cyber Prioritized Defended Asset List*), individuazione e gestione dei rischi specifici;
- aggiornamento della CPDAL, in cooperazione con il *Joint Defended Asset Working Group*, al fine di assicurare che i fattori inerenti l'area cibernetica e le relative vulnerabilità siano dettagliate e condivise con la leadership.

Per concludere, appare evidente come la *cyber defence* diventi, a livello operativo, un'area interfunzionale, interforze ed interagenzia. Passando obbligatoriamente per il superamento del concetto di protezione delle reti (INFOSEC) quale essenza della *cyber defence*, si giunge ad una visione in prospettiva omnicomprensiva e multidisciplinare di protezione della spazio o dominio cibernetico (analogamente alle altre dimensioni del campo di battaglia), nel quale la forza militare, le organizzazioni nazionali e internazionali e il comparto commerciale e industriale ad essi connessi, operano per il raggiungimento della mutuata condizione finale desiderata (*End State*) così come si erano prefissati.

La specificità della materia e le qualifiche richieste al personale ad essa dedicato, stante l'assenza attuale di un iter formativo definito, genera talora difficoltà nell'individuare una soluzione funzionale applicabile nel breve periodo. In questo contesto e con questi presupposti l'opzione SEWOC potrebbe essere una valida base di partenza concettuale quale catalizzatore delle operazioni nello spazio elettromagnetico, come peraltro già contemplato nella visione della NATO nel 2010.

Una struttura che già di per sé nasce in modalità *cross-functional,* ovvero abituata a fungere da punto di contatto tra le esigenze informative (J2) per la condotta delle operazioni (J3) salvaguardando il corretto uso dello spettro elettromagnetico (J6). Essa infatti appare quanto mai idonea a fungere da *framework* di un *Cyber and Electromagnetic Operations Center,* previa la dovuta aggiunta di personale competente in *cyber defence*, sia in termini di capacità procedurale (tra funzioni operative) sia in termini di capacità operativa, poiché già naturalmente orientati alla condivisione dell'analisi e dell'impiego di quello spettro elettromagnetico che racchiude in esso le radio frequenze, i GPS, le reti WiFi, le comunicazioni satellitari e le comunicazioni cellulari mobili.