IL SOLE 24 ORE – 6 DICEMBRE 2025

L’effetto deterrente della cyber Guerra fredda

di Pierguido Iezzi

L’arma fine di mondo del dottor Stranamore non funziona più. Lo scenario della deterrenza nucleare che aveva dominato la Guerra Fredda nel ’900, basato sulla teoria della mutua distruzione assicurata – nota come MAD (*Mutual assured destruction*) – che nella commedia di Kubrik assurge a dottrina, è completamente mutato nel contesto digitale in cui il quinto dominio del cyberspazio non assicura più la simmetria della guerra convenzionale, bensì apre gli infiniti orizzonti di una guerra ibrida in cui azioni, reazioni e attribuzioni non hanno più alcuna certezza.

Allo schema chiaro e brutale fatto di arsenali atomici dichiarati, dottrine pubbliche e sistemi di *early warning*, si è sostituito un equilibrio instabile, fondato su una insicurezza sostanziale. Un attacco cyber contro infrastrutture critiche non garantisce infatti né il risultato operativo né il controllo degli effetti collaterali, che in un domino incontrollato possono provocare danni anche per l’attaccante: il rischio? È una guerra batteriologica digitale, devastante ma impossibile da contenere.

L’attribuzione dell’aggressore poi è sempre contestabile, sul piano tecnico, politico e giuridico. Manca poi una soglia condivisa su quando un’azione digitale divenga atto di guerra. A ciò si aggiunge l’assenza di una vera conoscenza di sé e dell’avversario: nessuno è oggi in grado di sapere con certezza quanta resistenza e quanta resilienza abbia davvero il proprio sistema e quello dell’avversario davanti a un attacco prolungato, perché la tenuta reale si misura solo nel vivo della crisi.

Se il MAD impediva che il dito esitasse costantemente sul bottone rosso dell'attacco nucleare, allora, che cosa tiene distanti i polpastrelli dalla tastiera della Guerra Fredda Digitale? Il fatto che tutti siano esposti e che nessuno sia in grado di calcolare il punto di caduta di un'azione ibrida.

Qui entra in gioco il paradosso di questa fase storica. La forza cyber rappresenta la leva della deterrenza: sapere che l'avversario può rispondere, in modo imprevedibile e costoso, frena la tentazione di colpire. La non piena conoscenza degli effetti di una guerra ibrida "liberata" – blackout sistemici, collasso dei servizi, perdita di dati strategici, crisi di fiducia nei mercati e nelle istituzioni – diventa una utile ignoranza: tutti percepiscono che la posta in gioco è enorme, ma nessuno si sente abbastanza sicuro per spingersi oltre una certa soglia.

Non abbiamo davvero ben presente cosa significhi vivere settimane senza reti elettriche stabili, sistemi finanziari affidabili, ospedali operativi e flussi informativi non manipolati.

Eppure, uno scenario del genere è oggi del tutto possibile.

Questa opacità contribuisce a evitare la prova di forza totale: è un equilibrio basato sulla paura di ciò che non si conosce fino in fondo.

È in questo quadro, pertanto, che vanno lette le parole dell'Ammiraglio Cavo Dragone. Non una dichiarazione di guerra, ma una mossa di deterrenza. Che arriva da lontano, maturata nel corso di un processo le cui tappe sono ben evidenti.

E trova non a caso eco nel documento del Ministero della Difesa "Il contrasto alla guerra ibrida: una strategia attiva", in cui si legge che l'Italia «vive già dentro un conflitto non dichiarato» fatto di cyber attacchi, coercizione economica e campagne di disinformazione, cui serve una risposta strutturata, attiva e multidominio.

Da Bruxelles, quindi, parla Cavo Dragone e da Roma il ministro Crosetto risponde parlando la stessa lingua di deterrenza in cui il dominio cyber regge una stabilità intrinsecamente instabile fra Nato e Russia.

La reazione di Mosca conferma che il messaggio è stato ben percepito: non una cyber-offensiva imminente, ma un avvertimento. Se la Russia continua a usare la guerra ibrida contro l'Occidente, la Nato non esclude più azioni preventive nel dominio digitale.

Alle parole devono però corrispondere i fatti.

Se l'obiettivo è questo servono il riconoscimento del dominio cyber come spazio di difesa nazionale, il potenziamento del Cor in senso interforze, una riserva cyber che attinga ai saperi e alle conoscenze del settore privato, dei centri di ricerca e delle università e norme chiare su cosa è consentito fare in termini di "difesa attiva" e contrattacco. Solo cosi l'Italia sarà base credibile in una Nato pronta a rispondere anche nel cyber nella prossima crisi globale, che si giocherà sulla capacità di reggere e dissuadere nella guerra fredda digitale già in corso.