IL FOGLIO

MINISTERO DELLA DIFESA

Data 18-04-2012
Pagina 3
Foglio 1

• Il Pentagono chiede risorse per le armi informatiche, un think tank italiano invita invece il governo a concentrarsi sulle leggi

Le cyber guerre richiedono investimenti (soprattutto giuridici)

Roma. Il Pentagono ha appena chiesto al Congresso americano più poteri per attrezzarsi alle guerre del futuro, quelle informatiche. In Italia, invece, ci si potrebbe accontentare per ora di dare una definizione giuridica di "cyber weapon", senza avventurarsi in investimenti economici ad hoc. E' quanto emerge da una ricerca che in queste ore circola tra gli addetti ai lavori e che è stata curata dall'Istituto di studi strategici Niccolò Machiavelli presieduto dall'ammiraglio Marcello De Donno, già capo di stato maggiore della marina militare e ora presidente di AgustaWestland spa (Finmeccanica), la parte italiana del gruppo Westland. Di cosa parliamo quando parliamo di "cyber arma"? Non di generici "attacchi hacker" o crimini informatici, quanto piuttosto di dispositivi che, colpendo la rete telematica di un paese, allo stesso tempo ne danneggiano infrastrutture critiche. Il software Stuxnet, creato per infiltrare i sistemi informatici iraniani e sabotare il funzionamento di alcuni impianti nucleari, fu rilevato per la prima volta nel 2010 ed è considerato uno dei prototipi di queste "cyber armi". Ad oggi ancora non è dato sapere con certezza chi abbia progettato Stuxnet, anche se i media hanno spesso puntato il dito su Israele o Stati Uniti; certo è che i notevoli fondi necessari per l'ideazione e la costruzione del software sembrano indirizzare verso uno stato sovrano.

"Cyberweapons, aspetti giuridici e strategici" è il titolo del report dell'Istituto Machiavelli, uscito praticamente in contemporanea con una indiscrezione raccolta dal Washington Post: secondo un documento rivelato la settimana scorsa dal quotidiano statunitense, il dipartimento della Difesa americano ha proposto al Congresso di studiare corsie preferenziali per autorizzazioni e finanziamenti finalizzati alla creazione delle armi di ultima generazione. Herbert S. Lin, analista del National Research Council of the National Academy of Sciences, sostiene che in questo modo il Pentagono riconosce che "le cyberweapon sono radicalmente diverse dalle armi convenzionali": "Si può costruire un aereo da combattimento di impiego generale e questo poi funzionerà più o meno allo stesso modo nel Pacifico come nell'Atlantico – sostiene Lin – Ma lo stesso ragionamento non tiene se lo scopo è quello di colpire un obiettivo di tipo informatico in Russia oppure in Cina". Sia per la progettazione che per lo sviluppo di queste tecnologie, dunque, ai governi sono richieste maggiore rapidità e flessibilità d'azione.

Per quanto riguarda l'Italia, però, l'Istituto di studi strategici italiano diretto da Francesco D'Arrigo e presieduto da De Donno invita al realismo: "Gli alti costi, le alte variabili di rischio sulla loro realizzazione ed efficacia, nonché i risultati 'limitati' e comunque temporanei, portano a far ritenere attualmente le attività di ricerca e sviluppo nel settore delle cyber armi come strategicamente non convenienti". Dagli addetti ai lavori, comunque, non arriva un invito all'immobilismo. Soprattutto perché la normativa italiana non definisce ancora in maniera chiara e diretta cosa debba intendersi per "cyber weapon". Gli studiosi del think tank, rifacendosi a norme già presenti nel codice civile oltre che alla direttiva europea sulle infrastrutture critiche, suggeriscono a Parlamento ed esecutivo questa definizione: "Un'apparecchiatura, un dispositivo ovvero qualsiasi insieme di istruzioni informatiche dirette a danneggiare illecitamente un sistema informatico o telematico avente carattere di infrastruttura critica, le sue informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti". Inquadrare a livello giuridico il concetto di cyber arma è "un passaggio urgente e imprescindibile sia per valutare il livello di minaccia proveniente da un attacco informatico, che per le conseguenti responsabilità politiche e giuridiche ascrivibili a chi ha agito". Una "semplice" definizione, insomma, può aiutare il paese a tutelare i propri asset strategici, soprattutto a fronte delle recenti decisioni di paesi più o meno alleati (dagli Stati Uniti alla Russia, fino alla Cina) di condurre operazioni di offesa nel cyberspazio.

Twitter @marcovaleriolp