la Repubblica
Dir. Resp.: Maurizio Molinari
www.datastampa.it Tiratura: 217203 - Diffusione: 187327 - Lettori: 1624000: da enti certificatori o autocertificati
29-NOV-2020
da pag. 1-37
foglio 1 / 2
Superficie: 44 %

L'editoriale

Difesa cyber e interesse nazionale

di **Maurizio Molinari**

A metà dicembre la Commissione Ue adotterà la nuova strategia europea di cybersicurezza riconoscendo l'urgenza di proteggersi su questo fronte, di essere più autonoma nello sviluppo della tecnologia e di aumentare gli investimenti nell'innovazione. E ciò significa che tutti i partner dell'Unione, Italia compresa, sono chiamati a impegnarsi su questo terreno in tempi assai stretti.
L'urgenza della difesa dalle minacce cyber è stata affermata con chiarezza dalla presidenza di turno tedesca, in occasione dell'ultimo Consiglio Europeo, con un documento sui "crescenti pericoli di penetrazione della sicurezza collettiva dovuti all'aumento dell'uso di prodotti elettronici da parte dei cittadini".
È una situazione di allarme dovuto, secondo un recente rapporto dell'Agenzia Ue per la difesa cyber (Enisa), alla "pandemia che sta mettendo a dura prova la resilienza cyber delle nostre protezioni" perché molti operatori si trovano a lavorare da casa e le linee di protezione sono di conseguenza assai frammentate mentre "l'aggressività degli attacchi cresce". Come ha riassunto la Nato "siamo obiettivo di interferenze maligne che puntano alle nostre infrastrutture più impegnate contro il virus come ospedali e istituti di ricerca".

Difesa cyber e interesse nazionale

L'urgenza di proteggersi dagli attacchi sulla rete è stata affermata con chiarezza all'ultimo Consiglio Europeo

Questo secolo ci ha fatto comprendere che i maggiori pericoli alla sicurezza vengono da minacce di tipo globale

E la presidente della Commissione Ue, Ursula von der Leyen, si è spinta fino indicare nella Cina popolare la fonte di questi attacchi aggiungendo che "non saranno tollerati". Non sorprende dunque che il generale Claudio Graziano, capo del comitato militare dell'Ue, definisca le minacce cyber "non future ma presenti" e potenzialmente in arrivo "non solo da Cina e Russia ma da gruppi terroristici", spingendosi fino a suggerire all'Unione di dotarsi di una "infrastruttura di difesa digitale" basata su "unità di risposta rapida cyber". Se a ciò aggiungiamo che la Nato in questo mese di novembre ha impiegato mille specialisti per simulare la difesa collettiva da attacchi cyber contro strutture sanitarie di un Paese alleato non è difficile arrivare alla conclusione che la scelta dell'Ue di dotarsi di una strategia di cyber sicurezza corrisponde ad un necessità impellente condivisa dalla maggioranza dei partner nonché auspicata anche dal Parlamento Europeo con la risoluzione del 25 novembre scorso. Si spiega anche così la scelta da parte di Parigi e

Berlino di individuare nello sviluppo digitale uno dei terreni strategici per il successo del Recovery Fund europeo.

Da qui l'interrogativo su come l'Italia si presenterà all'appuntamento con il cyber europeo. La creazione del Nucleo per la sicurezza cibernetica nel 2017 ha posto le basi per istituire nel 2019 il Centro per la cyber sicurezza nazionale che nell'ultimo anno è servito per identificare e respingere più infiltrazioni maligne contro il nostro Paese e, segnatamente, le infrastrutture sanitarie. Si tratta ora di creare, attorno a questo nucleo operativo, una rete di interazione con la società civile – dalle imprese alle università – capace di ripetere sul fronte cyber la collaborazione civili-militari che si è rivelata negli ultimi anni decisiva nel proteggere il Paese dai rischi di attacchi terroristici. Lo scontro politico in atto sulla proposta creazione di un Istituto italiano di cybersicurezza – a prescindere dalle opposte posizioni in campo, legate a questioni di metodo e merito – non deve far venir meno la necessaria coesione nazionale sull'opportunità di fornire al Paese uno scudo cyber capace di far fronte a tre bisogni che rispondono al nostro interesse nazionale. Primo: creare un network integrato fra difesa, aziende e centri di formazione per far convergere le migliori risorse nazionali nella protezione digitale. Secondo: non rimanere indietro nel cyber rispetto ad altri partner Ue e Nato, per scongiurare pericolosi squilibri dentro le nostre tradizionali alleanze. Terzo: dotarci in fretta di un efficace sistema di difesa nazionale dalla minaccia di cyber attacchi che potrebbero causare danni perfino più seri rispetto a quelli dovuti alla pandemia Covid-19.

Questo secolo ci ha già fatto comprendere come i maggiori pericoli alla sicurezza collettiva vengono da minacce di tipo globale, che investono tutti superando ogni confine: è avvenuto l'11 settembre 2001 con gli attacchi terroristi contro Washington e New York che hanno fatto conoscere la pericolosità universale della violenza jihadista; si è ripetuto nell'autunno del 2008 con la crisi finanziaria di Wall Street che ha posto la necessità di proteggere singoli e Paesi interi dalle peggiori speculazioni; è tornato ad avvenire con il Covid-19 che ha portato morte e devastazione economica in ogni angolo del Pianeta, aggredendo ogni abitante senza distinzione. Ignorare che dal cyber potrebbe arrivare il nuovo attacco globale sarebbe il più grave degli errori. E ciò significa che questa volta dobbiamo tentare di prevenire la minaccia. Agendo nell'interesse nazionale come anche in una cornice di collaborazione multilaterale.