

UN ATTACCO TERRORISTICO AL WEB AVREBBE ESITI DISASTROSI SU TRASPORTI E INDUSTRIA

«Usa troppo esposti alla cyber war» - S. Marchetti – Corriere della Sera – 8-05-10

Secondo il noto consulente Richard Clarke, la rete internet degli Stati Uniti è troppo vulnerabile

MILANO - Una «Pearl Harbor elettronica» che in meno di 15 minuti porterebbe morte e distruzione in tutto il paese. Questo il rischio concreto a cui sarebbero esposti gli Stati Uniti in caso di cyber attacco terroristico su larga scala, stante l'incapacità del sistema informatico di far fronte alla minaccia. La prima rete a crollare sarebbe quella del Pentagono, seguita subito dopo dagli altri provider. Si scatenerebbero poi delle esplosioni nelle maggiori raffinerie di Philadelphia e Houston e il malfunzionamento degli impianti chimici porterebbe al rilascio di gas letali come il cloro. Paralizzato pure il traffico aereo come pure quello delle metropolitane di New York, Washington e Los Angeles, con numerose collisioni in volo e scontri fra treni, mentre più di 150 città resterebbero senza elettricità. Risultato: decine di migliaia di cittadini morti in un attacco paragonabile alla devastazione di una bomba nucleare e il tutto in nemmeno 15 minuti e senza che un singolo terrorista o soldato metta piede sul suolo americano.

SCENARIO APOCALITTICO - A dipingere l'apocalittico scenario non è un fanatico di Al-Qaeda in vena di minacce ma, nientemeno, che Richard Clarke, già consulente di Bill Clinton e George W. Bush e conosciuto come «lo zar dell'antiterrorismo», che nel libro «Cyber War: The Next National Security Threat» («Cyber war: la prossima minaccia alla sicurezza nazionale»), scritto con Robert Knake (membro anziano del «Council on Foreign Relations»), ha messo in guardia gli Stati Uniti dal cyber-rischio di una catastrofe di proporzioni inimmaginabili. E come sottolinea il «Daily Telegraph», già nel 2004 Clarke ci aveva visto giusto sulla mancanza di preparazione americana nei confronti di Al-Qaeda nel libro «Against All Enemies» («Contro tutti i nemici»). E a finire nel mirino è proprio l'espansione di internet, perchè ora i computer dominano quasi ogni aspetto del settore produttivo americano e questo ha portato ad un pericoloso livello di dipendenza. «Gli Stati Uniti stanno preparando l'offensiva alla guerra informatica ma, al tempo stesso, la politica del paese rende impossibile difendersi efficacemente da questi attacchi», è il giudizio comune di Clarke e Knake, che puntano il dito anche contro le successive amministrazioni, inclusa quella attuale del Presidente Obama, che non sarebbero riuscite a quantificare le dimensioni del problema. In altre parole, gli Stati Uniti possono aver inventato la Rete, ma almeno 30 nazioni sono oggi in grado di scatenare una guerra informatica che metta in ginocchio i sistemi economici, militari e finanziari degli altri paesi. E, ironia della sorte, proprio gli Usa sono adesso i più «cyber vulnerabili» rispetto a Russia, Cina e persino Corea del Nord, perché queste ultime hanno sempre fatto molto meno affidamento su Internet, sviluppando, al contempo, una miglior offensiva informatica.

VANTAGGIO ASIMMETTRICO - «Dobbiamo poter chiudere la nostra connessione ed essere comunque in grado di operare – ha spiegato Knake al quotidiano inglese – perché basarsi su un sistema precario come è, appunto, quello di Internet è davvero un grosso errore. Si tratta di un ecosistema fondamentalmente insicuro, pronto a scatenare conflitti e che dà un vantaggio asimmetrico alle nazioni svantaggiate per quanto riguarda le armi tradizionali». Nel recente passato, gli Stati Uniti hanno già avuto a che fare con i pirati informatici: la prima volta furono gli hacker russi o cinesi (o forse entrambi) ad inserirsi con successo sulla rete elettrica americana e a lasciarvi un software che si sarebbe potuto usare successivamente per sabotare l'intero sistema; la seconda, giusto l'anno scorso, quando degli hacker nordcoreani hanno fatto cadere i server del Dipartimento della Sicurezza Interna e del Tesoro insieme con quelli di normali provider, inondandoli di richieste dati. A farne le spese di quell'attacco fu anche un server del Pentagono e in quel caso le conseguenze sarebbero potute essere ben più drammatiche, visto che i militari si affidano proprio a quel server per le comunicazioni in un conflitto armato. «Abbiamo scritto il libro per dare il via ad un confronto – ha concluso Knake – ma credo sia necessario ripensare alla premessa iniziale secondo la quale, trattandosi di bits e bytes, non è un'azione pericolosa e destabilizzante».