Attacchi informatici e guerra planetaria

di Francesco Galofaro* per Marx21.it

***Politecnico di Milano**

Sembra la trama di un film di fantascienza: il 12 marzo il mondo intero, al risveglio, scopre di essere sotto attacco di un virus. I danni sono incalcolabili: fabbriche bloccate, università ferme, i centralini del pronto soccorso non sono più in grado di inviare un'ambulanza. A partire dall'Inghilterra e nel giro di poche ore, seguendo la rotazione terrestre, il virus si diffonde a oriente: duemila sistemi informatici si fermano in Iran, trentamila in Cina. In Italia si teme l'effetto-lunedì, il giorno in cui gli impiegati tornano al lavoro dopo il fine settimana.

“Voglio piangere” *(wannacry),* è un *ransomware:* un sistema escogitato per chiedere un riscatto. Entra nel tuo computer attraverso un “buco” delle vecchie versioni del sistema operativo Windows, cripta i dati del tuo disco e non li decodifica finché non paghi una somma in *bitcoin*, la moneta privata virtuale internazionale più amata dalle organizzazioni criminali.

Fin dal primo giorno il New York Times punta il dito contro la NSA, la National Security Agency statunitense: si sarebbero lasciati rubare *Eternal blue*, uno degli svariati sistemi che impiegano per infiltrarsi nelle reti dei PC [1]. E sì che la notizia non era nuova. Già in marzo Wikileaks aveva pubblicato un articolo che dava l'allarme: gli spioni americani hanno perduto il controllo dei propri strumenti [2]. Ma i nostri giornalisti ritraggono Assange come una Cassandra venduta ai russi. Assange divulga segreti inviati da talpe che lavorano per organizzazioni in conflitto coi valori che dovrebbero rappresentare: dunque, va fermato. Finché godrà di credibilità e carisma, continuerà a rappresentare una minaccia per tutte le operazioni informatiche che l'opinione pubblica non deve conoscere, scambi commerciali *poco l*egali e operazioni belliche molto controverse.

Ovviamente anche questa storia ha i suoi eroi: *Malwaretech,* nome in codice di un autodidatta ventiduenne disoccupato che vive coi genitori nel sud dell'Inghilterra. Venuto a sapere da un collega hacker che nel codice del virus si celava l'indirizzo di un dominio web, questo involontario James Bond ha prontamente *comprato* quel dominio, ancora non registrato: in quel momento l'attacco si è fermato [3]. Un meccanismo di sicurezza, nel caso che l'arma di massa, fuori controllo, si ritorcesse contro gli ideatori. Ma chi sono i cattivi? Chi si cela dietro il misterioso gruppo di pirati Shadowbroker? Chi sono questi emuli della Spectre, come hanno agito?

Costruire il nemico

C’è perfino chi ha dichiarato che il sistema utilizzato da Shadowbreaker attira eccessivamente l'attenzione per essere opera di criminali dediti al guadagno, e che si tratti di un'operazione di distrazione per mascherare furti più gravi [18]. La questione è a mio parere più semplice, se è lecito interpretare l'attacco nel contesto di uno scontro politico. Il Telegraph ipotizza una ritorsione russa dopo che gli USA avevano bombardato le truppe siriane regolari. Ma la Russia è a propria volta uno dei Paesi colpiti dal virus [4]. Qualcuno congettura una responsabilità della Corea del Nord, un altro dei così detti “stati-canaglia” [5]. Certamente, Shadowbreaker non ha solo scopi criminali; si dà anche giustificazioni politiche. Nelle ultime ore avrebbe messo all'asta le “armi del nemico”, attaccando le “élite danarose” che dominano il mondo e il cui potere dipende da conti correnti che possono essere cancellati [6]. Altre dichiarazioni attribuite al gruppo denunciano che le armi rubate sono state impiegate dagli USA in Medio Oriente per infiltrare il sistema bancario. Ovviamente non c'è modo di essere sicuri che queste rivendicazioni non siano a propria volta opera di emuli, agenti segreti o polizie di mezzo mondo.

Il significato della guerra informatica

Non stiamo semplicemente assistendo a un fiorire di leggende urbane, dietrologia e paranoia; il punto è che in guerra è la verità stessa a costituire oggetto di contesa. Le fonti di informazione filo-americane cercano di distrarre l'opinione pubblica dalle responsabilità della NSA. Governi seri dovrebbero chiedere i danni agli USA; conviene pertanto incriminare i malvagi russi, i siriani e i nord coreani. Dall'altra parte del fronte, le fonti di informazione di parte avversa sottolineano come gli USA impieghino comunemente queste armi per colpire i Paesi non sottomessi e mantenere gli alleati sotto ricatto. Si veda il caso di Stuxnet, un virus informatico creato dagli USA e da Israele nel 2010 per colpire la centrale nucleare iraniana di Natanz [17], e altri ben noti casi rivelati dall'ex collaboratore della CIA Edward Snowden [8]. Da un punto di vista semiotico [9], non vi è differenza tra guerra e comunicazione sulla guerra: in guerra gli enunciati sono armi e le armi sono enunciati. La propaganda è un'arma più potente di un bombardamento, in grado com'è di inventare o di occultare uno sterminio; d'altro canto, anche la così detta “madre di tutte le bombe” è un messaggio eloquente. Non senza ragione Bill Gates, nel denunciare le responsabilità dell'amministrazione USA, ha paragonato il furto di questi programmi allo smarrimento di un missile tomahawk [10]. Occorre un “cambio di analogia”: nell'immaginario giornalistico e di massa le attività di hacking sono considerate alla stregua di un furto, mentre sono una vera e propria guerra, condotta tra governi, tra governo e multinazionali, tra governo e gruppi politici.

Si tratta peraltro di armi estremamente economiche da sviluppare. E' certamente più semplice scrivere un'applicazione che arricchire l'uranio. Una parte crescente dell'economia degli Stati emergenti, dall'India a Israele (da cui provengono le chiavette USB), è legata all'informatica e alla programmazione. I computer sono tecnologie piuttosto economiche, e i giovani di quei Paesi sono concorrenziali sul mercato mondiale. Occorrerebbe sbarazzarsi anche dell'illusione per cui i Paesi occidentali sono i detentori di ogni segreto o innovazione tecnologica. E' un fatto: la guerra informatica riporta in equilibrio la *balance of power* a favore degli Stati più poveri, comunque essi siano schierati.

Quanto è semplice criptare i dati?

Come si è detto, il ricatto di Shadowbreaker si basa sul fatto di criptare i nostri dati e chiederci un riscatto. Ma quanto è semplice questa operazione? E non si può decodificare il messaggio criptato? Per fare un esempio, ritorniamo all'asta delle cyber-armi, sia essa indetta da veri pirati o da poliziotti. Come si partecipa? E' presto detto: chiunque può installare sul proprio computer in meno di cinque minuti PGP *(Pretty Good Privacy),* un software libero e gratuito di crittografia [7]. Il software genera una chiave, metà della quale è pubblica, riportata a chiare lettere in fondo all'annuncio dell'asta. Chi vuole partecipare scrive un'offerta, la cripta inserendo la chiave pubblica in PGP e la invia. Il pirata la decritta usando la propria metà della chiave, che è privata. E' il principio della *crittografia asimmetrica:* la chiave pubblica è il risultato del prodotto di due numeri primi molto grandi, facili da moltiplicare tra loro, che rappresentano la chiave privata. L'operazione inversa, ovvero risalire dal prodotto ai fattori primi, è estremamente difficile e richiede tempi di calcolo storici anche a un supercomputer.

Incognite

Mettere a disposizione una chiave pubblica è economicamente più conveniente che organizzare un incontro tra due spie che in una notte nebbiosa si scambino una valigetta su un ponte. Certo, pubblicare una chiave è una sfida a violarla; d'altro canto anche le spie possono essere intercettate, assassinate, la valigetta può essere rubata e così via. Occorre poi tener conto di fattori non noti: una gran parte della ricerca mondiale è orientata allo sviluppo di supercomputer che sfruttano la fisica quantica per eseguire calcoli in parallelo. Poiché la teoria prevede che questi computer siano fisicamente realizzabili, non si può escludere che qualche grande potenza non li abbia già – essere

paranoici è il primo dovere di una spia. Per lo stesso motivo, USA, Europa e Cina, in gara per la *quantum supremacy*, stanno sviluppando la crittografia quantistica [11]: reti in cui è possibile accorgersi immediatamente se un intruso è riuscito intercettare il nostro segnale. Nel 2016 la Cina ha ultimato la più grande rete di comunicazioni quantistica terrestre mai realizzata [12]. L'Italia è all'avanguardia in questo campo, con un progetto dell'Università di Padova che sfrutta i satelliti: nello spazio è più semplice ed economico mantenere per lunghe distanze la coerenza del segnale [13].

Esiste un sistema sicuro?

Chiunque senza spendere nulla può installare un software libero per la criptazione dei dati. Ad esempio, Veracrypt garantisce la cifratura di periferiche come Hard Disk e chiavi USB. Con EncFS è possibile criptare una cartella di Dropbox. Non esiste tuttavia una sicurezza assoluta: se un intruso può introdursi nel nostro Dropbox, può essere facilitato nell'attività di decodifica dei nostri segreti per il fatto di poter comparare diverse versioni dei nostri documenti criptati: Dropbox li conserva perché possiamo recuperare le versioni precedenti in caso di errore. Nella maggior parte dei casi queste intrusioni avvengono perché non esiste una cultura della sicurezza: se ad esempio utilizziamo sempre la stessa password per tutti i siti cui siamo registrati, è sufficiente violarne uno per intrufolarsi in ogni meandro della nostra vita, dalla posta al conto corrente. Non è chiaro a molti utenti quanto sia semplice cambiare la password del nostro computer portatile, una volta che ci sia stato sottratto. Infine, con la rivoluzione domotica, perfino elettrodomestici e videocamere in rete possono essere impiegati per fare calcoli mirati a violare un codice o per tempestare di e-mail il server di un governo o di un sindacato, in modo da bloccarlo. Il termostato che possiamo programmare in remoto, dal telefonino, è connesso a internet e usa un microprocessore per accendere l’interruttore del riscaldamento prima del nostro ritorno a casa. Lo stesso microprocessore può essere usato per operazioni più complesse, come inviare una mail. Questo accade anche perché alcuni produttori, più interessati al guadagno che alla sicurezza, non permettono all'utente di impostare la password del proprio termostato o frigorifero [16]. In questo modo, se la CIA entra in possesso della password aziendale della Samsung, può spiarci attraverso il tv-color [2].

Sicurezza e supremazia internazionale

Come abbiamo visto, la cyber-guerra in corso può essere interpretata in termini di politiche internazionali. Da un lato abbiamo un attore, gli USA, che impiega queste armi per colpire i Paesi avversari e i loro popoli, “spegnendo” una rete di centrali elettriche o infiltrandosi in un sistema bancario. Dall'altro le stesse armi possono essere impiegate contro gli USA da quei Paesi che ne contendono la supremazia, perché sono economiche e semplici da sviluppare. La competizione si sposta allora sulla potenza di calcolo e sullo sviluppo di nuovi sistemi. Tale guerra coinvolge multinazionali americane, europee, cinesi, e si estende ad ogni campo: Google sviluppa sistemi quantistici di intelligenza artificiale in modo che le macchine possano apprendere più in fretta e con risultati migliori [14]; la Banca Europea per gli Investimenti (BEI) ha erogato un prestito di 25 milioni di euro a *Qwant*, il motore di ricerca europeo che rispetta la privacy degli utenti [15], per impedire che ogni giorno esabyte di dati sui cittadini europei finiscano nei server degli alleati statunitensi.

Sicurezza e disuguaglianza

D'altro canto, la vicenda della cyber-sicurezza si presta a una lettura in termini di disuguaglianza. Malwaretech, eroe per caso, è un giovane disoccupato, un perdente come tanti altri. Al contrario, gli amministratori di società private e pubbliche colpite dal virus non sembrano avere competenze nell’ambito della sicurezza. Nessuno di noi lascia la porta aperta, nell'uscire di casa; il dirigente

d’azienda medio non si rende neppure conto che il portone è spalancato. Dieci anni di crisi economica in Occidente hanno avuto per effetto un mancato ricambio generazionale: tassi di disoccupazione giovanile alle stelle, precariato, impossibilità per un'intera generazione di accedere a ruoli dirigenziali. In questo modo si è ostacolata anche la diffusione di competenze fondamentali, data l'onnipervasività dell'informazione nella società tardocapitalistica. Inoltre, chi vive una condizione di esclusione non deve nulla allo Stato o a aziende che limitano creatività e libertà. Il risultato non può che essere una sorta di vendetta pre-politica: ecco che nascono gruppi dediti a pratiche illegali, legittimati dal fatto che il web è terreno di guerra tra grandi agenzie e organizzazioni pubbliche e private: un campo di battaglia in cui uno Stato può sabotare una centrale nucleare mettendo a rischio l’ambiente di una regione, e allo stesso modo un magnate può boicottare l’economia di una nazione speculando contro una certa moneta. In questo ritorno a uno stato di natura hobbesiano non c'è diritto che tenga. I gruppi di pirati adottano le giustificazioni ideologiche più varie, anarchiche, libertarie, o al contrario nazionaliste o religiose, ma sono ugualmente il frutto di due condizioni: (1) vivono in un territorio in guerra, il web; (2) sono il prodotto di un'*economia criminogena*, il capitalismo.

Quale futuro?

Qualsiasi organizzazione politica non può più permettersi oggi di non riflettere sul ruolo dell’informazione nella società contemporanea. Alcuni scenari sono senz’altro inquietanti: non è certo un futuro remoto quello in cui un governo, attraverso i propri servizi segreti, impiegherà l’informatica per carpire l’elenco degli iscritti di un partito politico, per bloccare tutte le vertenze in corso di un sindacato, per sabotare una manifestazione. Fin qui ci siamo occupati di un utilizzo brutale degli algoritmi, allo scopo di sorvegliare e punire, ma occorre sapere che vi è un loro utilizzo più sottile, finalizzato a persuadere e orientare. Occorre chiedersi chi ha le chiavi dei siti che ogni giorno raccolgono informazioni su di noi, sui nostri consumi, sulle nostre preferenze politiche. Occorre scoprire come questi dati vengono sottilmente utilizzati per orientare le nostre scelte in modo totalmente automatico e di massa da parte di governi e multinazionali d’oltreoceano: è questo in buona sostanza il rischio insito in quella che Rouvroy e Bernes hanno chiamato *governamentalità elettronica* [19].

[1] http://www.rainews.it/dl/rainews/articoli/pirateria-informatica-bbc-in-corso-attacco-in-europa-a5d2a1d4-1cf0-4293-99fe-0bc3a991d43c.html

[2] http://www.ansa.it/sito/notizie/mondo/2017/03/07/wikileaks-la-cia-spia-attraverso-telefoni-e-tv-_37582d0a-e9c5-46c9-8f73-0d35b942cce0.html

[3]http://www.ilmattino.it/societa/piaceri/22_anni_autodidatta_eroe_per_caso_cosi_ho_fermato_il_cyber_attacco-2439386.html

[4]https://it.sputniknews.com/mondo/201705134490251-hacker-Shadow-Brokers-Russia-UK-russofobia-Telegraph-Siria-Trump/

[5]http://www.corriere.it/esteri/17_maggio_16/attacco-hacker-esperti-usa-ombra-corea-nord-5af852a6-39f5-11e7-acbd-5fa0e1e5ad68.shtml

[6]https://archive.is/rdYpc#selection-1013.846-1013.976

[7]https://en.wikipedia.org/wiki/Pretty_Good_Privacy

[8]https://it.wikipedia.org/wiki/Edward_Snowden

[9]Montanari, F. *Immagini coinvolte. Conflitti media guerre spazi*, Bologna, Esculapio, 2016

[10]http://www.corriere.it/tecnologia/17_maggio_15/attacco-hacker-europa-situazione-sotto-controllo-ma-allarme-cina-9798ee5e-395b-11e7-8def-9f1d8d7aa055.shtml

[11]https://it.wikipedia.org/wiki/Crittografia_quantistica

[12]http://www.agenparl.com/cina-al-via-rete-quantistica-quattro-citta-principali-fornire-comunicazioni-sicure-al-governo-alla-difesa/

[13]http://www.unipd.it/ilbo/prima-comunicazione-quantistica-dallo-spazio

[14]https://research.google.com/pubs/QuantumAI.html

[15]http://www.affaritaliani.it/affari-europei/qwant-anti-google-finanziato-dall-ue-motore-di-ricerca-pro-privacy-461748.html

[16] “La tua casa anti-Hacker”, in *LinuxPro* n. 176, aprile 2017.

[17] https://it.wikipedia.org/wiki/Stuxnet

[18]http://www.ansa.it/sito/notizie/tecnologia/hitech/2017/05/15/cyberattacco-esperto-ipotesi-e-guerra-psicologica_75419bb5-1268-468f-85ef-659c40efa5b6.html

[19] Antoinette Rouvroy, Thomas Berns, “Gouvernementalité algorithmique et perspectives d’émancipation” in *Politique des algorithmes. Les métriques du web*. RESEAUX, Vol.31, n.177, pp. 163-196 (2013), disponibile all'indirizzo https://works.bepress.com/antoinette_rouvroy/47/.