In punta di anfibi

di ISABELLA RAUTI*

Se le trincee si spostano sul web

Quando su questa rubrica (ad aprile e a settembre 2020) affrontammo il tema dei *cyber*-attacchi e, in particolare, quello del furto dei dati sanitari, non sapevamo quanto sarebbe accaduto in seguito, ma era chiaro da tempo che la "sfida delle sfide" era (ed è) quella della sicurezza cibernetica. E della difesa del *cyber*-spazio si occupa anche il Comando per le operazioni in rete (Cor), con sede a Roma, che ha il compito di coordinare le attività di protezione cibernetica delle Forze armate e del ministero della Difesa. Un ruolo fondamentale spetta, ora, alla neonata Agenzia per la cyber-sicurezza nazionale, destinata, appunto, a fronteggiare le minacce cibernetiche e a rispondere alle esigenze di una sfida tecnologica globale, in cui la *cyber-security* è diventata il principale terreno di competizione degli Stati. Il comparto *cyber* è in continuo divenire e rappresenterà, quindi, sempre di più una frontiera strategica. In questo contesto un risvolto importante e preoccupante è quello della pirateria informatica dei dati personali e di quelli sanitari. Sono in costante aumento gli attacchi *cyber* sia ai fini di estorsione, sia terroristici: in dodici mesi (dal 31 luglio 2020 al primo agosto 2021) si sono verificate cinquemila aggressioni, secondo il Viminale, a fronte delle 460 del periodo precedente. Il settore dell'assistenza sanitaria è uno dei *target* più minacciati dal *cyber-crime*, non solo per l'hackeraggio ai *server* o le recenti frodi dei *Qr code* e delle chiavi dei Green pass, ma anche per le più sofisticate incursioni informatiche, in grado di far saltare l'intero sistema di una nazione.
Lo spazio cibernetico nazionale è diventato un *asset* strategico per la sicurezza del sistema-Paese ed è sempre più urgente implementare il progetto del Polo strategico, cioè il *cloud* nazionale, già previsto.
L'ottica con cui guardare allo spazio cibernetico infatti è quella di considerarlo un dominio da difendere, rispetto ai molteplici e multiformi attacchi che possono essere condotti sia da attori statuali, sia da soggetti non statuali che agiscono, nella rete globale, con *software* malevoli (*malware*). È una vera e propria minaccia potenziale e permanente alla sicurezza, una nuova frontiera, anzi un nuovo scenario di guerra asimmetrica.
È l'intero settore Itc che può essere considerato "una trincea". Nello spazio operativo cibernetico, infatti, i rischi informatici sono inquadrati (nella dichiarazione del *cyber-space* della Nato) come "dominio operativo" equiparato a quelli tradizionali "air, land, maritime". Lo stesso vale in ambito Ue, con la direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi, più nota come Nis.
Siamo nell'era della transizione digitale. Insieme con gli innumerevoli vantaggi, il processo porta con sé un aumento dei rischi di vulnerabilità. Ciò richiede, contestualmente, un crescente sistema di tutela delle informazioni e degli strumenti che garantiscano la sicurezza, nonché investimenti sulle infrastrutture per l'acquisizione dei requisiti necessari di affidabilità.
Siamo tutti immersi nel digitale globale. Con i nostri Pc e i nostri *smartphone* viviamo una dimensione di connessione permanente ai *network*; inevitabilmente ognuno di noi è portatore di strumenti e di sistemi informatici che costituiscono potenziali "finestre" nelle quali il nemico può introdursi e rubare i dati. Tale rischio diffuso deve imporre maggiore consapevolezza individuale e determinare un impegno costante nella difesa dello spazio cibernetico che coincide pienamente con ogni aspetto dell'interesse nazionale.

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