La dipendenza statunitense dalla rete: vulnerabilità, criticità e punti deboli della Network Centric Warfare (NCW)[1]

La guerra network-centrica (NCW) è definita come un concetto di operazioni basato sulla superiorità dell'informazione che genera una maggiore potenza di combattimento collegando in rete sensori, decisori e combattenti al fine di ottenere una consapevolezza condivisa, una maggiore velocità di comando, un più alto ritmo delle operazioni, una maggiore letalità, una maggiore sopravvivenza e un elevato livello di auto-sincronizzazione. In sostanza la *Network Centric Warfare* traduce la superiorità dell'informazione in potenza di combattimento, collegando efficacemente le diverse capacità nello "spazio di battaglia"[2].

La capacità militare degli Stati Uniti è di fatto dipendente dalla tecnologia di rete al punto che la dottrina stessa su cui si basa l'impiego dello strumento militare impone l'integrazione della tecnologia di rete in quasi tutti gli ambiti, in particolare proprio la *Network Centric Warfare* (NCW). Sebbene l'orientamento generale sia quello di impiegare personale e sistemi ad alta specializzazione, emerge sempre più la necessità di disporre di capitale umano in grado di operare anche all'interno della "vecchia dimensione analogica" nel caso in cui i sistemi informatici dovessero cessare di essere funzionali, in tutto o in parte. È quello che Matthew Crosston, nel suo sagace articolo *The Millenials' war: dilemmas of network dependency in today's military*, chiama "effetto MacGyver", ossia la capacità di sviluppare e disporre di talenti e soluzioni che consentano di condurre efficacemente operazioni militari anche quando i sistemi principali siano fuori uso (*offline*) e non vi sia la possibilità di accedere o attivare sistemi di rete alternativi.

La crescente minaccia associata alla dipendenza dalla rete è un tema relativamente poco studiato e ancora non tenuto in debita considerazione, sia dal punto di vista politico che militare. Sebbene in ambito accademico, così come in quello operativo, siano già state evidenziate alcune preoccupazioni, queste sono, però, poste in secondo piano a fronte della vasta gamma di vantaggi legati all'integrazione della tecnologia in ogni aspetto dell'esercito, dai singoli combattenti sul campo di battaglia al sistema di comando e controllo, fino alla *leadership* a livello operativo e strategico. Gli Stati Uniti hanno le forze armate tecnologicamente più avanzate a livello globale e questo è il risultato dei grandi investimenti e della crescente fiducia nello sviluppo delle *Network Centric Operations* (NCO) a cui, di fatto, sono indissolubilmente associate, grazie all'integrazione e alla proliferazione della rete, sia per le attività di *routine* che per quelle straordinarie. Ma il sistema, creato per garantire capacità di difesa, offesa e deterrenza porta con sé – rileva Crosston – alcune vulnerabilità potenzialmente micidiali dal livello più alto (strategico) a quello più basso (tattico).

La prima di queste vulnerabilità è rappresentata dall'approccio concettuale a livello strategico – adottato dalla leadership politica e militare, e avvalorato dalle teorie concettuali e accademiche del *Network Centric Warfare* e della rivoluzione negli affari militari – che di per sé rappresenta la prima vera grande vulnerabilità di sistema poiché si basa su una fiducia incondizionata nei confronti di strumenti informatici che sono ampiamente vulnerabili.

Il secondo grado di vulnerabilità lo si trova a livello tattico, dove gli operatori e gli utilizzatori dei sistemi di rete stanno diventando dipendenti dai sistemi informatici a un livello che possiamo valutare come allarmante dato che, da un lato, la maggior parte degli operatori militari interviene attraverso un computer connesso al sistema e, dall'altro lato, le tecniche, le tattiche e le procedure

---

1 Bertolotti C. (2022), *Cyber warfare e info warfare: politiche di sicurezza e difesa,* in Anghelone F. e Carteny A. (a cura di) *Sharp Power*, Istituto di Studi Politici S. Pio V, Roma (in attesa di pubblicazione).

2 Alberts D.S., Garstka J.J., Stein F.P. (1999), *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised).

si sono tutte evolute intorno alla disponibilità e alla capacità di elaborazione in tempo reale di informazioni in rete. L'attuale generazione di militari è nativa digitale, cresciuta immersa nel sistema di rete, con una residua componente "analogica" a livello gerarchico medio-alto e alto che di fatto si è adeguata, a livello dottrinale, all'utilizzo esclusivo del sistema di rete portando a una sostanziale dipendenza da esso. Gli sforzi a livello politico sono stati fatti con l'intento di mitigare le minacce informatiche, ma ponendo in secondo piano l'opzione di una guerra in un ambiente post-attacco informatico caratterizzato dalla disponibilità di reti danneggiate, inaffidabili o addirittura dal completo isolamento della rete. I militari più anziani, attualmente in servizio, hanno maturato un'esperienza operativa che va dalla fine degli anni '80 ai primi anni '90, un periodo in cui pochissimi ambiti erano gestiti attraverso il collegamento in rete. Questa generazione viene rapidamente sostituita dai *Millenials*, la generazione di Internet che conosce il mondo digitale, che non ha mai vissuto senza una connessione Internet affidabile e prontamente disponibile di cui sono fortemente dipendenti; e nell'arco del prossimo decennio, tutti i rami delle forze armate saranno completamente composti dalla generazione di Internet[3].

Possiamo così considerare sempre più come critico il livello di dipendenza dal sistema di rete poiché, quando una rete si guasta, il lavoro si ferma, e quando il lavoro si ferma nelle forze armate, gli obiettivi operativi non possono essere perseguiti. Oggi, come ben evidenzia Crosston, quando la rete non è operativa e gli operatori sono *offline*, l'unica soluzione è quella di chiedere l'intervento dell'*help desk* e aspettare, mettendosi in coda; nel frattempo, gli operatori non sono in grado di portare a termine il proprio compito. Tutto ciò a fronte di scelte organizzative e gestionali che, nel tentativo di ridurre i costi, hanno portato al trasferimento dei servizi di assistenza lontano dagli operatori, di fatto trasformando un collaudato ed efficiente modello decentralizzato per il supporto di rete, in uno centralizzato[4]. Possiamo immaginare cosa potrebbe accadere in caso di interruzione del collegamento alla rete per un'unità impegnata in combattimento e sotto il fuoco avversario mentre tutto intorno piovono bombe da artiglieria, oppure durante un'operazione di *targeting* effettuata con un velivolo a controllo remoto che non può essere gestito? Cosa potrebbe fare l'*help desk*?

Questa crescente e sempre più radicata cultura della dipendenza dalla rete è un effetto collaterale involontario della corsa all'efficienza e alla riduzione dei costi[5]. Gli Stati Uniti possono essere definiti i campioni della gestione della rete e dell'NCW ma, paradossalmente, i Paesi in ritardo nel progresso tecnologico, se è vero che sono più deboli e lenti nei loro processi decisionale e operativi, è altresì vero che saranno avvantaggiati da un minore livello di vulnerabilità agli attacchi informatici in rete. Inoltre, poiché lo strumento militare statunitense procede a tappe forzate alla sostituzione dei tradizionali sistemi considerati "obsoleti" con la moderna tecnologia di rete, il rischio di isolamento della rete diventa sempre più reale; e questo vale anche per il settore civile, che spesso anticipa quello militare[6]. Un'evoluzione che, di fatto, potrebbe imporre una modernizzazione della forza militare che la renderebbe incapace di operare efficacemente in un ambiente senza rete.

---

3 Crosston M.-, *The Millenials' war: dilemmas of network dependency in today's military*, "Defense & Security Analysis", 33:2, 2017, pp. 94-105.

4 Ibid.

5 Robinson T., *It's the Network, Stupid! Air Power and Network Centric Warfare – Trends and Challenges*, "Military Technology", 40–8, 2010.

6 Matthew Crosston, art. cit.

BIBLIOGRAFIA

Alberts D.S., Garstka J.J., and Stein F.P. (1999), *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (revised).

Bertolotti C. (2022) *Cyber warfare e info warfare: politiche di sicurezza e difesa,* in Anghelone F. e Carteny A. (a cura di) *Sharp Power*, Istituto di Studi Politici S. Pio V, Roma (in attesa di pubblicazione).

Crosston M., *The Millenials' war: dilemmas of network dependency in today's military*, "Defense & Security Analysis", 33:2, 2017, pp. 94-105.

Robinson T. (2010), *It's the Network, Stupid! Air Power and Network Centric Warfare – Trends and Challenges*, "Military Technology", 40–8.