Ucraina. Rapetto (esperto di cybersicurezza): "La guerra è partita da internet, salvare i dati off line"

C’è un’altra guerra oltre a quella combattuta dai carri armati e dalle molotov. È dietro gli schermi dei computer ed è molto più pericolosa di quanto possa immaginare la mente di un comune cittadino non abituato a masticare di informatica o elementi di cybersicurezza. Se da una parte ha sollevato sui social quasi un’onda di giubilo l’azione di Anonymous, il collettivo di hacker, che ha messo a segno numerosi black out di siti del Cremlino o delle principali testate russe, dall’altra non deve passare inosservata la risposta del team Conti, altro gruppo di pirati informatici foraggiati da Mosca. Al Sir, **Umberto Rapetto**, esperto di sicurezza informatica, docente universitario e autore, già generale della Guardia di Finanza a capo di numerose indagini, consiglia di aprire gli occhi: “Dobbiamo temere. Occorre fare copia di tutti i dati off line. Se ci fosse mai una ‘apocalisse digitale’ avremmo almeno una base da cui partire”. **Anonymous ha dichiarato guerra alla Russia di Putin. Ma quanto sono potenti gli hacker del collettivo?** Non è facile affondare una grande potenza cibernetica come la Russia che ha investito negli ultimi anni anche in attività criminali, come la mafia russa, andando a valorizzare iniziative private che da sempre speculano su interventi basati sul ransomware, il software capace di cifrare documenti e file con cui hanno messo a ferro e fuoco il mondo. La risposta ad Anonymous non ha tardato. Il gruppo hacker Conti, sponsorizzato dal governo di Mosca, ha risposto dicendo: ‘Siamo pronti anche noi a colpire l’Occidente’.

> Siamo di fronte a un conflitto che non prevede soggetti dominanti ma tante energie in grado di configurare una guerra virtuale che andrà a riverberarsi sulla vita di tutti i giorni.

In questo momento sono stati colpiti alcuni simboli russi da parte di Anonymous a cominciare dalla testata "Russia today", fabbrica di fake news, l’agenzia Tass, e il fermo alle ferrovie bielorusse che potevano essere un canale logistico utile per le truppe di Putin. Nel mirino ci sono, su un fronte e sull’altro, le infrastrutture critiche. Gli hacker russi avevano già cominciato ad attaccare l’Ucraina la notte fra il 13 e il 14 gennaio scorso. La guerra perciò è partita da internet. Ci sono stati attacchi superficiali che man mano sono andati a interferire sull’erogazione di servizi essenziali quali sanità, finanza o trasporti. La stessa cosa ora sta avvenendo ai danni dei russi ma la presenza di Anonymous, nonostante sia agguerrita, non costituisce una garanzia di riuscita. Teniamo conto che stiamo ritenendo dei benefattori coloro che fino a poco fa erano ritenuti dei banditi. **La nostra Agenzia per la Cybersicurezza nazionale raccomanda a tutti gli operatori di infrastrutture digitali nazionali di adottare "una postura di massima difesa cibernetica".** Mi sembra una raccomandazione poco efficace perché chiunque direbbe di tenere le difese alzate. L’Agenzia oggi non sa nemmeno quali esperti reclutare, lo sta facendo attraverso Linkedin. **Cosa dobbiamo temere di più in Italia?** Dobbiamo temere. Occorre fare copia di tutti i dati off line. Se ci fosse mai una ‘apocalisse digitale’ avremmo almeno una base da cui partire. Teniamo conto che i russi hanno già attaccato Nvidia (azienda tecnologica degli Stati Uniti, ndr) produttore di microprocessori. C’è un allarme del Centro di protezione cibernetica britannico che insieme al Cisa (Agenzia governativa americana per la protezione delle informazioni, ndr) dicono di stare attenti a un nuovo virus che ha capacità purtroppo straordinarie. Si chiama cyclops blink ed è destinato a essere drammatico. Il gruppo Conti è ritenuto dalle autorità come il più pericoloso perché usa le telefonate per installare il virus. Sono chiamate capaci di fare travasi dei dati dallo smartphone dell’utente. **Quando dice di salvare off line tutti i dati, suggerisce di farlo a tutti i cittadini non solo alle aziende o le istituzioni?** Il consiglio vale per tutti. L’obiettivo del virus cyclops blink è considerato "soho", cioè *small office home office*, è quindi indirizzato ai professionisti o chi ha un utilizzo domestico del pc. Meglio quindi tenere gli occhi aperti, investire in supporti esterni ed evitare di salvare sul cloud. **Specie chi usa i servizi home banking deve stare attento?** Meglio usare i codici tramite pennetta

usb in questo caso. La guerra sarà di carattere economico. Lo Swift (il circuito di pagamento internazionale, ndr) verrà superato dai russi tramite i canali delle criptovalute, come i bitcoin o altri circuiti.

Maria Elisabetta Gramolini