Quotidiano Torino

LA STAMPA

11-APR-2011

Diffusione: 300.578 Lettori: 1.908.000 Direttore: Mario Calabresi

da pag. 17

"L'Occidente deve prepararsi alla prima cyberguerra"

Generale Usa: potrà essere tra un anno, il nostro punto debole è la rete elettrica

il caso

MAURIZIO MOLINARI
INVIATO A WASHINGTON

Fra i prossimi 12 e 36 mesi il Pentagono si aspetta un massiccio attacco informatico contro una nazione sovrana: a rivelarlo è il generale Keith Alexander, direttore della «National Security Agency» nonché a capo del «Cyber Command» delle forze armate americane, creato su ordine del presidente Barack Obama per proteggere l'America dal pericolo degli hacker.

Atteggiamento spigliato, minuzioso nelle spiegazioni di informatica e attento a ribadire sempre la subalternità alle leggi del Congresso, Alexander parla nella cornice della sessione sulla sicurezza cybernetica dei lavori della Commissione trilaterale, che riunisce esponenti politici ed economici di Stati Uniti, Europa e Asia.

«Internet garantisce alle nostre società opportunità straordinarie di crescita e sviluppo, ma le espone anche a rischi molto seri», esordisce il generale al comando di alcune delle unità più segrete dell'apparato militare. E per dimostrare quanto afferma ricostruisce quanto avvenuto in una recente riunione in ambito Nato: «Ci siamo trovati a discutere l'ipotesi di ricorrere all'articolo 5 della Carta atlantica sull'autodifesa collettiva in caso di attacco cybernetico e c'era chi sollevava dubbi in merito. Ma quando è stato fatto lo scenario di un totale black-out elettrico e finanziario della durata di 60 giorni in un singolo Paese, tutte le obiezioni sono cadute».

Se l'ultimo summit della Nato, tenutosi a Lisbona, ha inserito nel concetto strategico la difesa cybernetica, è «perché subire attacchi massicci è diventata una possibilità reale», sottolinea Alexander, spingendosi fino a prevedere che «potrebbe avvenire in un periodo compreso fra i prossimi 12 e 36 mesi». Da qui l'interrogativo su quali settori della vita civile siano più vulnerabili, e la risposta è puntuale: «C'è una scala di vulnerabilità, il settore più protetto è quello delle Borse finanziarie, mentre ad essere più esposta è la rete elettrica», per il semplice fatto che, in America come in Europa o in Giappone, è stata creata senza avere all'origine sistemi di protezione da questo tipo di attacchi.

A concordare sui «pericoli per la rete elettrica» sono l'ammiraglio Dennis Blair, che è stato direttore nazionale dell'intelligence nei primi due anni dell'amministrazione Obama, e David DeWalt, ceo di McAfee, ovvero l'azienda informatica di Santa Clara, in California, roccaforte della produzione di antivirus. «Per avere un'idea delle minacce con cui ci troviamo a combattere - spiega DeWalt - bisogna guardare ai numeri, ogni anno vengono creati 48 milioni di infezioni informatiche, ad un ritmo di circa 55 mila al giorno, e ogni mese vengono messi online 2 milioni di siti per diffondere tali infezioni». Ciò significa «avere a che fare con attacchi continui e sempre differenti», con in aggiunta una complicazione che DeWalt e Alexander indicano all'unisono: l'assenza di coordinamento normativo fra Stati, organizzazioni internazionali e singole aziende consente agli hacker di trovare spazi sul web per creare siti, sviluppare virus e lanciare cyberattacchi. Né il generale né il ceo fanno i nomi degli Stati più sospettati di originare cyberaggressioni, ma i sospetti si indirizzano in primo luogo verso Cina e Russia. In attesa che «le politica e le istituzioni facciano le loro parte», come Alexander auspica, la migliore difesa resta quella dei singoli, perché il 65 per cento delle vittime dei virus sono computer non protetti da firewall o dove i firewall non sono stati aggiornati.