IL SOLE 24 ORE – 10 GENNAIO 2026

Avere informazioni è strategico nella cyber security

di Domitilla Benigni

Viviamo in un momento geopolitico caratterizzato da una guerra ibrida magistralmente descritta nel non paper del ministro Crosetto come «una aggressione subdola, costante e multidominio, che mira a destabilizzare le democrazie occidentali attraverso azioni sotto la soglia di reazione».

Quella a cui stiamo assistendo non è più dunque una minaccia teorica, ma una realtà quotidiana di attacco alla società civile il cui esempio più evidente, è la minaccia *cyber*. A questo si aggiungono gli attacchi a opera di droni malevoli che mirano a infrastrutture civili, come quelli che hanno bloccato per giorni snodi di importantissime connessioni internazionali, o all'emblematico caso dell'aereo della presidente Von der Leyen vittima di un *Gps spoofing* che ha falsificato la posizione dell'aereo e che rappresenta esattamente una guerra che non si dichiara formalmente, ma si combatte quotidianamente in ogni dominio: non un incidente tecnico, ma una dimostrazione di forza con un importante effetto di destabilizzazione, che è una delle conseguenze perseguite nei conflitti ibridi.

La prima grande consapevolezza oggi, non più solo per gli addetti ai lavori, è che i confini tra difesa militare e sicurezza civile si sono assottigliati. Non si può più parlare di guerra o pace perché viviamo in un continuum di minacce ibride che riguardano direttamente anche la società civile. La seconda certezza è che oggi i conflitti si sviluppano simultaneamente su tutti i domini: terra, mare, aria, spazio e cyberspazio, nonché in quello cognitivo con la propaganda ingannevole.

Oggi le azioni offensive o difensive vanno pensate nel multidominio. Immaginate una flotta navale in navigazione verso qualsiasi parte del mondo: dovremmo essere in grado di rilevare e neutralizzare minacce rappresentate da droni, aerei pilotati e sottomarini avversari, proteggere le comunicazioni

satellitari da attacchi *cyber*, monitorare minacce elettroniche e tutto questo deve avvenire coordinatamente e simultaneamente. Questo paradigma è alla base dei cosiddetti "sistemi di sistemi" di cui oggi si parla e che sostituiranno il modo in cui finora abbiamo pensato a navi, aerei o mezzi terrestri, isolati nelle loro operazioni.

Le comunicazioni e le azioni interconnesse tra domini avvengono dentro un ambiente che si chiama "spettro elettromagnetico" vale a dire, con estrema semplificazione, l'insieme di tutte le onde di energia che viaggiano nello spazio e possono essere riferite a comunicazioni radio, comunicazioni infrarossi, comunicazioni radar. Si tratta di tutte le informazioni volontarie o involontarie che vengono scambiate durante un'operazione.

Avere il management dello spettro significa quindi poter abilitare lo scambio di dati dentro lo scenario operativo e quindi avere la superiorità informativa per poi usarla a servizio di azioni difensive e offensive. Oggi se si impiegano 24 ore per capire di essere sotto attacco e altre 12 per decidere come rispondere, si è già perso.

Per questo motivo sono necessari campioni nazionali nel governo dello spettro elettromagnetico e con asset e capacità proprietarie nella *cyber intelligence* e *cyber security*. Aziende che grazie ai propri sistemi capacità abilitino le operazioni nel multidominio e permettano di avere la superiorità informativa in ogni dominio, compreso lo spazio e il *cyber*.

Per le ragioni appena indicate aziende come quella che rappresento e che possiedono tecnologie sovrane in grado di assicurare difesa e sicurezza contro l'instabilità generata dei conflitti ibridi devono sentirsi direttamente chiamate in causa dal non paper del ministro Crosetto.

In questo momento storico, dopo decenni, si torna a parlare delle necessità di assicurare una difesa solida e tecnologie indipendenti da catene di approvvigionamento instabili o a rischio. Questo è il momento giusto per ragionare come italiani ed europei sulle priorità di investimento, evitando duplicazioni nella collaborazione tra i campioni europei, nella definizione di requisiti comuni e sulla

necessità di accrescere competenze stem affinché l'essere umano resti colui che sappia governare l'algoritmo.

Ceo e COO Elt Group