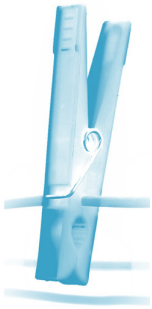
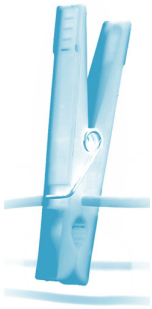


Il Pentagono svela la nuova strategia anti hacker

Dopo terra, cielo e mare è l' ora della guerra in rete

Di Olimpio Guido - Fonte: Il corriere della Sera

WASHINGTON - Gli avversari non dormono. Da mesi - o da anni - lanciano incursioni sulla rete. Azioni che potrebbero un giorno diventare un nuovo 11 Settembre. A sferrarlo terroristi o piuttosto qualche Paese rivale, magari con la complicità di organizzazioni criminali. Per rispondere a questa sfida il Pentagono ha presentato ieri la sua «cyber strategy» e ha designato un nuovo fronte operativo. Affiancherà gli altri spazi militari. La terra, il cielo, il mare. Il piano prevede diverse linee su cui devono attestarsi i nuovi guerrieri, una Linea Maginot del web: 1) un sistema di difesa attiva per il network militare, capace di rilevare la minaccia e contrastarla. 2) Sopravvivenza delle reti creando canali alternativi e intercambiabili. 3) Pianificazione e coordinamento con la Sicurezza interna (Homeland Security) per proteggere le strutture civili. Gli attacchi, infatti, potrebbero riguardare, ad esempio, centrali elettriche o apparati che dirigono il traffico aereo. 4) Collaborazione con i Paesi alleati. 5) Sviluppo di una partnership militari-privati. Alla Casa Bianca considerano concreto il rischio di un' aggressione. Tanto è vero che in primavera hanno fatto trapelare un messaggio chiaro: un' incursione cibernetica su larga scala sarà considerata un' azione di guerra e potrebbe provocare una risposta convenzionale. Ossia, gli Usa si riservano di replicare con raid aerei o missilistici. Oppure con azioni digitali. Su quest' ultimo punto la strategia spiega poco, forse per sottrarsi alle accuse di voler militarizzare Internet. Le fonti ufficiali insistono sul tasto «difesa» piuttosto che sull' offesa. Il Dipartimento di Stato ha suggerito cautela. Esistono nodi legali e problemi di rapporti. Per alcuni critici serviva maggiore chiarezza. Altri, invece, indicano un precedente importante: il virus Stuxnet , usato da un' intelligence (Israele? Germania?) per danneggiare gli impianti nucleari iraniani. Garantire la deterrenza non è per nulla semplice. Come ha osservato un esperto, se subisci un attacco missilistico «l' ordigno ha il mittente sulla testata». Se ti attaccano via Internet il nemico può diventare un fantasma. Serve tempo per decifrare l' origine del colpo. Basti pensare che ogni giorno gli Stati Uniti subiscono migliaia di «intrusioni». C' è poi la questione dei confini. La «Cyber-War» non li riconosce. Quando i russi hanno messo fuori uso i siti estoni si sono serviti anche di server negli Usa. Nel presentare il programma, il sottosegretario alla Difesa William J. Lynn ha rivelato che a marzo hacker stranieri hanno violato il database di una società legata al Pentagono riuscendo a impossessarsi di 24 mila file sensibili. Un furto che è solo l'ultimo di una lunga serie. Operazioni di spionaggio che hanno riguardato i velivoli senza pilota, i sistemi di guida dei missili, i progetti di aerei sofisticati. Le indagini - dagli Stati Uniti all' Europa - hanno spesso individuato nei cinesi i pirati più pericolosi. Le forze armate di Pechino pescano nelle università giovani hacker e li impiegano in missioni riservate. Lo stesso fa l' intelligence. Si esercitano a lanciare assalti, vanno a caccia di informazioni top secret. Ma dalla Cina arrivano anche sorprese. Dalla metà degli anni 90, il Pentagono ha acquistato decine di migliaia di microchip d' origine cinese poi impiegati su aerei, navi o altri mezzi. Bene, molte di queste componenti si sono rivelate «fallate» o, peggio, contenevano virus.



**** Cyberwar La parola Il termine guerra cibernetica (cyberwarfare) si riferisce alle azioni condotte da uno Stato per violare i computer o i network di un altro Stato con l' intento di causare ingenti danni e distruggere i sistemi di comunicazione nemici. Nel 2010 gli Stati Uniti hanno creato l' U.S. Cyber Command per difendere l' apparato militare da questo genere di attacchi. La cyberwarfare si può svolgere su diversi piani. 1) Lo spionaggio volto ad ottenere informazioni top secret attraverso l' hackeraggio. 2) Il sabotaggio: ordini e comunicazioni militari attraverso computer o satelliti possono essere intercettati o sostituiti, mettendo a rischio i soldati. 3) L' attacco alle infrastrutture di un Paese come i servizi energetici, idrici, di combustibili, di comunicazioni, commerciali e dei trasporti. ' '