

Orizzonti Tecnologie

Follower
di Chiara Maffioletti

Timberlake, chic ma non snob

Seguono su Twitter Justin Timberlake quasi 9 milioni di persone. Un'enormità che conferma una volta di più che grande lavoro sulla sua immagine sia riuscito a fare l'ex cantante per teenager, ora attore

apprezzatissimo. Ogni sua mossa è stata indovinata, il che lo ha reso uno dei divi più influenti. E pure nella scelta di chi seguire, ha saputo essere chic ma non snob: solo 21 persone. E quasi nessuna è famosa.

Fobie Le azioni di sabotaggio online contro governi e aziende diffondono il tecnopánico

Cyberwar: rischi tanti, interessi troppi

Più che un pericolo concreto per gli Stati, i crimini informatici sono un business
La corsa miliardaria alla e-security sta accelerando e l'Italia resta molto indietro

di FABIO CHIUSI

Lo scenario è da film hollywoodiano: il criminale informatico, al soldo della potenza straniera, si intrufola nei computer che gestiscono le infrastrutture del Paese e le manomette. Causando, a seconda della trama, l'interruzione della rete elettrica, il collasso delle transazioni finanziarie, il blackout dei sistemi di difesa militare. Risultato? L'apocalisse. O meglio, la cyber-guerra: l'uso di Internet da parte di uno Stato per causare vittime e danni a un rivale. Realtà o finzione? Negli Stati Uniti il moltiplicarsi degli attacchi e dei crimini informatici ha alimentato una pericolosa retorica allarmistica a base di «cyber 11 settembre», «Pearl Harbor digitale» e terroristi che, ha sostenuto il senatore democratico Joe Lieberman, «userebbero Internet contro di noi con la stessa facilità con cui hanno trasformato aerei di linea in missili guidati». Paure che si sono tradotte da un lato in oltre 50 disegni di legge presentati al Congresso, l'ultimo dei quali — il Cybersecurity Act 2012 — darebbe al governo il potere di controllare il traffico online delle aziende che «gestiscono infrastrutture critiche»; dall'altro, in minacce tutt'altro che virtuali: «Se

bor Networks, uno stratosferico +2000%. Avvisaglie di una cyber-guerra? È tutto da dimostrare.

«Il problema è l'uso del linguaggio», spiega Peter Sommer, autore di un rapporto sullo stato della cyber-sicurezza per l'Organisation for Economic Co-operation and Development, al «Corriere». «Se si deve usare la parola "guerra" insieme a "cyber" ci si deve aspettare qualcosa di simile a una guerra convenzionale, in termini di distruzione causata, perdita di vita umane e così via.

«La suggestione nella sua forma più pura afferma che ciò si possa ottenere tramite una interazione tra computer e computer. In questo senso non credo che esistano cyber-guerre, né che siano probabili». Semmai, prosegue Sommer, «è molto più utile parlare di "cyber-armi" come parte di un insieme di dotazioni a disposizione degli Stati per far progredire i loro scopi».

Ed è questo, infatti, che testimonia la storia recente: dal pesante attacco subito dall'Estonia nel 2007 (coinvolti 85 mi-

la computer per tre settimane) a quello in Georgia dell'anno successivo. Fino al caso più famoso e studiato, Stuxnet: il «worm» — cioè un virus in grado di autoreplicarsi — che ha colpito la centrale di arricchimento dell'uranio di Natanz, in Iran. In nessun caso ci sono prove conclusive, ma gli indizi puntano a una matrice russa nei primi due, e israelo-statunitense nel terzo. Ma anche qui: nessun morto, nessuna rivendicazione politica o militare, nessun deliberato atto di violenza.

Tuttavia spingere su quello che il ricercatore della George Mason University, Adam Thierer, definisce «tecnopánico», conviene. Alle agenzie governative, che vedono i propri budget per la cyber-sicurezza lievitare di centinaia di milioni di dollari proprio mentre in tutti gli altri settori subiscono pesanti tagli. Alle aziende che producono i sistemi di protezione informatica, che già oggi gestiscono un mercato da 100 miliardi di dollari nei soli Stati Uniti. Se si pensa che gli apparecchi connessi a Internet

i



In alto da sinistra a destra Peter Sommer, autore di un rapporto sullo stato della cyber-sicurezza per l'Oecd (Organisation for Economic Co-operation and Development)

passeranno da 5 miliardi nel 2010 a 30 miliardi nel 2020, si comprende che il giro d'affari è destinato a crescere a dismisura. Ancora, giova a chi ha interesse a sfruttare la paura per legittimare nuove e più restrittive regole di governance della Rete. Non a caso agli allarmi si è accompagnata una richiesta di norme che inizialmente intendevano fornire al presidente Barack Obama addirittura la possibilità di «spegnere» il web in casi estremi di minaccia per la sicurezza nazionale. Tentativi che potrebbero avere «conseguenze imprevedibili e sgradite», dice Sommer, «oltre a essere inutili».

Sgombrato il campo da una retorica che travisa la realtà del problema, sarebbe tuttavia sbagliato ignorare i pericoli di una totale impreparazione degli Stati ad affrontare la minaccia informatica. E se è vero che gli strumenti per condurre una ipotetica guerra sono in gran parte gli stessi utilizzati dai comuni cyber-criminali, e dunque noti, nuove e inedite minacce potrebbero essere all'orizzonte. «È molto complesso in questo momento riuscire a escludere che siamo di fronte a un cambio completo del metodo attraverso cui portare un atto di "cyber-warfare", cioè di guerriglia digitale, verso un altro Stato», ammonisce Stefano Mele, avvocato e coordinatore del



tro di noi con la stessa facilità con cui hanno trasformato aerei di linea in missili guidati». Paure che si sono tradotte da un lato in oltre 50 disegni di legge presentati al Congresso, l'ultimo dei quali — il Cybersecurity Act 2012 — darebbe al governo il potere di controllare il traffico online delle aziende che «gestiscono infrastrutture critiche»; dall'altro, in minacce tutt'altro che virtuali: «Se ci causate un blackout nazionale», ha spiegato una fonte militare americana al «Wall Street Journal» lo scorso giugno, «dovete sapere che vi infileremo un missile nella ciminiera».

Prima che ciò accada, è bene fermarsi a esaminare i dati, che testimoniano l'esistenza di un problema di sicurezza in Rete, ma civile prima che militare. Sommando costi diretti e indiretti dei crimini informatici negli ultimi 12 mesi, il colosso degli antivirus Norton ha calcolato che si raggiunge la cifra stellare di 388 miliardi di dollari. Più del mercato nero mondiale di marijuana, cocaina ed eroina messi insieme (295 miliardi), e quasi quanto il traffico complessivo di droga (411 miliardi). Gli attacchi DDoS (distributed denial-of-service) che impediscono temporaneamente l'accesso ai siti bersaglio, hanno negli ultimi tre anni fatto segnare, secondo Ar-

mi" come parte di un insieme di dotazioni a disposizione degli Stati per far progredire i loro scopi».

Ed è questo, infatti, che testimonia la storia recente: dal pesante attacco subito dall'Estonia nel 2007 (coinvolti 85 mi-

gli altri settori subiscono pesanti tagli. Alle aziende che producono i sistemi di protezione informatica, che già oggi gestiscono un mercato da 100 miliardi di dollari nei soli Stati Uniti. Se si pensa che gli apparecchi connessi a Internet



(FOTO CORBIS)

**Il giro d'affari
Il colosso degli antivirus
Norton calcola che il costo
dei crimini informatici
negli ultimi 12 mesi è stato
di 388 miliardi di dollari**

**Le conseguenze
C'è il pericolo che la paura
di un attacco venga
sfruttata per legittimare
più restrittive regole
di governance della Rete**



In alto da sinistra a destra Peter Sommer, autore di un rapporto sullo stato della cyber-sicurezza per l'Oecd (Organisation for Economic Co-operation and Development); Adam Thierer, ricercatore della George Mason University; Stefano Mele, avvocato e coordinatore dell'Osservatorio InfoWarfare e Tecnologie emergenti dell'Istituto italiano di studi strategici Niccolò Machiavelli; e Luisa Franchina, direttore generale della segreteria interministeriale di coordinamento delle Infrastrutture critiche della presidenza del Consiglio dei ministri

ad affrontare la minaccia informatica. E se è vero che gli strumenti per condurre una ipotetica guerra sono in gran parte gli stessi utilizzati dai comuni cyber-criminali, e dunque noti, nuove e inedite minacce potrebbero essere all'orizzonte. «È molto complesso in questo momento riuscire a escludere che siamo di fronte a un cambio completo del metodo attraverso cui portare un atto di "cyber-warfare", cioè di guerriglia digitale, verso un altro Stato», ammonisce Stefano Mele, avvocato e coordinatore dell'Osservatorio «InfoWarfare e Tecnologie emergenti» dell'Istituto italiano di studi strategici Niccolò Machiavelli. «Tutti gli indicatori ci fanno capire che gli Stati si stanno attrezzando a proteggersi e attaccare».

E, infatti, i documenti che delineano le strategie nazionali per affrontare la questione si moltiplicano, dalla Germania alla Francia passando per Regno Unito e Stati Uniti. E l'Italia? «È indietro, al momento non ce l'ha», dice Mele. Luisa Franchina, direttore generale della segreteria interministeriale di coordinamento delle Infrastrutture critiche della presidenza del Consiglio dei ministri, interpellata dal «Corriere» conferma. Rivelando tuttavia che una bozza preliminare del documento è stata sottoposta all'attenzione di Mario Monti non più tardi di due settimane fa. Tra le linee guida la cooperazione internazionale, a partire dalla Nato, ma nessuna intenzione di controllare il traffico online a scopo di prevenzione. «Il problema è che eravamo abituati a fare negoziati sull'aria, la terra, il mare. Ma quali sono i confini del cyberspazio?».

Twitter @fabiochiusi

© RIPRODUZIONE RISERVATA