DEEP WEB
La rete oltre Google

Personaggi, storie, luoghi dell'internet profonda

di Carola Frediani

Prefazione

Vai, guarda, racconta. In fondo le regole del cronista sono semplici. Non è scienza, tutt'al più artigianato. Eppure in Italia il giornalismo fatica quasi sempre a pensare se stesso come autosufficiente. Preferisce rincorrere la letteratura, o peggio piegare verso la militanza, il commento. Quasi che i fatti fossero una circostanza trascurabile. Ce ne accorgiamo quando ci capita di esser testimoni di un evento e non ne ritroviamo i tratti fondamentali nei resoconti dei media. Se poi il tema è il digitale, le cose - se possibile – peggiorano.

Per questo le pagine di Carola Frediani che state per leggere sono una boccata di aria fresca. Ecco una collega che ha installato Tor sul proprio computer, ha frequentato il deep

web per anni, si è incamminata sulla Via della seta, ha trascorso giornate nelle chat per conoscere chi quel mondo frequenta da semplice spettatore oppure da protagonista, vendendo e comprando. Nel farlo ha dovuto rispondere a ogni passo e senza manuale di istruzioni alle domande alle quali ogni cronista si trova di fronte: sto correndo rischi, queste fonti sono affidabili, di chi sto facendo il gioco?

Il risultato è un'istantanea ricca di profondità di campo. La narrazione tecnica del funzionamento di queste realtà non è che il modo per garantire l'autorevolezza del racconto, l'affidabilità della cronaca. Il fuoco è sui personaggi, sugli impatti dei fenomeni presi in esame, sulle cause e sugli effetti. Sia che si parli di Anonymous, di hactivismo, di Onion (o della sua versione italiana Cipolla), la scrittura di grado zero e lo stile piano non fanno che risaltare i fatti. La scena e il contesto sono delineati con precisione, il

riflettore illumina anche gli angoli bui, fruga dove il resoconto del potere o le verità precostituite di solito non permettono al nostro sguardo di indugiare. Come sempre accade in questi casi, ci si accorge che la realtà non è manichea, non esistono buoni e cattivi, ma infinite sfumature di grigio (ben più di 50).
Nessuna tesi precostituita, nessun giudizio morale. Quello potrà trarlo il lettore, se vorrà.
Solo due riflessioni su tutte. Nell'epoca del Datagate, in cui abbiamo lasciato ai motori di ricerca e ai social network il compito di definire le nostre personalità pubbliche, esiste per ognuno di noi un diritto alla riservatezza, all'invisibilità di una parte del nostro essere che è sempre più difficile da difendere senza il web profondo e gli strumenti di criptazione utilizzati dall'autrice di questo libro. È un pensiero autoritario ritenere che se non si ha nulla da temere non si debba aver nulla da nascondere. Ben venga

il deep web come spazio di espressione, consapevoli che ogni luogo in cui abbiamo maggiore libertà presuppone da parte nostra maggiori responsabilità.

In secondo luogo questo libro rende chiaro ancora una volta come l'erosione delle libertà individuali inizi sempre dai margini. È molto facile consentire tutti sul fatto che la libertà di espressione vada garantita in un regime autoritario. Ma quanti di noi sarebbero d'accordo nel sostenere che ciò vada fatto anche nel caso di tesi odiose, per nulla condivisibili, o nei confronti di persone che per altri versi violino la legge? Questioni da sempre irrisolte, che l'età digitale amplifica e torna a riportare al centro della discussione pubblica.

Deep Web non pretende di avere risposte. Ma è di grande aiuto nel definire le domande.

Massimo Russo, direttore di Wired Italia

Il 15 per cento dei ricavi dell’autrice andranno a sostenere Privacy International [vedi in rete], Ong che si occupa di difendere la privacy e i diritti digitali.

Introduzione

“La prima regola del Deep Web è che non si parla del Deep Web”. Chi lo pratica e lo vive, per i motivi più diversi, in genere non ama la pubblicità. Chi dovrebbe parlarne, ad esempio i media, di solito non va mai oltre l’immagine cupa e vaga di “web oscuro”, di antro buio della Rete, che a volte arriva a tratteggiare una specie di inferno dantesco. Il regno di spacciatori, pedofili, terroristi, hacker disposti a tutto. Un luogo che viene presentato come remoto e inaccessibile, manco fosse Mordor, il paese di Sauron nel *Signore degli Anelli*.

Questo libro nasce quindi da un’esigenza quasi personale, quella di andare oltre la solita rappresentazione di una certa parte della Rete per capire effettivamente di che si

tratta, chi ci sta e come funziona. E per quale ragione la sua rilevanza negli ultimi anni è andata crescendo.

Non si parla solo di *Deep Web* in senso stretto, ma anche di ciò che lo lambisce a livello sia tecnico che culturale, come ad esempio l'*hacktivismo*. E soprattutto non è un manuale per imparare a usarlo o muoversi al suo interno: di documentazione su simili aspetti è piena internet, e come si dice in certi ambienti: GIYBF (Google Is Your Best Friend), Google è il tuo migliore amico. Quello di cui sentivo la mancanza era un ampio reportage giornalistico sul tema, ed è quello che ho cercato di fare in queste pagine.

Il libro si divide dunque in quattro parti.

Nella prima tratto l'incredibile vicenda di *Silk Road* e del suo presunto fondatore, Ross Ulbricht, noto online come Dread Pirate Roberts. La trovo una storia eccezionale per la concentrazione di questioni, complicazioni

legali e tecniche, colpi di scena e risvolti culturali, che ho provato a descrivere mantenendo la narrazione il più comprensibile e sintetica possibile, anche se resta probabilmente il capitolo più denso (siete avvisati). Sono pronta a scommettere che a breve sulla vicenda Hollywood ci farà un film (e del resto, a quanto pare, ne farà uno Brad Pitt su Anonymous). Di sicuro, qualunque cosa si pensi di Silk Road e della compravendita di droghe, quel sito non è stato semplicemente una piazza di spaccio trasferita online. Peraltro, al suo posto sono nati molti altri mercati neri: anzi, negli ultimi mesi c'è stata una proliferazione di epigoni di Roberts, anche se con esiti non sempre felici.
Nella seconda parte passo a una narrazione più distesa, fatta anche di molte interviste, in cui cerco di descrivere chi sono alcuni dei protagonisti del *Deep Web*, a partire da una comunità italiana come *Cipolla*, ma non limitandomi solo a quell'ambiente. Qui mi

soffermo molto sulla cybercriminalità, anche se in genere di dimensioni modeste. Cracker che bucano conti, carders - cioè chi ruba e utilizza i dati di carte di credito -, spacciatori, truffatori, venditori di malware. Insomma quel web oscuro di cui parlavamo all'inizio, visto alla distanza più ravvicinata possibile.

Nella terza parte mi occupo invece di una mia precedente passione, l'interesse per l'*hacktivismo*. Anche quello è web profondo. Si muove su canali simili e usa gli stessi strumenti, così come ha la stessa necessità di nascondere la propria identità, ma è mosso da motivazioni ideali. Inoltre, per svolgere la propria missione, ha bisogno di emergere e vivere nello spazio pubblico del web *in chiaro*.

Il tema è amplissimo, io stessa ne ho già scritto in un precedente ebook, *Dentro Anonymous*, quindi in questo caso ho deciso di selezionare in modo insindacabile un numero limitato di aspetti e di operazioni, sulla

base di due criteri: le azioni che mi sembravano più importanti (e recenti, mi riferisco soprattutto all'ultimo anno); o su cui avevo testimonianze e materiali più originali. Di nuovo: non può certo uscirne una fotografia complessiva, ma piuttosto uno spaccato che però - almeno lo spero - dovrebbe poter offrire spunti di analisi.

Infine la quarta parte, più breve, parla della rete *Tor*, il progetto che ha creato il sistema ad oggi più solido per garantire l'anonimato in Rete, nonché l'ambiente in cui si muovono i soggetti descritti nei precedenti capitoli. E non solo loro ovviamente: anche una pletora di giornalisti, attivisti, dissidenti, whistleblower e utenti che vogliono sfuggire alla sorveglianza del loro governo o di quelli altrui, come il *Datagate* ci insegna. Senza dimenticare che ci sono ancora molti luoghi del pianeta in cui rivelare la propria identità online, se quello che si fa o si dice è sgradito

al potere dominante, porta dritti in prigione o alla morte.

Il filo rosso che lega quindi il libro è il *Dark Web* nel suo significato di luogo che assicura l'anonimato e la privacy, e che sfugge alla sorveglianza globale; di spazio tecnicamente non irreggimentabile da legislazioni e autorità; di territorio di frontiera non ancora conquistato dai grandi attori della Rete, governi e corporation; di grande emporio del "Far Web" (copyright: Corrado Calabrò), che vede un via vai di criminali, pirati, libertari, anarcocapitalisti, avventurieri del software, predicatori, rivoluzionari e reietti. A volte si passano vicino senza sfiorarsi, a volte si odiano e si *sparano* addosso, altre volte fanno affari tra loro, alcuni incarnano la loro identità in maniera monolitica, altri assommano più ruoli a seconda della situazione, ma tutti condividono quell'ambiente e anche molti dei suoi assunti di base. Tutti ne hanno bisogno. E non solo loro.

Per quanto paradossale possa sembrare, oggi, nell'era del *Datagate* e del controllo pervasivo sulle comunicazioni elettroniche, i più limpidi e sinceri attivisti dei diritti umani e i più incalliti cybercriminali non possono che condividere lo stesso spazio.

Concludo precisando che questo libro alla fine è - o almeno vuole essere - un libro di cronaca. Sono sempre più convinta che i temi tecnologici e digitali abbiano bisogno di essere trattati esattamente come si tratta un movimento sociale o politico, una rivoluzione, una rivolta di piazza. Bisogna frequentare i gruppi che la portano avanti, andare alle riunioni, fermarsi a bere a quel bar dove si radunano tutti la sera, scendere a vedere che succede in strada. Insomma, bisogna starci in mezzo, soprattutto in luoghi come quelli qua descritti.

Nel giornalismo che si occupa di temi digitali o legati alla Rete c'è tanta, troppa teoria, e poca cronaca, che è quella che dovrebbe

sostanziare qualsiasi analisi. Eppure esistono spazi di racconto e di reportage vergini e sconfinati.
Dunque quelle che troverete nel libro sono delle cronache digitali, in cui si mescolano modalità e approcci giornalistici vecchi e nuovi. Perché scrivere di questi temi significa confrontarsi continuamente con una serie di dilemmi che non si trovano sui manuali professionali: come gestire il rapporto con una fonte anonima? Come proteggere la stessa? Come proteggere se stessi? Come verificare e incrociare affermazioni e notizie in un simile ambiente? Come tutelarsi da depistatori, mitomani e malintenzionati? Come comunicare in modo sicuro? Non mi metto a rispondere qui perché servirebbe un altro libro - e perché non ho tutte le risposte - ma posso certamente dire che, nel trattare temi come questi, è d'aiuto frequentare il più possibile. Il rischio di prendere cantonate è sempre alto, ma aumenta vertiginosamente se il

giornalista va in certi posti alla ricerca di informazioni solo quando succede qualcosa di eclatante.

Ho dunque provato a fare questo reportage nell'unico modo che mi pareva sensato, immergendomi per mesi in quest'ambiente. Nel caso dell'*hacktivismo* e di *Anonymous* dovrei dire anni, ormai, perché ho cominciato ad occuparmene giornalisticamente nell'estate 2011, per poi passare a una full immersion a partire dall'estate del 2012.

Do per scontato che la maggior parte delle azioni narrate siano illegali, non credo di doverlo specificare a ogni piè sospinto. Lascio al lettore la valutazione e il giudizio di quanto emerge da queste pagine che vogliono essere soprattutto una cronaca; e anche quando mi permetto alcune considerazioni, cerco di farlo sempre alla luce della mia esperienza concreta in questo mondo. So che fare cronaca non è molto di moda, specie in Italia. E a volte rischia di apparire anche un

po’ sovversivo. Forse, in un certo senso, lo è davvero.
Post-scriptum:
Se hai scelto di leggere questo libro, è probabile che tu abbia già un’infarinatura generale su temi quali *Deep Web*, *Anonymous*, *Bitcoin*, malware etc. In ogni caso, non preoccuparti: ogni volta che viene utilizzato un termine meno comune, troverai un link che ti porterà al vocabolario con la spiegazione del suo significato.
Gli pseudonimi (nickname) delle persone che ho intervistato sono stati tutti cambiati da me, tranne dove indicato.
Nota per la lettura: le parentesi [quadre] presenti nel testo all’interno di interviste e virgolettati contengono informazioni aggiunte dall’autrice.

CAPITOLO 1 - La triste storia di un pirata libertario

Il nipote: Un libro?
Il nonno: Esatto. Quando avevo la tua età, la televisione erano i libri. E questo è un libro speciale. Era quello che mi leggeva mio padre quando ero ammalato e che io leggevo a tuo padre. E oggi lo leggerò a te.
Il nipote: Parla di sport?
Il nonno: Scherzi? Liti, combattimenti, torture, vendette, giganti, mostri, inseguimenti, fughe, vero amore, miracoli...
Il nipote: Non sembra male. Cercherò di stare sveglio.
Il nonno: Oh, beh, grazie, molto gentile da parte tua. La tua fiducia è soverchiante.
(Dal film *La storia fantastica - The Princess Bride*)

È sobria e luminosa, la biblioteca di Glen Park, una sezione della San Francisco Public Library. Sedie spartane in legno chiaro, parquet, un'utenza tranquilla e variegata, e soprattutto una connessione Wi-Fi. Ed è proprio qui, che nel pomeriggio del primo ottobre 2013 l'Fbi fa irruzione, inoltrandosi fino alle scrivanie della sezione Fantascienza. In una tipica scena da film americano, un gruppo di agenti in borghese – tra i 6 e gli 8 - circondano e tirano via dal pc un giovane in maglietta e jeans, spingendolo contro una vetrata. "Siamo l'Fbi, è tutto sotto controllo", esclamano di fronte allo sconcerto dei presenti. Non che l'uomo appena ammanettato sia fisicamente pericoloso, ma l'importante è impedirgli di chiudere il computer a cui era collegato e tramite il quale stava chattando, a sua insaputa, proprio con un collaboratore della polizia federale, dopo aver aperto il pannello di amministrazione di *Silk Road*.

Già, perché il discreto frequentatore della biblioteca, il ventinovenne Ross Ulbricht, laureato all'università del Texas e affittuario di una stanza in un appartamento a San Francisco con altri due coinquilini, altri non era, secondo gli inquirenti, che Dread Pirate Roberts (DPR). Ovvero il leggendario e fantomatico fondatore e proprietario di *Silk Road*, il più grande, popolare, efficiente mercato della droga online. L'"Ebay dell'illegalità", in una delle tante definizioni dei media, che non appena ne avevano scoperto l'esistenza, due anni prima, erano andati in sollucchero, in un crescendo di pezzi a metà fra il fantasy-horror e il genere "incontri ravvicinato del terzo tipo".

Nave affondata, comandante catturato

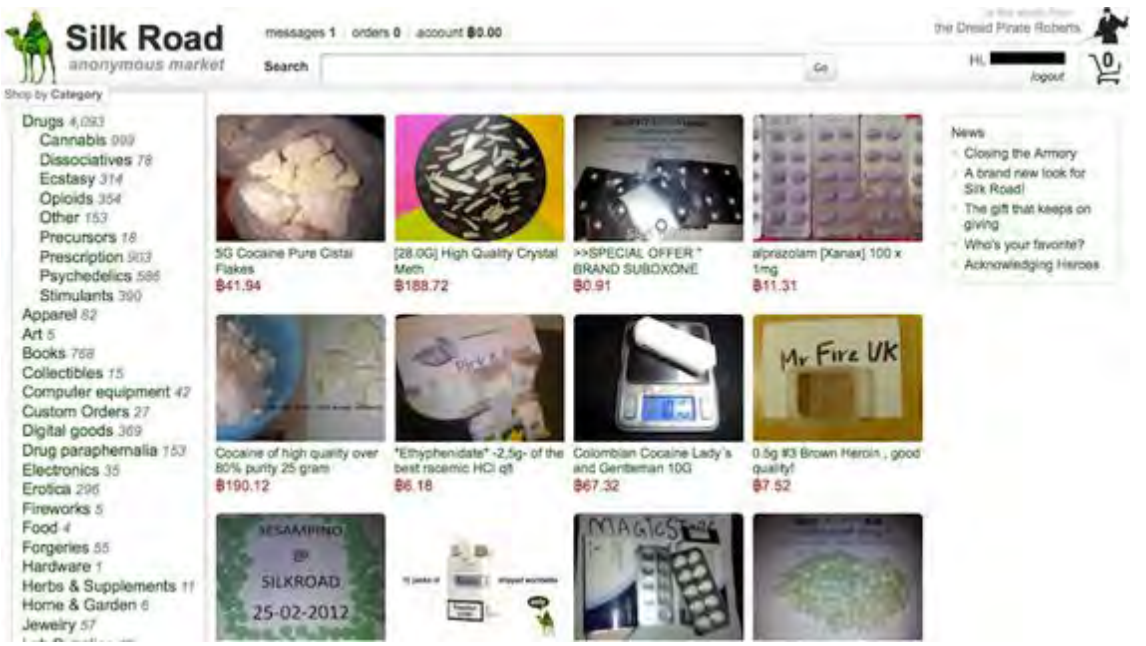
Sicuramente chiunque avesse visitato *Silk Road* per la prima volta, non avrebbe potuto evitare di farsi cogliere dallo stupore. Ordinato in comode categorie, presentava un vasto assortimento di stupefacenti - 13mila inserzioni nel settembre 2013 - molti dei quali, se non tutti, messi al bando in numerosi Paesi. Marijuana, LSD, MDMA, eroina, coca, ma anche sostanze e farmaci più esotici e di nicchia, tutti raccolti, prezzati e commerciati attraverso una miriade di venditori indipendenti, piccoli e grandi, sparsi in tutto il mondo, ognuno con una sua specialità e soprattutto una sua reputazione. Con feedback degli utenti, forum di discussione, meccanismi per risolvere eventuali dispute, un servizio clienti da far invidia ai giganti dell'ecommerce. Nel 2013 *Silk Road* aveva totalizzato quasi un milione di account, cioè

di persone che si erano iscritte, anche solo per curiosità e non necessariamente per vendere o comprare. Secondo le stime degli inquirenti, la piattaforma, nel corso dei suoi 2 anni e mezzo di vita, avrebbe facilitato l'equivalente di 1,2 miliardi di dollari di transazioni eseguite attraverso i *Bitcoin*, la criptomoneta sganciata da Stati e autorità centrali che tra i tanti vantaggi favorisce l'anonimato dei suoi utilizzatori (anche se va tenuto presente che la cifra appare *dopata* dalla crescita vertiginosa del valore di questa valuta elettronica).
La versione digitale della *Via della Seta* – dal nome dell'insieme di piste carovaniche e rotte commerciali che anticamente collegavano la Cina al Mediterraneo – nasce nel febbraio 2011, anche se a renderla popolare sui media sarà per primo il noto giornalista di Gawker Adrian Chen, che nel giugno dello stesso anno racconterà di questa sorta di incarnazione di romanzo cyberpunk.

“Attraverso la combinazione di una tecnologia di anonimato e di un sofisticato sistema di feedback, *Silk Road* fa diventare la compravendita di droghe tanto semplice quanto acquistare dell’elettronica usata online – e apparentemente ugualmente sicuro”, scrive il reporter. A metterlo sulla strada giusta un programmatore, Mark, che ha ordinato a casa sua dell’LSD: “Sono un anarchico libertario – gli spiega la fonte – e credo che tutto ciò che non sia violento dovrebbe essere depenalizzato”.

Un’idea condivisa e dichiarata dall’ancora giovane sito. “Lo Stato è la prima fonte di violenza, oppressione, ladrocinio, e di tutte le forme di coercizione. Smetti di finanziare lo Stato con le tue tasse e dirigi le tue energie produttive nel mercato nero”, aveva dichiarato a Chen, in una mail, l’allora amministratore di *Silk Road* (che però non si definiva ancora Dread Pirate Roberts: questo nickname appare sul forum del sito solo nel

febbraio 2012). Il riferimento culturale è all'agorismo [vedi], una filosofia politica libertaria anarco-capitalista, fondata da Samuel Edward Konkin III, decisamente anti-statale, che punta a una società in cui le relazioni fra persone siano basate su liberi scambi volontari, compiuti attraverso la realizzazione di mercati neri, non regolamentati da autorità esterne.



Da notare che fin dall'inizio *Silk Road* si configura come una realtà di condivisione e comunanza di idee, più che un business. "La nostra comunità è stupenda, composta da

persone intelligenti, oneste, giuste, comprensive e desiderose di cooperare le une con le altre”, scrive a Chen l’admin. Ciò nondimeno, in pochi mesi, il sito – ospitato e *nascosto* sulla rete *Tor* [vedi], la stessa che rende possibile ai suoi utenti di muoversi nell’anonimato – diventa davvero una eBay dei mercati neri. La sua cifra principale è proprio l’efficienza e l’affidabilità. Non si vendono solo droghe, naturalmente, ma anche servizi e strumenti di hacking, prodotti di elettronica, riviste e libri introvabili, oggetti di ogni tipo, più o meno legali o bizzarri, pornografia ma non contenuti pedofili. Viene infatti sviluppato anche un codice etico che esclude ciò che possa arrecare danno ad altri, e quindi, oltre che materiale su bambini, anche le armi sono off limits o i servizi violenti. Il sito sviluppa nel tempo un robusto sistema di reputazione dei venditori/compratori, un metodo di risoluzione delle dispute, nonché un fondamentale

meccanismo di salvaguardia delle transazioni basato sul concetto di *escrow*, cioè su dei depositi di garanzia, dove i compratori parcheggiano momentaneamente i soldi versati al venditore, per poi sbloccarli quando la transazione è andata a buon fine. Nasce un ricco forum dove, negli ultimi mesi prima della sua caduta, Dread Pirate Roberts aveva lanciato perfino dei gruppi di lettura, tra l'entusiasmo degli utenti.

La moneta usata sono ovviamente i *Bitcoin*, che un acquirente può comprare con uno dei tanti sistemi di cambio che oggi stanno proliferando dappertutto online, ma - all'epoca dei fatti - utilizzata soprattutto nel cosiddetto *Deep Web* o *Dark Web*, l'internet non indicizzata dai motori di ricerca e raggiungibile solo attraverso alcuni software, come Tor. Per ogni transazione *Silk Road* prende una commissione del 10 per cento, che va a diminuire col crescere delle operazioni effettuate dal singolo. In poco tempo diventa il

primo sito di ecommerce del *Deep Web*. Una ricerca della *Carnagie Mellon* stima che nel 2012 la *Via della Seta* fatturasse 1,2 milioni di dollari al mese. Altre stime più recenti collocavano il giro d'affari di questo mercato nero tra i 30 e i 45 milioni di dollari all'anno. Uno studio riportato da Forbes parla di circa 60mila visite al giorno al sito. "Nel 2012 pare che *Silk Road* avesse più di due milioni di transazioni al mese", mi dice The Architect in chat, un mese prima della rovinosa caduta di *Silk Road*, avvenuta il giorno dopo l'arresto di Ulbricht. The Architect è uno dei fondatori di *Cipolla*, la principale comunità italiana del Deep Web, e tra le persone più precise, disponibili e tecnicamente preparate – nonché attente alla sua privacy – che ho incontrato da queste parti. La prima volta che siamo entrati in contatto *Cipolla* si era appena inabissata col crollo di mezzo *Dark Web* (di cui racconto più avanti), e l'indirizzo fresco fresco del nuovo sito

e della chat l'avevo fortunosamente trovato su un un forum nascosto. Un altro mio contatto mi aveva indicato il suo nickname, in quanto uno degli amministratori storici della comunità. Così ero andata a colpo sicuro presentandomi al solito come giornalista, anche se non era mancato un momento di comico imbarazzo iniziale quando lui si era subito scagliato contro una serie di testate, incluse alcune per cui scrivevo. In realtà, appurato che non ero lì per chissà quale *scoop* mordi-e-fuggi, ha iniziato subito a spiegarmi un po' di cose. Peraltro io venivo da quasi due anni di immersione quotidiana nel mondo dell'*hacktivismo*, di chat e forum di *Anonymous*, per cui avevo sviluppato ormai una certa dimestichezza nel trattare con fonti anonime e nel muovermi nei loro ambienti.

Di lui, e di *Cipolla*, parlerò ampiamente più avanti. All'epoca della nostra conversazione *Silk Road* non era certo l'unico mercato nero digitale. I concorrenti erano molti: *Atlantis*,

Sheep Market, e soprattutto *Black Market Reloaded* (BMR). Ma The Architect non aveva dubbi: “ *Silk Road* è il migliore, è quello con le funzionalità migliori, ed anche il più sicuro contro il rischio di *scam*, di truffe. Però diventare venditori è più caro che altrove, costa circa 300 euro”.

Un meccanismo quasi perfetto che nell’estate 2013 sembra aver raggiunto la consacrazione. Il leader di *Silk Road*, l’anonimo e misterioso Dread Pirate Roberts, rilascia infatti un’intervista (attraverso il sistema di messaggistica interno del sito) alla testata americana *Forbes*. Dove dice alcune cose interessanti: “Non possiamo stare in silenzio per sempre”, dichiara il pirata. “Abbiamo un messaggio importante da dare e i tempi sono maturi per farlo. Quel che facciamo non ha a che fare col procurarsi una dose o con lo *sfidare le autorità*. Ha a che fare con la difesa dei nostri diritti come esseri umani e col rifiuto di essere soggiogati quando non abbiamo

fatto nulla di male”. Il boss del primo mercato di droghe online si spinge anche oltre, forse troppo. “Stiamo parlando della possibilità di un cambiamento epocale nella struttura di potere del mondo. Le persone ora possono controllare i flussi e la distribuzione delle informazioni e dei soldi. Settore dopo settore lo Stato viene tagliato fuori dall’equazione e il potere torna agli individui”.

Come sappiamo però, meno di due mesi dopo, lo Stato si è rifatto vivo, proprio nella biblioteca di San Francisco. E il giorno seguente *Silk Road* viene chiuso. A chi, come la sottoscritta, in quei giorni si è collegato al sito tramite il browser *Tor*, comparivano i simboli di varie agenzie americane e la scritta: “Questo sito nascosto è stato confiscato dall’Fbi”.

Un vero shock per gli aficionados, ma anche per tutti quelli che frequentano l'internet profonda. Il forum e la chat di *Cipolla*, la comunità italiana del Dark Web, ribollono di commenti allibiti.

"*Silk Road* è andato", mi saluta Colt, un utente che conosco e che fa parte del gruppo di amministratori di un altro sito, *Black Market Reloaded*, un concorrente della *Via della Seta*. Non è affatto contento però. Anche perché stava pensando di aprire un negozio proprio su *Silk Road*, dato che lui

stesso è un venditore di droga (e armi, anche se quelle non avrebbe potuto commerciarle). In compenso ora si devono preparare. Sanno già che ci sarà la diaspora degli utenti di *Silk Road* e l'assalto agli altri market. "Molti si stanno già spostando da noi", mi dice, facendo il punto della situazione. Allo stato attuale l'Fbi ha in mano, oltre ai *Bitcoin* sequestrati dal sito, 23mila [in realtà risulteranno poi essere 26mila], equivalenti in quel momento a oltre 3 milioni di dollari, "anche tutti i messaggi scambiati fra gli utenti, e gli indirizzi IP di login dei frequentatori. I messaggi si possono criptare, ma c'è chi non lo fa".

La *Via della Seta* ha infatti un suo sistema di messaggistica interna con cui i suoi utenti possono scambiarsi comunicazioni private, oltre a un forum e un wiki pubblici, in cui le persone si passano informazioni e consigli su una varietà di argomenti.

Un altro utente di *Silk Road*, anzi un suo *Top Reseller*, cioè un venditore affidabile che ha accumulato punti e feedback, e che contatto quella sera attraverso il sistema di messaggistica del forum, miracolosamente ancora online e pieno di commenti disperati, appare relativamente tranquillo. “Sono abbastanza sicuro che i venditori non corrano rischi se hanno seguito i giusti protocolli”, mi scrive. “Molti si stanno trasferendo su altri siti e riapriranno lì i negozi”. Lui fino al giorno prima spediva in giro delle barrette al cioccolato aumentate con funghetti e sostanze allucinogene.

Ma la cautela è d’obbligo e come vedremo l’arresto di Ulbricht sarà in realtà solo il primo di una serie. Nel contempo *Bitcoin*, la criptomoneta scambiata anche su *Silk Road*, fa un tuffo, scendendo di quotazione. Qualcuno subito si lancia in ardite previsioni di fallimento per la moneta *peer-to-peer*. Ma chi conosce bene il settore, non si fa

prendere dal panico. “La situazione ha creato un po’ di paura, reale e forzata”, mi spiega in quei giorni un esperto della valuta elettronica che però non vuole essere nominato. “C’è chi ha cercato anche di incentivarla, questa paura, per poter comprare *Bitcoin* a prezzi più bassi. Ieri c’è stato un grosso tonfo, un calo di circa 10 dollari, e lì qualcuno ha perso molto, mentre qualcun altro ha guadagnato tanto. Poi la quotazione è tornata su. In ogni caso credo che sul lungo termine il sequestro di *Silk Road* non creerà grossi problemi al mercato dei *Bitcoin*”. Ed è proprio così. Anzi, la critpomoneta sembra improvvisamente liberata dal fardello d’immagine che la associava ai black market e inizierà a volare, diffondendosi sempre di più in attività alla luce del sole e perfettamente legali.

Il lungo viaggio dell'operazione Marco Polo

Ma di cosa è accusato Ross Ulbricht, che i federali ritengono essere Dread Pirate Roberts? Di reati molto pesanti, ovviamente, per cui rischia almeno 20 anni di prigione. Associazione a delinquere per il traffico di droga, reati informatici e riciclaggio di denaro. Ma anche, ed è il capo d'imputazione più sorprendente, di aver commissionato almeno due omicidi (poi saliti a 6...) che - però - in realtà non sono mai avvenuti. Ma su questo torneremo più avanti.

Il giorno dell'arresto l'Fbi ha sequestrato il dominio di *Silk Road* nonché i *Bitcoin* che vi erano depositati dai vari utenti. Per gli investigatori il sito in questi anni avrebbe prodotto 80 milioni di dollari di commissioni. Le indagini sono iniziate molto presto, già nel novembre 2011, coinvolgendo diversi organismi americani, dalla DEA, l'ente di lotta

alla droga, all'*Internal Revenue Service* cioè l'Agenzia delle entrate, dalle divisioni investigative del Dipartimento di sicurezza interna fino all'Fbi. Ma da subito le investigazioni si sono scontrate contro il muro di gomma edificato dalla rete *Tor* da un lato e dal sistema di pagamento dei *Bitcoin*: entrambi, se usati con perizia, garantiscono un forte anonimato. Era quindi molto difficile sia *seguire i soldi*, secondo una tipica modalità d'indagine, che individuare i server che ospitavano *Silk Road*. La tesi più accreditata a questo punto, ma soprattutto quella che emerge dalla lettura degli atti, è che gli investigatori abbiano usato un approccio tradizionale e a tutto campo: si siano quindi messi sulle tracce dei primi segni di esistenza di *Silk Road* per scovare qualche indizio. Insomma, una ricerca su fonti aperte in rete per *beccare* i primi segnali interessanti relativi al mercato nero della droga. E hanno effettivamente cominciato a trovare

qualcosa: in particolare un messaggio, lasciato dal nickname Altoid su un forum di droghe, Shroomery.org [vedi in rete]}. “Ho trovato questo sito che si chiama *Silk Road*”, diceva l’utente, riportando anche l’indirizzo. “Volevo sapere se qualcuno lo conosceva o lo consigliava”.

anonymous market online? NEW 11
#13860995 - 01/27/11 04:28 PM (3 years, 2 months ago)

I came across this website called Silk Road. It's a Tor hidden service that claims to allow you to buy and sell anything online anonymously. I'm thinking of buying off it, but wanted to see if anyone here had heard of it and could recommend it.

I found it through silkroad420.wordpress.com, which, if you have a tor browser, directs you to the real site at http://tydgccykixpbu6uz.onion.

Let me know what you think...

Post Extras:

La cosa che ha fatto allertare l’Fbi è che si trattava della prima menzione pubblica di *Silk Road*. È il 27 gennaio 2011. Il post mandava i lettori su un blog Wordpress – silk-road420.wordpress.com - che a sua volta inviava all’indirizzo onion, su rete *Tor*, del mercato nero. Con un mandato i cyberpoliziotti vengono a sapere che il blog è stato aperto il 23 gennaio, solo 4 giorni prima del post di Altoid, che a questo punto appare

come una persona molto ben informata. O forse come uno che stava facendo astroturfing [vedi]: cioè stava cercando di fare pubblicità al neonato sito senza far capire che lui ne era il proprietario. Lo stesso nickname pubblica altri messaggi su una bacheca che tratta *Bitcoin*, e poi, nell'ottobre 2011, lascia un post dicendo di stare cercando un esperto informatico nella comunità della critpomoneta. E qui fa un errore madornale: dice di inviare le mail a `RossUlbricht@gmail.com`.

Dunque la prima menzione pubblica di *Silk Road* viene collegata a un'identità precisa. Infatti da Google l'Fbi viene a sapere che l'account è stato registrato proprio dall'omonimo giovane, e che è anche collegato a un profilo sul social network G+ dove si trovano foto di Ross e i suoi video preferiti su *YouTube*. Alcuni di questi linkano al *Mises Insitute*, il centro di ricerca della Scuola austriaca di economia, e in particolare agli studi di Ludwig von Mises, un economista che

ebbe un ruolo centrale nel diffondere le idee di questa dottrina libertaria e liberista e che influenzò anche il premio Nobel Friedrich August von Hayek. Anche Dread Pirate Roberts aveva citato e linkato i video dell'istituto. Ulbricht sta dunque diventando il primo e solo indiziato. Secondo gli atti d'indagine gli scritti di Ludwig von Mises hanno costituito la base filosofica di *Silk Road*. Che rappresentava l'espressione più radicale di libero mercato.

Ma i federali non si fermano qua. Vanno sul profilo di *LinkedIn* di Ulbricht, e notano un suo commento: "I miei obiettivi sono cambiati", scrive il giovane spiegando di non essere più interessato alla fisica. "Voglio usare la teoria economica come un mezzo per abolire l'uso della coercizione e aggressione nel genere umano. L'uso della forza più ampio e sistemico è esercitato da parte di istituzioni e governi, quindi ora questo è il mio interesse principale. Tuttavia il modo migliore di

cambiare un governo è modificare le menti dei governati. A questo fine, sto creando una simulazione economica per dare alle persone un'esperienza diretta di come potrebbe essere la vita in un mondo senza l'uso sistemico della forza". Un pensiero simile, ma molto più articolato, appare in un articolo anonimo pubblicato su un magazine online alternativo di Austin, Texas, la stessa città d'origine di Ulbricht.

Insieme al ritratto psicologico, gli investigatori continuano a cercare però altri indizi che leghino il giovane a *Silk Road*. E trovano un altro account, registrato sempre da Ross Ulbricht all'inizio del 2012 su *StackOverflow* – una specie di Yahoo Answers per programmatori - con cui l'uomo chiede un aiuto tecnico per un `hidden service`, un servizio o sito nascosto dietro alla rete *Tor*, proprio come il mercato nero delle droghe. In pratica cerca uno sviluppatore php con esperienza su *Tor*. Poco dopo Ulbricht cambierà il suo

nick in *frosty* e modificherà anche la mail, ma l'errore – se è davvero lui DPR, dal momento che il giovane professa la sua innocenza – era stato ormai fatto.

Questo è dunque il quadro indiziario. A cui, nell'estate 2013, si aggiunge un fatto rilevante: il 10 luglio la dogana intercetta un pacco, diretto proprio a casa di Ulbricht, nell'ambito di un controllo di routine, almeno così dicono, anche se la coincidenza in questo scenario appare davvero troppo fortuita. E ci trovano nove carte d'identità contraffatte, con nomi diversi, ma tutte con la foto di Ross.

Il 26 luglio agenti della *Homeland Security* vanno quindi a bussare alla sua porta chiedendo chiarimenti del pacco, lui risponde di non saperne niente e – incredibilmente – come possibile spiegazione dice che in teoria chiunque potrebbe andare su un sito come *Silk Road* usando *Tor* per poi ordinare droga e documenti falsi da inviare a qualcun altro per incriminarlo. Sul momento Ulbricht viene lasciato stare ma, a quanto pare, in contemporanea, l'Fbi ha finalmente scovato almeno uno dei server di *Silk Road*, sparsi in vari Paesi: in particolare ne ha trovato uno in una nazione straniera, cooperante col governo americano. E attraverso un trattato di mutua assistenza legale, ha ottenuto di avere una copia degli hard drive del server. Questa operazione è avvenuta il 23 luglio 2013 e segna probabilmente la vera data finale di *Silk Road*. Per la cronaca verrà poi fuori che i vari server erano dislocati fra Islanda, Belize, Arkansas e California.

Come ha fatto l'Fbi a trovare il server? Non si sa, e ci sono varie speculazioni. Ha compromesso *Tor* mentre veniva usato da Ulbricht? Hanno tracciato in qualche modo i soldi avendo comunque un sospettato su cui concentrarsi? Hanno hackerato il sito per scoprirne l'indirizzo IP e poi hanno contattato il Paese dove stava il fornitore di servizi hosting per avere l'immagine del server? Il tutto senza tirare ancora giù il sito per non insospettire Ulbricht? Non ci sono certezze tranne che, con la copia del server in mano, l'Fbi ha iniziato a trovare molto materiale interessante. Ad esempio, ha visto che la chiave pubblica di cifratura dell'amministratore di *Silk Road* terminava con *frosty@frosty*, stesso nick usato in precedenza dal giovane. Che una versione simile del codice che Ulbricht aveva postato su *StackOverflow* era usata nel sito. E poi hanno trovato i messaggi privati lasciati sul forum, che mostravano come Dread Pirate Roberts

avesse cercato dei documenti falsi proprio nel mese precedente al pacco inviato a casa di Ross.

Un furioso Walter White?

A questo punto, come hanno osservato alcuni, la storia di DPR-Ulbricht prende una piega a dir poco folle. Perché l'Fbi lo accusa anche di aver commissionato online ben due omicidi (che poi aumenteranno a sei!). Qui va aperta una parentesi su una delle leggende metropolitane del Deep Web: e cioè che tra le tante terribili nefandezze che vi si possano comprare ci siano anche degli anonimi killer. Ebbene, chiunque nell'ambiente vi dirà che si tratta quasi sempre di una truffa al 99,9 per cento. Che si tratti di annunci isolati sparsi per i forum delle darknet o di siti che si pubblicizzano come agenzie di assassini in affitto, quali *Hitman Network* o *C'thulhu Resume* – che non si fanno mancare slogan markettari del tipo: "Il miglior posto dove mettere i tuoi problemi in un sepolcro" - chi naviga queste acque profonde non può che nutrire una totale diffidenza e incredulità

verso gli stessi. Non dimentichiamo che, alla fine, l'attività criminosa più diffusa nel *Dark Web* resta la truffa. Eppure il boss del più grande mercato del *Dark Web* si sarebbe affidato proprio a questo strumento per risolvere... alcuni problemi inaspettati.
Secondo l'Fbi, il 13 marzo 2013, quando ancora tutto sembrava andare a gonfie vele per *Silk Road* anche se le indagini erano già in corso, Roberts viene avvicinato da un utente che si chiama friendlychemist, il quale dice di aver hackerato il pc di uno dei maggiori venditori della *Via della Seta*, sottraendo molte informazioni sui compratori. Dati che è pronto a rilasciare online, screditando la reputazione del sito, se il pirata non lo paga 500mila dollari sull'unghia. Insomma, una vera e propria estorsione. friendlychemist dice di aver bisogno di quella cifra per pagare a sua volta i suoi fornitori di droga con cui è indebitato. Il 20 marzo Roberts chiede di essere messo in

contatto con i creditori di friendlychemist e – per quanto strano possa sembrare – ottiene di parlare con uno di loro, Redandwhite, che sembrerebbe far parte degli *Hells Angels*, la nota gang americana. Roberts cerca di blandirlo e di convincerlo a venire a trafficare su *Silk Road*, quindi gli fa capire che se friendlychemist fosse fatto fuori non gli dispiacerebbe. E gli passa l'indirizzo (come l'abbia ottenuto non è chiaro) del suo ricattatore, che in teoria viveva a White Rock, in Canada. A quel punto Redandwhite chiede 150mila dollari per un'uccisione "non pulita" e 300mila per una "pulita". Roberts sostiene di aver già ingaggiato un killer in passato per la più ragionevole somma di 80mila dollari e pretende uno sconto.

Alla fine i due si accordano per 150mila. Secondo l'Fbi i log (il registro) della transazione in *Bitcoin* mostrano effettivamente questa somma di denaro inviata a Redandwhite. Il quale il primo aprile (mai

data fu più simbolica) manda il seguente messaggio al pirata: “Il tuo problema è stato risolto... Stai tranquillo perché non ricatterà più nessuno”. Sembrerebbe che Redandwhite abbia inviato almeno una foto, dato che il 5 aprile Roberts avrebbe risposto dicendo: “ho ricevuto l’immagine e l’ho cancellata”. E pare che il boss di *Silk Road* avesse dato al killer anche un codice da fotografare sulla scena del delitto per essere sicuro che l’immagine fosse autentica.

Ma dunque il morto c’è stato? Beh, in realtà non si trova. Alle autorità canadesi non risulta né che ci fosse un cittadino con quel nome né che ci sia stato un omicidio in quella zona in quei giorni.

In compenso l’Fbi sostiene che Roberts, prima di questo fatto, avesse commissionato anche un altro omicidio: a quello si sarebbe riferito parlando degli 80mila dollari con Redandwhite. E in questo caso l’agenzia federale dovrebbe essere bene informata sulla

vicenda dal momento che il killer ingaggiato sarebbe stato... un suo agente.
Nel gennaio dello stesso anno, sostengono infatti gli atti di indagine, Roberts era infuriato con un suo dipendente – pagato fra i mille e duemila dollari a settimana – perché, dopo avergli rubato dei soldi, si era fatto pure arrestare (e poi rilasciare) non senza aver trattato incautamente con un agente infiltrato. Come abbia fatto a sapere del suo arresto (non uscito sui giornali) o della sua identità non è chiaro. Ad ogni modo decide di farlo torturare finché non gli siano restituiti i soldi rubati, ma poi, temendo potesse spifferare troppe cose alla polizia, opta per farlo fuori. E con chi va a trattare l'operazione alla Pulp Fiction? Con lo stesso poliziotto sotto copertura che aveva incastrato il suo dipendente. Si accordano per 80mila dollari, 40mila pagati in anticipo da un conto bancario australiano a uno americano. L'agente procura quindi a Roberts una prova

del delitto, con tanto di foto. Secondo indiscrezioni uscite poi su Wired, il pirata avrebbe addirittura ricevuto cinque o sei foto, comprensive di pratiche di waterboarding [vedi] e di cadavere finale. Roberts si mostra un po' turbato, in quanto "nuovo a questo genere di cose". "Sono incazzato di averlo dovuto uccidere... ma quel che è fatto è fatto", scrive. "Solo non posso credere che sia stato così stupido... vorrei che ci fosse più gente onesta". Il primo marzo quindi il pirata invia la seconda tranche del pagamento.

Chi era il dipendente che sarebbe dovuto morire? Di lui sappiamo qualcosa di più. Il suo nome infatti in seguito è stato reso noto: si chiama Curtis Clark Green, ha 47 anni, abita nello Utah, ha una moglie, due figlie, e un cane. Nella vita offline aveva fatto il paramedico per un'associazione che aiuta disabili, più altri lavori precari, e con la moglie aveva avuto qualche piccolo guaio con la giustizia. Appassionato di poker, pare abbia

anche un passato di tossicodipendenza. Di sicuro faceva sfoggio delle sue conoscenze al riguardo su *Silk Road*, dove era piuttosto noto e dove condivideva molte informazioni personali. Infatti Green nella vita online era conosciuto come Flush o Chronicpain, e riceveva uno stipendio come uno degli amministratori del sito. Proprio come Roberts (e come Ulbricht), dichiarava idee libertarie e nutriva una passione per il politico repubblicano Ron Paul, un punto di riferimento dei *libertarians* negli States (apprezzato anche da figure come Edward Snowden, il `whistleblower` [vedi] del *Datagate*, e Julian Assange, il fondatore di *WikiLeaks*). Il suo lavoro consisteva soprattutto nel gestire lamentele e richieste degli utenti del sito, si occupava come dire della customer care. In tale ruolo poteva accedere ai messaggi (non criptati) scambiati fra venditori e compratori e ai conti degli utenti dove venivano

depositati i *Bitcoin*; inoltre doveva inviare rapporti regolari sulla sua attività a Roberts.
Come sono arrivati a Green gli investigatori? Torniamo indietro, all'aprile 2012: da mesi è in corso un'ampia indagine su *Silk Road*, significativamente ribattezzata *Marco Polo*. Compito principale del moderno esploratore veneziano, reincarnato in vari agenti infiltrati, è di approcciare i contatti più vicini a Roberts per imboccare finalmente il viottolo giusto che porti al cuore del sito.
Un agente si finge così un trafficante di droga che sta cercando un intermediario per fare arrivare una partita di media entità a un altro venditore. In modo incauto, e forse all'insaputa di Roberts, Green si offre per questo ruolo: ciò significa che accetta di ricevere un chilo di cocaina a casa sua, per un controvalore di 27mila dollari, che lui dovrebbe poi passare a a un'altra persona. Ma poco dopo la consegna di *bamba*, si presenta a casa sua anche l'Fbi, che lo

arresta. Green non rimane molto in custodia, presumibilmente perché inizia a collaborare, al punto da prestarsi anche a una macabra messinscena. Quando gli agenti lo informano del fatto che Roberts avrebbe commissionato - a loro stessi, come sappiamo - il suo omicidio, viene allestito un set in cui lo fotografano *morto*.

Non c'è da stupirsi della capacità di iniziativa mostrata dai federali. Secondo la stessa ordinanza di arresto di Ulbricht, nel corso delle indagini gli agenti hanno compiuto

almeno un centinaio di acquisti di sostanze di ogni tipo, registrando un livello di purezza degli stupefacenti superiore rispetto a quelli presi in strada. Avevano inoltre una schiera di agenti infiltrati e di informatori, in genere venditori che dopo essere stati individuati si erano prestati a collaborare, mentre veniva congelato o silenziato il loro iter giudiziario per non farne trapelare notizia. Fra questi anche Nod, uno dei più grossi commercianti di droghe di *Silk Road*, che per mesi ha continuato a smerciare cocaina, eroina e metanfetamina sotto la supervisione dell'Fbi.

La cattura di Green ha segnato però un salto di qualità. Anche se il responsabile del servizio clienti non conosceva la reale identità di Roberts, arrivare al pirata e al suo computer è stata sicuramente una mossa decisiva per l'operazione *Marco Polo* - nella quale le agenzie investigative americane sembrano aver profuso molte energie. "Solitamente i casi di cybercrime non si affidano ad analisi

forensi o alla ricerca dell' indirizzo IP, nonostante sia quello che molti credano, e vengono risolti più prosaicamente con tecniche di *normale* indagine, perché la gente dice molto di più di quanto dovrebbe e c'è sempre uno che poi parla e fa i nomi degli altri", mi spiega Giacomo Paoni, esperto di cybersecurity e criminalità informatica. "Quello che invece ho notato in questo caso, almeno in base alle informazioni pubbliche, è stato l'enorme sforzo per trovare *prove* digitali, o meglio indizi. Insomma, non c'è una *pistola fumante* contro Ulbricht: sono tutte supposizioni che si basano non su un singolo errore eclatante ma su una lunga serie di indizi che uniti danno un'idea di insieme". Per questi motivi Paoni ritiene che si tratti di uno dei casi di cybercrimine più interessanti.

La vicenda è indubbiamente molto complessa e articolata, e tanti restano i punti oscuri. Di sicuro Ulbricht - dando per buono un suo coinvolgimento nella gestione del sito

senza per forza identificarlo con Dread Pirate Roberts – ha commesso alcuni errori. Nei giorni successivi al sequestro di *Silk Road*, sebbene molti commenti lasciati dagli utenti sul forum siano a sostegno di Ulbricht/Roberts, non mancano messaggi allibiti e critici. Uno dei thread più letti s'intitola: *Dread Pirate Roberts era davvero così stupido?*, con l'utente che passa in rassegna tutte le presunte leggerezze del giovane: "Ha pubblicato un indirizzo Gmail che conteneva il suo nome in relazione al nickname usato per pubblicizzare *Silk Road* all'inizio; ha usato una Vpn [Virtual private network, una rete usata in genere per aggirare filtri web], e non *Tor*, per accedere a *Silk Road*, e con la stessa anche alla sua Gmail, il tutto dallo stesso IP; utilizzava un hotspot WiFi poco distante da casa sua; ha fatto capire il fuso orario in cui viveva; sul suo vero profilo LinkedIn si descriveva come uno che stava progettando di creare un mondo senza l'uso sistemico

della forza da parte di governi e istituzioni; ha ordinato dall'estero dei documenti falsi e se li è fatti spedire a casa per comprare nuovi server per *Silk Road* – quel che è peggio le foto ritraevano proprio lui e, considerato per cosa sarebbero i serviti i documenti, non aveva proprio senso; quando gli agenti del DHS si sono presentati alla sua porta per le carte d'identità ha citato *Silk Road*". E poi avrebbe fatto troppo lo sbruffone nell'intervista a *Forbes*, se davvero rilasciata da lui - anche se le indagini erano in stadio avanzato, e difficilmente l'articolo ha fatto la differenza, al massimo ha accelerato i tempi. In generale, comunque, avrebbe rivelato troppo di sé.

Vedendo il quadro complessivo col senno di poi, sembra che il giovane Ross abbia fatto davvero molti passi falsi. Ma non tutti nel *Dark Web* sono così severi. "Non è così facile dare tutta la colpa a lui", mi dice il già citato The Architect, uno dei fondatori e

amministratori di *Cipolla*, nei giorni successivi alla caduta di *Silk Road*. “Chi avrebbe mai pensato, con un esperimento nato nel 2011, di arrivare a questi livelli? Purtroppo essere paranoici retroattivamente non funziona. Non penso che sia uno stupido, affatto, Roberts era uno che sapeva il fatto suo. Considerato che non era nemmeno laureato in informatica e chiedeva aiuto su come usare *Tor* col php è stato fin troppo bravo. Purtroppo però da una parte i soldi danno alla testa, e lo dimostrano la mole di *Bitcoin* accumulati [il portafoglio di Ulbricht ne conterrebbe 144mila, come vedremo più avanti] e gli omicidi commissionati; dall’altra c’è il fatto che non puoi prevedere se avrai successo quando lanci qualcosa del genere, e lui probabilmente non l’aveva messo in conto”. Insomma, anche per The Architect il caso mostra errori umani ma anche una grande coordinazione e impiego di risorse.

Le carte segrete giocate dall'Fbi

Questa ipotesi, allo stato attuale la più verisimile, non fuga però i dubbi e gli angoli bui, nonché le paure di chi conta sulla rete *Tor* per garantirsi l'anonimato, indipendentemente dall'attività cui sia dedito. Perché una delle domande ricorrenti, in quell'ottobre 2013, era se l'Fbi o altre agenzie investigative fossero riuscite a individuare i server e/o alcuni utenti di *Silk Road*, malgrado l'anonimato teoricamente garantito da *Tor*. Il fatto che la chiusura dell'eBay delle droghe sia avvenuta in pieno scandalo *Datagate*, che ha fatto emergere settimana dopo settimana l'elefantiaco sistema di sorveglianza delle comunicazioni globali messo in piedi dagli statunitensi, ha alimentato le speculazioni al riguardo.
Come ha notato anche l'avvocato americano Bernie King, le prove contro Ulbricht sono

quasi interamente circostanziali. La mail che si lega a quei primi messaggi, le simpatie politiche dell'indagato sono sicuramente un punto di partenza per approfondire le indagini, ma dopo mesi e mesi di sforzi per identificarlo l'Fbi è arrivata a fornire un quadro accusatorio con molti punti interrogativi. Non sarà che la pistola fumante a cui facevamo riferimento anche prima c'è ma non si può menzionare? Qui entra in gioco un'ipotesi dalle implicazioni più vaste del caso specifico, ovvero l'idea che sia stata usata contro *Silk Road* la pratica della *ricostruzione parallela*.

Si tratta di un processo usato per ricreare un filone di indagine che mascheri la fonte originaria di informazioni con cui si è arrivati a individuare una persona o un sito. In pratica quello che succede è che un'agenzia come la Nsa (National Security Agency, che gestisce i programmi di sorveglianza delle comunicazioni globali, e che in teoria

avrebbe un mandato che le consente di usare i suoi amplissimi poteri di monitoraggio solo per casi di terrorismo e di minaccia alla sicurezza nazionale provenienti dall'estero) ottenga delle dritte attraverso i suoi strumenti, che possono essere i più vari, dalle intercettazioni di mail e telefonate ad ampio raggio all'hackeraggio vero e proprio di computer e siti. A quel punto passa le informazioni ottenute ad altre agenzie, come la Divisione di Operazioni Speciali della DEA, che si occupa di lotta alla droga, la quale a sua volta li passa all'Fbi. Gli agenti federali però devono omettere il coinvolgimento delle altre agenzie nel costruire il caso, il che significa creare altre situazioni, attraverso le normali pratiche investigative, per fingere di essere venuti in possesso di quelle informazioni. In questo caso il sospetto è che la Nsa sia riuscita a compromettere almeno in parte l'anonimato garantito da *Tor*, ad esempio nella individuazione di alcuni utenti specifici

o del server di *Silk Road*, tracciando in tal modo la connessione Ulbricht/Roberts. A quel punto la ricostruzione parallela avrebbe usato l'escamotage del controllo di routine e casuale da parte degli agenti della dogana che sono incappati nei documenti falsi inviati a Ulbricht – salvo che quel controllo non sarebbe affatto avvenuto per caso. Questo ha dato un asso nella manica ai federali che hanno sfruttato la visita all'appartamento di Ulbricht per stringere il cerchio della caccia all'uomo e giustificare nel contempo il modo in cui sono arrivati al capo della *Via della Seta*, mentre usavano l'accesso al server per estrarre altre informazioni utili. Una volta arrestato il giovane Ross e messo le mani sul suo pc, hanno chiuso tutti i buchi rimasti.

Tutto ciò potrebbe sembrare una questione di lana caprina: l'importante sono i risultati no? si chiederà il lettore. Ma, come nota lo stesso King (e anche altri), la ricostruzione parallela solleva molti interrogativi e viola il

diritto costituzionale di un imputato a una giusta difesa. Se infatti i suoi avvocati non sanno come un'indagine ha avuto inizio, sono limitati nella loro capacità di revisionare potenziali fonti di prova (errori, pregiudizi, testimoni non affidabili) che potrebbero discolpare i loro clienti. Come ha notato anche la professoressa di legge della *Harvard Law School* Nancy Gertner, la Nsa ha come obiettivo fermare il terrorismo e per questo gode di più ampi poteri; mentre programmi come quello del DEA investigano casi di comune criminalità, soprattutto legata alla droga. "Un conto è creare regole speciali per la sicurezza nazionale", ha obiettato Gertner, "ma il crimine comune è interamente diverso. In questo modo è come se contaminassero le indagini". Anche perché le fonti originarie di prova sono tenute nascoste non solo agli avvocati degli indagati ma anche ai giudici e alla pubblica accusa.

Silk Road è stato dunque scovato grazie a uno degli exploit della Nsa? E non lo si vuole far sapere anche per tenersi buono lo stesso strumento per altri casi?

Quanti pirati ci sono?

C'è poi un altro aspetto su cui aleggia un certo mistero. E cioè che Dread Pirate Roberts non era probabilmente una figura unica, o non è sempre stato la stessa persona. Questa ipotesi era data per certa da quasi ogni frequentatore assiduo di *Silk Road* e del *Deep Web*. E del resto è avallata dalla stessa scelta del nickname. Sappiamo infatti che questo pseudonimo deriva dal noto e temibile pirata Bartholomew Roberts, che fra '600 e '700 razziò il mar dei Caraibi. Ma la sua rinascita moderna, come Dread Pirate Roberts, è avvenuta con il ruolo sotto forma di coprotagonista del film *La storia fantastica* (*The Princess Bride* - 1987), tratto a sua volta da un romanzo. La specificità di questo personaggio leggendario nella versione cinematografica è proprio quella di non essere un solo individuo, ma di coincidere con una serie di persone diverse che si

passano il nome di Dread Pirate Roberts, nonché la sua temibile fama, come un testimone.
“Roberts era diventato così ricco che voleva andare in pensione. Mi ha condotto nella sua cabina e mi ha confidato il suo segreto: Mi chiamo Ryan. Io non sono Dread Pirate Roberts, ha detto. Ho ereditato la nave dal precedente Roberts, come tu la erediterai da me. Ma anche quello che me l’ha passata non era il vero Roberts, Il suo nome era Cummer-bund. Il vero Roberts si è ritirato 15 anni fa e vive come un re in Patagonia”. Così parla il pirata della Storia fantastica.
Una identità multipla, ripresa dal Roberts del *Dark Web*, che fa venire in mente altri fenomeni digitali del genere: *Anonymous*, dove la sigla è ancora più diluita e diffusa, data quasi in franchising; o anche Satoshi Nakamoto, il misterioso inventore di *Bitcoin*, che si pensa possa essere un nome collettivo

(anche se c'è chi, come *Newsweek*, ritiene di averlo individuato invece).

Del resto, nella stessa intervista a *Forbes* dell'estate 2013 il presunto Roberts, confermando la *vox populi* , dice di non essere il fondatore di *Silk Road*. È dunque lecito domandarsi, come fa la giornalista australiana Eileen Ormsby che da tempo scandaglia il *Dark Web* attraverso un suo blog, "quanti pirati ci sono là fuori?" "Sono al cento per cento sicura che ci sia più di una persona che pubblica sul forum come DPR", ha scritto la reporter. La sua personificazione più recente, aggiunge, non ha nulla a che fare col precedente DPR, e non solo perché ha cambiato lo stile di scrittura, cosa che potrebbe fare anche chi volesse depistare. "Ha proprio cambiato il suo QI e l'intera personalità. Sono certa che il DPR con cui ho scambiato messaggi nel corso degli anni sia mutato almeno una volta". Ormsby è persuasa che ci siano stati multpli DPR. Questa sua

convinzione è stata espressa in un post precedente all'arresto di Ulbricht – dove diceva che secondo lei ci sarebbero stati nel tempo 3 o 4 DPR – ed è stata ribadita successivamente. La giornalista riconosce che il collegamento Altoid/Gmail di Ulbricht smentirebbe l'ipotesi dei multipli DPR, ma aggiunge che quando ricercò in passato l'origine di *Silk Road* imbattendosi negli stessi messaggi postati da Altoid non aveva trovato alcun riferimento alla mail di Ulbricht. Forse, ipotizza, l'Fbi è riuscita ad accedere a post cancellati.

A rendere il tutto più intrigante c'è il fatto che a guidare le operazioni dell'Fbi che hanno portato alla cattura di Ulbricht sia stato Christopher Tarbell. Si tratta di un agente speciale che era già stato protagonista dell'identificazione di un hacker molto noto, Hector Xavier Monsegur, conosciuto online come Sabu, uno dei leader di *Lulzsec*, costola di *Anonymous*. Qualcuno considera Tarbell l'

Eliot Ness dei tempi digitali, cioè il brillante investigatore che incastrò Al Capone, anche se il paragone fra le figure di arrestati non regge molto. Sta di fatto che Tarbell, e l'hacker che ha prima catturato e poi messo al lavoro come informatore, Sabu, è riuscito a smantellare *Lulzsec*, facendo arrestare, tra gli altri, l'hacktivista Jeremy Hammond, condannato a 10 anni di carcere per aver diffuso le mail di una azienda di intelligence americana. Secondo le accuse dello stesso Hammond, attualmente in prigione, Sabu, nel ruolo di spia, ha hackerato o spinto altri ad hackerare aziende e governi. È possibile che quello stesso Sabu abbia contribuito anche alle indagini su *Silk Road*? si chiede qualcuno. È forse lui il misterioso e abile *Agente-1* nominato negli atti d'indagine?

In ogni caso, mentre si dipanava la vicenda di Ulbricht/Roberts, con dettagli sulle indagini che uscivano in ondate successive e che a un certo punto hanno portato a sei il

numero di omicidi teoricamente commissionati (ma mai commessi) dal giovane texano, il *Dark Web* non restava fermo. A un mese dalla sua chiusura, come un'araba fenice *Silk Road* rinasceva dalle sue ceneri: molto simile nella grafica alla prima versione, con un nuovo indirizzo [vedi in rete] onion [vedi], e con alcune funzionalità aggiuntive, ad esempio la possibilità per gli utenti di usare una chiave di cifratura PGP come ulteriore sistema di autenticazione. La pagina del login, con la frase "Questo sito nascosto è rinato", parodiava quella di chiusura del vecchio sito postata dall'Fbi. Ma chi lo ha rimesso in piedi così velocemente? Ed era davvero affidabile?

Tra i nuovi admin sembrano esserci nomi noti del vecchio sito, a partire da un certo Libertas. Ma naturalmente, negli ispirati messaggi postati sul forum, ricompare anche Dread Pirate Roberts, o almeno il suo

pseudonimo. “Benvenuti di nuovo nella libertà”, scrive.

“Sono gli ex moderatori del forum di *Silk Road*”, mi dice Colt, il già citato admin del sito concorrente, *Black Market Reloaded*. “Non credo che sia necessario però un sostituto ufficiale del vecchio sito”, interviene The Architect, mentre parliamo in una chat di gruppo. “Io infatti non mi iscriverei, e penso che in pochi lo faranno”, aggiunge un altro utente. “Il fatto è”, aggiunge The Architect, “che nel Dark Web non ci si può più fidare, e del resto farsi una reputazione non è facile. Secondo me le persone tenderanno ad affidarsi agli altri siti già esistenti”.

Anche perché l’onda lunga della chiusura di *Silk Road* deve ancora lambire molti lidi. Nel dicembre 2013, in un’operazione internazionale, vengono arrestate altre tre persone collegate alla prima *Via della Seta*, tre ex moderatori. Andrew Michael Jones (noto come Inigo) in Virginia, Gary Davis

(noto come Libertas) in Irlanda e Peter Phillip Nash (che aveva diversi nick, come Anonymousasshit) in Australia. Inigo e Libertas sono anche due degli amministratori del rinato *Silk Road*, da cui infatti spariscono gettando il panico fra gli utenti rimasti.

Ma già nelle settimane precedenti erano stati raggiunti una serie di venditori della prima *Via della Seta*, tra Stati Uniti, Svezia e Gran Bretagna. È solo in questo momento che viene ufficialmente arrestato anche Nod, il noto venditore di *Silk Road* con un *negozio* di 1400 clienti, che da mesi faceva ormai da informatore.

“La cattura di tanti venditori potrebbe far pensare che *Silk Road* non criptasse i messaggi degli utenti e che dalla copia del server l’Fbi abbia ricavato molte informazioni”, commenta The Architect. Infatti la cifratura dei messaggi scambiati attraverso la *Via della Seta* era a discrezione degli utenti.

Tuttavia, nota The Architect, “è abbastanza scontato che un sito nascosto (`hidden service`) critti il disco: ma forse quello non era criptato”. Insomma ci sarebbero dovute essere due protezioni almeno: i singoli che cifravano i loro messaggi volontariamente e il disco che cifrava tutto. “Su *Cipolla* ho appena implementato tre livelli di protezione”, aggiunge The Architect.“ Un sito con le possibilità di *Silk Road* avrebbe potuto, anzi avrebbe dovuto fare molto di più”.

Di tutta la vicenda, comunque, l’elemento più sfuggente alla fine rimane Ross Ulbricht. Malgrado le prime foto circolate di lui lo ritraggano con un’espressione un po’ allucinata (che s’inseriva bene nella cornice mediatica del nerd trafficante), in quasi tutte le altre è l’immagine del bravo ragazzo, solare e amante della natura [vedi in rete]. C’è quella che lo mostra abbracciato alla nonna; quella in cui sorride insieme ad altri famigliari; quella con gli ex-compagni scout (sì, è

stato un boy scout). Qualcuno nota che è pure bello.

Ma chi era veramente Ulbricht?

Un brillante studente di fisica, interessato alle celle solari, tanto da aver pubblicato alcuni studi accademici su questo argomento. Intorno al 2008 però inizia a perdere interesse per la vita da ricercatore, e soprattutto le sue riflessioni sembrano spostarsi sull'economia. Come già detto in precedenza, nel suo profilo *LinkedIn* cita la scuola economica austriaca e scrive di voler lavorare su un progetto per abolire l'uso della coercizione e dell'aggressione tra gli uomini.
Per il resto ha una vita apparentemente simile a molti suoi coetanei americani: college, amici, ragazze, qualche episodio di consumo occasionale di droghe. Nonché esperienze di volontariato: è stato infatti il presidente di una no-profit che raccoglieva libri usati da donare alle prigioni. Chissà se ora che si trova in un carcere di Brooklyn può

beneficiare di alcuni di quei volumi. In ogni caso non sembra essersi troppo abbattuto: nel dicembre 2013 teneva delle lezioni di yoga che hanno riscosso grande successo tra gli altri detenuti.
Ulbricht è anche bravo a disegnare e alcuni dei suoi lavori, che denotano una certa inquietudine, sono circolati ampiamente sulla stampa.

Di sicuro ha alle spalle una famiglia che lo difende a spada tratta. Il fondo legale per la

sua difesa - gestito dai genitori – dà un'immagine di Ross del tutto incompatibile con quella di trafficante internazionale di droga e soprattutto di freddo mandante di omicidi ordinati online. "È una persona non violenta, pacifica e compassionevole", ha dichiarato la madre Lyn, che pochi giorni prima dell'arresto era andata con il figlio a campeggiare in un bosco. Il sito, che raccoglie donazioni per le spese legali, mette in fila la testimonianza di amici e conoscenti, che parlano di un giovane intelligente, equilibrato, socievole e gentile. In effetti nella storia personale dell'indagato non c'è nulla, al di là delle sue idee libertarie, che possa fare presagire una simile parabola: cioè non solo mettere in piedi il più grande eBay di droghe online, ma arrivare a programmare perfino degli assassinii. Una vicenda alla *Breaking Bad* che malgrado le molte evidenze resta nel suo complesso oscura e contraddittoria.

Nei documenti presentati dall'accusa alla richiesta di libertà su cauzione, poi negata, avanzata da Ulbricht lo scorso autunno, i tentati omicidi salgono a sei. Secondo le carte, il presunto killer Redandwhite, cui Roberts aveva affidato il compito di far fuori il suo estorsore friendlychemist, cioè il canadese che lo stava ricattando, gli avrebbe detto che la vittima aveva un complice, che viveva con altre tre persone. A quel punto il capo di *Silk Road* avrebbe deciso di farli eliminare tutti. Inutile dire che anche in questo caso non c'è traccia di tali assassinii.

Tuttavia l'accusa ha tirato fuori anche quanto trovato sul computer di Ross il giorno dell'arresto: ci sono i pannelli di amministrazione del sito; c'è il riferimento a un nick usato anche da Dread Pirate Roberts; c'è addirittura un diario che dettaglia molte attività legate alla *Via della Seta*, in cui l'autore si definisce il suo creatore, e in cui racconta come nel 2011 coltivò in un

capanno diversi chili di funghetti allucinogeni da rivendere su *Silk Road*, anche se – scrive - “non ho ancora il sito online”. Sempre sul suo pc i federali hanno trovato un portafoglio contenente 144mila *Bitcoin* che al momento del sequestro equivalevano a 20 milioni di dollari. Ulbricht ha presentato un’istanza contro la confisca del borsellino digitale, dicendo che è suo, non legato alla *Via della Seta*. I *Bitcoin* sequestrati direttamente da *Silk Road* sono stati 26mila.
Da quanto emerso finora sembra oggettivamente difficile escludere un coinvolgimento di Ulbricht in *Silk Road*. Resta però in piedi l’ipotesi che non fosse un uomo solo al comando: troppo diffusa in molti osservatori e utenti era la sensazione che ci fossero più Dread Pirate Roberts; inoltre il trentenne di Austin non era così preparato a livello informatico; infine, il clone di *Silk Road* è rinato nello spazio di qualche settimana.

“Noi crediamo che Ross Ulbricht sia innocente”, è scritto sul sito del fondo ufficiale per la difesa del ragazzo. “Tuttavia questo caso va oltre il singolo individuo. Ross è solo la punta dell’iceberg, con questioni molto più grosse in gioco. Si tratta di un caso storico il cui risultato impatterà sulle nostre vite. Infatti stabilirà un precedente su questioni come: la privacy in internet, sia personale che finanziaria; l’autonomia in Rete; l’interferenza del governi e la loro invasività, sia online che offline; il controllo governativo del commercio”.

Può sembrare che i familiari del giovane vogliano capitalizzare sullo scandalo del Datagate, dando al caso legale delle implicazioni più generali che non ha. Ma in verità queste posizioni sono le stesse sostenute da Ulbricht da ben prima dell’arresto, nonché da Dread Pirate Roberts, dai moderatori del sito, da molti suoi utenti, oltre che da una comunità che va oltre i confini di *Silk*

Road. Che include persone come Mike Gogulski, un traduttore, libertario, appassionato di *Bitcoin*, apolide per scelta, che subito dopo la chiusura di *Silk Road* aveva autonomamente messo in piedi un sito [vedi in rete] per raccogliere soldi per Ulbricht. Oggi quel fondo rimanda a quello ufficiale della famiglia, e come mi scrive la stessa madre di Ross, "accetta donazioni in *Bitcoin* per le spese legali, in modo indipendente dal nostro sito che finora non è strutturato per ricevere offerte con la criptomoneta".

Lo stesso Gogulski in passato aveva cofondato il *Bradley Manning Support Network*, un sito a favore di quella che è poi divenuta Chelsea Manning, la soldatessa americana che è stata la fonte di *WikiLeaks*, condannata a ben 35 anni di prigione.

"Non mi importa del fatto che DPR fosse un cosiddetto trafficante di droga" scrive sul sito Reddit un utente che appoggia l'iniziativa di Gogulski "per quanto anche questa sia una

definizione impropria, dato che tutto quello che ha fatto (a parte le accuse non provate) era di gestire un sito che connetteva compratori e venditori. Molte persone che conosco compravano il loro fumo occasionale su *Silk Road* invece di dover frequentare loschi trafficanti di strada (...). No, le sole imputazioni che mi interessano sono quelle relative ai presunti omicidi su commissione. Se sono veri, avrei dei problemi a sostenere il fondo legale. Tuttavia, ho bisogno di qualcosa di più della parola dell'Fbi per credere a quelle accuse, dato che ognuno conosceva DPR, le sue azioni e i suoi ideali. Certo sarebbe dura supportare un ipocrita sociopatico, se risultasse vera la storia; ma siccome molte di queste stessi soggetti infestano anche gli apparati statali, darò a DPR il beneficio del dubbio. Per tutti questi motivi sostengo gli sforzi di Gogulski per assicurare a Ulbricht una difesa adeguata".

Tuttavia, per i pm statunitensi, non ci sono dubbi: il giovane di Austin ha mostrato una “sinistra indifferenza per la vita degli altri mentre operava il suo cartello della droga online”. I tentati assassinii minano non solo l’immagine del pirata libertario, ma anche l’idea che il suo sito fosse un esperimento per liberarsi dalla violenza e dalla coercizione statali. Ma era davvero Ulbricht il Roberts che commissionava gli omicidi? E quanto ha pesato l’intervento degli agenti infiltrati che a un certo punto, tra informatori, infiltrati, compravendita di droghe e messinscene, sembrano aver guidato le danze di *Silk Road*? E il sito era davvero paragonabile a un cartello come quelli del traffico internazionale? In realtà sembrava esserne così distante da obbligare Roberts, se le accuse dell’Fbi reggeranno, a cercare un killer nel primo truffatore che capitava online. E dando per autentico e attendibile il *diario di Ulbricht*, il tutto sarebbe nato con una

partita di droga coltivata in quegli stessi boschi dove il giovane Ross andava a fare il boy scout. Insomma, l'ex-studente di fisica s'inventa il sito, lo realizza chiedendo informazioni e aiuti qua e là, lo pubblicizza e si autoproduce la prima merce da venderci sopra. Sembra la realizzazione perfetta del mito americano del self-made man.

"Chiudere *Silk Road* ha reso il mondo più pericoloso? Finché i narcotici saranno illegali, verranno venduti su mercati neri. Meglio che accada online che in strada", scrive Gogulski citando a sua volta un corsivo della rivista americana *The Atlantic*. "Paragonata alla violenza epidemica che ha caratterizzato il commercio delle sostanze durante tutta la Guerra alle Droghe, e che non mostra segni di attenuazione per il futuro, un commercio di stupefacenti senza frizioni in confronto sembra un'utopia".

La *Via della Seta* – che, come ha confermato la stessa polizia, offriva in media sostanze

più pure di quelle reperibili in strada - avrebbe potuto essere una reale alternativa ai cartelli violenti, ma – secondo un corsivo sul *Guardian* – era solo un target più facile per l'Fbi .

"Sei libero? Sì e no. La libertà è qualcosa di relativo e non quantificabile. La domanda è: "Come posso essere più libero?" E la risposta dipende da TE". Così aveva scritto Ross nel suo profilo Facebook. Paradossalmente, la sua ricerca di libertà l'ha portato alla sua negazione massima, in prigione. L'originario *Silk Road* è affondato, e il suo epigono ha avuto finora un'esistenza molto difficoltosa. "Dovessimo vincere la battaglia, nascerà una nuova era. Anche se perdiamo, il genio è fuori dalla bottiglia e loro stanno comunque combattendo una guerra perdente", declamava il vecchio *Silk Road*.

Alla fine la domanda da porsi non è tanto quanti Dread Pirate Roberts ci siano là fuori. Ma, piuttosto, quanti altri Ross Ulbricht.

CAPITOLO 2 - Cinquanta sfumature di Dark Web

Erano chiamati i “rinnegati di tutte le nazioni” - pregiudicati, prostitute, debitori, vagabondi, schiavi fuggitivi e servi contrattualmente vincolati, religiosi radicali e prigionieri politici, tutti che erano migrati o erano stati esiliati nei territori oltre la linea.
(Da *I ribelli dell’Atlantico. La storia perduta di un’utopia libertaria*, di Peter Linebaugh e Marcus Rediker. Titolo originario in inglese: *The Many-Headed Hydra: Sailors, Slaves, Commoners, and the Hidden History of the Revolutionary Atlantic*)

“Ho per le mani uno stock di Taser. C’è qualcuno interessato? Pistola elettrica Taser da 800KV, è destinata alla sicurezza personale. Una volta messa in funzione manda, tramite

due cavi che vengono lanciati, una scossa elettrica di 800Kv, in grado di immobilizzare l'aggressore, garantendo così la vostra sicurezza". A parlare, in una chat pubblica su un sito nascosto del *Deep Web*, è Kali, una cracker donna, una criminale informatica. "Ma è di quelli che sparano o sono i classici che non funzionano?", le domanda un altro utente. "Spara". "Quante ricariche hai?" "Ci sono pacchetti da 3 dardi. Cento euro la scatola. Cinquecento il Taser".

Scampoli di ordinaria conversazione all'interno di una comunità del profondo web. Dove si alternano personaggi, situazioni e discorsi di tutti i tipi, spesso divertenti, a volte decisamente bizzarri, talvolta inquietanti e tendenzialmente al limite o ben oltre la legalità. Un calderone che però non può essere facilmente inquadrato in semplificazioni o classificazioni di maniera. E su cui bisogna fare la tara per la tendenza alla provocazione, l'ironia, il sarcasmo e l'effetto di

amplificazione provocato dalle comunicazioni online, specie dalle chat.

Hacker, cracker e biscotti

Non è però il caso di Kali, che parla senza fronzoli o il bisogno di impressionare nessuno. Lei è una degli operatori principali di questa chat. La conoscono tutti, e tutti la temono. Delle persone che ho incontrato nel *Dark Web* è infatti la cybercriminale più a tutto tondo: truffe su *eBay*, creazione e gestione di `botnet`, violazione di conti correnti online, commercio di credenziali di carte di credito, falsificazione di documenti, traffici di varia natura con diversi tipi di monete virtuali. Non si fa mancare nulla, sembra vivere di questo, e non si preoccupa di parlarne alla luce del sole. La sua è una piccola impresa di cracker: ha infatti dei collaboratori con cui si divide diversi compiti, alcuni in posizione nettamente subalterna, perché comunque è lei la più brava. È davvero una donna? In questi posti il sesso femminile è nettamente minoritario, ma non c'è nulla nella sua

presenza online che contraddica la sua identità sessuale dichiarata.

Sul forum, come mercanzie esposte sul banco di un bazar, dettaglia in lunghe liste la sua offerta commerciale. C'è il *recupero* password email / *Facebook* / *Twitter* / *PayPal* / *eBay* etc.: prezzi a partire da 200 euro, in base alle informazioni ricevute e al target. C'è la registrazione dei tasti schiacciati (`keylogging`) e di audio/video dell'attività di un computer vittima (solo sistemi Windows), attività raccolta in genere dopo aver infettato in qualche modo il pc obiettivo con un software che poi ne prende il controllo: a partire da 300 euro. C'è il recupero di credenziali di accesso a conti bancari o sistemi di pagamento (solo Windows) che costa intorno ai 500 euro. I prezzi, scrive, sono indicativi, mentre la possibilità di riuscita è intorno al 70 per cento, anche se, *ça va sans dire*, il pagamento viene effettuato solo a lavoro completato. Poi ci sono servizi più

mirati e speciali, di tipo *investigativo* diciamo: un tabulato di un noto operatore telefonico con numerazioni entranti/uscenti in chiaro: 800 euro (lo storico va indietro al massimo un anno); tabulato di qualsiasi gestore fisso o mobile italiano: duemila euro; audio conversazione GSM/UMTS e consegna della conversazione su chiavetta: 800 euro all'ora su orario fornito dal cliente.

Le chiedo come mai si trova qua a fare da operatore della chat. "Ho dato una mano a cercare un canale IRC (Internet Relay Chat) nuovo e sicuro quando hanno chiuso quello vecchio", mi dice. "Prima frequentavo altri forum del *Deep Web*, tipo il vecchio *HackBB*". Quest'ultimo era un grosso sito/forum che raccoglieva scambi di informazioni e di strumenti per l'hacking: software, vulnerabilità, pezzi di database violati, credenziali di accesso a siti o carte di pagamento. Insomma, il ferramenta dei criminali informatici. Si è però inabissato nell'estate del 2013,

dopo il più grande attacco a una parte del *Deep Web* mai registrato negli ultimi anni, quello contro *Freedom Hosting*, e di cui parlerò più avanti. “Poi mi sono accorta che esisteva una community italiana e che mancavano dei servizi che io già proponevo su *HackBB*”, prosegue. “Ad esempio non c’era nessuno che vendeva database utenti, o che proponeva dei servizi di hacking di alto profilo; o nessuno che commerciava bot”. I bot sono computer che sono stati violati senza che il loro proprietario se ne sia accorto e che sono comandati da remoto da un hacker (il botmaster) per svolgere un’ampia gamma di operazioni: possono essere usati tutti assieme all’interno di una `botnet` per sferrare attacchi informatici oppure venire spolpati pezzo dopo pezzo, nel senso che il botmaster li usa per spiare l’attività o le credenziali dei loro utilizzatori. Per poi magari rivendersi o riutilizzare in altro modo i dati ottenuti. “Alla

fine è stata una questione di mero business”, dice Kali.

Le chiedo che cosa sta facendo in questo momento e se mi può dare un’idea dei suoi guadagni. “Ho appena venduto un database con nome, cognome, mail e password in chiaro di circa 1000 utenti a 40 euro”. Non è tantissimo e non ci si può certo dedicare solo a quello. Kali in realtà è specializzata in servizi più avanzati, ha smesso di bucare banche dati. La sua attività più redditizia è come BotMaster [vedi], anzi BotMistress, specifica. “Più che affittare `botnet` le vendo o vendo direttamente i bot. Sono di prima qualità, cioè di prima mano, con solo il mio server sopra, e il prezzo è di 30 euro ogni 100”. In pratica passa i suoi bot ad altri che stanno creando una loro `botnet`. Quando possibile Kali buca anche conti bancari. Oppure aiuta *colleghi* che hanno violato dei conti a fare il cashout, cioè a tirarci fuori dei soldi, dato che è l’operazione più delicata e difficile. In

tal caso si prende il 50 per cento della cifra. Nel conto in genere ci si entra violando il pc dell'utente, anche se, dice Kali, "è capitato di bucare il frontend [la parte di sito che gestisce l'interazione con gli utenti] di qualche banchetta e immetterci una pagina di phishing [una pagina finta, sotto controllo dell'hacker] per poi rubare credenziali da lì". La tecnica per sottrarre i soldi invece è abbastanza complessa: semplificando, si devono avere tutte le password della vittima, e ottenerle violando all'occorrenza anche il suo cellulare (nel caso in cui ci siano password veicolate via sms). Ovviamente la presenza di un `token`, la chiavetta che genera codici seduta stante, rende le cose molto più difficili. "Poi il bonifico deve esser calibrato in base agli spostamenti che fa in genere la vittima, rendendolo il più possibile credibile. Insomma, non deve destare sospetti e va inviato ad un Iban italiano o al massimo europeo in area SEPA". Kali ha dei

collaboratori che le aprono dei conti, in gergo si chiamano muli. I quali a loro volta le rigirano i soldi, magari in *Bitcoin*, dopo una serie di passaggi per rendere le transazioni irrintracciabili. Le chiedo se i muli non corrano dei rischi. “Un po’, ma fondamentalmente devono solo avere la faccia di bronzo di andare in banca con una carta di identità che gli procuro io stessa, con sopra la loro foto, anche se il nome è diverso”.
Kali svolge tutte queste attività a tempo pieno. Dice che per anni ha fatto l’esperta di sicurezza informatica (la *white hat*), e “non venendo pagata praticamente nulla... ho deciso di passare al lato oscuro della forza”. Il che ha i suoi pro e i suoi contro. “La cosa positiva è che non devi rendere conto a nessuno, e che quanto guadagnato è veramente legato alle tue abilità. D’altra parte, se non hai la capacità di scindere il lavoro dalla vita reale, ti uccidi di ansia e paranoie. Naturalmente tra gli aspetti negativi c’è pure il

rischio di essere beccata un giorno... Ma prima che ciò avvenga spero di essermi già sistemata”. Le chiedo se non prova mai dispiacere o rimorso per le vittime. “Per arrotondare a volte mi capita di fare truffe su *eBay*, e lì è un po’ più pesante, ad esempio quando gabbi la ragazzina tutta eccitata perché pensa di aver trovato a buon prezzo l’iPhone da regalare al suo fidanzato. Devo dire che in quel caso un po’ mi dispiace, poi però mi dico che tutti devono vivere in un modo o nell’altro. È un po’ come la legge naturale... e comunque con il tempo ci si fa il callo e non si hanno più scrupoli”. Tutto è lecito se genera soldi, conclude. Le domando se non abbia dei limiti: armi, pedopornografia, cose del genere. “Per le armi non ho contatti, purtroppo. Il pedoporno mi limito a ignorarlo o al limite a sfruttarlo a mio favore, magari ricattando utenti che hanno hard-disk stipati di materiale. In realtà sono abbastanza impassibile di fronte a tutto: anni

di frodi e lavori del genere ti portano ad essere depredata della morale”.
Kali infatti fa questo *mestiere* da tempo. Anche se cambia nickname in continuazione, e cerca di non rivelare troppe informazioni su di sé. Si definisce totalmente apolitica, e accetta di collaborare con alcuni soci, solo online e anonimi, tranne qualche contatto di vecchia data. I suoi amici nella vita reale sanno unicamente che lavora col pc, a parte ovviamente il suo partner. Ha anche alcuni schiavetti online, che l’aiutano in compiti minori, e con i quali ha instaurato un rapporto di dominanza in pieno stile e linguaggio sadomaso. Non mi dice la sua età per ovvie ragioni, ma come si può intuire non sembra giovanissima.
Decisamente sbarazzino è invece Holden, un giovane che probabilmente non supera i venticinque anni. Sveglio e gioviale, online è l’immagine del simpatico ragazzo della porta accanto. Che però conviene tenere molto

lontano dal proprio pc. Anche lui cerca di mungere in vario modo carte di credito/debito, conti *PayPal*, e conti bancari. So che non è un mitomane perché lavora con altri utenti che conosco e che mi confermano le sue attività. Una sera mi fa anche vedere degli screenshot (tagliati in modo da renderli non identificabili) del pannello di controllo di un conto di una nota banca italiana. Gli chiedo come fa a entrare in sistemi che in genere sono ritenuti piuttosto blindati. “Di solito i conti di banche grosse e importanti, che hanno una sicurezza adeguata, li buchi solo lato utente [cioè come dicevamo prima infettando il computer del cliente, e rubandogli dati e credenziali di accesso, anche in tempo reale]. Ma a volte si trovano anche istituti *di nicchia* i cui sistemi di sicurezza lasciano molto a desiderare, e che quindi consentono un attacco lato server [ovvero direttamente al sito della banca]”. Anche lui ribadisce che il token è il loro nemico principale. Ma a

quanto pare non tutti gli istituti lo utilizzano. “Alcuni forniscono un servizio di avviso sms”, prosegue Holden, “però anche quello può essere bypassato”.

Gli chiedo allora come fa a infettare i computer delle persone, se utilizza il phishing, una tecnica molto conosciuta per cui si invia a qualcuno una mail finta che sembra provenire da un servizio noto e affidabile (la stessa banca, *LinkedIn*, etc.) ma che in realtà è controllato dall’hacker. Se l’utente abbocca e clicca sui link della mail può iniziare la procedura di infezione del suo pc. “In realtà non ho mai mandato una mail di phising”, mi dice. Non vuole dare troppi dettagli sul come, ma di fatto il suo obiettivo è quello di far scaricare ai target - che dice di selezionare in qualche modo, cioè di non sparare a caso nel mucchio - dei malware di tipo RAT, che prendono il controllo del computer. Funzionano in modo simile a quelli usati per agganciare dispositivi da attaccare a una

botnet, con la differenza che quest'ultimo tipo di software è più semplice e ha meno funzioni, perché deve infettare migliaia di apparecchi senza appesantire la rete. Anche Holden conferma che comunque la fase più difficile, una volta entrati nell'internet banking di qualcuno, è come rendere credibile e *invisibile* il bonifico con cui si cerca di estrarre soldi.

In quanto alle botnet, lui non è particolarmente interessato. Ne compra qualcuna più che altro per *spulciarla*. Ovvero per rastrellare profili di social network, conti *eBay* e *PayPal*, mail, comunicazioni... In pratica acquista pc già infettati da qualcuno, li infetta a sua volta, elimina l'infezione preesistente e passo dopo passo cerca di assumere il maggior controllo possibile degli stessi, finalizzato all'estrazione di dati di qualità.

"Ieri ho fatto partire la webcam a uno slave [schiavo, cioè un pc infettato all'insaputa del proprietario, e quindi per sineddoche anche

questo ultimo] che se n’è accorto e ha guardato allibito nella videocamera, era come se mi guardasse dritto in faccia”, ha raccontato una sera Holden a me e ad altri nel corso di una chat di gruppo. Seguono risate e commenti divertiti. “Aveva un’espressione stupefatta. Ovviamente gli ho inviato il solito messaggio di errore del driver, solo che era sbagliato, era quello preimpostato. Così gli è apparsa la scritta: Visita il mio sito: www.prova.it”. “Sarà rimasto scioccato”, replica un altro. “Non ho capito, hai attivato senza volere la sua webcam?”, gli chiedo. “No, l’ho fatto di proposito: di solito ti accorgi subito della reazione dall’altra parte... Se la webcam ha un pallino verde che avvisa l’utente dell’attività, te ne accorgi dalla faccia... Come in questo caso. E allora ti affretti a mandare un messaggio di errore driver, o qualcosa di simile, solo che in questo caso ho pure inviato il messaggio sbagliato”. “Ma non rischi che l’utente si insospettisca?”,

domando. “Un utente comune fa spallucce e se non succede di nuovo, amen, la cosa finisce lì”. “Ma perché attivi la webcam?” “ Farsi gli affaracci altrui... non ha prezzo! E poi non sia mai che ci possa essere qualche bella fanciulla”.

Holden si descrive – ed effettivamente appare – come un ragazzo brillante e problematico. Ha un background sociale medioalto, ma una tarda adolescenza da scavezzacollo. Piccolo spaccio di erba, feste, risse, orari impossibili, un ribellismo generale e un desiderio di adrenalina. Mi racconta che in passato voleva addirittura entrare nei reparti speciali di un corpo militare. Sembra un giovane come tanti altri, ma tendenzialmente più intelligente e inquieto. Non coltiva interessi politici, ma ha una sua morale. “Ti giuro che non entrerei mai nel tuo pc”, mi dice una volta per rassicurarmi ottenendo come risultato di farmi controllare subito la webcam (che tengo peraltro schermata con un

adesivo). “E perché mai?”, gli chiedo. “Perché tu sei qua in pace solo per sapere delle cose. E comunque mi è capitato più di una volta di rinunciare a un colpo per rimorso”. Rimorsi o meno, Holden mi dice di guadagnare circa 3mila euro al mese, quando va male; ben di più, quando va bene. Gli chiedo che ci fa con tutti quei soldi. “Li metto da parte, ci pago affitto e bollette, li passo con qualche scusa ad alcuni familiari, faccio tanti regali, e mi diverto come posso”. Ama viaggiare e gli sport estremi. Gli dico di smetterla di fingere di fare il boy scout. Mi risponde di esserlo stato, una volta.

Colt invece non è un hacker o cracker che dir si voglia. Però frequenta assiduamente il Deep perché ha messo in piedi un suo *negozio* di droghe. Vediamo cosa offre leggendo le inserzioni che ha messo in un forum: innanzitutto, specifica, “Non accetto perditempo”. E nemmeno *escrow*, cioè depositi di garanzia, perché, date le grandi

quantità, i soldi devono scorrere. Di che quantità stiamo parlando? Cocaina, pura al 90 per cento, dai 5 grammi (540 euro) a salire fino a 1 chilo (65mila euro); Mdma, dai 100 grammi (1450 euro) fino a 1 chilo (13500 euro); speed, dai 200 grammi (1200 euro) ai 5 chili (12mila euro); pillole da 100-140 mg, da 1200 (2100 euro) a 5mila (6900 euro).
Gli domando allibita del chilo di coca... Lui si mette a ridere. “Sì, stupisce sempre tutti”. Normalmente le richieste che riceve sono di quantità di gran lunga inferiori, spiega, tuttavia è in grado di scalare fino ai limiti massimi indicati. Gli chiedo se ha mai venduto tutta quella roba in una botta e risponde affermativamente, un ordine arrivato da un utente di un altro Paese. L’idea che qualcuno tratti online con una controparte del tutto anonima una simile entità di droga e di soldi mi lascia perplessa, ovviamente, però Colt – anche se non intende dirmi nulla sulla provenienza di queste sostanze - le

vende veramente, *conosco* altri utenti che acquistano da lui. Del resto lui fa parte anche di un vero e proprio mercato nero, *Black Market Reloaded*, di cui avevo già accennato. Si tratta del principale concorrente di *Silk Road*, anche se non ha mai raggiunto quei livelli di popolarità. Lì si trovano anche armi, e Colt infatti vende qualcosa pure in quel settore: pistole e carabine, fra i mille e tremila euro. Restiamo sul tema delle droghe e gli chiedo cosa tira di più. “Coca e Mdma in rocce e pillole sono quelle che vanno maggiormente”, mi dice. “Lo speed un po’ meno ed è anche la cosa meno costosa. Poi ovviamente quella che è più richiesta in assoluto è l’erba, è un mercato senza fine, lo sanno tutti”. Quella però lui non la commercia perché non abbastanza profittevole. Mi spiega che prima aveva un lavoro normale, ma che successivamente lo ha lasciato e ora campa così. “Non è che non voglia lavorare ma, sai, farsi un sacco di ore al giorno per un

millino al mese... Prima avevo un lavoro, sì, ma di merda. Ora vivo contento”. Colt dice di avere diversi contatti ma sulla sua vita offline preferisce non riferire quasi nulla. Al Deep è arrivato perché un giorno ha letto alcune cose al riguardo, e “siccome mi piace espandere i miei orizzonti me ne sono impratichito”.

Colt non ha solo un negozio su *Black Market Reloaded*, fa anche parte dello staff che lo gestisce. Prima è stato moderatore, a titolo volontario: aiutava gli utenti, rispondeva sul forum, sedava liti o dispute. Successivamente è diventato uno degli admin, anche se il fondatore o quanto meno il boss di questo mercato nero è abbastanza noto, anche col suo nick, e si chiama Backopy. La caduta di *Silk Road* non ha portato fortuna al suo competitor. Dopo la prima ondata di utenti che vi si sono rifugiati, sovraccaricandolo, sono iniziate una serie di vicissitudini. Un giorno ad esempio uno dei fornitori di un nuovo

Vps, cioè di un server privato virtuale, su cui si appoggiava il sito, ha indebitamente curiosato nel codice di BMR e dopo aver trovato alcune vulnerabilità ne ha rilasciato dei pezzi su un forum tedesco. Come conseguenza Backopy ha deciso di mandare offline il sito per un periodo e di fare una revisione di tutta la sua sicurezza. Incrocio Colt in chat una di quelle sere ed è decisamente seccato. “Il provider di Vps si è fottuto il codice sorgente del sito” mi dice “quindi abbiamo dovuto tirare giù il market in emergenza”. Altri utenti della chat gli fanno delle domande preoccupati, alcuni avevano dei negozi sopra o delle contrattazioni in corso. “Stiamo già lavorando alla nuova versione di BMR, in un mese dovremmo tornare”, risponde lui. Anche in questo caso, come avvenuto con *Silk Road*, il forum sta a un altro indirizzo, quindi le comunicazioni fra gli avventori del mercato continuano lì. “Stiamo restituendo i soldi che erano rimasti nel

bilancio, negli account personali, ai vari utenti”, spiega Colt. “Come faccio ad aspettare un mese?”, gli domanda un altro. “C’è *Sheep Market* [un altro bazar di droghe, nda] ma è sovraccarico e lentissimo, tra un po’ esplode per il numero di utenti”, replica Colt.

A lavorare su Black Market sono una manciata di admin e moderatori. Che comunque non erano contenti della caduta di *Silk Road*, “troppa attenzione mediatica”. In realtà BMR tornerà online dopo pochi giorni, proseguendo la sua attività in maniera ancora più frenetica. Salvo incorrere dopo un breve periodo di tempo in nuovi guai. Infatti il mercato viene pure rapinato da un hacker. Che lo viola e riesce a rubare dagli account dei clienti 280 *Bitcoin*: all’epoca equivalgono a circa 300mila euro. Backopy, il leader, annuncia di mettere mano ai propri fondi personali e di essere pronto a rimborsare tutti quelli interessati, tra il plauso generale. La

gente tira un sospiro di sollievo e il sito continua ad andare avanti ancora un po' finché prima del Natale 2013 annuncia di chiudere per un periodo. La spiegazione ufficiale è che ci sarebbero troppi problemi tecnici, e quindi si preferisce attendere che i vari admin mettano finalmente a punto una versione del tutto rinnovata. Anche in questo caso gli utenti possono andare a ritirarsi i soldi. Insomma, non si tratta di una chiusura *scam*, truffaldina, come spesso avviene da queste parti. Anzi, l'atteggiamento di BMR è simile a quello di un'azienda attenta a non deludere i propri *stakeholder*. Colt non appare preoccupato, anche se non vuole pronunciarsi sulla data di una possibile rinascita. Sta di fatto che questo è il momento più basso per la vita dei bazar illegali del Deep. *Silk Road* è crollata, e la sua reincarnazione stenta a decollare. BMR, dopo una serie di problemi, è messa in stand-by. Mentre qualche mese prima un altro mercato del genere, *Atlantis*

[vedi in rete], che era stato lanciato prima dell'estate manco fosse una startup, con tanto di video di marketing postato su *YouTube*, aveva chiuso di colpo sparendo insieme ai soldi degli utenti.

In realtà chi vive di piccoli traffici non ha bisogno di grandi siti del genere: gli basta circolare su forum o chat dell'ambiente. The Baker ad esempio se la cava con poco: la domenica sera fa una bella infornata di biscotti fatti in casa, accuratamente *aromatizzati* alla marijuana, li impacchetta per bene con repellenti per cani, e li spedisce in tutta Europa. Venticinque euro per dieci pezzi. "Tutti ingredienti naturali, e sono anche anticulone garantiti", assicura, facendomi vedere anche le foto. Sono rotondi, dorati, e punteggiati. "Farina, burro, poco zucchero e ottima erba, solo cimette selezionate... come li faceva la nonna di Bob Marley".

I tanti strati di comunità libertarie

È il 4 agosto 2013. Da un paio di mesi è scoppiato il *Datagate*, la pubblicazione di documenti segreti sui mastodontici programmi di sorveglianza delle comunicazioni mondiali messi in piedi, in una escalation progressiva a partire dall'11 settembre 2001, dagli americani e in particolare dalla *National Security Agency*. Sembra che nulla – telefonate, mail, chiamate via *Skype*, chat, documenti salvati nel cloud delle grandi aziende – sia rimasto immune dalla riedizione hi-tech e globalizzata del Grande Fratello. Solo il mondo sotterraneo delle darknet - almeno in base ai documenti diffusi fino a quel momento sui media da Edward Snowden, l'ex-contractor della Cia e della Nsa – sembra essere riuscito a sfuggire alle straordinarie capacità di monitoraggio delle agenzie di intelligence. *Silk Road* è ancora al suo posto, e Dread Pirate

Roberts ha rilasciato da poco una trionfante intervista, inconsapevole del fatto che il cerchio si sta stringendo intorno a lui. Il *Deep Web* pullula di siti di tutti i tipi. E gli hacker di mezzo mondo sono riuniti in una delle loro conferenze principali, il Defcon di Las Vegas. Ma proprio in questo momento, l'Fbi sferra il più clamoroso attacco alle darknet mai registrato prima. Il risultato è che metà *Deep Web* si oscura del tutto, inabissandosi come un sommergibile colpito da un siluro. Infatti i federali sono riusciti a compromettere uno dei maggiori fornitori di servizi per siti anonimi, *Freedom Hosting*, ufficialmente perché ospitava pedopornografia. Dopodiché la polizia ha usato la piattaforma infettata per cercare di colpire gli utenti che visitavano i suoi siti e carpirne le identità attraverso una vulnerabilità del browser *Firefox*, su cui si basa lo stesso *Tor* Browser. Finché a un certo punto non si è oscurato tutto, *Freedom Hosting* e la marea di servizi

che reggeva. Il risultato è che metà dei siti del Deep vanno offline, mentre tra gli utenti si diffonde il panico. Strumenti di comunicazione anonima come *Tormail*, che si appoggiavano a quel provider, e che sono molto usati da una fetta trasversale ed eterogenea di persone, scompaiono nel nulla. Nei giorni successivi all'attacco, *il ventre di internet* ribolle di sgomento, interrogativi e teorie complottiste. Le bacheche e i forum si riempiono di domande, c'è chi è alla ricerca di siti, chi di persone, come dopo un terremoto. Gli amministratori e gli utenti più accorti cominciano però da subito a rimboccarsi le maniche e a rimettere in piedi strumenti e servizi. È proprio in questo periodo convulso che nasce un sito di informazione del Deep dedicato a diffondere notizie utili, *Onion News* . Una specie di Gazzetta del *Dark Web*, raggiungibile solo via *Tor*. Contatto il suo proprietario, che chiamerò Kane, e lo intervisto in una chat. Dice di essere un tedesco di

circa quarant'anni, e di aver deciso di creare un sito dopo che molti servizi nascosti erano spariti. "Penso che le persone abbiano bisogno di avere informazioni su quello che sta succedendo", mi dice in una chat criptata. "Il mio vuole essere solo un servizio alla comunità, affinché non si disperda troppo". Kane sta anche amministrando altri servizi nascosti, che preferisce non associare a Onion News, e che in parte gli danno anche da vivere. Inoltre sta lavorando per rimettere on line alcuni forum scomparsi. Kane nella vita si occupa di diverse attività nell'ambito dell'IT, soprattutto legate a *Bitcoin* e a *Tor*. Della criptomoneta dice che si tratta di una grande tecnologia abilitante che, insieme a *Tor*, renderà possibile molte realtà nuove. Specialmente in tempi di PRISM, specifica riferendosi al più noto programma di sorveglianza della Nsa. "E *Silk Road* è stato solo l'inizio". Lui vive vendendo *Bitcoin*: ha iniziato a occuparsene due anni fa, quindi ha

accumulato una riserva di moneta elettronica che, essendo cresciuta enormemente di valore, si è trasformata in un discreto capitale. Gli chiedo cosa ne pensa dell'attacco a *Freedom Hosting*. "A essere sinceri penso che l'Fbi volesse davvero colpire il traffico di pedopornografia, e anche se non sono certo uno a favore di censure, non mi importa se il 90 per cento della pornografia infantile è scomparsa da *Tor*. Anzi, tutto ciò renderà questo posto più legittimo per chi sta qua ad occuparsi di affari". Secondo Kane il cataclisma appena avvenuto sul lungo termine costringerà le persone a gestire i loro server rendendo l'ambiente più decentralizzato. "Ovviamente occuparsi in prima persona di queste cose aumenta anche i rischi, perché serve molta più esperienza. Ma i *Bitcoin* potrebbero risolvere il problema, nel senso che ci sarà più gente disposta a pagare chi offre servizi a pagamento".

Di questa idea sono anche alcuni utenti che scrivono su *Onionforum v3*, appena rinato dopo che il precedente era affondato. “Bisogna smetterla di usare l’hosting altrui, è tempo che ognuno si configuri un servizio sul suo computer. Metà *Onionland* (la terra della cipolla, insomma il *Dark Web*) è stata uccisa perché tutti si appoggiavano a piattaforme esterne. La centralizzazione è una cattiva idea”.

La pensa in modo simile anche The Architect, che abbiamo già incontrato nel primo capitolo. Lui è uno degli amministratori di *Cipolla*, storica comunità italiana del Deep. La prima versione di questo servizio nascosto – composto da un sito/forum/chat /mercatino – stava su *Freedom Hosting*, e quindi è precipitata. Ma lui si è messo subito al lavoro per la seconda versione e in poco tempo ha rimesso in piedi tutta la baracca. “Sapevo che Freedom Hosting non sarebbe durato per sempre, per il resto è bastato

dedicarci il tempo necessario”, mi dice. “E il bello è che ora è meglio di prima, più sicuro, con più possibilità. Fai conto che per tirare su un sito onion serve un server dedicato o un Vps (Virtual private server) su cui far girare *Tor*, e qualche capacità di configurazione. Quando *Freedom Hosting* è nato, qualche anno fa, i server avevano prezzi abbastanza inaccessibili, mentre quella piattaforma offriva spazio gratis. Quindi credo che più di metà dei siti nascosti fossero ospitati lì sopra”. Anche lui, come Kane, non si dispera della sua caduta, perché su *Freedom Hosting* il 90 per cento di siti erano pagine di scam, truffe, o finti mercati. “E non mi dispiace che i pedofili si siano presi una bella batosta”. Il vero colpo, semmai, è che sia stata messa fuori uso *Tormail*, uno strumento veramente utile e unico, perché il server con le mail archiviate era di fatto inarrivabile, e quindi al di fuori della portata delle agenzie investigative e di intelligence di tutto il mondo.

Almeno fino al sequestro di *Freedom Hosting*.

In quanto a *Cipolla*, il link al nuovo indirizzo è iniziato a circolare in maniera underground sulle varie bacheche del Deep. E in poco tempo il forum e la chat rinati hanno iniziato a ripopolarsi.

Gli utenti che alla spicciolata approdavano sul nuovo sito erano salutati dal seguente messaggio: “ *Cipolla 1.0* come tutti saprete è morto insieme a *Freedom Hosting* ed il database è compromesso, così come il vecchio dominio onion è perduto per sempre. Nonostante io avessi un backup del 25 maggio è stato scelto di ricominciare, perché a parere comune è risultata decisamente una pessima idea rimettere in funzione un database che di fatto è nelle mani delle forze dell’ordine, anche se straniere. Di conseguenza, la vecchia versione di *Cipolla*, disponibile al link *Cipolla 1.0* è utilizzabile in sola lettura. Gli utenti e i messaggi privati sono stati

interamente eliminati, mentre sono disabilitate nuove registrazioni, ma ci sembrava uno spreco buttare via tutto quello che avevamo raccolto”.

Cipolla 2.0 sta infatti su un nuovo server, interamente gestito dagli amministratori. E cripta anche i messaggi privati scambiati tra gli utenti del forum. “Ci sono più messaggi personali che post”, mi dice dopo qualche giorno con un certo orgoglio The Architect. “Dopo che ho scritto che sono criptati asimmetricamente e sicuri, la gente si è fidata”. Il nuovo sito ha anche una funzione denominata *Wallet*, un borsellino di *Bitcoin* che si collega con l’escrow, i depositi. “Si tratta del cardine di tutte le transazioni sulle darknet”, prosegue l’amministratore di *Cipolla*. “Come su *Silk Road*, quando compro qualcosa i soldi rimangono bloccati, e quando il prodotto mi arriva allora mi loggo e li rilascio al venditore. Se invece la roba non mi arriva apro una disputa e a seconda

delle reputazioni, le prove etc. si stabilisce come distribuire la perdita. Se dopo un tot di giorni non si è aperta una disputa, i soldi vengono automaticamente rilasciati”. Il meccanismo può essere gestito manualmente o in modo automatico, dipende dal volume di utenza.

Cosa si fa su *Cipolla*? Di tutto, di più. Nel forum si discute degli argomenti più vari, dalla politica alla droga, dall’hacking al sesso. Ovviamente qua molti si dedicano a piccoli traffici e commerci, in alcuni casi legali, ma protetti dalla privacy del Deep; in altri casi illegali, anche se difficilmente circolano grossi criminali. La policy del sito rifiuta servizi violenti e pedofili, ma per il resto è abbastanza tollerante. The Architect ama tenere un basso profilo, e non sembra essere qui per i soldi. “Non vivo certo di questo”, mi spiega. “Siamo in tre amministratori e finora, cioè dalla nascita due anni fa del sito, avremo guadagnato intorno ai mille euro, da

dividere, e solo perché i *Bitcoin* sono cresciuti a dismisura. In realtà per me questo è più un progetto a lungo termine”.

Nel *Cipolla 1.0* c’era anche qualche lunga discussione filosofica, aggiunge, “ad esempio le ragioni per cui ci si droga, con i diretti interessati che dicevano la loro. Le persone sono piene di pregiudizi e opinioni false in tutti i campi che non conoscono, ma la libertà delle darknet permette di prendere coscienza delle altre realtà da un loro punto di vista. Almeno per me è così, sarà perché sono giovane, ma ho aperto la mente su tante cose. Alla fine un sacco di gente è qui solo per la comunità, magari ha anche i suoi affari, ma partecipa al forum perché gli piace. Chi è in cerca di soldi facili sparisce in fretta perché capisce che anche in questo posto non sono così immediati”.

In effetti da queste parti, tolti alcuni elementi di spicco che sono dediti ad attività specifiche, si aggira soprattutto una massa di

curiosi, giovani, programmatori, appassionati di criptomonete e crittografia, libertari, anarcocapitalisti, individualisti e cani sciolti. “Non sono qui per truffare”, mette subito le mani avanti un utente di nome Niko, “ma solo perché sono curioso e voglio sapere, vedere e toccare con mano. Prima bazzicavo alcuni forum, come *HackBB* o lo stesso *Silk Road*, anche se secondo me le cose più interessanti non si trovano facilmente”.

Come ha commentato una volta Colt, con una battuta, “qui si spaccia anche il sapere, mica solo l’ignoranza”. The Thinker è abbastanza d’accordo. Ha circa quarant’anni, è un’operatore della chat, il che significa che gode di una certa fiducia all’interno della comunità, e mi dice di essere qui – oltre che per comprare i biscotti di The Baker – perché gli piace l’idea di poter “comunicare in modo relativamente svincolato dai sistemi di controllo globale”. Anche se, ammette, in

alcuni casi la libertà può anche essere usata male. “Ma è meglio essere liberi e poter scegliere, anche sbagliando e pagando per i propri errori, che non esserlo. Dopo Snowden sappiamo che le nostre comunicazioni sono controllate... cioè lo sapevamo anche prima, ma ora ne siamo sicuri. Per cui avere uno spazio tutelato diventerà sempre più importante, così come sapere che la Nsa non sta intercettando quello che sto scrivendo”. Ma voi eravate qua anche da prima, faccio notare a lui e ad altri in una chat di gruppo. “Sì, perché lo sapevamo anche prima di essere controllati”, risponde The Thinker. “Ci sono anche ragioni ataviche”, interviene The Baker. “Il piacere della sfida... forse mi potete leggere, ma dovete gettare *o’sangue* per capire chi sono”. The Baker ad esempio è approdato in questi luoghi dopo alcune ricerche in rete per trovare una Vpn per amici iraniani, “e il resto è venuto da sé”. Compresi anche i biscotti della nonna di Marley. The

Thinker mi dice che vorrebbe scrivere un manuale su come cifrare le proprie comunicazioni: “dopo il Datagate tutti dovrebbero saper usare le chiavi di criptografia”, aggiunge. “Non è necessario criptare tutto, ma al bisogno tutti devono saperlo fare”.

Gibbons, intorno ai 40 anni, un passato vicino ai movimenti, cultura informatica e cyberpunk, ha le idee molto chiare riguardo il significato del *Dark Web*. “È come tornare a prima dell’internet per idioti”, mi dice in una lunga conversazione in cui, fra le altre cose, parliamo di letteratura e fantascienza. “Prima della bolla speculativa, del web 2.0, dei markettari, dei social. Qui non hai la pappa pronta con motori che ti dicono cosa cercare”. Infatti nel *Dark Web* ci si muove avendo e cercando direttamente gli indirizzi dei siti nei forum, in directory di link, come il noto *Hidden Wiki*, o col passaparola. Ci sono alcuni motori di ricerca, ma non funzionano neanche lontanamente come *Google*. Il

search engine di Big G, così come gli altri usati sul web, non possono indicizzare i siti .onion, quel dominio non sta nei server DNS usati per tradurre un indirizzo web in IP. Esistono dei motori che sono di fatto dei client del software *Tor* e che quindi interrogano i server del network *Tor*. Ma di fatto il modo migliore per muoversi nel Deep è attraverso directory di link preparate da altri. Un po' come accadeva una volta sul web.

Inoltre anche quando i servizi nascosti non scompaiono nel nulla, come è accaduto a *Silk Road*, comunque cambiano spesso di indirizzo: è come vivere in una città la cui toponomastica (ma anche i sensi delle strade e la loro stessa configurazione) venga rivoluzionata in continuazione. Ogni utente deve diventare un po' cartografo.

"La Rete doveva essere un posto di liberazione per tutti" continua Gibbons "ma quell'ideale si è perso. Venti anni fa respiravi davvero aria di frontiera. Ecco, il Deep

ripropone quell'atmosfera, ma nello stesso tempo è anche una riserva, un recinto, un biotopo". Insomma, una specie di *Taz* [Scarica gratuitamente il testo], di zona temporaneamente autonoma, così come veniva formulata anni fa dal filosofo anarchico Hakim Bey.

Ancora più tranchant Typhon, che circola e traffica con `botnet` sul Deep, ma che è soprattutto un hacktivista, e usa spesso i suoi mezzi per fini di azione politica. "La Rete non è stata creata per le multinazionali che ora la dominano, ma per diffondere conoscenza", mi dice una sera parlando del Deep. "Deve essere un posto libero, con le sue usanze e le sue leggi. In fondo, è la darknet la vera internet".

In tutto ciò la visibilità mediatica, e le sue conseguenze, non sono molto apprezzate da queste parti. E non solo perché i titoli dei giornali sui mercati neri aumentano anche l'attenzione delle forze dell'ordine – Adrian

Chen, il giornalista che per primo diede la notizia di *Silk Road*, è ancora adesso oggetto di variopinte maledizioni. Ma anche perché c'è l'idea che queste siano comunità autoregolate, e anche un po' elitarie, in cui l'infrazione peggiore è la stupidità, o la totale inconsapevolezza. "Il *Deep Web* è nato insieme a *Tor*, ma ha iniziato ad essere frequentato dal 2006-2007", mi dice The Architect. Il fenomeno poi è cresciuto sempre di più, "ma non è detto che sia un bene, perché si è ingrandito a causa di quella carta straccia di riviste che hanno scritto titoli sensazionalistici su droga, armi e pedofili", mi dice una sera l'amministratore di *Cipolla*, che combatte quotidianamente con troll, provocatori, domande e inserzioni insulse da ripulire sul forum, oltre che una miriade di espressioni di pura ottusità.

E ancora non sa quello che lo aspetta...

Nell'ottobre 2013 infatti il programma tv *Le Iene* fa un servizio sul Deep, in cui cita

ampiamente anche la comunità italiana, che aveva visitato qualche tempo prima. Il risultato è che nei giorni successivi forum e chat esplodono di nuovi utenti.
Mi collego una di quelle sere e trovo un The Architect funereo. “Tu non hai presente... ” dice in chat rivolgendosi all’ennesimo curioso arrivato a fare domande sconcertanti “...il danno che ci hanno fatto quelli delle Iene, che hanno fatto arrivare una immensa orda di *nabbi* [utente nuovo, inesperto e ingenuo] assassini, senza alcuna utilità”. “Lo so, vi capisco”, abbozza una replica amichevole il tipo. “Te compreso”, lo congeda The Architect.
“Tutto bene”, mi saluta l’admin di *Cipolla* un’altra sera, “a parte che si perde del gran tempo”. “Continuano ad arrivare persone?” chiedo. “Sì, non se ne può più. La peggio ignoranza italiana, come JakeLaFuria”. “E chi è?”. “Un tizio che avrà scritto sul forum una trentina di messaggi, tutti senza

punteggiatura, tutti demenziali. Appena arriva a 50, lo elimino con tutti i post. E comunque”, prosegue, “ti sei persa la tipa che chiedeva come guardare film porno con *Tor*... perché fa l’università e le dispiaceva non averne mai visto uno, ma aveva paura di lasciare tracce...”.

Giù nel profondo

Uno degli incontri più curiosi che ho avuto nel *Deep Web* è stato con un utente italiano che non era un hacker, un carder, uno spacciatore, un libertario, un crittografo o altro. Era un appassionato di moda, chiamiamolo Rocco. Gli chiedo che ci fa da queste parti. Dice che cerca prodotti di marca contraffatti. “Sai quelle cose che dicono siano false ma sono identiche alle vere? Spesso i laboratori cinesi che fanno i falsi sono gli stessi che fanno quelli autentici. Poi ne fanno un po’ di più con microdifferenze e dicono che li ha fatti qualcun altro. Ma sarebbe impossibile per altri fare le cose perfette partendo da zero e soprattutto da subito, da quando escono le nuove collezioni”. Rocco si dichiara un *fashion victim*, ma gli piace comprare senza svenarsi. Quindi cerca prodotti “non originali” – anche se come sostiene lui di fatto di una qualità e fattura molto simile ai brand

famosi – li compra e li rivende. Ma in piccole quantità, cercando di non dare nell'occhio. "Ora sto cercando Gola e Hogan" mi dice "mentre magari a un altro interessano Abercrombie & Fitch e Desigual: ci scambiamo delle dritte. Si mette un annuncio sul forum, si chiede in giro. Se sei una donna, non prendere scarpe col tacco alto dai cinesi però... non sono capaci. Avevo preso delle Christian Louboutin, ma la ragazza che le ha usate le ha buttate dopo una sera".
Gli domando dove e a chi rivende quello che trova online. "Non ho ho canali abituali, a volte in rete, a volte amici e amiche, o negozi. Se ti serializzi e ti fai prendere dall'avidità è molto più facile che ti becchino". Rocco dice di essere arrivato qua per curiosità, e di aver visto su altri forum internazionali che c'erano delle possibilità. Gli stranieri, specie i russi, per il solo fatto che lui era italiano, gli chiedevano delle indicazioni. A quel punto ha approfondito la questione. Tuttavia

ribadisce che la sua non è una vera attività. “Hai presente quelli che spacciano erba per fumare gratis e poco più?” mi dice. “È la stessa cosa”.

In realtà la parte più ricca delle darknet ha a che fare ovviamente con il mondo dell’hacking. Ci sono forum e servizi nascosti su invito, in cui è quasi impossibile entrare se non si è presentati da qualcuno di fidato, dove ci si scambiano informazioni e avviene una compravendita di strumenti, vulnerabilità, malware. Poi ci sono i cani sciolti, non necessariamente persone che sono qui per hackerare qualcosa, ma che vendono ad altri i propri servizi. Una sera ne incontro uno, Hal, che stava trattando con un tizio la vendita di alcuni `RAT`, software per l’infezione e il controllo da remoto di un computer. “Sì, vendo programmi, per lo più di hacking”, mi dice in chat, “fatti da me. `RAT`, `crypter`, `crypting service`, `jdb`, `sjdb`, `exploit`, puoi chiedere della mia referenza”, mi dice subito prima

ancora di darmi il tempo di spiegargli che sono una giornalista e che non voglio comprare nulla. Successivamente, dopo un primo momento di diffidenza, mi spiega di essere un ricercatore di security, quello che in gergo si definirebbe un *white hat*, contrapposto ai *black hat*, ai criminali informatici. Però resta qua anche lui, presumibilmente per arrotondare, e non si pone molte domande su chi compra i suoi prodotti e perché. Gli chiedo cosa acquistano in genere da lui: “perlopiù `crypter`, e qualcuno qualche exploit”, mi dice. I `crypter` sono dei software che nascondono e offuscano un file eseguibile in modo da renderlo irrintracciabile agli antivirus. Sono come dei mantelli di invisibilità con cui ricoprire un software malevolo, un virus usato per infettare un dispositivo.

“I miei clienti non sono ragazzini”, prosegue Hal. “Considera che un `crypter` personalizzato costa dai 700 euro in su, e comunque richiede quasi un mese di lavoro

per farlo. Serve per rendere invisibile i trojan o file di qualsiasi genere agli antivirus”. Un RAT invece, quindi nel caso specifico un trojan, un virus che come un cavallo di Troia entra surrettiziamente in un pc e ne cede il controllo all’attaccante, costa dai 700 ai 3/4mila euro, specifica, a seconda delle funzioni. Gli exploit – che sono dei codici che sfruttando una vulnerabilità dei software permettono di effettuare operazioni dannose ai danni dell’utente - dai 500 euro in su. “A me non interessa quello che ci fanno, non lo chiedo e non voglio neanche entrare nel merito”.

Commercio di malware, vulnerabilità, database hackerati sono attività molto diffuse, anche se forse quella più visibile e popolare - almeno a giudicare dalla quantità e la frequentazione dei forum - è il *carding*, ovvero lo scambio e compravendita di carte di credito (più precisamente dei loro dati) e il loro utilizzo per acquistare beni o trasferire

fondi ai danni dei titolari legittimi delle stesse. Molte delle informazioni che circolano sono guide dettagliate su come funzionano i diversi tipi di carte e come gestirle. Su *HackBB Reloaded*, un sito dedicato all'hacking, si trova un utile compendio di "Cose che non sai sulla tua carta di credito". Oltre ai "9 modi per non essere beccato" (nell'usare quella altrui). Informazioni che peraltro pullulano anche fuori dal *Dark Web* nella Rete in chiaro. Così come in chiaro si trovano anche forum internazionali di *carders*, spesso setacciati dalle stesse banche per raccogliere informazioni e comprarsi indietro i dati di carte rubate, così come mi ha spiegato il giornalista Brian Krebs, un vero esperto di criminalità informatica e soprattutto un cacciatore infaticabile di carder russi o dell'Est Europa. "Ci sono letteralmente centinaia di negozi che vendono carte rubate. Alcuni sono più affidabili di altri e hanno più assortimento. In realtà non ci si

guadagna molto a chiudere questi siti, che tendono a essere utili alle banche e alla polizia. E poi anche se li blocchi i loro gestori aprono facilmente un nuovo dominio e spostano il negozio. Lo fanno in continuazione".
Ad ogni modo come sempre, anche nel Deep, i livelli sono multipli. C'è ad esempio Canopy che aggancio mentre sta discutendo in una chat la vendita di un set di carte di credito, cioè una serie di informazioni rubate che comprendano tipo di carta, nome, cognome, numero, scadenza e Cvv2. Lui le vende a 10 euro l'una in blocchi da dieci. Va detto però che avere queste informazioni non garantisce in automatico la possibilità di intascarsi dei soldi o di usarle a piacimento. Se si fa una mossa sbagliata il rischio di avere la carta bloccata è molto alto. "Bisogna conoscere i siti, sapersi proxare, investigare sulla persona, creare situazioni realistiche", mi dice Canopy. "La figata è comprarci moneta

virtuale” come i *Linden Coin*, il denaro usato su *Second Life* “e riciclarla ma è difficile, quindi in genere si acquistano degli oggetti e si fanno arrivare da qualche parte con degli escamotage [casa abbandonata, casella postale aperta con documenti falsi etc.]”.

Le carte si ottengono in vari modi: quello più diretto hackerando un sito di ecommerce. “Queste che ho adesso le ho rubate a un venditore”, mi dice. Prima si dedicava all’hacking per divertimento. Ora ha deciso di monetizzare.

Ma, appunto, riuscirci, fare cioè il *cash out* di una carta, non è affatto così semplice.

“Il problema principale è non farsi arrestare mentre lo si fa”, mi spiega Giacomo Paoni, esperto di *cybersecurity* anche in relazione al settore bancario. “I modi per fare *cash out* sono molteplici, uno dei più elementari è quello di acquistare prodotti con le carte rubate e poi rivenderli. Come si sottraggono le carte? Avendo accesso al database di un

sito di ecommerce; oppure compromettendo un negozio *fisico*, i suoi server di gestione dei pagamenti, e di conseguenza sniffando la *track2* della carta e le altre informazioni utili a clonarla; o ancora compromettendo i PoS di un retailer con un malware; o facendo *skimming* [cioè clonandole]". Fino ai casi in cui si compromette direttamente un provider di carte prepagate o un processore di carte di credito. "In genere chi viola grossi database di carte non le utilizza per sé ma le vende un tanto *al chilo* a criminali di più *basso* livello che poi le utilizzeranno per estrarci i soldi prendendosi i rischi [spesso infatti le *crew* di *cash out* sono le prime che vengono arrestate]".

Il sito più noto di hacking e carding, nel Deep, si chiama *Tor Carding Forum* (TCF). Lo conoscono tutti e in effetti è molto frequentato, con tante sezioni specifiche. Ogni aspetto del furto e dell'utilizzo di carte è

trattato ampiamente, ma soprattutto questo è un grande mercato di scambio di dati.

Mi iscrivo al forum e contatto il suo amministratore, che è molto noto, e si fa chiamare Verto (questo è proprio il suo nick). Mi spiega, nel corso di una chat criptata, che il sito è stato fondato nel giugno del 2012. “All’epoca il numero di siti onion era abbastanza basso e non ce n’era di dedicati al carding. Per cui è stato progettato come luogo centrale per scambiarsi idee, conoscenze e abilità”. In pratica, mi spiega Verto in una conversazione molto garbata e professionale, il forum è solo un posto per incontrarsi e condurre i propri affari in modo controllato, compratori e venditori in primo luogo. “Avere siti/negozi indipendenti non funziona molto bene. La maggior parte sono truffatori”, mi dice senza alcun filo d’ironia. Mi fa un esempio, il servizio *Rent A Hacker* (Affitta un hacker), pubblicizzato su una delle principali directory del Deep, *Hidden*

Wiki, chiaramente una fregatura. “Di qui il bisogno di un forum in cui i venditori possano essere valutati dai loro pari”, aggiunge. E non solo da loro, mi viene da pensare: la storia di come l’Fbi infiltrò la criminalità informatica al punto da arrivare a gestire un grosso sito di carders, in passato, è ben raccontata nel libro *KingPin* di Kevin Poulsen. Ma il ragionamento di Verto non fa una piega: “la fiducia si costruisce col tempo e con la prova di molte vendite andate a buon fine. È il solo modo in cui le cose possono funzionare in un mercato anonimo”. È il modello del sito con feedback e reputazione alla eBay, che è stato così efficace anche con *Silk Road*. E diventa particolarmente importante in un ambiente aleatorio, sfuggente e irrintracciabile come quello del *Dark Web*.

Nel momento in cui sto parlando con Verto *TCF* ha circa 13mila membri, anche se non sono tutti attivi. “Di fatto ogni giorno si

loggano 500-600 iscritti al giorno, poi ci sono molti altri ospiti che leggono il forum senza iscriversi”. Verto mi spiega che lo scenario del carding – e delle attività per la sua prevenzione e contrasto – è in continua mutazione. Ed è reso sempre più difficile da misure di sicurezza come lo standard EMV [sviluppati da alcuni dei maggiori vendor], carte IC (che integrano microchip), sistemi di protezione antifrode come *3-D secure* per la verifica online. Ritiene anche che le stime sul giro di affari del carding siano gonfiate: “ogni indagine delle forze dell’ordine calcola che l’ammontare di una frode relativa al carding sia in media di 500 dollari a carta. È chiaramente ridicolo pensare di arrivare fino a una simile cifra. Includono nel conteggio anche carte non valide, e comunque per le frodi online la cifra media è molto inferiore. È solo un esercizio per dimostrare il bisogno di aumentare i poteri investigativi e di spionaggio, e per giustificare i soldi e il tempo

dedicati alle indagini”. Gli chiedo se pensa mai al rischio di essere individuato. “Sono consapevole della possibilità, ma mi fido di *Tor* e dei suoi servizi nascosti. Tutti gli arresti più recenti sono derivati da errori umani, in alcuni casi piuttosto prominenti. Mentre non c’è una prova che *Tor* sia stato compromesso nei suoi fondamentali”.

C’è una sola categoria di frequentatori del *Dark Web* disprezzata da tutte le altre. Ed è quella dei pedofili. Non mi sono soffermata sull’argomento, non solo per la sua pesantezza, ma perché la pedopornografia ha trovato sì un luogo ulteriore nella internet più nascosta, ma di fatto prospera ovunque. Non è un tratto distintivo del Deep. E non è nemmeno così facile imbattersi in siti di quel genere. Sicuramente ha pesato la caduta di *Freedom Hosting* nell’estate 2013, che si è portata dietro moltissimi forum e servizi nascosti. È anche molto difficile quantificare il fenomeno: due ricercatori hanno provato a

farlo (col Project Artemis) concludendo che il porno/pedo ammonterebbe solo al 4 per cento del Deep. L'hacking sarebbe invece l'attività principale, ma comunque solo al 28 per cento; il cybercrimine al 23; propaganda politica e/o terroristica al 17; hacktivismo al 4 etc. Più altre varie attività minori .

Category	%
E-commerce	5%
Hidden Services	6%
Wiki/Dictionaries/ Collections of Links	6%
Hacktivism	3%
Porno/Pedo	4%
Hacktivism	1%
Politic/Terrorists Propaganda	17%
Hacking	28%
Cybercrime	23%
Others	8%

“Il problema non riguarda solo il Deep, anche se qui si sono spostati in molti dopo il giro di vite sui network *peer-to-peer*, usati per diffondere materiali”, mi spiega Francesca Bosco, project officer all’unità sui crimini emergenti di UNICRI, Istituto Inter-regionale delle Nazioni Unite per la Ricerca sul Crimine e la Giustizia. “Il problema principale che vedo per il futuro è il boom dei contenuti generati dagli utenti e dei rischi che ne conseguono. Ad esempio, i video hard girati coi telefonini da adolescenti e diffusi tramite *Whatsapp*”. Insomma, la questione è complessa.

Tra l’altro i siti pedo, chi li gestisce e i loro frequentatori, sono tallonati e attaccati sia dalle forze dell’ordine che da altri soggetti dello stesso Deep. Nel febbraio 2014 la *Polizia Postale*, in collaborazione con l’Fbi e l’*Europol*, ha arrestato dieci pedofili italiani, che gestivano alcuni dei loro traffici nella parte nascosta della Rete. Ma non ci sono

solo agenti sotto copertura a dare loro la caccia. In una inedita e metaforica alleanza, si aggiungono anche alcuni membri di *Anonymous*: Pedobuster (anche questa volta il nick è stato cambiato) è uno di questi. Circola nel gruppo di hacktivisti italiani, anche se è mediamente più vecchio e non del tutto assimilabile al collettivo; inoltre fa parte di una crew internazionale che gestisce *OpRiptide*, la cui missione è smascherare pubblicamente pedofili. Per farlo il gruppo – 6 o 7 persone, mi dice Pedobuster – si divide i compiti. C'è chi si finge una preadolescente e frequenta siti e chat come *Teen Chat* per agganciare pedofili (alcune conversazioni sono riportate sul loro sito [vedi in rete]); chi si occupa di scovare siti pedo e cercarne vulnerabilità; chi attacca informaticamente singoli utenti. Pedobuster è specializzato in questo, nel cosiddetto `pedo-bait`: si infettano i pc di pedofili, si ottengono informazioni sulla loro identità e si pubblicano. "Abbiamo

chi *ratta* [ovvero infetta] e *doxa* [cioè svela l'identità dei target]; chi sta sui forum e sulle chat; chi lavora sui file; chi su *Facebook*. Nei casi più gravi proviamo a girarle in qualche modo alle forze dell'ordine", mi dice. "Ovviamente - specifica – la maggior parte dei pedofili stanno nel web in chiaro, perché è lì che vanno ad adescare, specie nelle chat. Nel Deep hanno solo uno spazio non regolamentato dove scambiare la loro merda".

Pedobuster mi mostra due file Excel. Sono due lunghissimi elenchi di siti pedopornografici, minuziosamente e scientificamente catalogati dal suo gruppo: indirizzo, IP, Paese, tipologia di contenuti, eventuali vulnerabilità. Ce ne sono un migliaio per file. In un documento sono indirizzi .onion, cioè del Deep. Ma nell'altro – ed è la cosa forse più scioccante – ci sono invece indirizzi in chiaro, del web normale, accessibile da tutti. Decido che per me è abbastanza: saluto Pedobuster, che sta per iniziare una delle sue

sessioni notturne di caccia al pedofilo, e vado avanti.

CAPITOLO 3 - Vita hacktiva

Chi sono i sostenitori di Edward Snowden?
"Nichilisti, anarchici, attivisti, Lulzsec, Anonymous, ventenni che non parlano col sesso opposto da 5 o 6 anni" – Michael Hayden, ex-direttore della Cia e della *Nsa*
"Il problema che ho con internet è che è anonimo" - Michael Hayden, ex-direttore della Cia e della *Nsa*

"Oggi Typhon è in buona", mi dice scherzando in chat Drugo. Drugo è uno degli hacktvisti italiani più attivi, almeno sul piano della comunicazione e organizzazione. Non è un hacker di eccezionali capacità ma, contrariamente ad altri più esperti sul fronte tech, ha il polso della situazione politica, pur non avendo affatto un passato di attivismo nella vita reale, come mi ha spiegato lui

stesso in una delle innumerevoli conversazioni via chat che abbiamo avuto negli ultimi due anni. Sarà pure anonimo, ma ormai la mia percezione è di conoscerlo molto bene: da tempo fa parte della ristretta cerchia di *anons* di cui mi fido di più. Con alcuni di questi ho contatti che risalgono appunto a due anni fa, in un caso addirittura all'estate 2011. Ma sono pochi quelli con cui si riesce a mantenere un rapporto così lungo. Molti, nel corso di questo tempo, sono spariti nel nulla. Drugo non è fra questi. Il suo coinvolgimento è cresciuto nel tempo. In un certo senso *Anonymous* è stata la sua educazione sentimentale. Ha un carattere molto equilibrato, ed è un abile mediatore delle istanze più divergenti di *Anonymous*.

Typhon era entrato da poco sul canale di chat usato da *Anonymous Italy*. Anche lui è una presenza a sua modo storica, anche se discontinua, intermittente, discreta e meno politicizzata. Soprattutto, Typhon è uno di

quelli che, quando arrivano, fanno la differenza.
“Non so cosa stia fumando, ma deve essere roba di qualità”, commenta Drugo. “Gli sto passando dei *target* e lui li sta buttando giù senza fiatare, uno dopo l’altro”. I target sono siti web, e non proprio irrilevanti.
È il 19 ottobre 2013. Per il secondo giorno consecutivo le strade di Roma sono attraversate da cortei e manifestazioni. Il 18 c’è stata infatti una manifestazione dei sindacati di base, con sciopero di 24 ore del trasporto pubblico. Ma ora è la volta del *#190*: movimenti, comitati, gruppi territoriali, centri sociali, collettivi studenteschi, lavoratori, No-Tav, No Muos, il comitato No Expo. La parola d’ordine è: “Una sola grande opera: casa e reddito per tutti”, e alla base c’è il rifiuto delle politiche di *austerity* che stanno impoverendo fasce sempre più ampie di popolazione. Per i media e i servizi segreti si tratta di un evento ad alto rischio: secondo

un'indicazione dell'intelligence ripresa acriticamente da alcune testate, il livello di pericolo è 8 su 10, anche se non è chiaro cosa starebbe a significare 10.

I manifestanti si sono organizzati soprattutto attraverso la rete e i social media. Il gruppo *Cyber Resistance* del centro sociale milanese Cantiere [vedi in rete] ha anche diffuso online una guida ad hoc: *Piccolo manuale di autodifesa digitale* [vedi in rete], dove si spiega come comunicare in modo sicuro e cifrato, o anche quali programmi usare sul telefonino per eliminare i volti dalle foto delle manifestazioni. Soprattutto, molti manifestanti e organizzatori hanno adottato la maschera di Guy Fawkes, utilizzata da *Anonymous*, come firma informale di volantini, art-work e striscioni.

Da Milano il comitato abitanti di San Siro, ribattezzato *V per Vendetta*, diffonde dei video che mostrano le azioni effettuate pochi giorni prima, dove alcuni dei militanti

percorrevano le strade dell'omonimo quartiere popolare firmando con una *V* gli appartamenti vuoti, nell'ambito delle lotte per la casa. Giorni prima l'ufficio assistenza clienti delle Ferrovie dello Stato della stazione di Bologna era stato occupato per un'ora da un centinaio di attivisti – collettivi studenteschi e universitari, laboratorio *Crash!* - che chiedevano la possibilità di usufruire di un treno a basso costo per raggiungere Roma. Anche loro, tutti con la maschera degli *anonimi*, perlopiù autoprodotta e non acquistata per evitare di dare soldi a Time Warner sotto forma di royalties. Maschera che in quei giorni compare anche ridipinta da alcuni writer su un treno.

In questo contesto un'azione di *Anonymous* durante le manifestazioni di piazza è quasi data per scontata. E infatti arriva puntuale. Mentre il corteo sta sfilando davanti al ministero dello Sviluppo economico, raggiungendo il punto massimo della tensione, tra

tafferugli, fumogeni, petardi e lancio di uova, il sito dello stesso va offline. Non sarà l'unico: finiscono in tangodown [vedi], diventando irraggiungibili, anche il ministero delle Infrastrutture e Trasporti, la Corte dei Conti e la Cassa Depositi e Prestiti.

Il canale di chat usato da *Anonymous Italy* è particolarmente popolato e vivace quel pomeriggio. C'è chi commenta le notizie sulla manifestazione, chi rilancia sui social media i tangodown dei siti istituzionali, chi si mette a scrivere un comunicato da mettere sul blog di *Anonymous* Italy. E poi c'è Typhon. L'attacco ai siti governativi è stato condotto con vari mezzi e da più persone. Ma sicuramente nel buon esito dell'azione, considerato che si tratta di siti di un certo spessore, ha pesato la sua botnet, un'ampia rete di computer, device, decoder infettati con un virus e controllati da remoto da un botmaster, cioè da lui. Che può decidere di usare questa armata in continua evoluzione e crescita per

tempestare un sito di richieste al punto da farlo collassare, utilizzando una varietà di tecniche, pacchetti di dati da inviare, e modalità di attacco. Typhon è un hacker di buon livello, e nel campo delle `botnet` è considerato un luminare, come una volta l'ha definito un altro *anon*, peraltro niente affatto digiuno di hacking.

"Bene, ho sistemato le cose per cui [i siti] dovrebbero stare giù per un po'. Vado a mangiarmi un panino", mi dice Typhon a un certo punto con leggiadria, come se fosse un tecnico che ha finito di aggiustare l'antenna di casa e non uno che ha appena *dossato* quattro siti istituzionali, rischiando di essere perseguito per il reato di "Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche" (art. 617-quater del Codice penale) con la possibile aggravante dell'attacco a siti statali, con pene previste da uno a cinque anni.

Non è la prima volta che *Anonymous*, malgrado la volatilità della sua identità fluida e delle sue stanze virtuali, si muove in sintonia con movimenti sociali radicati sul territorio. E a dire il vero, il collegamento del movimento hacktivista con la strada c'è stato fin dagli esordi della sua esistenza, da quando nel 2008 durante *OpChanology*, la campagna contro la *Chiesa di Scientology*, alcuni manifestanti si radunarono anche davanti alle sedi della confessione religiosa americana. Una commistione online/offline che si ritrova anche nell'appoggio a Occupy Wall Street. "In Gran Bretagna è proprio lo stesso movimento di *anonimi* che in parte si è mescolato e trasformato in gruppi di protesta che stanno sul territorio", mi ha detto in quei giorni uno dei membri più anziani di *Anonymous* UK, che conosco da almeno due anni, intervistato sulla chat del loro sito di riferimento Anonuk [vedi in rete]

Del resto qualche settimana dopo, il 5 di novembre 2013, data simbolo di rivolta al potere tratta da *V per Vendetta* e come la maschera adottata dal movimento hacktivista, si svolgeranno manifestazioni *anons* (la cosiddetta *MillionMaskMarch*) in molte città del mondo, come Washington, Filadelfia, Berlino, Dublino, Varsavia, Beirut e ovviamente Londra. Qui centinaia di persone con e senza maschera si riverseranno davanti a Buckingham Palace, confrontandosi anche con la polizia [vedi in rete].

Questo per sgombrare subito il campo dall'equivoco per cui *Anonymous* sarebbe solo un'entità virtuale, che vive unicamente dietro a un monitor. Ma sicuramente le manifestazioni di ottobre per l'Italia segnano un passaggio ulteriore, e rimpiazzano in qualche modo il 5 novembre tricolore (la *MillionMaskMarch* appena citata, che forse per questo da noi nel 2013 ha raccolto alla fine poche adesioni) perché per la prima

volta sono i militanti formatisi nelle strade, nei centri sociali e nelle scuole a parlare un po' la lingua di *anon*.

Si tratta di una sintonia, di una commistione, non di una identificazione. La mia netta impressione, sulla base delle conversazioni e delle frequentazioni avute con gli *anons* italiani più attivi negli ultimi anni, ma anche con molti *anonimi* stranieri, è che politicamente *Anonymous*, anche qualora appoggi movimenti di lotta concreti e connotati, non sia mai sovrapponibile agli stessi. Soprattutto, gli *anons* non sono inscrivibili in alcun modo nelle categorie tradizionali dell'attivismo o dell'antagonismo. Non solo perché molti di loro non hanno legami, nella vita offline, con quei movimenti, e se una definizione deve proprio incasellarli è quella di cani sciolti; ma anche perché ogni anonimo, una volta online, abbandona parte della sua identità e si unisce davvero a una entità collettiva altra, che ha delle proprie specificità,

linguaggi, regole, ma di fatto è più diluita di quella sua originaria, di appartenenza (sempre che ci sia, e in molti casi non c'è). In pratica il primo `deface` [vedi], defacciamento, che *Anonymous* opera è quello sulla identità politica dei propri partecipanti. Questa è al contempo la sua forza e la sua debolezza, a seconda dei punti di vista. Ma senza questo processo *Anonymous* non sarebbe potuta essere quella macchina furiosa di hacktivismo globale e a getto continuo quale è stata fino ad oggi.

"Fin dall'inizio ho ammirato l'eterogeneità di *Anonymous*, ma anche la sua capacità di muoversi all'unisono verso gli obiettivi più disparati. Così, a un certo punto, sono passato all'azione. Anche per dare un contributo tangibile allo sviluppo dell'hacktivismo in Italia". Così mi ha detto una volta un altro degli *anon* italiani più attivi e di vecchia data, The Elder. È stato uno dei miei primi contatti. Serio e insieme ironico, riservato

ma determinato, individualista e insieme collaborativo; e poi preparato, gentile, disponibile. Ce ne sono pochi come lui. E incarna perfettamente l'identikit dell'*anon* di cui scrivevo poco sopra. Passato direttamente da *4chan* all'hacktivismo; forte coscienza politica di base, scarso coinvolgimento nella vita reale. "Alla base c'è la voglia di contrastare con mezzi informatici le ingiustizie e i soprusi, di riscattarsi, di rimpossessarsi del potere decisionale che ci viene negato dagli Stati. Vogliamo mandare un segnale chiaro: esistono sacche di dissenso e si esprimono in Rete, perché questa è intrinsecamente democratica. Chiunque, con poche risorse, può mettere in difficoltà aziende e governi".

Anonymous Italy – termine con cui indico il raggruppamento più attivo di *anons* nazionali degli ultimi anni, che si ritrova in genere su un certo canale di chat, un blog [vedi in rete] e vari profili social – continua a

marcare da vicino i movimenti sociali di quell'autunno. Nei giorni successivi al 19 ottobre, durante le mobilitazioni degli studenti, finisce offline anche il sito del ministero dell'Istruzione. Dopodiché il gruppo torna a uno dei suoi temi più amati, l'appoggio al movimento *No-Tav*. Il 25 ottobre, con una tripletta, sono di nuovo bombardati con dei DDoS, finendo offline, i siti dello Sviluppo economico, delle Infrastrutture e Trasporti e della Regione Piemonte. L'attacco a quest'ultimo target ha un effetto collaterale non previsto.

La sua caduta rovinosa si porta dietro una cinquantina di altri siti di enti locali piemontesi, ospitati sullo stesso server gestiti da Csi, il consorzio informatico piemontese. La notizia si diffonde subito sui media, che raccontano allarmati di un'intera regione sotto attacco informatico, manco si fosse scatenata una cyberguerra. E con effetti abbastanza comici gli stessi *anons* apprendono

in diretta di aver abbattuto una buona parte dei siti piemontesi dai quotidiani online. Qualcuno pubblica i primi link in chat. Qualcun altro scherza e dice che bisogna aggiornare il comunicato appena pubblicato sul blog (dove ancora oggi sono rivendicati solo i primi tre siti che erano l'oggetto originario dell'azione).

Come avviene di frequente nelle vicende che riguardano *Anonymous*, l'informazione sui media mainstream è spesso la prima vittima. Diversi articoli online, supportati pure da dichiarazioni di amministratori locali, tratteggiano l'epica resistenza di chi avrebbe salvato i dati dei cittadini dal tentativo di furto dei pirati informatici. Tentativo che non c'è mai stato, ovviamente, visto che si trattava di un DDoS, cioè un attacco di negazione distribuita del servizio, che può portare al massimo a rendere inagibile un sito sovraccaricandolo di richieste, ma che non è un'effrazione dei

server e che non può risultare di per sé nella sottrazione di dati.

I DDoS sono lo strumento di protesta preferito da *Anonymous*, e a meno che non si esercitino contro siti che vivono di e-commerce o che svolgano effettivamente funzioni essenziali, producono danni limitati: in ultima analisi rendono solo irraggiungibile un sito per un tot di tempo. Ed è proprio sulla durata di questo tangodown che si basa alla fine la sfida tra chi attacca e chi difende, perché mandare un sito offline per qualche minuto non è un'impresa titanica, tenercelo per un tempo prolungato è già più rilevante.

Dal punto di vista politico, cioè dell'uso che ne fa *Anonymous*, sono lo sviluppo alimentato a steroidi dei netstrike [vedi] degli anni '90, quando un ampio numero di utenti si metteva d'accordo per connettersi a un sito contemporaneamente e sovraccaricarlo. Oggi per mandare in tangodown un obiettivo basta anche un individuo solo dotato di botnet. E i

DDoS, che sono diventati sempre più potenti, vengono usati da un'infinità di soggetti diversi (anche i governi, come vedremo più avanti), con scopi malevoli o criminali. Ma l'utilizzo fatto dagli *anons*, specie quando è *collettivizzato* in un gruppo, è molto simile a una manifestazione non autorizzata. Soprattutto, l'intento è di richiamare l'attenzione dei media, della politica e della cittadinanza sulla questione in oggetto.

Certo, a volte non tutto gira per il verso giusto. Quando nel febbraio 2014 *Anonymous* decide di aiutare le lotte dei facchini e dei lavoratori della logistica di Granarolo, da tempo in mobilitazione a Bologna dopo una serie di licenziamenti e una vertenza molto dura, mandando offline per un bel po' di ore il sito della centrale del latte, l'azione si è prolungata alla fine più del previsto. "Non riesco a fermare l'attacco", mi dice quel giorno a un certo punto Drugo, dopo che le proteste di piazza erano rientrate e si stava

delineando uno spiraglio nelle trattative. Per quanto assurda possa sembrare l'affermazione, il fatto era che il giovane cyberattivista non riusciva in quel momento a connettersi al server della `botnet` che stava inondando di pacchetti il target per dare il comando di stop.

Hacker, montanari e il vento

Tornando al rapporto coi movimenti, la relazione di *Anonymous Italy* con le lotte *No-Tav* risale almeno al dicembre 2011, quando il gruppo italiano attaccò il sito informativo della linea ferroviaria ad alta velocità Torino-Lione: “Uniamo oggi la nostra protesta a quella dei cittadini della Val di Susa”, scrivevano nel comunicato dell’azione, condotta sotto l’etichetta *OperationGreenRights*, che ritroveremo più avanti. Da allora gli interventi *anon* a favore della mobilitazione nella valle piemontese sono stati numerosi, e sono culminati, soprattutto dal punto di vista dell’esito dell’azione, nella cosiddetta *OpPolizia* dell’ottobre 2012, una intrusione nel sito della polizia di stato.

Quando nel corso di tale azione – compiuta in quel caso di nascosto, diversamente dagli attacchi DDoS - gli hacker sono riusciti a estrarre dai server della polizia ben 1,3 Giga di

dati, per un totale di 1500 documenti, spiccavano proprio le informative sui *No-Tav*, e molti materiali legati alle attività di repressione e indagine sul movimento. Documenti da cui emerge l'attenzione minuziosa da parte di questura, prefettura e polizia verso qualsiasi azione dei manifestanti e verso tutte quelle realtà considerate antagoniste. In particolare, in una relazione riservata inviata dalla questura di Torino al ministero dell'Interno, vengono tratteggiate in dettaglio le aggregazioni politiche della provincia considerate estremiste: dagli anarchici, con indirizzi e indicazioni di stabili occupati, al centro sociale *Askatasuna* o al *Gabrio*, ai siti *Infoaut.org* e *Indymediapiemonte.org*; fino a un elenco fitto di presunti leader, con eventuali trascorsi ma anche informazioni sui rispettivi compagni/e di vita. E in questo elenco sono inclusi anche gli ambientalisti del *Comitato Settimo Non Incenerire* di Settimo Torinese, *Greenpeace*,

i comitati *No-Tav* della Bassa Val di Susa, con indicazioni precise sulla biografia politica dei suoi leader, da Alberto Perino a Luca Abbà, l'agricoltore che dopo essersi arrampicato per protesta su un traliccio, nel tentativo di sfuggire all'agente che lo inseguiva, era caduto ed era rimasto gravemente ferito.

L'azione suscita un'ondata di interesse, sia per la qualità dell'effrazione (essendo vittima la polizia), sia per i materiali pubblicati. All'inizio non sono mancate anche polemiche da parte di alcune frange dei movimenti sociali, che hanno condannato la leggerezza di *Anonymous* nel diffondere i nomi e gli indirizzi di singoli attivisti. Questa è una delle critiche e dei problemi ricorrenti nelle azioni che prevedono la messa online di *leak* da parte degli hacker. Che spesso non vogliono o non sono in grado – in genere per mancanze di risorse e di una vera organizzazione nel gestire grandi quantità di materiali – di

eliminare informazioni sensibili dai documenti che rilasciano. “In genere cerchiamo di farlo, ma è vero che qualcosa ci sfugge sempre”, ammette con me Drugo, l’hacktivista *mediatore*, parlando una sera in una chat delle loro operazioni in generale, non di quella in particolare. “Sai, spesso ci ritroviamo in pochi a gestire moltissimi documenti, in fretta, a orari improbabili, con la necessità di non far trapelare notizie prima di aver finito, e dovendo seguire molte procedure di sicurezza per proteggerci. L’organizzazione non è il nostro forte...”.

Malgrado l’incidente – e a dire il vero alcuni degli interessati mi hanno detto di non essere rimasti turbati dalla pubblicazione di quelle informazioni personali – l’episodio ha ulteriormente rafforzato il rapporto coi *NoTav*, al punto che *Anonymous* è finita perfino nei ringraziamenti del documentario autoprodotto *Fermarci è impossibile* sulle lotte in Val Susa. Grazie ai documenti usciti

dalla *OpPolizia*, ad esempio, i *No-Tav* hanno appreso che il 3 luglio del 2011, giorno dell'assedio al fortino/cantiere della Maddalena, le forze dell'ordine avrebbero sparato ben 4357 lacrimogeni, oltre al lancio di acqua di tre idranti. "I lacrimogeni, seppur in un uso così massiccio, si sono rilevati inefficaci nell'allontanamento dei manifestanti che, respinti, ritornavano sull'area rapidamente, vuoi perché attrezzati con maschere antigas, farmaci nonché secchi d'acqua in cui spegnere i lacrimogeni e guantoni per rilanciarli all'indirizzo del personale operante, attenuandone di fatto l'effetto, vuoi per il peculiare contesto boschivo, ricco di vegetazione ed infine per le condizioni del vento, non sempre a favore", è scritto nel documento.

Ambientalisti anonimi

La capacità di *Anonymous* di distaccarsi da quelli che sono i suoi temi fondanti – la difesa della Rete, della circolazione delle informazioni, della libertà di espressione e il rifiuto di forme di censura – e di legarsi a battaglie sociali e radicate nei territori è evidente in *OperationGreenRights*, una delle campagne storiche degli *anons*. Organizzata su uno specifico canale della rete di chat *AnonOps*, raccoglie membri di tutte le nazionalità, e si muove su diversi continenti, anche se ha spesso avuto una forte componente italiana. Dal nostro punto di vista alcune delle sue azioni più potenti degli ultimi anni hanno riguardato due colossi italiani, *Eni* ed *Enel*.

Alla fine dell'ottobre 2013, dopo aver pubblicato sul blog dei preavvisi sibillini - "*Enel*, *Eni*, *Ansaldo* siete stati hackerati. Leak in arrivo presto..." – *Anonymous Italy* rilascia

online una serie di mail e di documenti su *Eni* e *Saipem*. Non è chiaro da dove arrivino questi file, anche se sembra probabile la violazione dell'account di qualche impiegato. Molti documenti riguardano la *Saipem*, controllata di *Eni* che si occupa della realizzazione di infrastrutture e servizi riguardanti la ricerca di giacimenti di idrocarburi e la costruzione di oleodotti. Ci sono una serie account, di dati personali su dipendenti delle due aziende: nomi, email, società di appartenenza, cognome, password, nickname, telefono. Documenti preliminari su gare e valutazioni di offerte tecniche rivolti ad altre aziende internazionali come la *Qatar Petroleum*. Un file in cui si parla in dettaglio del ruolo di *Saipem* nel *Filanovsky Project*, dove la sussidiaria di *Eni* deve installare due oleodotti sottomarini da una piattaforma nel Mar Caspio. Mail che trattano di viaggi in Congo, dove *Saipem* l'estate precedente ha avuto un grave incidente, quando è affondata

una piattaforma per la perforazione. File Excel, vecchi di qualche anno, che contengono dati sulle flotta di navi usate per le attività di costruzione. A prima vista non sembrano esserci nel *leak* dei documenti particolarmente scottanti, o pistole fumanti di specifici progetti che gli hacktivisti, che hanno preso di mira *Eni* e *Saipem* contestando l'impatto sull'ambiente di alcune loro attività, forse cercavano. Di certo c'è stata, da parte degli *anons*, una netta violazione della sicurezza di importanti colossi energetici. *Eni* è la prima multinazionale italiana, e si colloca alla dodicesima posizione nella classifica mondiale, secondo i dati 2013 di R&S Mediobanca.

Tuttavia è solo l'inizio. Nei giorni successivi avvengono altri rilasci, che riguardano scambi di mail tra dipendenti *Ansaldo*, *Eni* e loro fornitori. In particolare ci sono dei documenti che riguardano la *centrale nucleare di Mochovce* in Slovacchia, controllata dalla

multinazionale dell’energia italiana. Si tratta di un impianto che è da tempo nel mirino degli ambientalisti. Proprio in quei giorni è arrivato al punto critico lo scontro tra *Greenpeace* da un lato, *Enel* e autorità slovacche dall’altro. Gli attivisti contestano infatti la decisione dell’azienda di spendere 4 miliardi di euro per rimodernare la centrale, una struttura vecchia, basata su una tecnologia che risale agli anni ’70. Non varrebbe quindi la pena investire una simile cifra per un impianto non abbastanza sicuro – è la tesi dell’associazione ecologista – quando si potrebbe costruire con la stessa somma una centrale di ultima generazione, o meglio ancora investire in fonti rinnovabili e pulite. Per *Enel* e il governo slovacco invece la scelta sarebbe fondamentale per garantire al Paese la piena autonomia energetica. *Greenpeace* ha ottenuto ad agosto una parziale vittoria, quando la Corte Suprema slovacca ha deciso di accogliere il suo ricorso, annullando la

decisione dell'autorità di regolamentazione nucleare di autorizzare i lavori di completamento dei reattori 3 e 4. Anche se il permesso di costruzione rimane in vigore, il processo di autorizzazione deve essere ripetuto.

In questo scenario subentra l'azione di *Anonymous* che rende pubbliche alcune mail in cui alcuni tecnici parlano proprio di aspetti delicati della centrale. In una si fa cenno al fatto che "da un controllo eseguito presso il cantiere di Mochovce si evince che l'ispettore che ha seguito le attività di montaggio non ha gestito la qualità dei processi e la documentazione in modo appropriato", anche se "attualmente la documentazione è stata resa conforme, nonostante l'immensità di incongruenze riscontrate". E che non sarebbero stati "fatti i dovuti controlli". "La situazione riscontrata è ancor più grave" prosegue chi scrive "se si considera che trattasi di componente montato in una centrale nucleare".

Anonymous Italy cerca di dare il massimo della visibilità alle mail in questione. E nel comunicato sul suo blog scrive: “Il materiale pubblicato con questa azione rende evidente che l’impianto di Mochovce, di proprietà *Enel*, è stato costruito con materiali scadenti ed assemblato frettolosamente senza competenze né controlli. Tutto ciò è ancor più ributtante poiché *Enel* limita gli investimenti nell’energia da fonti rinnovabili ad un livello poco più che simbolico”.

L’azione però cade nel vuoto pneumatico dei media. Nessuno ne parla. Gli unici che sembrano accorgersene sono gli attivisti italiani e slovacchi di *Greenpeace*: questi ultimi chiedono all’autorità di regolamentazione nucleare del Paese di esaminarli. Lo fa anche un loro esperto di nucleare, Jan Haverkamp, secondo il quale, come ha dichiarato all’epoca alla stampa slovacca e ribadito con me via mail più recentemente: “I documenti rilasciati da *Anonymous Italy* confermano quello

che *Greenpeace* sa già da precedenti progetti nucleari nel mondo. La costruzione di centrali è complessa, e ciò significa che dietro al velo di documenti ben impostati si nasconde un caos quotidiano. A volte la punta dell'iceberg di questa realtà diviene pubblica. E la documentazione su Mochovce mostra una simile realtà. Ogni impianto nucleare ha delle debolezze congenite perché la realtà è diversa dai modelli teorici. E questo è tanto più preoccupante nel caso dei reattori 3 e 4 di Mochovce, perché abbiamo a che fare con un progetto degli anni'70 con solo dei miglioramenti marginali che non soddisfano gli attuali concetti di sicurezza. Questa documentazione inoltre mostra che l'autorità di regolamentazione (UJD) ovviamente non è in grado di rimediare alla approssimazione che emerge dal leak, e ci fa domandare ancora una volta cosa ci voglia per far prendere atto della situazione a *Enel* e alle autorità slovacche. È tempo di fermare questo

progetto nato male e lavorare seriamente su alternative più economiche, pulite e orientate al futuro”.

Insomma, in ultima analisi per Havrkamp il leak in sé non è esplosivo – anche ammesso che ci sia qualcosa da scoperchiare, più facile che esca attraverso leak mirati da insiders, da *whistleblower* alla Snowden, difficile riuscirci pescando a caso dalle mail o gli hard disk di dipendenti – e tuttavia ha il merito di svelare al pubblico la realtà niente affatto patinata e sicura del nucleare.

L’azione di *Anonymous* sarebbe dunque degna di nota, da un punto di vista dell’informazione, ma non riesce a uscire sui giornali. GreenRiot non si dà pace di questo silenzio. “Perché non ne hanno parlato, mentre quando c’è di mezzo l’hackeraggio di qualche politico il fatto esce dappertutto?”, mi chiede in chat. Lui è uno dei tre fondatori del canale *OperationGreenRights*, mi fa vedere addirittura un frammento di conversazione

dell'epoca, nel 2011, quando decisero il nome. È uno degli *anonimi* più dediti alla causa ambientalista, e tecnicamente piuttosto versato. Entra in chat in orari improbabili, e inizia a incollare frasi di comunicati chilometrici, un misto di dettagli tecnici e svolazzi retorici. Trascorre ore a spulciarsi mail e documenti, oltre che hackerare siti ed account. Passa da una campagna in Congo a una in Italia, da un'azione in Venezuela a una contro la Monsanto in Corea. Non ha mai tregua, conosce molto bene gli argomenti che tratta, dagli OGM al nucleare, dall'inquinamento delle acciaierie ai problemi legati alla costruzione della Tav. Non l'ho mai visto perdere tempo a scherzare più di tanto nel canale di chat pubblica o anche in quelle private, ma è sempre dedito alla *causa*, che sia il comunicato da redigere, il sito da *dossare* o violare, o le mail da esaminare. Di sé dice pochissimo, anche se non sembra eccessivamente giovane. A volte la

notte, complici i *tour de force* cui si sottopone e magari qualche bicchiere di vino, ha una conversazione tumultuosa e spezzata, stargli dietro è quasi impossibile. È uno dei personaggi più misteriosi e devoti ai propri ideali che ho incontrato in *anon*. E probabilmente è anche uno dei più *monitorati* dalle forze dell'ordine o dall'intelligence.

Il giustiziere del web

Anonymous ha sempre avuto, tra le tante sue anime, quella del giustiziere. In un certo senso è nato come il Charles Bronson della Rete, pronto a mobilitarsi ogni qual volta qualcuno o qualcosa la minacciava nei suoi assunti. Ma questa componente da vendicatore un po' superomistico si è espressa progressivamente con una serie sempre più varia di soggetti, colpevoli di aver violato quelli che sono considerati elementari principi di giustizia. Una delle battaglie storiche di *Anonymous*, o quanto meno di una sua parte, è quella contro la pedopornografia. Ma una simile modalità di intervento si riversa di volta in volta su target diversi, a seconda del contesto socio-politico. A mio modo di vedere, e dato per assodato il suo Dna originato in internet, capire tale capacità trasformistica è fondamentale se si vuole cogliere l'essenza di questo movimento. E

soprattutto se si vuole evitare di cadere nell'aporia concettuale per cui una certa azione condotta in un Paese non assomiglia a quelle realizzate in un altro. Chi è più *Anonymous*: il gruppo di italiani che lancia delle operazioni a sostegno delle vittime di violenze delle forze dell'ordine, o quello americano (che peraltro ha una componente internazionale molto forte) pronto a concentrarsi sulla caccia agli stupratori di ragazzine del college?

Non c'è differenza. La modalità e anche il principio di base sono gli stessi; cambia solo (e questa, certo, non è cosa da poco) il contesto storico-sociale. Nel marzo 2013 gli anonimi tricolori ad esempio hanno mandato offline per un po' di tempo il sito del *Coisp*, il sindacato autonomo di polizia che aveva raccolto un coro di biasimi e condanne dopo che alcuni suoi rappresentanti avevano manifestato in solidarietà con i poliziotti condannati per l'omicidio di Federico

Aldrovandi proprio sotto le finestre del Comune di Ferrara dove lavorava la madre del ragazzo, Patrizia Moretti. Che in un fotomontaggio *anon* viene addirittura abbracciata, in modo protettivo, dalla maschera di Guy Fawkes.

“Insabbiate la verità, sprezzanti di una madre orfana di un figlio strappatole barbaramente da quattro assassini, rendendovi complici di una sanguinosa mattanza e di un dolore che non può essere sopito. Infangate i diritti umani incarnando il ruolo di capri espiatori, mentre vi prodigate in azioni violente, repressive e deplorevoli. L’ombra del sangue di Federico è più viva che mai”, scrivono gli hacktivisti nel loro comunicato, pubblicando anche un elenco di persone rimaste uccise in azioni di polizia dal 1962 ad oggi. L’attacco contro il *Coisp* si ripeterà nel giugno dello stesso anno, quando offline andrà anche il ministero della Giustizia, in seguito alla decisione del sindacato di presentare delle denunce per diffamazione, una delle quali contro Ilaria Cucchi, sorella di Stefano, morto durante il ricovero in ospedale una settimana dopo il suo arresto per droga.

Le campagne da *giustiziere* di *Anonymous* in America si sono concentrate, quanto meno per quanto riguarda i casi più clamorosi, sulla difesa di vittima di stupri. Una delle storie più emblematiche è stata quella avvenuta nella cittadina di Steubenville, Ohio, dove un hacktivista è riuscito a esporre informazioni che hanno portato all'incriminazione di due giocatori della squadra di football di una scuola superiore, accusati di aver violentato una ragazzina di 16 anni. Il paradosso della vicenda è che l'*anon*, Deric Lostutter, un programmatore ventiseienne del Kentucky, identificato successivamente dagli inquirenti, rischia ora 10 anni di carcere, una pena superiore agli stessi stupratori che ha contribuito a inchiodare.

Un altro episodio che aveva fatto molto rumore è stato quello di Maryville. Nell'ottobre 2013 la cittadina del Missouri si trova improvvisamente sulla ribalta mediatica. Davanti al tribunale in cui si sta svolgendo

un’udienza per un caso di presunto stupro perpetrato ai danni della sedicenne Daisy Coleman (quattordicenne all’epoca dei fatti), e su un’altra ragazzina di cui non viene diffuso il nome, si raduna una piccola folla di reporter, manifestanti e giovani con la maschera di Guy Fawkes. Protestano perché gli inquirenti hanno scagionato l’accusato, un giocatore di football di 17 anni, nipote di un politico dello Stato, malgrado le evidenze nei suoi confronti e il fatto che lui stesso avesse ammesso il rapporto sessuale, perché quest’ultimo sarebbe stato giudicato *consensuale*.

Ma, sull’onda anche di un’inchiesta giornalistica che svela i pregiudizi di provincia della città e l’atmosfera di persecuzione che si è creata nei confronti della stessa vittima e della sua famiglia, *Anonymous* entra in azione, lanciando l’*OpMaryville*. È soprattutto una campagna informativa, condotta a tamburo battente sui social media,

attraverso TwitterStorm e video. In pochi giorni riesce a portare il caso all'attenzione dei giornali globali. "Ci domandiamo: come fanno a dormire la notte i residenti di Maryville? Se il sistema giudiziario ha abbandonato queste ragazze, allora qualcun altro dovrà lottare per loro", proclama un video su *YouTube* con la voce sintetizzata. Alla fine il caso verrà riaperto.

OpMaryville è stata condotta da un gruppo ristretto di persone. Tra questi un *anon* che si fa chiamare *Cryptonymous* [vedi in rete] e che è da sempre molto visibile col suo nickname. Frequentava da tempo le reti di chat di *Anonymous*, dove lo avevo incontrato mesi prima, e dove svolgeva spesso il ruolo di *video maker*. Che lui sia coinvolto in *OpMaryville* è testimoniato anche dai suoi profili social – su cui lo contatto oltre che in chat per una doppia verifica sulla sua identità – dove è stato il primo a pubblicare i materiali relativi all'operazione. "Eravamo in

quattro o cinque”, mi racconta. “In passato avevo lavorato con altra gente anche sul caso di Steubenville, facendo ricerche *per doxare* le identità degli stupratori”. Mi spiega che questo genere di operazioni a volte nascono perché qualcuno va da loro e gli sottopone una storia, oppure, come nel caso di *OpMaryville*, sulla spinta di inchieste giornalistiche. “A quel punto ci incontriamo online, iniziamo a discutere della vicenda e a pianificare quello che c’è da fare, si tratti di hackerare un account, lanciare un `Twitter-Storm`, un kit media (video, comunicati etc.). Una volta definito il piano, ognuno si occupa di un pezzo. Il mio video inizialmente era stato eliminato da *YouTube*, ma il bello di *Anonymous* è che la gente ha iniziato a copiarlo e ripubblicarlo online”. Ovviamente, precisa Crypt0nymous, *OpMaryville* non è stata una grossa campagna come quelle contro accordi internazionali quali il SOPA, il CISPA o l’ACTA, che dietro il vessillo della

lotta alla pirateria avrebbero ristretto una serie di libertà nonché il diritto alla privacy degli utenti – campagne alle quali peraltro lui ha partecipato. “Si è trattata di un’azione basata sulla coscienza e la giustizia. Ma anche se eravamo in pochi *Anonymous* ha fatto diventare Maryville una questione nazionale. Molte persone, specie le più giovani, sono state colpite dalla vicenda e dai contenuti che abbiamo fatto circolare al riguardo. Alla fine l’operazione era ovunque, dai giornali ai social media ai blog. Il video puntava il dito contro il trattamento di favore riservato alle famiglie ricchi e potenti. È stata la mia coscienza a spingermi ad aiutare Daisy, anche se non la conoscevo”.

Quest’idea di intervenire in difesa dei più deboli, declinata sulle specificità e le sensibilità socio-culturali di un Paese, si ritrova anche in un’altra campagna a favore degli homeless, e non a caso partita dalla Gran Bretagna. Lanciata nell’autunno del 2013,

OpSafeWinter [vedi in rete] è un caso interessante perché è un'azione [vedi in rete] che è riuscita a far parlare di sé senza hackerare. E perché è stata lanciata inizialmente da tre soli utenti incontratisi in chat, come mi ha raccontato uno dei suoi fondatori, l'*anon* che si fa chiamare mele2511 e che gestisce uno dei profili *Twitter* di riferimento, *OpSafeWinter Ops* [vedi in rete]." L'idea è nata a causa degli inverni sempre più rigidi", mi spiega il cyberattivista. In sostanza la campagna vuole portare l'attenzione su chi vive per strada, cercando di dare un aiuto concreto, si tratti di trovare strutture di accoglienza, coperte, cibo, medicinali etc., e coordinandosi quindi con associazioni e cittadini offline. "Facciamo tutto via *Twitter* e *Facebook*", continua l'*anon*, fornendo una lunga lista di città dove si sono mobilitati dei gruppi o sono nate delle azioni. Il tutto è partito dalla Gran Bretagna ma si è presto esteso anche agli Stati Uniti, al

Brasile, alla Germania, e in altri Paesi. Gli chiedo come mai hanno scelto questo tipo di operazione: “ *Anonymous* è un’idea che molti possono usare per sostenere una causa in cui credono”, mi risponde. “Siamo divisi in molti gruppi a seconda delle capacità, on-line e offline. Ad esempio c’è molta gente in *Anon* che non sa nulla di hacking ma che è molto brava a creare materiale di protesta, kit media, o a fare lavoro di coordinamento. Inoltre penso che in passato abbiamo avuto anche una copertura mediatica negativa, e un’operazione del genere non può che fare bene alla nostra immagine, oltre che natural-mente agli homeless per cui in primo luogo è nata”.

L'interesse degli *anon* inglesi verso i senza tetto è testimoniato anche da un'altra operazione di tipo prettamente culturale. Un gruppo di hacktivsti britannici si è messo d'accordo con degli editori per realizzare un libro su *Anonymous* interamente scritto da *anonimi*. Per farlo si sono coordinati su un forum online. Me lo ha raccontato per la prima volta un *anon* inglese di vecchia data, chiamiamolo Defencer, spiegandomi anche che tutti i diritti del libro sarebbero andati agli homeless. Già, perché il libro è scaricabile gratuitamente in versione digitale, ma si può anche acquistare in versione cartacea. "Abbiamo pensato fosse una bella idea, un libro su *Anon* fatto da *anons*. È venuto un po' Uk-centrico però. Vorremmo farne uno più globale".

A pubblicare il volume è *The Imaginary Book Co*, una piccola casa editrice alternativa. "Negli anni '70 ero un punk, sono cresciuto con l'idea di ribellione, protesta e

anarchia”, mi spiega uno dei due fondatori di *The Imaginary Book Co*, Rob Agasucci. “Invecchiando sono rimasto disilluso dalle vecchie forme di mobilitazione e attivismo; semplicemente non funzionano nel mondo moderno. Ma *Anonymous* stava facendo qualcosa di realmente nuovo ed eccitante. Ho davvero ammirato le sue attività fin dall’inizio, e ho pensato che sarebbe stato bello fare un libro su di loro. Ma sapevo anche che non volevo una specie di analisi sociologica: c’è altra gente, più qualificata, che può farla. Ho pensato che fosse meglio lasciar parlare direttamente loro, e permettere che i lettori si facessero la loro idea”. Quindi Rob si è presentato online, ha spiegato cosa voleva fare e ha atteso il passaparola. La risposta, dice, è stata entusiastica: ha ricevuto moltissimi articoli, riflessioni, disegni, artwork. Ne ha stampato il 98 per cento, con un editing quasi inesistente. Pochissime le stupidate o le *trollate* inviate. “Sono stato piacevolmente

sorpreso di vedere l'entusiasmo di alcuni di quegli scritti, ma anche l'intelligenza di certe considerazioni. C'è quest'idea diffusa che *Anonymous* sia solo un gruppo di ragazzini che non escono mai dalle loro camerette e hackerano per divertimento. In alcuni casi può esserci del vero, in questa immagine, ma è evidente che lì si trovano anche persone molto in gamba. *Anonymous* è cresciuta. Mi ha deliziato leggere riferimenti al situazionismo, dato che è stato un gruppo che mi ispirò. È stupendo vedere che una nuova generazione è spinta dall'idea di cambiare non solo alcune organizzazioni corrotte, bensì tutto nelle nostre vite. Credo che sia un momento molto eccitante per il mondo. Ci troviamo alla vigilia di una nuova forma di democrazia; e a chi oggi detiene il potere questa cosa non piacerà, e farà di tutto per mantenere lo status quo. Bisognerà vedere cosa come evolverà il fenomeno, in fondo è

per questo che volevamo fare il libro, per cercare di catturare questo momento”.

Sono ancora legione?

Ma a essere catturati sono stati anche molti *anons* negli ultimi due anni. La parabola di *Anonymous* è andata crescendo dal 2008 in poi, dalla prima campagna contro *Scientology* (definita *OpChanology*, operazione Chanology) ; ha quindi attraversato *Occupy Wall Street*, la *Primavera Araba*; ha avuto un exploit scoppiettante con la sigla affiliata di *LulzSec*; e probabilmente ha toccato il suo massimo di visibilità nel 2012. Poi le sue attività sono in parte diminuite, o meglio, sono diventate meno visibili, e soprattutto hanno dominato di meno i media, che non trovavano più i `DDoS`, i `leaks` e la maschera di Guy Fawkes così attraenti come all'inizio.

Naturalmente ha pesato anche la repressione, una serie di arresti e di indagini in diverse nazioni che per ora si sono concluse con sentenze piuttosto pesanti. C'è stata la vicenda di Jeremy Hammond, condannato a

10 anni per aver violato l'azienda di intelligence *Stratfor*, da cui sono usciti molti documenti riservati sul complesso cyber-industriale, ripubblicati da *WikiLeaks*. Oppure c'è stata l'incredibile storia di Barrett Brown, l'ex-portavoce non ufficiale di *Anonymous*, e poi giornalista, che è da oltre un anno rinchiuso in prigione negli Usa in attesa di processo col rischio di una pena di quasi cento anni: anche se non era un hacker e non era nemmeno in grado di hackerare, è rimasto coinvolto nell'attacco informatico alla stessa *Stratfor*, accusato, tra le altre cose, di aver condiviso in una chat pubblica il link che rimandava ai documenti trafugati. Un caso che ha fatto scalpore, anche se mentre scrivo stanno cadendo alcuni dei capi d'imputazione più controversi. Le vicende giudiziarie di Hammond e Brown sembrano voler fare di questi due giovani un esempio che faccia da deterrente per altri.

Tanto più se si confronta la loro situazione con quella di Hector Xavier Monsegur, noto online come Sabu, leader di *LulzSec*, che ha avuto solo 7 mesi di prigione malgrado gli innumerevoli reati collezionati, in virtù del suo ruolo di informatore e, di fatto, di provocatore. Tra l'altro mentre lavorava per l'Fbi Sabu avrebbe addirittura coordinato centinaia di cyberattacchi a siti stranieri, inclusi governi quali l'Iran, la Siria, il Brasile, il Pakistan. In un caso avrebbe guidato un altro hacker in modo da fargli estrarre grandi quantità di dati dai server di alcuni Paesi, facendoli poi caricare su un sito controllato dai federali.

Non solo: secondo alcuni documenti processuali ripubblicati dalla stampa americana proprio mentre scrivo, lo stesso attacco a *Stratfor* sarebbe stato gestito da Sabu, che avrebbe ricevuto una vulnerabilità da un terzo misterioso hacker e l'avrebbe poi passata ad Hammond, il quale portò a termine

l'operazione. L'Fbi - che all'epoca controllava Sabu perfino con un keylogger, un software che registra tutto quello che si digita sul computer - avrebbe quindi quanto meno avallato, per non dire coordinato, fin dall'inizio una pesante violazione informatica a un importante contractor di intelligence che tra i clienti aveva personale della Cia e della Nsa. Perché? Solo per incastrare Hammond alzando la posta in gioco?

Come sappiamo la collaborazione *proattiva* di Monsegur ha portato a molti arresti, incluso quello dello stesso Hammond; inoltre, secondo diverse testimonianze, Sabu avrebbe anche cercato, con scarso successo, di coinvolgere in attività illecite programmatori, attivisti anti-sorveglianza e chiunque fosse troppo vicino ad *Anonymous*, come Jacob Applebaum e Nadim Kobeissi, oltre a Julian Assange.

Secondo Applebaum, che è uno dei principali sviluppatori di *Tor*, Sabu farebbe parte "di

una moderna operazione di *COINTELPRO* dell'Fbi e del Dipartimento di giustizia per attaccare, screditare e danneggiare i moderni movimenti sociali su internet". Il riferimento è al programma di infiltrazione e spionaggio attuato negli anni'50 e '60 negli Usa contro i movimenti sociali, i gruppi di sinistra e quelli per i diritti civili.
Interessante anche che Hammond sia descritto, dalle carte processuali di Monsegur/Sabu, come "il principale obiettivo cybercriminale dell'Fbi". Stiamo parlando di un giovane di 29 anni, con un passato di attivista contro la guerra in Iraq, per i diritti civili, ambientalista, anarchico, che propugnava pubblicamente la disobbedienza civile elettronica, che avrebbe hackerato *Stratfor* - attacco che, abbiamo visto, è stato servito su un piatto d'argento da Sabu/l'Fbi - non per soldi o per altri vantaggi ma mosso dalla volontà di far luce sugli opachi apparati di sorveglianza pubblico-privata (emersi

successivamente nella loro maestosità con il *Datagate*). Ebbene, per il governo Usa nel 2012 era il cyber nemico pubblico numero uno.

Ma si potrebbero ricordare molti altri episodi, come i 18 mesi dati in Gran Bretagna a Nerdo, Christopher Weatherhead, 22 anni, colpevole essenzialmente di essere stato un operatore su un network di chat dove veniva gestita la campagna contro *PayPal* (e Mastercard, e Visa) in difesa di *WikiLeaks*, *OpPayback*. In Italia l'indagine legata al blitz del maggio 2013 – che portò a 4 arresti ai domiciliari e altre sei indagati, con relative perquisizioni – ha formulato un'ipotesi di associazione a delinquere che se dovesse essere confermata potrebbe condurre a condanne pesanti, oltre a imporre su un'entità virtuale e liquida come *Anonymous* lo schema tradizionale e rigido dei reati associativi.

Lo stesso network *AnonOps*, il principale luogo di ritrovo di *anons*, è meno popolato di

un tempo, basta dare un'occhiata alle presenze di utenti nei vari canali per cogliere la differenza. Tuttavia *AnonOps* non coincide con *Anonymous*, e la sua minore attività potrebbe semplicemente registrare un calo della popolarità di quello specifico network, non del movimento hacktivista di per sé. Proprio gli arresti che ci sono stati, in molti casi ottenuti attraverso il lavoro di agenti infiltrati, provocatori e informatori, hanno accresciuto la diffidenza verso reti troppo visibili o centralizzate, e considerate non abbastanza sicure. Molti *anons*, e lo dico per averlo visto coi miei occhi, si sono spostati su network collaterali, si sono sparpagliati in piccoli gruppi. Un fenomeno che peraltro rende più difficile lanciare e coordinare campagne massicce come quelle del passato (un esempio per tutti: *OpPayback*, che coinvolse migliaia di utenti).

Poi nell'estate 2013 è esploso il caso Snowden, con la pioggia di rivelazioni sulla

sorveglianza globale messa in piedi in primo luogo dall'agenzia americana Nsa e da quella inglese Gchq. E *Anonymous* è stata relegata nelle terze file dell'attenzione mediatica. Nello stesso tempo non ha mai veramente lanciato una vasta campagna di attacchi contro l'*Agenzia di sicurezza nazionale* per protestare contro i programmi di sorveglianza globali, come qualcuno si sarebbe aspettato.

"Credo che uno dei problemi sia: da dove iniziamo? Cominciamo a *dossare* tutti i siti governativi?", mi ha risposto uno degli operatori di *AnonOps*, chiamiamolo Vigilante, addetto tre le altre cose proprio ai rapporti con la stampa (sì, c'è una stanza di chat apposita, anche se non è sempre la via migliore per parlare con qualcuno). "Inoltre c'è da dire che *AnonOps* non è più quella di una volta. Il canale principale raggiunge al massimo 200 utenti ora, mentre una volta c'erano migliaia di persone su questo solo

network. È vero che il numero di utenti non coincide con la forza di un movimento; così come *AnonOps* non è *Anonymous*. Ma certo è indicativo".

Gli chiedo se hanno pesato gli arresti. "Direi di sì, hanno spaventato alcuni", mi dice. Ma è chiaro che non è solo una questione di manette, che pure hanno il loro peso, specie se significano anni di prigione per una violazione informatica. Il fenomeno è più complesso.

Ad esempio, dopo lo scandalo sulla sorveglianza globale, su *AnonOps* è nata una campagna apposita, *OpNsa* [vedi in rete]. Che però non si proponeva di hackerare nulla, anzi: "No fottuti DDoS e Hacking", esplicitava l'argomento del canale. L'operazione era soprattutto informativa, e aveva una sua intelligenza politica. A fronte dell'enorme macchina di monitoraggio della Rete disvelata da Snowden, aveva senso mettersi a buttare giù qualche sito? Non rischiava di apparire come

uno sforzo lillpuziano e velleitario alle prese con un gigante? E soprattutto, per contrastare un simile sistema, non è più utile una consapevolezza diffusa che porti a un'azione politica? Insomma, *OpNsa* si proponeva di informare i cittadini americani e di fare lobbying sui loro rappresentanti al Congresso, attraverso una serie di video che esponevano i legami di alcuni parlamentari con l'intelligence e l'industria della sorveglianza. E attraverso un'attività di sensibilizzazione anche offline, per strada, con volantinaggi.

Ne parlo col gruppo di *anon* più attivi all'interno della stanza di chat dedicata all'operazione. Sono tre o quattro operatori, e in quanto tali gestiscono il canale *OpNsa*, oltre che il sito web [vedi in rete] che raccoglie i filmati e i materiali informativi sulla campagna. "L'obiettivo è smascherare i nostri politici attraverso dei video, mostrare i soldi che sono stati investiti in una sorveglianza incostituzionale a beneficio dei *contractor*

della Difesa, e di quei parlamentari che hanno votato in loro favore. Vogliamo creare un'informazione virale in modo da non farli rieleggere alle prossime elezioni nel 2014", mi dice uno di loro, Poison. Ma perché rifiutate i DDoS e le altre azioni di hacking? gli domando. "Da un lato vogliamo allargare la campagna a più persone possibili ed evitare che chi si unisce possa passare dei guai". "E poi i DDoS funzionano a breve termine, mentre noi cerchiamo una soluzione più duratura al problema: una soluzione politica", interviene un'altra attivista donna, Diana. "Le questioni che affrontiamo sono ben più vaste di un semplice DDoS", concorda un terzo, Bruto. "Abbiamo bisogno di cambiare proprio le leggi". Parole condivisibili. E tuttavia la *OpNsa*, anche per il fatto di essere annegata nella copertura mediatica sul *Datagate*, non ha ottenuto quella visibilità che meritava.

“Quando guardi ai numeri, *OpNsa* è la campagna principale”, mi dice ancora Vigilante nell’autunno 2013. “Ma come dicevamo prima i numeri non equivalgono necessariamente al potere. Le operazioni che hanno avuto più successo sono spesso nate dal nulla, da pochi attivisti. Gli arresti sono stati un deterrente perché hanno colpito anche e soprattutto i promotori. E le operazioni hanno sempre bisogno di qualcuno che le lanci e le gestisca. Credo che ora ci sia meno gente disposta a ricoprire questo ruolo. Poi certo oltre a ciò l’altro ingrediente fondamentale per il successo di una campagna è che ci sia gente disposta a unirsi e a rischiare l’osso del collo”. Vigilante è molto equilibrato nelle sue valutazioni. Capita infatti di trovare l’*anon* paranoico e disilluso (spesso con le sue ragioni) che getta fango su tutto il resto; o quello che difende a spada tratta il movimento qualunque cosa succeda. Lui sembra ragionare in tempo reale su ogni domanda.

“Quando i DDoS erano divertenti tutti volevano partecipare, ma ora che alcuni sono stati arrestati la gente è più cauta. A parte il fatto che arrestare per un DDoS è ridicolo, visto che non c’è differenza con una manifestazione in strada.... Nondimeno un’altra ragione per cui *Anonymous* è più quieta ultimamente è la seguente: finché si trattava di DDoS, partecipare era facile per tutti; ora che gli attacchi si sono fatti più sofisticati, e più complesse le tecniche per non farsi individuare, molte persone semplicemente non hanno le capacità per farli”.

Decido di continuare a sviscerare la domanda “come sta oggi *Anonymous* e dove sta andando?” con altri contatti di vecchia data. The Admnistrator ad esempio, figura *storica*, IRCop, cioè amministratore del network di *AnonOps*, da anni sempre presente nel gruppetto di riferimento che gestisce materialmente quella rete e non solo. Gli vado a parlare qualche tempo dopo la famosa uscita

dell'Fbi dell'agosto 2013, quando i federali americani annunciarono di aver smantellato *Anonymous* [vedi in rete] a seguito degli arresti del gruppo *LulzSec*. (Per inciso, il giorno dopo la dichiarazione di vittoria dell'agente speciale Austin P. Berglas, capo della divisione cyber dell'Fbi, *Anonymous* ha pubblicato una serie di documenti della stessa agenzia prelevati dai suoi server [vedi in rete]).

"Non penso che qualcosa come *Anonymous* possa essere smantellato, se togli una persona ce ne sono altre pronte a prendere il suo posto", mi dice The Admnistrator. "L'affermazione dell'Fbi può essere in parte vera solo nel senso che gli arresti possono aver fatto da deterrente, anche se va detto che le persone abbastanza competenti per essere ricercate dai federali non si spaventano facilmente per questo. Il problema di *Anonymous* è che c'è tanta gente che finisce col rovinare le operazioni, a volte intenzionalmente,

altre volte no; ad esempio i ragazzini che fingono di fare gli hacker e fanno solo danni. Poi ci sono quelli che non hanno nulla da offrire e sanno solo lamentarsi. Ma il fatto è che ci sono anche alcuni che cercano volutamente di distruggere le nostre attività o la disponibilità dei nostri canali di comunicazione, come l'IRC".
Quanto spesso viene attaccato *AnonOps*? gli domando.
"Quasi ogni settimana siamo oggetto di piccoli attacchi, per qualcosa di più rilevante, cioè che davvero compaia nel nostro radar, deve trattarsi di attacchi più grossi, dato che siamo ben strutturati per difenderci, e questi sono più rari, ma accadono comunque quasi una volta al mese". Naturalmente stiamo parlando di attacchi DDoS che puntano a rendere inagibile il network di chat. Per chi frequenta queste reti non è raro ricevere un messaggio che avvisa di possibili rischi di malfunzionamento. "Vi consigliamo di

agganciare le cinture di sicurezza. Previste turbolenze”, recitano in genere simili moniti globali visualizzati sugli schermi di tutti gli utenti connessi. Molte volte la ragione è che la chat è sotto attacco informatico. “Qualche idiota sta provando a farci ballare con un attacco DDoS. Ma noi teniamo saldo il comando”, è ad esempio un genere di alert standard.

La conversazione che ho avuto con The Administrator si è svolta più di un mese prima che uscisse uno dei documenti di Snowden in cui si evinceva che l’intelligence britannica, in un paradossale ribaltamento delle parti, usava proprio degli attacchi di tipo DDoS per colpire i network degli anonimi. Nel febbraio 2014 è infatti emerso [vedi in rete] che una unità operativa della Gchq, il *Joint Threat Research Intelligence Group* (Jtrig), avrebbe usato, contro il movimento che usa la maschera di Guy Fawkes, le stesse tecniche che hanno portato in carcere alcuni

hacktivisti. E quindi attacchi per mandare offline un sito o una rete di chat, ma anche la diffusione di link che indirizzavano a pagine infette, così come la propagazione di messaggi sui social network, indirizzati a presunti attivisti o simpatizzanti, con l'intento di spaventarli. Secondo la Jtrig simili metodi avrebbero allontanato dalle stanze di chat di *Anonymous* l'80 per cento degli individui. La cifra è probabilmente gonfiata. Ma l'idea che uno stato democratico compia attacchi informatici contro un network che raccoglie soprattutto attivisti, molti dei quali non hackerano nulla ma stanno lì per scambiarsi informazioni o condurre campagne d'opinione, è a dir poco discutibile. Nel giugno 2012 gli amministratori di *VoxAnon* – altro grosso network di *anons* che raccoglieva molti utenti europei, e molte operazioni e campagne d'opinione – informavano gli utenti che un pesante DDoS stava distruggendo le loro attività. Lo stesso è avvenuto

nel marzo 2013. “Era enorme”, mi ha detto Vigilante. “È andato avanti per trenta giorni: primi giorni di bombardamento a tappeto, poi a bassa intensità e prolungato. Gli attacchi statali o condotti da grandi organizzazioni li riconosci per durata e intensità. Il risultato è stato di disperdere la base degli utenti”. E infatti *VoxAnon*, a causa di dissidi interni ma anche dei pesanti attacchi ricevuti, è collassata entro l’estate 2013. “Colpire un network di attivisti in modo indiscriminato silenziando tutti quelli che non fanno nulla di male è incredibile”, continua Vigilante “E penso che questa vicenda sarà d’interesse anche per i team legali degli indagati e arrestati: che tecniche hanno usato gli investigatori? Hanno commesso illeciti?”.

“E’ pieno di operazioni condotte contro *AnonOps*”, mi conferma The Brit, ancor prima che uscissero i documenti di Snowden. Lui è un altro della stretta cerchia di amministratori del network. Abbiamo parlato molte

volte, anche perché è una persona molto piacevole, gentile e disponibile. È ovviamente anglofono anche se non ho idea (e del resto non sono domande da farsi qui) di che Paese sia. So solo che sfoggia un aplomb e un humour finemente britannici, oltre che qualcosa di rassicurante e maturo nel modo in cui si relaziona. Me lo immagino un programmatore non più di primo pelo, placidamente seduto nel suo ufficio o nel suo studio con una tazza di *Earl Grey* davanti. Il che significa, conoscendo come la comunicazione online e il social engineering *anon* possano sviare l'interlocutore, che probabilmente è un diciannovenne punk di Detroit crestadotato. O un attempato impiegato della Gchq...

In ogni caso si è sempre rivelato una buona fonte. "È tutto molto caotico", mi dice. "Molti degli attacchi sono probabilmente di matrice governativa, altri arrivano da gruppi hacker ostili. DDoS, bot che loggano [cioè software

automatici che registrano le attività delle chat], malware... I server della radio di *AnonOps* sono stati attaccati in continuazione nel 2013”. Nel momento in cui parliamo, The Brit si muove con più circospezione rispetto al passato. Lui amministra solo la rete, non partecipa - almeno così afferma - ad operazioni di hacking, di certo non in modo visibile. Però si sente comunque braccato. Mi spiega che alcuni ex-*anon* che sono stati individuati dalle forze dell’ordine sono rientrati di nascosto in chat per avvisarlo del fatto che lui sia sotto osservazione in più di un Paese. “Sto molto attento”, mi spiega. “So che il mio Paese mi sta cercando anche se evidentemente non sanno chi sono. E stanno cercando di far compiere dei passi falsi a noi amministratori [che, in teoria, non partecipano mai ad operazioni di hacking], come farci commettere degli illeciti, così da poter dire che *AnonOps* è gestita

da cybercriminali e smantellarla definitivamente”.

OpLastResort

Ma non tutti sono d'accordo con l'idea che *Anonymous* sia stata meno attiva nel 2013. Anzi, c'è chi sostiene l'esatto contrario. E non è una voce di poco peso. Nelson è un *anon* di vecchia data, lo avevo intervistato molto tempo prima quando era *alla guida* di una grossa operazione internazionale, e già all'epoca, come oggi, era fra quelli più in vista su *AnonOps*. Gli sottopongo i miei dubbi sul 2013 come anno meno rampante per gli hacktivisti e lui si mostra in totale disaccordo. "Il 2013 è stato un anno importante, ci sono state operazioni come *OpLastResort* [in cui lui ha avuto un ruolo di primo piano] che hanno giocato col governo americano. Poi c'è stato Snowden e gli altri leaks sulla privacy...".

Lo blocco su Snowden. Siamo tutti d'accordo che sia stato l'evento dell'anno, ma non c'entra molto con *anon*... "Che ne sai?", mi dice

lui a bruciapelo. “Forse noi abbiamo cambiato il modo in cui operiamo. E poi ci sono stati altri leaks, hacks, prima che uscisse fuori Snowden”. `Leakers`, violazioni, `whistleblower`, *anons*, *WikiLeaks*, Snowden... fanno parte della stessa foto di gruppo, mi dice in sostanza. “Abbiamo preso per i fondelli per tre giorni la *US Sentencing Commission* [la commissione federale che si occupa di elaborare le linee-guida per i giudici nel procedimento di determinazione della pena]. Abbiamo hackerato la Federal Reserve; l’Fbi. Un migliaio di siti governativi infiltrati. Il 5 di novembre ci sono state manifestazioni in tutto il mondo. Può darsi che sia cambiato il modo in cui lavoriamo, e che la gente sia più sparsa, o tenda a organizzarsi su server privati. *Anonymous* è in ottima forma, è reattiva. E continuerà a concentrarsi sui suoi temi principali: privacy, libertà d’espressione, libertà della Rete e in alcuni casi ingiustizie”.

Provo a seguire il ragionamento di Nelson - che sulla questione Snowden non intende dirmi altro - ed esamino il 2013 alla luce soprattutto di *OpLastResort*, che in effetti è stata una operazione notevole, ma sparpagliata e frammentata. Il problema con *Anonymous*, in questi casi, è riuscire a mantenere una prospettiva storica, una visione d'insieme nel tempo.

E allora bisogna partire da una data molto triste, l'11 gennaio 2013, quando Aaron Swartz si suicida nel suo appartamento di Brooklyn. Aveva solo 26 anni, ma una lunga carriera alle spalle da figlio prediletto della Rete. Programmatore, attivista, startupper, e convinto sostenitore del libero accesso alla conoscenza - al punto da aver scritto un ardente pamphlet al riguardo, intitolato *Guerrila Open Access Manifesto* [vedi in rete] - la sua vita, la sua morte e le sue idee meritano un libro a parte. Quello che va ricordato qui è che quando Swartz si toglie la vita ha

davanti un processo che potrebbe costargli 35 anni di prigione e un milione di dollari di multa per hacking e frode. E questo solo per aver scaricato - attraverso la rete del *Massachusetts Institute of Technology* (MIT) cui aveva accesso - una grande quantità di articoli accademici dalla biblioteca digitale *Jstor* per renderli disponibili al mondo, secondo la filosofia che l'informazione è potere e non può restare accentrata nelle mani di pochi.

La morte del ragazzo prodigio di internet scuote il mondo intero. Inclusi gli *anons*, che sicuramente si sentono vicini a molte delle battaglie condotte da Swartz e che vedono nel suo caso l'esemplificazione più paradossale di leggi ingiuste e persecutorie.

Molti hacktivisti dunque reagiscono, e quello che colpisce è la velocità della loro reazione. Nel giro di poche ore nasce una *OpAngel*, la quale per prima cosa s'incarica [vedi in rete] di *proteggere* il funerale di Swartz, che rischia di essere assaltato dagli invasati della

Westboro Baptist Church - già oggetto in passato di attacchi *anon*. Subito dopo la morte del giovane la congregazione aveva infatti twittato un messaggio alquanto disgustoso: “Lodate Dio, codardi nemici della sua chiesa. Aaron Swartz, hacker, si è ucciso”. Il timore è che qualcuno della setta possa comparire alla cerimonia con uno dei suoi famigerati picchetti. Evento che fortunatamente, anche per la netta reazione online e offline, non si verifica. Ma il 13 gennaio gli *anons* colpiscono anche il MIT, al centro di polemiche feroci per come avrebbe gestito la questione Swartz: il sito dell’istituto viene defacciato [vedi in rete]. “Chiediamo che questa tragedia sia la base per una riforma delle leggi sui crimini informatici, e dei fanatici pubblici ministeri che le usano”, scrivono sullo stesso sito. “Chiediamo che questa tragedia sia la base per una riforma delle leggi sul copyright e sulla proprietà intellettuale, tornando ai giusti principi del

bene comune per molti, più che del guadagno privato per pochi.(...) Chiediamo che questa tragedia sia la base per un rinnovato e deciso impegno a una internet libera e senza restrizioni, libera dalla censura con uguaglianza di accesso e diritto per tutti”.

Il 25 gennaio l’account Twitter *OpLastResort* pubblica il suo primo messaggio, il link a un video sull’assurda vicenda giudiziaria di Swartz. Nelle stesse ore *Anonymous*, sotto la sigla *Operation Last Resort*, prende letteralmente possesso del sito della *US Sentencing Commission*, cui abbiamo già accennato prima, agendo in modo spettacolare. L’austero sito, nel corso di almeno 3 attacchi successivi, viene infatti trasformato in un videogioco, *Asteroids*, un classico arcade. L’account *Twtter* pubblica le istruzioni per

giocare. I visitatori del sito possono sparare ai blocchi di testo della home originale e fare piazza pulita della Commissione federale sulla definizione delle linee guida per le sentenze, target quanto mai simbolico. Il sito a un certo punto va offline ma *Anonymous* aveva già creato un piano di riserva, riproponendo Asteroids su un altro sito governativo (https://twitter.com/OpLastResort/status/295747510163632128).

Il 4 febbraio *OpLastResort* pubblica account e credenziali di 4mila dirigenti bancari statunitensi; e lo fa mettendo il file online su un altro sito governativo, *Alabama Criminal Justice Information Center*. Comincia a delinearsi lo scenario di un'infiltrazione pesante degli hacktivisti nei server federali. Il video *Operation Last Resort*, pubblicato sul sito della *US Sentencing Commission*, raggiunge in pochi giorni oltre un milione di views [vedi in rete] Il 6 febbraio la *Federal Reserve* ammette di essere stata hackerata,

confermando di fatto il leak di due giorni prima.

Il 9 febbraio la stessa campagna *anon* annuncia [vedi in rete] la violazione informatica, il `deface` e un `leak` consistente di dati sui clienti della società d'investimento *G.K. Baum*, già apparsa nei file pubblicati da *WikiLeaks* come collegata a *Stratfor*, l'azienda di intelligence hackerata tempo prima da *Anonymous*, episodio per il quale sia Hammond che Brown sono in prigione.

Dopo questo notevole *tour de force* antigovernativo, *OpLastResort* sembra entrare in una fase di inattività. Si arriva così al giugno 2013, quando sui media scoppia il caso *Datagate*. Il 5 giugno sono pubblicati i primi documenti sulla sorveglianza globale messa in piedi dalla Nsa. Pochi giorni dopo viene fuori l'identità del `whistleblower` che sta dietro a questo colossale leak, Edward Snowden, ex-impiegato della Cia e del

contractor Booz Allen Hamilton, che si trova in fuga dagli Stati Uniti.

Già il 12 giugno *Anonymous* lancia [vedi in rete] una petizione in favore del giovane, con la sigla *#OpSnowdenJustice*, chiedendo il pieno perdono da parte del governo Usa dal momento che Snowden avrebbe semplicemente esposto i programmi illegali e segreti di sorveglianza della Nsa, e quindi non avrebbe commesso alcun crimine. Il giorno prima era uscito un curioso articolo su Gawker, in cui veniva notato come la ex-fidanzata del whistleblower, Lindsay Miller, si era fatta fotografare in passato con la maschera di Guy Fawkes addosso. Sembrerebbe solo un pezzo di colore, ma va notato che l'autore è un giornalista piuttosto ben informato su hacking e dintorni, Adrian Chen (lo stesso che per primo aveva scritto di *Silk Road* tra l'altro). Chen scrive [vedi in rete]: "Ovviamente questo fatto [della maschera] non dice nulla di definitivo su

alcuna connessione con *Anonymous* - la maschera di Fawkes è diventata una sorta di simbolo generalizzato della controcultura - ma è una interessante coincidenza considerando che Snowden lavorava per Booz Allen, che era stato hackerato in modo spettacolare da *Anonymous* nel 2011. Per non dire del fatto che il tipo di materiale che Snowden ha per le mani è qualcosa che la maggior parte degli hacktivisti si sognerebbero di poter esporre”.

Il 17 luglio *Anonymous* annuncia [vedi in rete] di essere entrata nei server della *Federal Emergency Management Agency* (FEMA) e che rilascerà dati su impiegati governativi. Il 19 agosto *OpLastResort* viola un sito dell'amministrazione pubblica inglese e diffonde da lì dati su personale militare e diplomatico americano. L'azione è in

risposta al fermo di 9 ore all'aeroporto di Heathrow cui è stato appena sottoposto David Miranda, compagno del giornalista Glenn Greenwald, autore dei principali scoop del *Datagate*. Il 23 agosto, in pieno scandalo Nsa, e a parecchi mesi di distanza dalla fine del sottogruppo *anon LulzSec*, l'Fbi sente la necessità di fare la seguente dichiarazione [vedi in rete]: *Anonymous* è stata smantellata. Gli arresti del 2012 avrebbero distrutto la leadership del movimento, di fatto neutralizzandolo. Nel giro di poche ore, *OpLastResort* rilascia [vedi in rete] un copioso dump [vedi] di dati personali su impiegati dell'Fbi.

Infine, sempre per restare alle vicende più visibili, il 18 novembre 2013 *Reuters* pubblica un memo dell'Fbi secondo il quale hacktivisti di area *anon* avrebbero infiltrato di nascosto sistemi governativi americani per quasi un anno. Gli attacchi sarebbero iniziati nel dicembre 2012 e sarebbero ancora in

corso al momento del memo. Molti di questi avrebbero sfruttato una falla nella web app *ColdFusion* di Adobe per inserire delle `backdoor` nei sistemi compromessi. Tra i target l'esercito Usa, il dipartimento dell'Energia, quello della Sanità. L'Fbi chiedeva con urgenza agli amministratori di sistema di prendere delle contromisure, affermando che la maggior parte delle intrusioni non erano ancora state rese pubbliche. E che "non è esattamente noto quanti sistemi siano stati compromessi, ma si tratta di un ampio problema che bisogna risolvere".

A ben vedere, forse non erano stati del tutto smantellati.

Paranoia

Josher: Ho fatto una cosa interessante di recente.. Vuoi sentire?
Freezy: Che cosa hai fatto?
Josher: Sono andato... insomma... ad arrendermi
Freezer: Che?? Sei matto?
Josher: Ti spiego. Mi sono svegliato una mattina, due giorni fa, e mi sentivo in uno stato d'animo del cavolo, annoiato, e ho detto: vado ad arrendermi. Così sono andato al quartier generale del dipartimento antiterrorismo del mio Stato, che ha anche a che fare con gli hacker, ok? Dunque sono andato lì, un posto che sta a 15 minuti da dove vivo tra l'altro (ironia della sorte), e quando sono arrivato, sono finito dall'ingresso sul retro, e la guardia mi fa: "devi andare all'entrata principale", così ho girato intorno a tutto il fottuto palazzo, che è enorme peraltro, chiedendo a chi incontravo dove stava questa

entrata. Nessuno lo sapeva. Alla fine ci sono riuscito e sono arrivato, era tipo semi-nascosta nel palazzo (un nascondiglio segreto, maledetti). Così arrivo ma la guardia che sta lì mi dice fermo dove vai? E io, “ehi, voglio arrendermi, sono un hacker ricercato”, e il tipo mi dice: “Non puoi farlo qua, devi andare all’altro quartier generale”. Al che volevo sbattere la faccia sulla sua scrivania, ma sono andato all’altro quartier generale, stavolta prendendo un taxi. Naturalmente il taxista non sapeva dove fosse questo edificio, che alla fine era comunque solo 5 minuti distante, imbecilli entrambi che eravamo... Insomma alla fine arrivo anche lì, entro, vado dalle guardie e dico: “Sono qui per arrendermi”. Allora prendono i miei dati, come già avevano fatto all’altro palazzo, e mi mandano in un altro edificio, più piccolo, e vado anche lì. Ci sono 5 o 6 segretarie, entro e dico: “Voglio arrendermi, sono un hacker ricercato”. E queste vanno in

panico, una inizia a tremare, che cazzo, la segreta organizzazione anti-terrorismo...
Freezy: Forse temevano che le assaltassi con una tastiera e un mouse.
Josher: Insomma mentre queste si agitano, mi dicono di compilare un modulo dove dichiaro di essere colpevole di qualcosa e poi di andare a casa, e mi mettono letteralmente fuori dalla porta.
Freezy: Eh?
Josher: Mentre siedo sulle scale guardando il modulo mi dico: “Ma che cazzo sta succedendo? Possibile?”. Così lascio il foglio e la matita lì ed esco, vado dalle guardie e gli faccio: “Ma che cazzo succede?”. E loro si mettono a ridere. Uno mi dice di andare alla stazione di polizia di dove vivo, peraltro sempre 5 minuti da dove mi trovavo. E quindi ci vado veramente.
Freeze: Mio dio, sto morendo
Josher: C’erano alcuni agenti lì fuori su una panca, vado da loro e gli dico: “Salve, sono

qui per consegnarmi, sono un hacker ricercato a livello internazionale”. Si mettono a ridere, e uno mi chiede: “Come fai a sapere che sei ricercato?”. “Lo so e basta, amico, fidati”. Mi dicono di entrare, mi metto in coda, sudando come un maiale, era caldissimo. Alla fine raggiungo il bancone con l’impiegato e ripeto: “Salve, sono qua per parlare con qualcuno di attività legate a frodi informatiche”. Il tizio mi fa: “Che tipo di frodi?”. “Beh, sono un hacker ricercato”. Si mette a controllare un database insieme a un altro tizio, poi arriva e mi dice che non sono ricercato... Al che me ne vado a casa. Mi butto sul letto. Mi viene da piangere, e sto depresso tutto il giorno. Ah, tra l’altro ti ho detto che ho fatto tutto questo portandomi dietro la mia maschera di Guy Fawkes?

Questa è una conversazione che Josher ha avuto con un altro noto membro di *Anonymous* via chat e che lui stesso mi ha mostrato una sera. Ovviamente la probabilità che

l'episodio sia stato decisamente manipolato nel racconto, se non inventato di sana pianta, è altissima. Però, anche se immaginario, l'ho trovato estremamente simbolico. E probabilmente anche verisimile. C'è tutto in poche righe. Il protagonismo e la paranoia di alcuni hacktivisti, che alternano irrisione e sfida verso corporation e poteri statali a un forte senso di ansia, tale che a volte fa quasi desiderare loro di essere arrestati, per porre fine quanto meno alla minacciosa incertezza in cui si sentono galleggiare; la totale estraneità e incomprensione degli apparati statali nei confronti di questi soggetti, di cui le stesse autorità hanno una percezione distorta e ovattata, mediata da un rozzo immaginario che identifica l'hacker con il cyberterrorista col cappuccio; la farraginosità e opacità degli organismi che si occupano di *law enforcement* e intelligence; e infine la dimensione extraterritoriale degli hacktivisti, che si

muovono slegati non solo da ideologie, ma anche da confini e identità nazionali.

Il racconto getta anche uno squarcio sulla complessa psicologia di Josher, uno degli *anon* più divertenti ed enigmatici che abbia mai incontrato. Giovane, anglofono e brillante, è stato protagonista di alcuni hack che hanno avuto una copertura sui media internazionali (ovviamente non con questo nick, che come al solito ho inventato). Eppure, anche dopo innumerevoli serate passate a parlare via chat, non sono mai riuscita a distinguere in lui la linea sottile tra verità e bugia, tra capacità effettive e tendenze alla mitomania, tra gusto per la provocazione e paranoia. Era come se lui ti inondasse con un fiume di `lulz` [vedi] e provocazioni, in mezzo alle quali a volte brillavano delle pepite. “C’è pieno di storie di spie e federali”, mi dice una sera. “Di solito la gente che sta qua, su *AnonOps*, sono vecchi attivisti ricomparsi con nuove identità. E questo vale anche per

gli infiltrati, i peggiori. Sono quelli che entrano in un gruppo e cercano di influenzarlo a colpire determinati obiettivi. Non hackerano mai, li puoi riconsocere facilmente: Sabu [l'ex-LulzSec divenuto informatore e che ha fatto arrestare i suoi ex-compagni, tra cui Jeremy Hammond. Secondo le testimonianze degli stessi *anons*, Sabu continuava ad hackerare anche quando lavorava per l'Fbi] era un'eccezione. Per questo qua la gente va in paranoia quando qualcuno cerca di fargli hackerare qualcosa. Alcuni hanno imparato la lezione".

Le vicende giudiziarie e la solitudine degli *anon* una volta che sono individuati (privi a differenza di altri movimenti sociali e politici di una vera rete di appoggio), l'uso di infiltrati e informatori, gli attacchi diretti ai network *anon* hanno reso l'atmosfera più pesante di qualche anno fa. I `lulz` sono rimasti ma sono diventati più amari. La paranoia, da virtù principe di chi si muove nel mondo

dell'hacking, è diventata un fardello che appesantisce e rallenta il cyberattivismo. Ci sono membri di *Anonymous* che non hanno mai fatto una violazione informatica, né ne farebbero alcuna, né hanno partecipato in qualche modo a quelle altrui, ma che si limitano ad organizzare campagne d'opinione, e ciò nonostante mantengono nascosta la loro identità come fossero pericolosi cybercriminali. Il timore è che l'azione repressiva si abbatta, in mancanza dei veri artefici di specifiche azioni, su chi abbia la sventura di essere identificato e catalogato come parte di *Anonymous*.

Come detto in precedenza, questa paranoia non risparmia più neppure i network *anon*. *VoxAnon* è stata chiusa dopo gli attacchi DDoS subiti e a causa di problemi di gestione interna fra gli amministratori; *AnonOps* è viva e vegeta, ma meno frequentata rispetto al passato; molti anons si sono sparsi su reti più piccole e defilate. Un'attivista piuttosto

nota, chiamiamola Artemis, che ora staziona sul network *Cyberguerrilla.org*, mi racconta una sera una lunga sequenza di attriti che lei e altri hanno avuto con alcune delle principali aggregazioni *anon*, da *AnonOps* a chi gestisce l'account *Twitter @YourAnonNews*. Le recriminazioni sono sempre le stesse: scarsa chiarezza nella gestione di reti e operazioni. È certamente un paradosso e un problema per *Anonymous*, che reclama con forza la trasparenza da parte di Stati, aziende e politici, trovarsi a sua volta nell'impossibilità di essere trasparente.

"I grossi soggetti o profili Twitter non sono più così efficaci", dice Artemide. "Meglio seguire gruppi e profili più piccoli a seconda delle specifiche campagne. Del resto è anche la natura di *Anonymous* di tagliarsi la testa per essere sicuri che nessuno concentri troppo potere".

In quanto a Josher, dopo aver parlato con lui via chat per circa un anno, con alti e bassi,

ma di fatto instaurando alla fine un rapporto molto amichevole e di relativa fiducia, una sera mi ha salutato dicendo che sarebbe sparito. Convinto di avere addosso diverse agenzie internazionali, annoiato dalle attività *anon*, indeciso sul proprio futuro, ha deciso – almeno temporaneamente, chissà – di sparire dai radar. Non prima però di dirmi, con una certa soavità, che sospettava potessi essere un agente rumeno. L'idea a dir poco balzana gli era venuta perché aveva notato che avevo un nickname secondario che coincideva con quello di qualcuno che lui reputava essere evidentemente un membro di qualche servizio. Solo che quel nick era scaduto da tempo e io, senza saperne niente, me l'ero semplicemente preso. Inutile fargli notare che avevamo parlato più volte anche attraverso i miei account sui social media, o che decine di *anon* italiani potevano facilmente verificare la mia identità. Nulla sembrava convincerlo se non l'idea di fare una

videochiamata con *Skype*. Che ovviamente ho declinato, trovando a dir poco pretestuosa la richiesta. Questo è stato l'ultimo mio abboccamento con Josher. Credo (e spero) che questa sua assurda paranoia finale sia stata in realtà solo un modo divertente per salutarmi. La trollata finale di un ragazzo intelligente e contradditorio.

Cosa dobbiamo aspettarci?

Dunque quale futuro attende *Anonymous*? Gli arresti, le infiltrazioni, l'applicazione severa di leggi spesso inadeguate, la decisione di trattare attivisti che non si muovono per scopo di lucro o di vantaggio personale o statale alla stessa stregua dei più pericolosi cybercriminali - che, come è noto, a differenza di *Anonymous*, tendono a muoversi in silenzio, e a non cercare visibilità, bucando magari gli stessi siti colpiti dagli hacktivisti, che da questo punto di vista dal mondo della security dovrebbero essere percepiti più come un campanello d'allarme che una reale minaccia - hanno indubbiamente avuto un peso nell'attenuare il fenomeno hacktivista, che in fondo era ancora ai suoi albori.

Il fatto è che, al di là di singoli leaks o attacchi informatici più o meno eclatanti, *Anonymous* costituisce essenzialmente una minaccia ideologica, che va controcorrente

rispetto ai soggetti e alle forze che hanno dominato il cyberspazio negli ultimi anni. Il movimento hacktivista è l'esemplificazione quasi tangibile, a partire dal suo immaginario, di una sorta di resistenza alle tendenze dominanti che vorrebbero una Rete controllata, monitorata, un enorme bacino di dati per alimentare industrie di vario tipo, che spaziano dai giganti del web alle imprese della sorveglianza. Una Rete dove le persone leghino le proprie attività online alla loro identità, in cui l'anonimato sia impossibile ai più, in cui le conoscenze e i contenuti siano irreggimentati in una rigida nomenclatura di formati e contratti, in cui la tendenza a distribuire l'accesso e la produzione di informazione e sapere sia incanalata in un numero limitato di gateway. Una internet in cui gli strumenti per nascondersi, difendersi e attaccare siano saldamente in mano a soggetti statali e parastatali, che come il *Datagate* (e non solo) ha dimostrato sono indirizzati

verso una crescente militarizzazione del cyberspazio.

Anonymous, a volte in modo ragionato, spesso in maniera quasi intuitiva e viscerale, è stata l'improvvisa reazione a questa tendenza globale. E tutto ciò ben prima di Snowden. In questo senso hanno ragione quelli che, come Nelson, vedono i due fenomeni in una sorta di continuità. E non importa il fatto che Snowden abbia avuto o meno contatti con questo movimento - di certo li ha avuti con *WikiLeaks* e *Greenwald*, entrambi vicini ad *Anonymous*. Di certo il suo sito di raccolta fondi [vedi in rete] rimanda esplicitamente, oltre ad Assange e Manning, ai casi di Hammond e Brown. La continuità è di tipo ideale e ideologico. Nello stesso tempo la rottura - quasi generazionale - col sistema tradizionale, con i suoi schemi e pregiudizi, è radicale. Per quanto si parli di soggetti diversi, con storie e relazioni fra di loro differenti, c'è un filo rosso che lega

Anonymous, WikiLeaks, *The Pirate Bay*, *Bitcoin*, la comunità crypto, gli attivisti pro-privacy, i `whistleblower`, così come una medesima barriera li separa spesso dalla capacità di comprensione di buona parte dei media, delle istituzioni, della politica. Alcuni di questi soggetti potrebbero avere parabole differenti, alcuni potrebbero essere cooptati, come spesso accade, dai processi di commercializzazione della Rete e dall'irresistibile distruzione creatrice del capitalismo, alcuni potrebbero trasformarsi e altri estinguersi. Ma complessivamente stanno giocando - a volte con buone, altre volte con pessime carte - la stessa partita. Potrebbero essere l'inizio di una trasformazione profonda dei rapporti di potere online e offline. O ridursi a un'enclave resistente, destinata a una progressiva marginalizzazione. Il futuro di *Anonymous* è quanto mai incerto. Ed è in qualche modo connesso col futuro della Rete.

CAPITOLO 4 - Tor e libertà

> L'unico modo di avere a che fare con un mondo non libero è di diventare così del tutto liberi che la tua stessa esistenza è un atto di ribellione - Albert Camus

"Scaricate *Tor* finché siete in tempo". Così twittavano numerosi attivisti della Rete nei giorni in cui il primo ministro turco Erdogan, nel marzo 2014, aveva deciso di impedire l'accesso a *Twitter* nel Paese, prima attraverso un blocco a livello di DNS, del sistema dei nomi di dominio, che tecnicamente è facilmente aggirabile da un utente (basta cambiare le impostazioni DNS sul proprio computer mettendo l'indirizzo di altri DNS, come quelli di *Google*); poi attraverso dei

blocchi a livello di indirizzo IP (in cui il trucco del cambio DNS non funziona più). A quel punto l'utente che voglia circumnavigare il bando ha solo due opzioni: usare una Vpn (un *Virtual Private Network*) oppure la rete e il software *Tor*.

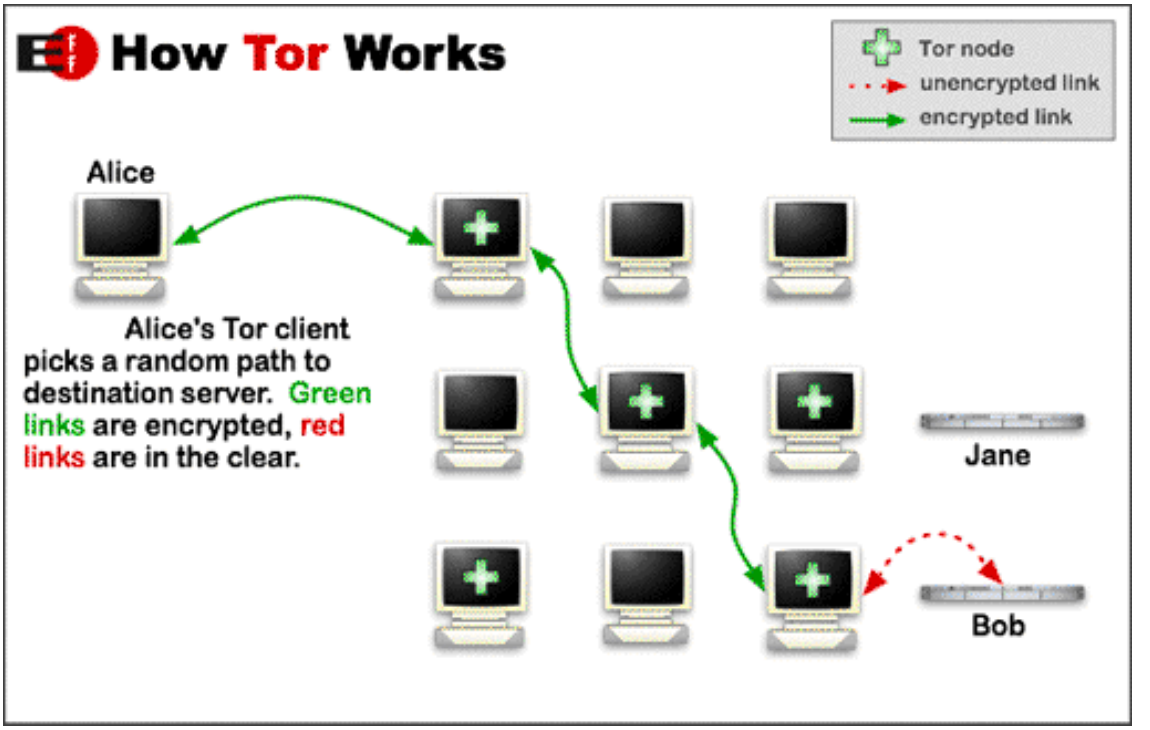
E infatti nei giorni della censura turca, poi estesa anche a *YouTube*, i download del *Tor Browser Bundle* si sono impennati. Il consiglio di scaricare prima possibile il software derivava dalla consapevolezza che il passo successivo del governo di Ankara sarebbe stato quello di rendere più difficile l'accesso al suo sito (di cui comunque erano disponibili in giro per la rete delle copie, o mirrors, a un diverso indirizzo) o al network stesso. Ma ancora una volta il caso ha mostrato come *Tor* incarni davvero una duplice funzione: proteggere la privacy e l'identità di chi lo usa; aggirare la censura e i blocchi sulla Rete. E, nello specifico, superare gli stessi evitando al contempo di essere *tracciati* come utenti

scomodi e da tenere, al minimo, sotto osservazione.

La preoccupazione non è affatto teorica: a un certo punto gli Isp turchi si sono messi a fingere di essere DNS di *Google* – cioè proprio quelli che gli utenti usavano per bypassare il blocco – allo scopo di spiare sul traffico internet degli stessi. L'allarme è stato lanciato dalla stessa azienda di Mountain View. Anche se l'uso di *Tor* avrebbe neutralizzato anche questo tentativo di monitoraggio.

La cipolla che avvolge gli utenti

Che cos'è *Tor*? In estrema sintesi è una rete che cifra il traffico internet utilizzando più strati dopodiché lo fa rimbalzare attraverso i propri nodi prima di farlo giungere a destinazione. E in questo modo lo rende anonimo. La rete è costituita da una serie di `relays` (circa 5mila al momento in cui scrivo, circa 1 milione gli utenti che la usano quotidianamente) che di fatto sono persone o organizzazioni che hanno installato il suo software e lo fanno girare. Ci sono nodi più importanti e delicati di altri, come quelli di entrata e quelli di uscita, nonché molte altre questioni tecniche.



Ma quello che qui preme sottolineare è il fatto che *Tor* – inteso come software e come rete - è al momento attuale il miglior strumento antisorveglianza e anticensura. Usato da giornalisti, attivisti, dissidenti di ogni colore e grado in molti Paesi, oltre che da normali utenti che vogliano aggirare filtri, blocchi o semplicemente proteggere la propria privacy, *Tor* permette non solo di navigare e comunicare in modo anonimo, ma anche di realizzare siti web non rintracciabili, i cosiddetti `hidden service`, servizi nascosti, che terminano nel dominio .onion.

Su *Tor* si è dunque edificato gran parte del *Dark Web*, anche se esistono altre reti anonime, altre darknet, basate su diversi tipi di software.

Questo spazio, che è uno spazio libero, almeno il più libero che si possa avere oggi in Rete, non può che essere condiviso da una miriade di soggetti diversi: gli utenti *normali*, i dissidenti, i giornalisti, gli attivisti di cui dicevamo prima ma anche cybercriminali, e altri ancora. Ma deve essere chiaro che questa commistione, e soprattutto la presenza di cybercriminali o di traffici illeciti, non è qualcosa che si può eliminare mettendo delle barriere, o oscurando quello spazio, ammesso che ciò sia possibile. Quella strana, ma in fondo non così insolita, mescolanza di soggetti diversi, e non tutti graditi, all'interno delle darknet ha a che fare con la libertà. Dove c'è vera libertà bisogna mettere in conto di poter trovare qualsiasi cosa. D'altra parte, se domani *Tor* dovesse

sparire, i cybercriminali e altri soggetti odiosi o pericolosi per la società potrebbero tranquillamente costruirsi delle proprie darknet. L'unico motivo per cui usano *Tor* è che funziona meglio di altre soluzioni.

"Il principale problema di *Tor* è la stampa. Nessuno viene mai a sapere di quella volta in cui qualcuno è scampato allo stalking di un molestatore proteggendosi attraverso il nostro software. Ma ne vengono a conoscenza dell'esistenza solo quando viene beccato qualcuno che si scaricava della pedopornografia", ha dichiarato Eva Galperin, analista globale della *Electronic Frontier Foundation*, su *Business Week* [vedi in rete]. "La ragione per cui i *cattivi* usano *Tor* è che funziona meglio di qualsiasi altra cosa. Ma potrebbero trovare comunque un modo di mantenere il loro anonimato anche senza *Tor*, mentre tutti gli altri che ne hanno bisogno sarebbero lasciati a terra".

Questo è un concetto fondamentale perché di tanto in tanto qualcuno spolvera contro *Tor* l'argomentazione principe della maggior parte dei tentativi di censura su internet. Quella che Julian Assange, nel libro *Internet è il nemico*, ha riassunto nei *Quattro Cavalieri dell'Apocalisse Informatica*: il riciclaggio del denaro sporco, il commercio di droga, il terrorismo e la pornografia.

La nascita fra i militari

Peraltro la stessa origine ed evoluzione di *Tor* sono particolarmente affascinanti. *The onion router*, cioè il router a cipolla – dove l'ortaggio allude ai diversi strati di protezione crittografica che vengono mano a mano pelati via mentre i pacchetti rimbalzano tra i nodi della rete – è un software open source portato avanti dal *Tor Project*, una no-profit che si basa su una comunità di volontari (sviluppatori, traduttori etc.) e che riceve finanziamenti da una pluralità di soggetti, oltre che da migliaia di minuscoli donatori: tra i pezzi grossi, *Google*, la *Electronic Frontier Foundation*, la *National Science Foundation*, *Human Rights Watch*, *Radio Free Asia*, l'agenzia di cooperazione svedese *SIDA*, e lo stesso *Dipartimento di Stato USA*. Quest'ultima presenza non deve stupire.

Tor nasce come progetto del governo americano, in particolare esce dai laboratori di ricerca della Marina militare, che avevano bisogno di uno strumento per muoversi e comunicare in modo segreto e anonimo. Così iniziano a lavorare a metà degli anni ’90 a un sistema di routing a cipolla, che cioè costruisce un circuito crittografato su una serie di computer sparsi e distribuiti in giro. A un certo punto però sentono l’esigenza di estendere il network e di farlo sviluppare su internet. La ragione è che l’unico modo per far funzionare un sistema del genere è che lo costruisca e utilizzi una quantità di soggetti diversi: non poteva gestirlo la Marina. “Se hai un sistema [per l’anonimato] che è solo della Marina, qualsiasi cosa ne venga fuori ovviamente proviene dalla stessa”, ha dichiarato Paul Syverson, uno dei creatori originari di *Tor*. Che oggi ha nella sua plancia di comando una serie di programmatori internazionali e di attivisti per i diritti digitali,

come l'americano Jacob Applebaum. O il tedesco Bartl Moritz.

"È difficile stimare il numero di siti nascosti presenti nel Dark Web", mi dice Moritz. "Uno studio [vedi in rete] ci ha provato e ne ha contati 40mila, ma è probabilmente una cifra sottostimata. È come internet: per un lungo periodo nella sua storia, non c'erano motori di ricerca utili. Non esiste infatti un *Google* per il *Dark Web*, per i servizi nascosti. In un certo senso è un po' come essere sulla Rete di una volta. Non ci sono veri motori, è lenta, le gente si focalizza sui contenuti, senza tutto quel Flash o Javascript a distrarre. C'è a chi piace di più così".

Dopo il Datagate

A mano a mano che emergevano le dimensioni e la scala dei programmi di sorveglianza delle comunicazioni elettroniche, portati avanti dalla Nsa e dalla Gchq, nonché le cassette degli attrezzi con cui le agenzie di intelligence violano, proprio come degli hacker, la sicurezza di reti, computer, software e protocolli, si faceva sempre più chiaro il fatto che strumenti come *Tor* sono tra i pochi a costituire una valida difesa da chi vuole spiare, tracciare, identificare, profilare gli utenti che stanno in Rete. In qualche modo - ed è paradossale (ma non così assurdo) considerata l'origine stessa di quel progetto e il fatto che ancora oggi sia finanziato per il 60 per cento da varie agenzie americane - *Tor* è diventato negli ultimi anni il nemico segreto degli sforzi di controllo della Nsa.
Come hanno dimostrato i documenti diffusi da Edward Snowden, questo progetto è

rimasto l'ultimo baluardo contro quell'apparato internazionale di sorveglianza, di cui le principali democrazie del pianeta sono le prime (e non uniche ovviamente) fautrici. Sappiamo che il suo software e la sua rete sono strutturalmente resistenti agli spioni globali. Che non sono stati compromessi, che non hanno `backdoor`; e del resto, da questo punto di vista, il fatto che il codice sia aperto e verificabile da chiunque, è una garanzia.

La comunicazione fra Snowden e i tre giornalisti chiave del *Datagate* – Laura Poitras, Glenn Greenwald e Barton Gellman, che con le testate di riferimento, *Guardian* e *Washington Post*, hanno vinto il Pulitzer per la loro copertura dello scandalo Nsa – è avvenuta soprattutto attraverso un sistema operativo particolare, *Tails*, interamente basato e ottimizzato su *Tor*, cioè come si dice in gergo, *torificato*.

"Tails è stato vitale per la mia capacità di lavorare in modo sicuro sulla storia della Nsa",

ha dichiarato [vedi in rete] Greenwald. “Più ho imparato cose sulla sicurezza delle mie comunicazioni, più *Tails* è diventato centrale per me”.

Si tratta di un sistema operativo live che punta sulla sicurezza e la privacy di chi lo usa, e che è progettato e configurato per contenere tutto il necessario al riguardo. Può essere lanciato da qualsiasi computer attraverso un Dvd o una chiavetta Usb, e a quel punto forza tutto il traffico web attraverso il network di *Tor*. Insomma, con un solo sistema, un utente può: garantirsi il proprio anonimato in Rete; aggirare filtri e censure nazionali; comunicare in modo sicuro e criptato con chi vuole; difendersi nel modo migliore possibile dal rischio di attacchi informatici. E vincere un Pulitzer...

Secondo le slide della stessa Nsa, *Tor* è “il re dell’anonimato altamente sicuro e a bassa latenza” (nella trasmissione e ricezione dei dati). Vale a dire, è la loro bestia nera. “Non

riusciremo mai a de-anonimizzare tutti gli utenti *Tor*”, hanno scritto gli analisti dell’intelligence americana, cioè a identificarli.
Il che non significa che non ci abbiano provato. Che non abbiano tentato di attaccarlo in vari modi, mirando a singoli utenti, a partire da alcune vulnerabilità specifiche. Come per esempio il caso di un attacco, quello di cui abbiamo già parlato in riferimento alla caduta di *Freedom Hosting*, fatto passare attraverso una versione non aggiornata del browser Firefox su cui si basa il *Tor Browser Bundle* [vedi in rete].
Oggi il progetto è in mano ai suoi stessi utenti. Chiunque può dare una mano, poiché il sistema ha vari livelli di utilizzo. Il primo è scaricare il *Tor Browser Bundle* e navigare in modo sicuro e anonimo. “Usarlo è la prima cosa da fare”, mi ha spiegato in un articolo per *Wired.it* un altro dei suoi sviluppatori, l’italiano Arturo Filastò, 23 anni. “Anche perché le persone che ne hanno

bisogno spesso hanno problemi solo per il fatto di averlo utilizzato. Quindi è un bene che lo impieghi anche chi non è necessariamente un attivista del Bahrein, della Cina o un potenziale Edward Snowden". *Tor Browser Bundle* si può usare sia per navigare anonimamente sui soliti posti online, leggere il giornale etc., sia per esplorare il mondo .onion, cioè i siti ospitati solo sulla rete *Tor*, irraggiungibili via browser normale.

Ma il secondo livello è far girare il software sul proprio pc come un `relay`, cioè come un nodo della sua rete. Non comporta alcun rischio, se non si decide di fare da `exit node`, nodo di uscita, che può presentare qualche complicazione in più, anche legale.

E poi ci sono ancora altri sistemi per dare un contributo. Attraverso `Flash Proxy`, chiunque abbia un sito o un blog può aiutare utenti che vivono in Paesi soggetti a filtri e censure a superare quei blocchi. "È uno

strumento mirato”, spiega ancora Filastò. “Si installa questo widget sul proprio blog e così si fa in modo di donare a *Tor* gli indirizzi IP di chi ci clicca sopra . L’IP serve solo per il primo ingresso degli utenti nella rete *Tor*, quindi anche in questo caso non c’è alcun rischio per l’utente donatore”. E c’è anche un’estensione per *Chrome* che si chiama *CupCake* [vedi in rete]. Quando la si attiva e l’icona diventa azzurra vuol dire che si sta facendo da ponte (bridge) per qualche altro utente.

Infine, si può sempre decidere di donare qualcosa al progetto. Tempo [vedi in rete], se si è programmatori o anche bravi con le lingue per aiutare a tradurre la documentazione; oppure soldi [vedi in rete].

Come ha dichiarato il suo presidente Roger Dingledine: “*Tor* serve: puoi prendere di mira utenti individuali attraverso vulnerabilità del browser, ma se ne attacchi troppi qualcuno se ne accorgerà. Quindi anche se la

Nsa punta a sorvegliare tutti e ovunque, devono essere per forza molto più selettivi nel selezionare gli utenti *Tor* da spiare (...) In generale gli attacchi della Nsa hanno chiarito che noi – e la comunità Internet - dobbiamo continuare a lavorare per migliorare la sicurezza".

Ovviamente il progetto *Tor* non è l'unico a tutelare la sicurezza e l'anonimato delle comunicazioni, o a permettere di creare una rete anonima e nascosta. Ci sono altri sistemi, che però sono meno diffusi, come *Freenet*, un software libero progettato nel 2000 per assicurare la libertà delle comunicazioni. Crea un network che permette a chiunque di pubblicare e leggere informazioni in totale anonimato. Non è però un `web proxy`, non funziona da intermediario per anonimizzare il proprio browsing sulla Rete *normale*. Non è possibile usarlo per navigare su siti come *Google* o *Twitter*, perché la sua funzione è di creare una rete nella

rete, in cui fare tutte le attività che si fanno sul web in chiaro: creare siti, servizi di file sharing, forum, chat, microblogging, email, ma tutti ospitati su *Freenet*. Attraverso una rete di computer su cui gira il suo software, genera infatti un sistema di archiviazione dei contenuti distribuito, P2P, condiviso dagli utenti. Una volta che qualcosa è caricato sulla sua Rete, è quasi impossibile censurarlo, proprio perché sparso in pezzi in giro, salvato e criptato su diversi computer, senza risiedere in un luogo centrale. È chiaro che *Freenet*, più di *Tor*, anche per la sua natura di rete autonoma e separata, è un fenomeno di nicchia, che conta su 10mila utenti (subito schizzati a 13mila in concomitanza col *Datagate*) dove coesistono programmatori, informatici, libertari, dissidenti, utenti che vogliono condividere file in modo nascosto e pedofili. “Vorrei poter far sparire l’ultima categoria, ma nessuna censura significa nessuna censura”, mi spiega Matthew Toseland,

che è stato sviluppatore capo dal progetto dal 2002 al 2013.“ Nel 2003 c’erano molti utenti cinesi, ora molti russi e giapponesi – credo che la presenza di questi ultimi sia legata a una forte repressione sul file sharing nel loro Paese. Nel caso della Russia la questione è più legata invece alla censura di tipo politico”. Gli chiedo come vede il futuro: “Abbiamo bisogno di un network più ampio, con più contenuti, per farlo decollare”, mi dice. “Ingenuo pensare di riuscire ad arrivarci? Non credo. *Freenet* offre la possibilità di creare siti e servizi anonimi e liberi, senza pubblicità, violazioni di massa della privacy e limiti al traffico, ed è pure immune da attacchi informatici del tipo di negazione distribuita del servizio (DDoS)”.

Malgrado l’ottimismo, per questi sistemi le minacce non mancano. Nel caso di *Tor* - il più diffuso, noto ed efficace - possono prendere forme diverse. Anche quella di una misteriosa botnet che nell’estate 2013 aveva

intasato la sua rete. L'organizzazione criminale che la gestiva aveva infatti avuto la bella pensata di usare il network a cipolla per farci girare la sua armata di bot. Così ha fatto scaricare il software per l'anonimato ai suoi zombie (cioè ai computer infettati e controllati da remoto) e li ha fatti connettere a *Tor*, anche se non era chiaro con quale intento. In passato piccole `botnet` hanno usato *Tor* per nascondersi meglio, ma – hanno notato gli sviluppatori – se hai una rete di milioni di pc è assurdo infilarsi in *Tor*, perché puoi crearti da solo un sistema di anonimato peer-to-peer. Così la `botnet` in questione ha causato grossi problemi al mondo onion, rallentandolo. "Il furbone che ha scritto il codice dei bot non ha previsto che, per rendere il network stabile con un così grande aumento di utenza, i suoi zombie sarebbero dovuti diventare a loro volta `relays` [vedi] [contribuendo a dare risorse alla rete, invece di usarla in modo parassitario]. Così invece

si va verso il collasso", mi ha spiegato all'epoca The Architect, l'amministratore di *Cipolla* [vedi in rete].

Anche se l'obiettivo della `botnet` (oggi ormai non più funzionante per fortuna) non sembrava esplicitamente malevolo nei confronti di *Tor*, di fatto quel tipo di azione si configurava come un'offensiva. "Intasare la rete saturandone le risorse, proprio come un net-strike, è uno dei possibili scenari di attacco a *Tor*", mi ha spiegato Claudio Agosti, presidente del centro *Hermes* [vedi in rete] che tra le altre cose lavora su progetti software di supporto a *The Onion Router*.

Resta il fatto, nonostante i problemi e gli attacchi, che *Tor* continua ad essere raccomandato dai massimi esperti di crittografia e sicurezza come Bruce Schneier. In un contesto globale in cui censura e sorveglianza vanno a braccetto e riguardano ormai la maggior parte degli Stati, anche i più insospettabili, e in cui le stesse aziende tech

sono parti attive di una più generale tendenza alla profilazione degli utenti, progetti di questo tipo sono tra i pochi alleati rimasti degli utenti della Rete. Sembra avverarsi la profezia dark dei cypherpunk secondo la quale solo le leggi della matematica e della fisica, e non quelle umane, potranno difendere valori come privacy e libertà di espressione.
Chiedo a Bartl Moritz di replicare una volta per tutte a chi obietta che *Tor* agevolerebbe il crimine e altre attività pericolose.
“Non è un discorso facile, anche a me c’è voluto del tempo per capirlo veramente”, mi risponde. “Stiamo parlando di facilitare le comunicazioni e solo di quello. Pensa a una lettera di carta, al sistema postale dove puoi addirittura mandare degli oggetti fisici in totale anonimato. Ci sono molte ragioni per argomentare in difesa della possibilità di esprimersi in modo libero e anonimo. Alla fine è anche una questione di

proporzionalità: credo che ogni giorno siano commessi crimini ben più numerosi e peggiori nel mondo reale che non su *Tor*. Dunque che alternativa abbiamo? Tra l'altro la tecnologia alla sua base è ben nota e pubblica. Se noi decidessimo di chiudere o di rendere illegali i servizi nascosti, ai criminali non importerebbe. Non puoi sterminare una tecnologia. I delinquenti sono interessati a commettere crimini, non gli importerebbe, impiegherebbero un loro *Dark Web* su misura, ad esempio utilizzando una `botnet`. E, comparato a certe `botnet`, il network *Tor* è ridicolmente piccolo. Senza contare che ormai il prezzo per affittare una di queste è relativamente basso.Quindi alla fine tutto quello che ottieni rendendo illegale una tecnologia per il pubblico è che i criminali continueranno a usare quella tecnologia, mentre il resto della popolazione non potrà più beneficiarne. E invece la gente ha bisogno di anonimato e libertà di

espressione. Voglio un mondo dove le persone possano pubblicare cose in modo anonimo, anche cose che non sono normalmente accettate nel luogo dove vivono, cose che magari anche gli amici o la famiglia non capirebbero, cose che semplicemente si ha paura di dire pubblicamente. Tutto ciò rientra nei diritti umani. Lo dicono esplicitamente". Nell'articolo 19 della Dichiarazione universale dei diritti dell'uomo [vedi in rete] così è scritto: "Ogni individuo ha il diritto alla libertà di opinione e di espressione, incluso il diritto di non essere molestato per la propria opinione e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere".

Dizionario

Agorismo

È una filosofia politica libertaria e liberista, di area anarco-capitalista, che propugna una società in cui le relazioni fra persone si basino su scambi volontari per mezzo di una contro-economia fondata su mercati neri e *grigi*. È stata diffusa negli anni'70 dal filosofo Samuel Edward Konkin III attraverso il suo *Nuovo Manifesto Libertario*.

Astroturfing

È la pratica di mascherare i promotori di un messaggio o un'organizzazione facendo credere che provenga da qualcun'altro.

Bitcoin

È una moneta e un sistema di pagamento elettronico e peer-to-peer, che non ha bisogno di autorità centrali o banche. La gestione delle transazioni e l'emissione di *Bitcoin* viene effettuata collettivamente dalla rete. Si basa sulla crittografia, e anche per questo viene definita criptomoneta. Non è l'unica, ce ne sono diverse, ma è la più diffusa e stabile. Permette un alto livello di anonimato nelle transazioni.

Botmaster

Chi gestisce una rete di bot, di computer (o altri device) zombie che, dopo essere stati infettati, sono controllati da remoto.

Botnet

Rete di bot, ovvero di computer infettati da bot, da un malware. I

computer infettati (detti anche zombie) possono essere controllati da remoto dall'hacker il quale può utilizzarli per diffondere virus, attaccare siti, commettere frodi, inviare spam.

Carder

I carders sono persone che comprano, vendono e utilizzano online i dati di carte di credito, dati rubati violando siti, computer di utenti, o anche i sistemi di pagamento dei retailer.

Dark Web (o Deep Web)

In questo libro uso le espressioni Dark Web o Deep Web nella loro accezione giornalistica. Dunque mi riferisco a quella parte di internet che è anonima, che non è raggiungibile dai normali browser e che non è indicizzata dai motori di ricerca come Google. Le URL di questo

universo terminano con l'estensione .onion e per accedere alle stesse serve il software *Tor* (o altri simili).

Datagate

Lo scandalo mediatico emerso nell'estate 2013 con la pubblicazione dei documenti sottratti da Edward Snowden alla Nsa, l'Agenzia di sicurezza nazionale americana. Documenti che hanno rivelato una serie di programmi di sorveglianza globale delle comunicazioni elettroniche, e che hanno mostrato come la Rete sia un ambiente estremamente insicuro e controllato.

DDoS

Distributed Denial of Service attack, attacco di negazione distribuita del servizio, in cui l'hacker colpisce un sito inondando di richieste un server

finché non collassa per il sovraccarico e quindi va offline.

Deface

Il defacciamento di un sito, cioè un tipo di attacco informatico in cui l'hacker, dopo aver ottenuto l'accesso alle password di scrittura di un sito web, in genere attraverso una vulnerabilità software dello stesso, ne modifica la home inserendo immagini e messaggi.

Dump

Una grande quantità di dati sottratta da un hacker e pubblicata online in genere così com'è.

Hidden service

Servizio nascosto, un sito che sta su un server nascosto dietro la rete *Tor*.

Indirizzo onion

L'indirizzo internet di un `hidden service`, un servizio nascosto che sta sulla rete *Tor*, e che termina in `.onion`

IP

L'indirizzo IP è una serie di numeri che identifica una connessione internet e quindi chi la sta usando. Obiettivo principale di ogni hacker ma anche di chiunque voglia essere anonimo in Rete è quelli di mascherare il proprio IP, nascondendolo dietro altri. Lo si può fare in vari modi: usando un web proxy; una VPN; la rete *Tor* etc.

Leak

La fuoriuscita di informazioni confidenziali o riservate di una organizzazione, azienda o Stato. C'è

chi, come WikiLeaks, ci ha costruito sopra un modello di giornalismo.

Lulz

Risate, divertimento, specie se nati a scapito di qualcun'altro. Una derivazione di LOL.

Netstrike

Una forma di protesta collettiva via internet, nata negli anni '90, che consisteva nel connettersi in contemporanea al sito target per *intasarlo* e farlo andare offline [vedi in rete].

Relays

Nodi della rete Tor.

Vpn

Virtual private network, rete privata virtuale. Permette di incanalare il proprio traffico internet attraverso

una rete privata, che in questo modo maschera l'indirizzo IP dell'utente.

Tangodown

Termine che indica, in gergo militare, l'abbattimento di un nemico. Nel caso di hacker e hacktivisti si usa per indicare l'abbattimento di un sito web, la sua messa offline.

Tor

Il software e la rete che consentono di navigare in Rete in modo anonimo ma anche di costruire siti e servizi anonimi; è una delle strutture fondanti del Dark Web.

Waterboarding

Una forma di tortura che riproduce la sensazione di un annegamento.

Whistleblower

Letteralmente *colui che soffia il fischietto*, termine che indica chi, dall'interno di una organizzazione, ne rivela e denuncia presunte malefatte. In Italia viene tradotto, in modo riduttivo, come *talpa*, *gola profonda*, e via dicendo.

Indice interattivo dei nomi

Aaron Swartz, vedi in *OpLastResort*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7).
Adrian Chen, vedi in *I tanti strati di comunità libertarie*, vedi (1), *OpLastResort*, vedi (1), vedi (2), vedi (3).
Agente-1, vedi in *Quanti pirati ci sono?*, vedi (1).
Al Capone, vedi in *Quanti pirati ci sono?*, vedi (1).
Alberto Perino, vedi in *Hacker, montanari e il vento*, vedi (1).
Altoid, vedi in *Il lungo viaggio dell'operazione Marco Polo*, vedi (1), vedi (2).

Andrew Michael Jones, vedi in *Quanti pirati ci sono?*, vedi (1).
Anonymousasshit, vedi in *Quanti pirati ci sono?*, vedi (1).
Artemide, vedi in *Paranoia*, vedi (1).
Artemis, vedi in *Paranoia*, vedi (1).
Arturo Filastò, vedi in *Dopo il Datagate*, vedi (1), vedi (2).
Backopy, vedi in *Hacker, cracker e biscotti*, vedi (1), vedi (2), vedi (3).
Barrett Brown, vedi in *Sono ancora legione?*, vedi (1), vedi (2), *OpLastResort*, vedi (1), *Cosa dobbiamo aspettarci?*, vedi (1).
Bartholomew Roberts, vedi in *Quanti pirati ci sono?*, vedi (1).
Bartl Moritz, vedi in *La nascita fra i militari*, vedi (1), vedi (2), *Dopo il Datagate*, vedi (1).
Barton Gellman, vedi in *Dopo il Datagate*, vedi (1).
Bernie King, vedi in *Le carte segrete giocate dall'Fbi* , vedi (1), vedi (2).

Black Market Reloaded, vedi in *Hacker, cracker e biscotti*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6).
Bob Marley, vedi in *Hacker, cracker e biscotti*, vedi (1).
Booz Allen Hamilton, vedi in *OpLastResort*, vedi (1), vedi (2).
Brad Pitt, vedi in *Introduzione*, vedi (1).
Brian Krebs, vedi in *Giù nel profondo*, vedi (1).
Bruce Schneier, vedi in *Dopo il Datagate*, vedi (1).
Bruto, vedi in *Sono ancora legione?*, vedi (1).
Canopy, vedi in *Giù nel profondo*, vedi (1), vedi (2).
Charles Bronson, vedi in *Il giustiziere del web*, vedi (1).
Chelsea Manning, vedi in *Cosa dobbiamo aspettarci?*, vedi (1).
Christopher Tarbell, vedi in *Quanti pirati ci sono?*, vedi (1), vedi (2).

Christopher Weatherhead, vedi in *Sono ancora legione?*, vedi (1).
Chronicpain, vedi in *Un furioso Walter White?*, vedi (1).
Cia, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1), vedi (2).
Claudio Agosti, vedi in *Dopo il Datagate*, vedi (1).
Colt, vedi in *Nave affondata, comandante catturato*, vedi (1), *Quanti pirati ci sono?*, vedi (1), *Hacker, cracker e biscotti*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), *I tanti strati di comunità libertarie*, vedi (1).
Cryptonymous, vedi in *Il giustiziere del web*, vedi (1), vedi (2).
Curtis Clark Green, vedi in *Un furioso Walter White?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6).
Daisy Coleman, vedi in *Il giustiziere del web*, vedi (1).

Dark Web, vedi in *I tanti strati di comunità libertarie*, vedi (1).
David Miranda, vedi in *OpLastResort*, vedi (1).
Defencer, vedi in *Il giustiziere del web*, vedi (1).
Deric Lostutter, vedi in *Il giustiziere del web*, vedi (1).
Dread Pirate Roberts, vedi in *Introduzione*, vedi (1), *CAPITOLO 1 - La triste storia di un pirata libertario*, vedi (1), *Nave affondata, comandante catturato*, vedi (1), vedi (2), vedi (3), *Il lungo viaggio dell'operazione Marco Polo*, vedi (1), vedi (2), vedi (3), *Un furioso Walter White?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), vedi (13), vedi (14), vedi (15), vedi (16), vedi (17), *Le carte segrete giocate dall'Fbi* , vedi (1), *Quanti pirati ci sono?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), *Ma chi era veramente*

Ulbricht?, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), *I tanti strati di comunità libertarie*, vedi (1).
Drugo, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), *Hacker, montanari e il vento*, vedi (1).
Edward Snowden, vedi in *Un furioso Walter White?*, vedi (1), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), *CAPITOLO 3 - Vita hacktiva*, vedi (1), *Ambientalisti anonimi*, vedi (1), *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), vedi (4), *OpLastResort*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), *Cosa dobbiamo aspettarci?*, vedi (1), vedi (2), *Dopo il Datagate*, vedi (1), vedi (2), vedi (3), *Dizionario*, vedi (1).
Eileen Ormsby, vedi in *Quanti pirati ci sono?*, vedi (1), vedi (2).
Eliot Ness, vedi in *Quanti pirati ci sono?*, vedi (1).

Erdogan, vedi in *CAP 4 - Tor e libertà*, vedi (1).
Eva Galperin, vedi in *La cipolla che avvolge gli utenti*, vedi (1).
Federico Aldrovandi, vedi in *Il giustiziere del web*, vedi (1).
Flush, vedi in *Un furioso Walter White?*, vedi (1).
Friedrich August von Hayek, vedi in *Il lungo viaggio dell'operazione Marco Polo*, vedi (1).
friendlychemist, vedi in *Un furioso Walter White?*, vedi (1), vedi (2), vedi (3), vedi (4), *Ma chi era veramente Ulbricht?*, vedi (1).
Gary Davis, vedi in *Quanti pirati ci sono?*, vedi (1).
Gawker Adrian Chen, vedi in *Nave affondata, comandante catturato*, vedi (1), vedi (2), vedi (3), *OpLastResort*, vedi (1), vedi (2), vedi (3).

Giacomo Paoni, vedi in *Un furioso Walter White?*, vedi (1), *Giù nel profondo*, vedi (1).
Gibbons, vedi in *I tanti strati di comunità libertarie*, vedi (1).
Glenn Greenwald, vedi in *OpLastResort*, vedi (1), *Dopo il Datagate*, vedi (1), vedi (2).
GreenRiot, vedi in *Ambientalisti anonimi*, vedi (1).
Guy Fawkes, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1), *Il giustiziere del web*, vedi (1), vedi (2), *Sono ancora legione?*, vedi (1), vedi (2), *OpLastResort*, vedi (1), vedi (2), *Paranoia*, vedi (1).
Hakim Bey, vedi in *I tanti strati di comunità libertarie*, vedi (1).
Hal, vedi in *Giù nel profondo*, vedi (1), vedi (2).
Hector Xavier Monsegur, vedi in *Quanti pirati ci sono?*, vedi (1), *Sono ancora legione?*, vedi (1), vedi (2), vedi (3).
Holden, vedi in *Hacker, cracker e biscotti*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5).

Ilaria Cucchi, vedi in *Il giustiziere del web*, vedi (1).
Inigo, vedi in *Quanti pirati ci sono?*, vedi (1).
Jacob Applebaum, vedi in *Sono ancora legione?*, vedi (1), vedi (2), *La nascita fra i militari*, vedi (1).
JakeLaFuria, vedi in *I tanti strati di comunità libertarie*, vedi (1).
Jan Haverkamp, vedi in *Ambientalisti anonimi*, vedi (1), vedi (2).
Jeremy Hammond, vedi in *Quanti pirati ci sono?*, vedi (1), vedi (2), *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), *OpLastResort*, vedi (1), *Paranoia*, vedi (1), *Cosa dobbiamo aspettarci?*, vedi (1).
Josher, vedi in *Paranoia*, vedi (1), vedi (2), vedi (3), vedi (4).
Julian Assange, vedi in *Un furioso Walter White?*, vedi (1), *Cosa dobbiamo aspettarci?*,

vedi (1), *La cipolla che avvolge gli utenti*, vedi (1).
Kali, vedi in *CAPITOLO 2 - Cinquanta sfumature di Dark Web*, vedi (1), *Hacker, cracker e biscotti*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8).
Kane, vedi in *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3).
Kevin Poulsen, vedi in *Giù nel profondo*, vedi (1).
Laura Poitras, vedi in *Dopo il Datagate*, vedi (1).
Libertas, vedi in *Quanti pirati ci sono?*, vedi (1), vedi (2).
Lindsay Miller, vedi in *OpLastResort*, vedi (1).
Luca Abbà, vedi in *Hacker, montanari e il vento*, vedi (1).
Ludwig von Mises, vedi in *Il lungo viaggio dell'operazione Marco Polo*, vedi (1), vedi (2).

Marco Polo, vedi in *Un furioso Walter White?*, vedi (1).
Matthew Toseland, vedi in *Dopo il Datagate*, vedi (1).
mele2511, vedi in *Il giustiziere del web*, vedi (1).
Michael Hayden, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1), vedi (2).
Mike Gogulski, vedi in *Ma chi era veramente Ulbricht?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5).
Nadim Kobeissi, vedi in *Sono ancora legione?*, vedi (1).
Nancy Gertner, vedi in *Le carte segrete giocate dall'Fbi* , vedi (1).
Nelson, vedi in *OpLastResort*, vedi (1), vedi (2), *Cosa dobbiamo aspettarci?*, vedi (1).
Nerdo, vedi in *Sono ancora legione?*, vedi (1).
Niko, vedi in *I tanti strati di comunità libertarie*, vedi (1).

Nod, vedi in *Un furioso Walter White?*, vedi (1), *Quanti pirati ci sono?*, vedi (1).
OpRiptide, vedi in *Giù nel profondo*, vedi (1).
Patrizia Moretti, vedi in *Il giustiziere del web*, vedi (1).
Paul Syverson, vedi in *La nascita fra i militari*, vedi (1).
Pedobuster, vedi in *Giù nel profondo*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5).
Peter Phillip Nash, vedi in *Quanti pirati ci sono?*, vedi (1).
Poison, vedi in *Sono ancora legione?*, vedi (1).
Redandwhite, vedi in *Un furioso Walter White?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), *Ma chi era veramente Ulbricht?*, vedi (1).
Reddit, vedi in *Ma chi era veramente Ulbricht?*, vedi (1).
Rob Agasucci, vedi in *Il giustiziere del web*, vedi (1), vedi (2).

Rocco, vedi in *Giù nel profondo*, vedi (1).
Roger Dingledine, vedi in *Dopo il Datagate*, vedi (1).
Ron Paul, vedi in *Un furioso Walter White?*, vedi (1).
Ross Ulbrich, vedi in *Nave affondata, comandante catturato*, vedi (1), vedi (2).
Ross Ulbricht, vedi in *Introduzione*, vedi (1), *CAPITOLO 1 - La triste storia di un pirata libertario*, vedi (1), *Nave affondata, comandante catturato*, vedi (1), *Il lungo viaggio dell'operazione Marco Polo*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), *Un furioso Walter White?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), *Le carte segrete giocate dall'Fbi* , vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), *Quanti pirati ci sono?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), *Ma chi era veramente Ulbricht?*, vedi (1), vedi (2), vedi (3), vedi (4),

vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), vedi (13).
Sabu, vedi in *Quanti pirati ci sono?*, vedi (1), vedi (2), vedi (3), vedi (4), *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), *Paranoia*, vedi (1).
Samuel Edward Konkin III, vedi in *Nave affondata, comandante catturato*, vedi (1), *Dizionario*, vedi (1).
Satoshi Nakamoto, vedi in *Quanti pirati ci sono?*, vedi (1).
Stefano Cucchi, vedi in *Il giustiziere del web*, vedi (1).
Teen Chat, vedi in *Giù nel profondo*, vedi (1).
The Admnistrator, vedi in *Sono ancora legione?*, vedi (1), vedi (2), vedi (3).
The Architect, vedi in *Nave affondata, comandante catturato*, vedi (1), vedi (2), vedi (3), *Un furioso Walter White?*, vedi (1), vedi (2), *Quanti pirati ci sono?*, vedi (1), vedi

(2), vedi (3), vedi (4), vedi (5), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), *Dopo il Datagate*, vedi (1).
The Baker, vedi in *Hacker, cracker e biscotti*, vedi (1), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3).
The Brit, vedi in *Sono ancora legione?*, vedi (1), vedi (2).
The Elder, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1).
The Thinker, vedi in *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3).
Typhon, vedi in *I tanti strati di comunità libertarie*, vedi (1), *CAPITOLO 3 - Vita hacktiva*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6).
Verto, vedi in *Giù nel profondo*, vedi (1), vedi (2), vedi (3), vedi (4).
Vigilante, vedi in *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), vedi (4).

Indice interattivo delle cose citate

#190, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1).
#OpSnowdenJustice, vedi in *OpLastResort*, vedi (1).
3-D secure, vedi in *Giù nel profondo*, vedi (1).
4chan, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1).
@YourAnonNews, vedi in *Paranoia*, vedi (1).
ACTA, vedi in *Il giustiziere del web*, vedi (1).
Adobe, vedi in *OpLastResort*, vedi (1).
Agenzia di sicurezza nazionale, vedi in *Sono ancora legione?*, vedi (1).

Agorismo, vedi in *Nave affondata, comandante catturato*, vedi (1).
Alabama Criminal Justice Information Center, vedi in *OpLastResort*, vedi (1).
AnonOps, vedi in *Ambientalisti anonimi*, vedi (1), *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), *OpLastResort*, vedi (1), *Paranoia*, vedi (1), vedi (2), vedi (3).
Anonymous, vedi in *Introduzione*, vedi (1), vedi (2), vedi (3), *Nave affondata, comandante catturato*, vedi (1), *Quanti pirati ci sono?*, vedi (1), vedi (2), *Giù nel profondo*, vedi (1), *CAPITOLO 3 - Vita hacktiva*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), vedi (13), vedi (14), vedi (15), vedi (16), vedi (17), vedi (18), vedi (19), *Hacker, montanari e il vento*, vedi (1), vedi (2), vedi (3), *Ambientalisti anonimi*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6),

Il giustiziere del web, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), vedi (13), *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), vedi (13), vedi (14), *OpLastResort*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), *Paranoia*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), *Cosa dobbiamo aspettarci?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7).

Anonymous Italy, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1), vedi (2), vedi (3), *Hacker, montanari e il vento*, vedi (1), *Ambientalisti anonimi*, vedi (1), vedi (2), vedi (3).

Ansaldo, vedi in *Ambientalisti anonimi*, vedi (1), vedi (2).

Askatasuna, vedi in *Hacker, montanari e il vento*, vedi (1).

Asteroids, vedi in *OpLastResort*, vedi (1).
Astroturfing, vedi in *Il lungo viaggio dell'operazione Marco Polo*, vedi (1).
Atlantis, vedi in *Nave affondata, comandante catturato*, vedi (1), *Hacker, cracker e biscotti*, vedi (1).
Bitcoin, vedi in *Introduzione*, vedi (1), *Nave affondata, comandante catturato*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), *Il lungo viaggio dell'operazione Marco Polo*, vedi (1), vedi (2), vedi (3), *Un furioso Walter White?*, vedi (1), vedi (2), vedi (3), *Quanti pirati ci sono?*, vedi (1), *Ma chi era veramente Ulbricht?*, vedi (1), vedi (2), vedi (3), vedi (4), *Hacker, cracker e biscotti*, vedi (1), vedi (2), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), *Cosa dobbiamo aspettarci?*, vedi (1), *Dizionario*, vedi (1), vedi (2).
Black hat, vedi in *Giù nel profondo*, vedi (1).

Black Market Reloaded, vedi in *Nave affondata, comandante catturato*, vedi (1), *Quanti pirati ci sono?*, vedi (1), *Hacker, cracker e biscotti*, vedi (1), vedi (2).
BotMaster, vedi in *Hacker, cracker e biscotti*, vedi (1).
BotMistress, vedi in *Hacker, cracker e biscotti*, vedi (1).
Bradley Manning Support Network, vedi in *Ma chi era veramente Ulbricht?*, vedi (1).
Breaking Bad, vedi in *Ma chi era veramente Ulbricht?*, vedi (1).
Business Week, vedi in *La cipolla che avvolge gli utenti*, vedi (1).
C'thulhu Resume, vedi in *Un furioso Walter White?*, vedi (1).
CISPA, vedi in *Il giustiziere del web*, vedi (1).
COINTELPRO, vedi in *Sono ancora legione?*, vedi (1).

Cantiere, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1).
Carding, vedi in *Giù nel profondo*, vedi (1), vedi (2), vedi (3).
Carnagie Mellon, vedi in *Nave affondata, comandante catturato*, vedi (1).
Centrale nucleare di Mochovce, vedi in *Ambientalisti anonimi*, vedi (1).
Chiesa di Scientology, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1).
Chrome, vedi in *Dopo il Datagate*, vedi (1).
Cia, vedi in *I tanti strati di comunità libertarie*, vedi (1), *Sono ancora legione?*, vedi (1), *OpLastResort*, vedi (1).
Cipolla, vedi in *Introduzione*, vedi (1), *Nave affondata, comandante catturato*, vedi (1), vedi (2), vedi (3), vedi (4), *Un furioso Walter White?*, vedi (1), *Quanti pirati ci sono?*, vedi (1), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), *Dopo il Datagate*, vedi (1).

Cipolla 1.0, vedi in *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3).
Cipolla 2.0, vedi in *I tanti strati di comunità libertarie*, vedi (1).
Coisp, vedi in *Il giustiziere del web*, vedi (1), vedi (2).
ColdFusion, vedi in *OpLastResort*, vedi (1).
Comitato Settimo Non Incenerire, vedi in *Hacker, montanari e il vento*, vedi (1).
Crash!, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1).
Crypter, vedi in *Giù nel profondo*, vedi (1), vedi (2).
Crypting service, vedi in *Giù nel profondo*, vedi (1).
CupCake, vedi in *Dopo il Datagate*, vedi (1).
Cyber Resistance, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1).
Cyberguerrilla.org, vedi in *Paranoia*, vedi (1).

DDoS, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1), vedi (2), vedi (3), vedi (4), *Hacker, montanari e il vento*, vedi (1), *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), vedi (13), *Paranoia*, vedi (1), *Dopo il Datagate*, vedi (1).
DEA, vedi in *Il lungo viaggio dell'operazione Marco Polo*, vedi (1), *Le carte segrete giocate dall'Fbi* , vedi (1), vedi (2).
Dark Web, vedi in *Nave affondata, comandante catturato*, vedi (1), vedi (2), *Un furioso Walter White?*, vedi (1), vedi (2), vedi (3), *Quanti pirati ci sono?*, vedi (1), vedi (2), vedi (3), *Hacker, cracker e biscotti*, vedi (1), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3), *Giù nel profondo*, vedi (1), vedi (2), vedi (3), *La cipolla che avvolge gli utenti*, vedi (1), *La nascita fra i militari*, vedi (1), *Dopo il Datagate*, vedi (1).
Datagate, vedi in *Introduzione*, vedi (1), vedi (2), *Un furioso Walter White?*, vedi (1),

Le carte segrete giocate dall'Fbi , vedi (1), *I tanti strati di comunità libertarie*, vedi (1), *Sono ancora legione?*, vedi (1), vedi (2), *OpLastResort*, vedi (1), vedi (2), *Cosa dobbiamo aspettarci?*, vedi (1), *Dopo il Datagate*, vedi (1), vedi (2).

Deep Web, vedi in *Introduzione*, vedi (1), vedi (2), vedi (3), *Nave affondata, comandante catturato*, vedi (1), vedi (2), *Quanti pirati ci sono?*, vedi (1), *CAPITOLO 2 - Cinquanta sfumature di Dark Web*, vedi (1), *Hacker, cracker e biscotti*, vedi (1), vedi (2), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3), *Giù nel profondo*, vedi (1).

Dipartimento di Stato USA, vedi in *La nascita fra i militari*, vedi (1).

eBay, vedi in *Hacker, cracker e biscotti*, vedi (1), vedi (2), vedi (3), vedi (4).

Electronic Frontier Foundation, vedi in *La cipolla che avvolge gli utenti*, vedi (1), *La nascita fra i militari*, vedi (1).

Enel, vedi in *Ambientalisti anonimi*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7).
Eni, vedi in *Ambientalisti anonimi*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8).
Escrow, vedi in *Nave affondata, comandante catturato*, vedi (1).
Exploit, vedi in *Giù nel profondo*, vedi (1), vedi (2).
Europol, vedi in *Giù nel profondo*, vedi (1).
Facebook, vedi in *Hacker, cracker e biscotti*, vedi (1), *Giù nel profondo*, vedi (1), *Il giustiziere del web*, vedi (1).
Fbi, vedi in *Nave affondata, comandante catturato*, vedi (1), *Il lungo viaggio dell'operazione Marco Polo*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), *Un furioso Walter White?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), *Le carte segrete giocate dall'Fbi* , vedi (1), vedi (2), vedi (3), vedi (4), *Quanti pirati ci sono?*, vedi (1),

vedi (2), vedi (3), vedi (4), *Ma chi era veramente Ulbricht?*, vedi (1), vedi (2), vedi (3), vedi (4), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), *Giù nel profondo*, vedi (1), vedi (2), *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), *OpLastResort*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), *Paranoia*, vedi (1).

Federal Emergency Management Agency, vedi in *OpLastResort*, vedi (1).

Federal Reserve, vedi in *OpLastResort*, vedi (1).

Fermarci è impossibile, vedi in *Hacker, montanari e il vento*, vedi (1).

Filanovsky Project, vedi in *Ambientalisti anonimi*, vedi (1).

Firefox, vedi in *I tanti strati di comunità libertarie*, vedi (1).

Freedom Hosting, vedi in *Hacker, cracker e biscotti*, vedi (1), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), *Giù*

nel profondo, vedi (1), *Dopo il Datagate*, vedi (1).
Freenet, vedi in *Dopo il Datagate*, vedi (1), vedi (2), vedi (3), vedi (4).
G.K. Baum, vedi in *OpLastResort*, vedi (1).
Gabrio, vedi in *Hacker, montanari e il vento*, vedi (1).
Gchq, vedi in *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), *Dopo il Datagate*, vedi (1).
Google, vedi in *I tanti strati di comunità libertarie*, vedi (1), *CAP 4 - Tor e libertà*, vedi (1), vedi (2), *La nascita fra i militari*, vedi (1), vedi (2), *Dopo il Datagate*, vedi (1).
Greenpeace, vedi in *Hacker, montanari e il vento*, vedi (1), *Ambientalisti anonimi*, vedi (1), vedi (2), vedi (3), vedi (4).
Greenwald, vedi in *Cosa dobbiamo aspettarci?*, vedi (1).
Guardian, vedi in *Dopo il Datagate*, vedi (1).

Guerrila Open Access Manifesto, vedi in *OpLastResort*, vedi (1).
HackBB, vedi in *Hacker, cracker e biscotti*, vedi (1), vedi (2), *I tanti strati di comunità libertarie*, vedi (1).
HackBB Reloaded, vedi in *Giù nel profondo*, vedi (1).
Hacktivismo, vedi in *Introduzione*, vedi (1), vedi (2), vedi (3), *Nave affondata, comandante catturato*, vedi (1).
Hells Angels, vedi in *Un furioso Walter White?*, vedi (1).
Hermes, vedi in *Dopo il Datagate*, vedi (1).
Hidden Wiki, vedi in *I tanti strati di comunità libertarie*, vedi (1), *Giù nel profondo*, vedi (1).
Hitman Network, vedi in *Un furioso Walter White?*, vedi (1).
Homeland Security, vedi in *Il lungo viaggio dell'operazione Marco Polo*, vedi (1).
Human Rights Watch, vedi in *La nascita fra i militari*, vedi (1).

Indymediapiemonte.org, vedi in *Hacker, montanari e il vento*, vedi (1).
Infoaut.org, vedi in *Hacker, montanari e il vento*, vedi (1).
Internal Revenue Service, vedi in *Il lungo viaggio dell'operazione Marco Polo*, vedi (1).
Internet Relay Chat, vedi in *Hacker, cracker e biscotti*, vedi (1).
Internet è il nemico, vedi in *La cipolla che avvolge gli utenti*, vedi (1).
Joint Threat Research Intelligence Group, vedi in *Sono ancora legione?*, vedi (1), vedi (2).
Jdb, vedi in *Giù nel profondo*, vedi (1), vedi (2).
Jstor, vedi in *OpLastResort*, vedi (1).
Le Iene, vedi in *I tanti strati di comunità libertarie*, vedi (1).
Leakers, vedi in *OpLastResort*, vedi (1).
leaks, vedi in *Sono ancora legione?*, vedi (1), vedi (2), vedi (3).

Linden Coin, vedi in *Giù nel profondo*, vedi (1).
LinkedIn, vedi in *Ma chi era veramente Ulbricht?*, vedi (1), *Hacker, cracker e biscotti*, vedi (1).
LulzSec, vedi in *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), *OpLastResort*, vedi (1).
Lulzsec, vedi in *Quanti pirati ci sono?*, vedi (1), vedi (2).
Marco Polo, vedi in *Un furioso Walter White?*, vedi (1).
Massachusetts Institute of Technology, vedi in *OpLastResort*, vedi (1), vedi (2).
MillionMaskMarch, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1), vedi (2).
Mises Insitute, vedi in *Il lungo viaggio dell'operazione Marco Polo*, vedi (1).
National Science Foundation, vedi in *La nascita fra i militari*, vedi (1).
National Security Agency, vedi in *Le carte segrete giocate dall'Fbi* , vedi (1), vedi (2), vedi (3), vedi (4), *I tanti strati di*

comunità libertarie, vedi (1), vedi (2), vedi (3), vedi (4), *CAPITOLO 3 - Vita hacktiva*, vedi (1), vedi (2), *Sono ancora legione?*, vedi (1), vedi (2), *OpLastResort*, vedi (1), vedi (2), vedi (3), *Dopo il Datagate*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), *Dizionario*, vedi (1).

No-Tav, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1), *Hacker, montanari e il vento*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5).

Nuovo Manifesto Libertario, vedi in *Dizionario*, vedi (1).

Occupy Wall Street, vedi in *Sono ancora legione?*, vedi (1).

Onion News, vedi in *I tanti strati di comunità libertarie*, vedi (1).

Onionforum v3, vedi in *I tanti strati di comunità libertarie*, vedi (1).

Onionland, vedi in *I tanti strati di comunità libertarie*, vedi (1).

OpAngel, vedi in *OpLastResort*, vedi (1).

OpChanology, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1), *Sono ancora legione?*, vedi (1).
OpLastResort, vedi in *OpLastResort*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8).
OpMaryville, vedi in *Il giustiziere del web*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5).
OpNsa, vedi in *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5).
OpPayback, vedi in *Sono ancora legione?*, vedi (1), vedi (2).
OpPolizia, vedi in *Hacker, montanari e il vento*, vedi (1), vedi (2).
OpSafeWinter, vedi in *Il giustiziere del web*, vedi (1), vedi (2).
OpSafeWinter Ops, vedi in *Il giustiziere del web*, vedi (1).
Operation Last Resort, vedi in *OpLastRe-sort*, vedi (1), vedi (2).

OperationGreenRights, vedi in *Hacker, montanari e il vento*, vedi (1), *Ambientalisti anonimi*, vedi (1), vedi (2).
PRISM, vedi in *I tanti strati di comunità libertarie*, vedi (1).
PayPal, vedi in *Hacker, cracker e biscotti*, vedi (1), vedi (2), vedi (3), *Sono ancora legione?*, vedi (1).
Polizia Postale, vedi in *Giù nel profondo*, vedi (1).
Primavera Araba, vedi in *Sono ancora legione?*, vedi (1).
Qatar Petroleum, vedi in *Ambientalisti anonimi*, vedi (1).
RAT, vedi in *Hacker, cracker e biscotti*, vedi (1), *Giù nel profondo*, vedi (1), vedi (2).
Radio Free Asia, vedi in *La nascita fra i militari*, vedi (1).
Rent A Hacker, vedi in *Giù nel profondo*, vedi (1).
Reuters, vedi in *OpLastResort*, vedi (1).

SIDA, vedi in *La nascita fra i militari*, vedi (1).
Sjdb, vedi in *Giù nel profondo*, vedi (1).
SOPA, vedi in *Il giustiziere del web*, vedi (1).
Saipem, vedi in *Ambientalisti anonimi*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5).
Scientology, vedi in *Sono ancora legione?*, vedi (1).
Second Life, vedi in *Giù nel profondo*, vedi (1).
Sheep Market, vedi in *Nave affondata, comandante catturato*, vedi (1), *Hacker, cracker e biscotti*, vedi (1).
Shroomery.org, vedi in *Il lungo viaggio dell'operazione Marco Polo*, vedi (1).
Silk Road, vedi in *Introduzione*, vedi (1), *CAPITOLO 1 - La triste storia di un pirata libertario*, vedi (1), vedi (2), *Nave affondata, comandante catturato*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), vedi (13), vedi (14), vedi (15), vedi (16),

vedi (17), vedi (18), *Il lungo viaggio dell'operazione Marco Polo*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), *Un furioso Walter White?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), *Le carte segrete giocate dall'Fbi* , vedi (1), vedi (2), vedi (3), vedi (4), *Quanti pirati ci sono?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), *Ma chi era veramente Ulbricht?*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), *Hacker, cracker e biscotti*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), *Giù nel profondo*, vedi (1), *OpLastResort*, vedi (1).

Skype, vedi in *I tanti strati di comunità libertarie*, vedi (1), *Paranoia*, vedi (1).

StackOverflow, vedi in *Il lungo viaggio dell'operazione Marco Polo*, vedi (1), vedi (2).
Stratfor, vedi in *Sono ancora legione?*, vedi (1), vedi (2), vedi (3), vedi (4), *OpLastResort*, vedi (1).
Tails, vedi in *Dopo il Datagate*, vedi (1), vedi (2).
Tangodown, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1), vedi (2), vedi (3), vedi (4).
Taz, vedi in *I tanti strati di comunità libertarie*, vedi (1).
The Imaginary Book Co, vedi in *Il giustiziere del web*, vedi (1), vedi (2).
The Onion Router, vedi in *Dopo il Datagate*, vedi (1).
The Pirate Bay, vedi in *Cosa dobbiamo aspettarci?*, vedi (1).
Tor, vedi in *Introduzione*, vedi (1), *Nave affondata, comandante catturato*, vedi (1), vedi (2), vedi (3), *Il lungo viaggio dell'operazione Marco Polo*, vedi (1), vedi (2), vedi

(3), vedi (4), vedi (5), vedi (6), *Un furioso Walter White?*, vedi (1), vedi (2), *Le carte segrete giocate dall'Fbi* , vedi (1), vedi (2), vedi (3), *I tanti strati di comunità libertarie*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), *Giù nel profondo*, vedi (1), vedi (2), vedi (3), vedi (4), *Sono ancora legione?*, vedi (1), *CAP 4 - Tor e libertà*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), *La cipolla che avvolge gli utenti*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), *La nascita fra i militari*, vedi (1), vedi (2), vedi (3), vedi (4), *Dopo il Datagate*, vedi (1), vedi (2), vedi (3), vedi (4), vedi (5), vedi (6), vedi (7), vedi (8), vedi (9), vedi (10), vedi (11), vedi (12), vedi (13), vedi (14), vedi (15), vedi (16), vedi (17), vedi (18), vedi (19), vedi (20), vedi (21), vedi (22), vedi (23), vedi (24), vedi (25), vedi (26), vedi (27), *Dizionario*, vedi (1), vedi (2), vedi (3), vedi (4).

Tor Browser Bundle, vedi in *CAP 4 - Tor e libertà*, vedi (1), *Dopo il Datagate*, vedi (1), vedi (2), vedi (3).
Tor Carding Forum, vedi in *Giù nel profondo*, vedi (1), vedi (2).
Tor Project, vedi in *La nascita fra i militari*, vedi (1).
Tormail, vedi in *I tanti strati di comunità libertarie*, vedi (1), vedi (2).
Twitter, vedi in *OpLastResort*, vedi (1), *Hacker, cracker e biscotti*, vedi (1), *Il giustiziere del web*, vedi (1), vedi (2), vedi (3), vedi (4), *Paranoia*, vedi (1), *CAP 4 - Tor e libertà*, vedi (1), *Dopo il Datagate*, vedi (1).
TwitterStorm, vedi in *Il giustiziere del web*, vedi (1), vedi (2).
US Sentencing Commission, vedi in *OpLastResort*, vedi (1), vedi (2), vedi (3).
V per Vendetta, vedi in *CAPITOLO 3 - Vita hacktiva*, vedi (1).
Via della Seta, vedi in *Nave affondata, comandante catturato*, vedi (1), vedi (2),

vedi (3), vedi (4), *Un furioso Walter White?*, vedi (1), *Le carte segrete giocate dall'Fbi* , vedi (1), *Quanti pirati ci sono?*, vedi (1), vedi (2), vedi (3), *Ma chi era veramente Ulbricht?*, vedi (1), vedi (2), vedi (3).
Virtual Private Network, vedi in *CAP 4 - Tor e libertà*, vedi (1).
VoxAnon, vedi in *Sono ancora legione?*, vedi (1), vedi (2), *Paranoia*, vedi (1).
Washington Post, vedi in *Dopo il Datagate*, vedi (1).
Westboro Baptist Church, vedi in *OpLastResort*, vedi (1).
Whatsapp, vedi in *Giù nel profondo*, vedi (1).
Whistleblower, vedi in *Un furioso Walter White?*, vedi (1), *OpLastResort*, vedi (1), vedi (2), *Cosa dobbiamo aspettarci?*, vedi (1).
White hat, vedi in *Hacker, cracker e biscotti*, vedi (1), *Giù nel profondo*, vedi (1).
WikiLeaks, vedi in *Un furioso Walter White?*, vedi (1), *Ma chi era veramente*

Ulbricht?, vedi (1), *Sono ancora legione?*, vedi (1), vedi (2), *OpLastResort*, vedi (1), vedi (2), *Cosa dobbiamo aspettarci?*, vedi (1), vedi (2).
Wired.it, vedi in *Dopo il Datagate*, vedi (1).
YouTube, vedi in *Hacker, cracker e biscotti*, vedi (1), *Il giustiziere del web*, vedi (1), vedi (2), *CAP 4 - Tor e libertà*, vedi (1).

Biografia

Carola Frediani è giornalista e co-fondatrice di *Effecinque.org*, agenzia giornalistica indipendente che si occupa di fornire contenuti e prodotti digitali secondo formati innovativi e sperimentazioni attraverso i social media. Scrive soprattutto di cultura digitale, privacy, ambiente, hacking e hacktivism per *L'Espresso*, *Wired*, *Il Secolo XIX*, *Pagina99* e *TechPresident*. In passato ha anche scritto per il *Corriere della Sera* e *Sky.it*, dove tra l'altro ha lavorato al progetto *Beautiful Lab*. In precedenza ha lavorato per quasi dieci anni con Franco Carlini per l'agenzia giornalistica *Totem*. Nel 2012 ha scritto *Dentro Anonymous*, un viaggio nelle legioni del cyberactivism.