il manifesto

Quotidiano

Editori Laterza

Data 22-03-2017
Pagina 10
Foglio 1 / 2

CODICI APERTI

* La convergenza tra «intelligence» e imprese per fare di Internet un prototipo della sorveglianza di massa

* Spyware, malware, exploit, le parole chiave delle attività criminali e della cyber-sicurezza

Il login alla società del controllo

La sicurezza on line e le «Guerre della Rete». Un saggio di Carola Frediani

BENEDETTO VECCHI

Ricatti, frodi, furti d'identità, spionaggio industriale e politico. Ma anche guerriglia condotta senza esclusione di colpi. Sono solo alcune delle *tag* che accompagnano le recenti cronache della Rete, divenute ormai un flusso che travolge narrazioni consolidate su internet come regno della libertà radicale di parola e espressione. In questo flusso, i social network si arrogano il ruolo di guardiani del politicamente corretto; e per questo monitorano e censurano i contenuti che veicolano in nome proprio della libertà di espressione e della privacy individuale. Di fronte a questo cambiamento di scenario, la reazione punta l'indice contro gli hacker e i governi, spesso in conflitto tra loro, ma ritenuti responsabili dello snaturamento della Rete da ultima frontiera della libertà a prototipo della «società del controllo». Carola Frediani è una delle poche giornaliste che, con un paziente lavoro investigativo, restituisce una rappresentazione meno approssimativa, e dunque più realistica, di quanto si muove nel palcoscenico e nei *backstages* della «società in Rete».

Con una rigorosa capacità di raccolta, verifica le elaborazioni delle informazioni, restituisce nei suoi articoli un avvincente affresco delle *Guerre della Rete*, come recita il libro pubblicato da Laterza (pp. 184, euro 15), che raccoglie il distillato pregiato di un più che decennale lavoro quotidiano giornalistico che l'ha portata a intervistare «smanettoni», informatici forensi, hacker, esperti in sicurezza, poliziotti.

IL LIBRO È DENSO DI EPISODI, notizie, racconti di guerriglie mediatiche, di spie che svolgono il loro lavoro stando davanti a uno schermo. Non mancano spiegazioni di come funzionano i programmi di *spyware*, *malware* e i *trojans* che possono consentire l'intercettazione in remoto delle attività in Rete dei singoli, o anche scatenare, sempre a distanza, *exploit* (attacchi o infestazioni di virus informatici). Nulla è però concesso all'improvvisazione; tutto è documentato con l'umiltà e la testardaggine dell'antico mestiere di giornalista di cronaca che squaderna fatti, intrecciando informazioni dissonanti per fornire un arazzo chiaro e nitido sulle trasformazioni della Rete in tecnologia del controllo.

L'autrice scandisce in diversi capitoli le tante guerre condotte da servizi segreti, criminali informatici, hacker, poliziotti. Per quanto riguarda la «malavita» informatica, emerge il fatto che i ricatti e le frodi fanno parte di una fiorente industria criminale diffusa in tutto il mondo. Attività illecite che colpiscono nel mucchio degli utenti della Rete (quasi due miliardi di persone sono quelli che usano il computer, mentre un numero ben più superiore è ormai on line attraverso il proprio smartphone).

LE TECNICHE SONO SEMPLICI. I potenziali ricattatori infettano un computer attraverso una apparente innocua mail per poi successivamente inviare un messaggio: «paga se vuoi che il tuo computer sia *bonificato*». Una tecnica che ha avuto un vero boom tra il 2014 e il 2016. Le imprese specializzate in sicurezza informatica invitano a non pagare e a chiedere l'intervento di esperti, eppure la maggioranza dei ricattati preferisce assecondare la richiesta. Un altro tipo di ricatto riguarda invece la minaccia di divulgare segreti inconfessabili. Così, vengono violati i data base di siti internet per incontri e viene avanzata la minaccia di diffondere le preferenze sessuali di chi, magari, usa i siti per infedeltà coniugali «mordi e fuggi». Anche in questo caso, sono molti coloro che decidono di pagare per evitare che le amate pratiche fetish, sadomaso o altro diventino di pubblico dominio.

Le frodi hanno invece una antica tradizione. Furto del numero della carta di credito, del pin relativo al bancomat per prelevare soldi o fare acquisti. Ma sono pratiche in declino, visto che le forme di sicurezza e verifica dell'utente sono diventate solide.

LE GUERRE DELLA RETE più eclatanti sono tuttavia quelle combattute dagli stati, che si avvalgono di virtuosi della consolle e di imprese della sicurezza per carpire i segreti di altri stati o per mettere sotto sorveglianza i cittadini.

A squarciare il velo di questa sorveglianza di massa sono stati Wikileaks, le rivelazioni di Edward Snowden e le azioni condotte da hacker usando la sigla di Anonymous sulle attività di monitoraggio e intercettazioni messe in campo dalla Nasa, ma che costituiscono ormai una pratica diffusa, seppur con eguale e talvolta maggiore intensità, in tutti i paesi, dalla Cina all'Iran, dagli Emirati arabi a Israele, dall'Italia all'Inghilterra, alla Russia.

Gli stati moderni hanno sempre voluto controllare i comportamenti dei loro cittadini. E se il panopticon era la rappresentazione di tale volontà di sorveglianza nella società disciplinare, la situazione diventa più complicata con le tecnologie della comunicazione digitale.

LA RETE CONSENTE cioè una comunicazione dai molti ai molti. È in questa pervasività d che ha trovato spazio e ruolo l'azione dei mediattivisti per contrastare e denunciare le ingerenze statali. Le campagne contro le proposte dell'*intelligence* di usare software preposti a spiare i contenuti oppure di «porte di ingresso» attivabili da polizia o servizi segreti si sono alternate alla rivendicazione di usare programmi informatici per crittografare i contenuti delle comunicazione. È stata questa azione la spinta a importanti innovazioni tecnologiche (il software, anche se immateriale, è da considerare manufatto tecnologico) che hanno consentito, per esempio, il commercio elettronico, lo spostamento di capitali in totale sicurezza.

La recente decisione di WhatsApp di usare la crittografia per garantire la riservatezza delle conversazioni è la ciliegina sulla torta del circolo virtuoso, per le multinazionali, tra attitudine hacker e innovazioni tecnologiche.

L'AUTRICE allude a una dimensione militare, d'altronde sempre presente su Internet, come ha scritto già alcu-

il manifesto

Quotidiano

Editori Laterza

Data 22-03-2017
Pagina 10
Foglio 2 / 2

ni lustri fa Manuel Castells nel suo *Internet Galaxy*. In quel testo, lo studioso catalano sottolineava che quella militare era una delle sottoculture, assieme a quelle di hacker, imprenditori e imprese che hanno favorito lo sviluppo della Rete. Carola Frediani scrive di corse agli armamenti (il software e i microprocessori), di investimenti colossali di imprese e stati nazionali nello sviluppo di tecnologie del controllo. Scrive, cioè, senza mai però soffermarsi sulle implicazioni teoriche e politiche, del complesso militare-digitale che si è formato in questi decenni. Come quello militare-industriale è una minaccia alla democrazia, quel che conta però sono le differenze che emergono. In primo luogo: chi punta a controllare i naviganti sono sì le agenzie di *intelligence*, ma soprattutto le imprese. La raccolta di dati, la loro elaborazione per definire profili individuali in base al «consumo» di contenuti è parte integrante del loro *model business*.

LA SOCIETÀ DEL CONTROLLO è però sorella gemella del «capitalismo delle piattaforme». Da questo punto di vista, le imprese collaborano con i governi nazionali fino al punto di diventare «complici» nella sorveglianza di singoli, ma sono anche ostili a tale ingerenza statale perché mette a rischio l'accesso alla materia prima del loro business, la comunicazione.

È cioè un rapporto di cooperazione e, al tempo stesso, di competizione con i militari e l'*intelligence*. Solo così si spiega la presa di distanza, la critica, il conflitto tra alcune imprese e i servizi di *intelligence*. Il caso più eclatante è quello che ha visto Apple resistere e rifiutare ogni forma di collaborazione con la Fbi, quando questa ha chiesto di avere codici di accesso a un modello di smartphone. Tim Cook, il boss della mela morsicata, ha affermato che mai si sarebbe piegato alla richiesta, perché la privacy è un valore assoluto. Posizione lodevole, anche se Apple è una delle imprese che fa del segreto il suo vangelo: nulla si sa circa l'utilizzo dei dati personali raccolti, invocando il rapporto di fiducia con i suoi clienti. Un lessico commerciale che con la privacy e la libertà di espressione ha ben poco a che fare.

IL COMPLESSO militare-digitale è dunque una delle architravi del capitalismo delle piattaforme e della sua forma politica, la società del controllo. Ma è in questo frangente che nascono alleanze spurie, mediattivisti che lavorano con le imprese, queste ultime con i militari che, a loro volta, fanno uso di hacker. Un groviglio che andrebbe sciolto, affinché la libertà di parola e il rispetto della privacy di parola perdano il sapore dolciastro che nel capitalismo delle piattaforme legittima lo status quo.

Cresce il numero di siti violati

Sempre più siti web «bucati»: tra il 2015 e il 2016 sono aumentati del 32%. Per gli estensori del «Rapporto sullo stato della sicurezza del web» finanziato da Google, ciò è dovuto al fatto che i siti sono sempre più «vecchi» e meno protetti. La forma più usata è carpire le password e usarle per entrare negli archivi digitali e nei computer. Diffusa è sostituire la home page con una creata per ingannare gli utenti.

La contraddittoria formazione di un ramificato complesso militare-digitale

La crittografia di Whatsapp evidenzia il legame tra attivismo e innovazione

Un'installazione di Jakub Geltner