In punta di anfibi

di ISABELLA RAUTI*

La cittadella cibernetica della Difesa italiana

Nel cuore di Roma nord c'è una vera e propria cittadella informatica. È il Comando per le operazioni in rete (Cor), che ha il compito di coordinare le attività di protezione cibernetica delle Forze armate e del ministero della Difesa. L'operatività del Cor Difesa è stata ufficialmente annunciata ad Ancona nel febbraio scorso, durante lo svolgimento di ItaSec, la conferenza italiana sulla sicurezza informatica, evidenziandone la finalità di difesa dello spazio cibernetico.

Il comando – posto alle dirette dipendenze del capo di Stato maggiore della Difesa – è stato costituito il 9 marzo e, sul piano ordinativo-organico, nasce dalla fusione in area interforze, tra i preesistenti comandi C4 difesa (Communications, command & control, computer) e interforze per le operazioni cibernetiche (Cioc). Il Cor Difesa offre il supporto tecnico-operativo al ministero della Difesa nell'ambito della sua partecipazione al Dipartimento informazioni per la sicurezza (Dis) e al suo Nucleo per la sicurezza cibernetica (Nsc), previsto in attuazione del Quadro strategico nazionale per la sicurezza del *cyber*-spazio.

Il Cor rappresenta il fulcro organizzativo delle scelte della Difesa in termini di riordino e di razionalizzazione del settore. Un comando unico e di alto rango per la gestione tecnico-operativa in sicurezza di tutti i sistemi in servizio, per armonizzare le competenze dei diversi attori già operanti nel settore (incluse le componenti di postura di *cyber-defence*, di operazioni di sicurezza e la protezione dalla minaccia cibernetica) e per consolidare la dimensione interforze delle "Cyber network operations".

La centralizzazione e la riorganizzazione in un'architettura omogenea di un complesso di competenze e servizi risponde all'esigenza di rafforzare le capacità di difesa dello spazio cibernetico nazionale, di fronte all'evoluzione sempre più veloce della minaccia *cyber* e del suo crescente rilievo negli scenari di conflitto e nei metodi di lotta "asimmetrica".

Gli attacchi *cyber* possono essere condotti da attori statuali ma, nella rete globale, anche in modo occulto da soggetti non statuali e secondo le diverse e le molteplici modalità di *software* malevoli (i cosiddetti *malware*). Ormai, il settore Ict rappresenta una trincea nel dominio cibernetico e un asse strategico per la sicurezza di ogni sistema-Paese. Ed è in questo contesto globale di rischi informatici che si inquadrano, in ambito Nato, la dichiarazione del *cyber-space* come "dominio operativo" equiparato a quelli tradizionali, nonché in ambito Ue la direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi, meglio nota come Nis (Network and information security"). Ed è per le crescenti esigenze di *cyber-defence* che a livello nazionale si sta investendo sulle infrastrutture e gli assetti di "Information and communication technology", nella speranza che la Nato accetti di inserire le spese per la sicurezza informatica nella quota prevista del 2% che gli alleati devono – o dovrebbero – destinare alla Difesa.

Ma il perimetro di sicurezza nazionale cibernetica e la vulnerabilità delle reti informatiche riguardano tutto e tutti, nessuno escluso: operatori nazionali pubblici e privati, amministrazioni pubbliche, istituzioni locali, aziende, i dati personali di ognuno di noi e la nostra vita quotidiana. E non sappiamo neanche quanto.

*senatrice, giornalista e scrittrice, ufficiale dell'Esercito (Ris. Sel.)