La guida pratica per dittatori alla conservazione del potere tramite Internet

Edizione Globale
di Laurier Rochon
email: l@pwd.io
testo disponibile su: http://pwd.io/guide
Giugno 2012, Rotterdam, Olanda
Tradotto da Salvatore Uras, Agosto 2012

1. Obiettivo di questa guida

lo scopo di questa guida è di fornire ai leader di regimi autoritari, autocratici, teocratici, totalitari, ed altri regimi basati su un unico leader o su un unico partito, un insieme fondamentale di linee guida su come usare Internet per assicurarsi di mantenere il maggior potere possibile per il tempo più lungo possibile.

Il miglior modo per conseguire questo obiettivo è quello di non permettere mai che la vostra autorità venga contestata. Questa guida vi accompagnerà nel processo di annullamento della dissidenza politica. Se fate in modo che chiunque sia d'accordo con voi, o che chiunque creda che tutti sono d'accordo con voi, la vostra permanenza al vertice dello Stato sarà lunga e prospera.

Poiché esiste un'incredibile varietà di regimi non democratici, alcune delle raccomandazioni qui presentate saranno di maggiore pertinenza per alcuni dittatori che per altri, a seconda di una lunga lista di fattori relativi allo Stato che voi governate. In generale, gli Stati con tassi di crescita economica più elevati comportano scelte più semplici [58]. Questa guida tenterà di trattare l'argomento in maniera più estesa possibile, ma tende in primo luogo e soprattutto ad offrire consigli di natura generale.

I valori autoritari sono sotto attacco in ogni parte del mondo, e i dittatori usano solo una frazione delle potenzialità di Internet per quanto riguarda il controllo della loro popolazione.

Questo può essere attribuito in parte all'efficacia delle tecniche repressive tradizionali, alla falsa credenza che la tecnologia abbia insite delle caratteristiche democratiche, o alla mancanza di interesse nello sviluppo di una forte cultura tecnologica. I leader degli Stati non democratici hanno bisogno di cambiare il loro punto di vista e adattarsi meglio a questo nuovo panorama traboccante di opportunità.

Come vedrete, alcune di queste opportunità non sono prive di rischi, ma le ricompense per la loro adozione sono immense, e le possibilità quasi infinite.

Contrariamente alle credenze popolari, lo sviluppo tecnologico non si traduce automaticamente in istituzioni democratiche. Molti paesi autoritari che hanno sperimentato livelli costanti o rapidi di diffusione di informatica e telecomunicazioni sono felicemente rimasti autoritari: per esempio il Brunei, l'Eritrea, il Gambia, l'Iran, il Giordano, il Marocco, l'Oman, la Russia ed altri [59]. Questa guida ambisce a distillare esperienze comuni e pratiche utili al fine di emulare il successo che alcuni di questi stati hanno conseguito.

2. Condizioni essenziali: tre libertà

al fine di ottenere da Internet il massimo beneficio, dovete assolutamente soddisfare tre prerequisiti. Come potrete vedere nel prossimo capitolo essi sono essenziali per disinnescare con successo l'anonimato e la sicurezza, le maggiori minacce per voi. Queste libertà vi permetteranno di esercitare i meccanismi di controllo con efficace sicurezza e spesso ad un costo relativamente basso. Ci sono innegabili vantaggi (economici, politici e sociali) e molti benefici collaterali associati ad una implementazione riuscita delle raccomandazioni seguenti, ed è vitale per il vostro dominio dispotico prendere questi prerequisiti molto sul serio.

2.1 Libertà dal disordine politico

in primo luogo, il paese che governate deve essere in qualche modo politicamente stabile. È ovvio che "stabile" può essere definito in maniera diversa in diversi contesti. È essenziale che almeno negli anni più recenti non si siano viste troppe dimostrazioni, proteste che mettono in discussione la vostra legittimità, agitazione, dissidenza politica, eccetera. Se è questo il caso, tentare di sfruttare Internet a vostro vantaggio può rapidamente rivolgersi a vostro svantaggio, specialmente se non potete fidarvi interamente dei vostri compagni di partito (questo è collegato alla condizione #3). Se necessitate di ispirazione, esistono molti esempi di stati guidati da un singolo individuo e relativamente stabili: per esempio la Cuba di Fidel castro. Castro ha regnato con successo sul paese per decenni, proteggendo con efficacia il suo popolo dai controrivoluzionari. Ha nominato suo fratello comandante in capo dell'esercito di Cuba ed ha gestito il suo regime usando elaborate tecniche di sorveglianza e stretti meccanismi di dissuasione contro i nemici dello Stato [49]. Come è normale, potrà accadere che si verifichino degli incidenti politici che metteranno alla prova la resilienza del vostro regime (come nel caso di Cuba l'invasione della Baia dei Porci o la crisi dei missili), ma perfino stati molto grandi sono riusciti a funzionare stabilmente secondo un modello a partito unico e si sono adattati meravigliosamente all'era digitale - nonostante ad esempio, nel caso della Cina, circa 87.000 episodi di protesta nel 2005 [2]. Seguite l'esempio di questi Stati e cercate la stabilità, di qualsiasi tipo sia il vostro regime. Senza di essa, state mettendo in forse i due prerequisiti successivi, e state rendendo nulle le vostre possibilità di governare con Internet al vostro fianco. Se vi trovate nel corso di

una trasformazione politica importante, siete impegnati a dare la caccia a dissidenti controrivoluzionari o mandare i vostri militari nelle strade per educare i dimostranti, avrete bisogno in primo luogo di domare questi fuochi e solo in seguito tornare a questa guida.

2.2 Libertà dalle infrastrutture di telecomunicazione decentralizzate

La maggior parte dei paesi possiedono già, almeno fino a un certo punto, le infrastrutture per supportare Internet. A prescindere dal livello delle infrastrutture, dovete porvi alcune domande importanti: chi possiede i cavi in fibra ottica che attraversano il vostro paese? Dove si trovano i vostri datacenter più importanti? Quanto sono sicuri (sia fisicamente che digitalmente)? Esistono degli hub principali di controllo del traffico? Chi possiede questi hub? Il vostro governo ha a disposizione abbastanza professionisti addestrati per far funzionare questa infrastruttura?

Le risposte a queste domande sono utili per valutare se andare avanti o meno con l'implementazione delle strategie di questa guida. Dovete avere o potere esecutivo diretto oppure un'influenza preponderante su tutti gli elementi della catena dei servizi Internet, inclusi gli hub connessi ad altri Paesi, i cavi all'interno del vostro Paese, gli hubs di traffico domestico, gli ISP e le compagnie correlate.

Dovete essere in posizione tale da staccare la spina se necessario, e da poter azzerare i cyberspazi (siti web, parole chiave, ricerche, server) facilmente come gli spazi fisici (una località, una provincia, una compagnia). Appena poche ore prima dell'inizio dei sondaggi per le elezioni del 2009 in Iran, "la rete SMS venne oscurata, [...] I siti chiave dell'opposizione andarono off line. Il governo iniziò a disturbare le frequenze delle trasmissioni satellitari in linguaggio farsi della BBC e anche della Voice Of America." [53] Dover negoziare con il proprietario di una rete per ottenere certi favori non è un'opzione. Voi siete il mainframe e tutti i processi secondari obbediscono ai vostri comandi.

Fortunatamente in alcuni casi sarà difficile avere controllo perfetto di tutte le infrastrutture a causa dei diversi fattori (diversi fornitori di telecomunicazioni, eredità politica e strutturale di regimi passati). La Russia e la Cina, che rappresentano enormi aree geografiche, fronteggiano questa difficoltà. Anche loro hanno adottato approcci diversi, e ciononostante questi due Paesi sono riusciti a mettere insieme una convincente quota di proprietà fisica con un sistema legislativo forte e una pesante supervisione governativa negli affari digitale. Comunque lo facciate, assicuratevi di avere sempre l'interruttore di Internet vicino alla punta delle vostre dita.

2.3 Libertà dai rappresentanti eletti democraticamente

Chiunque sia responsabile della regolazione sul come, cosa e quando del servizio Internet per i cittadini, che sia un ministro degli affari interni, un ministro

della pubblica sicurezza o un funzionario nominato appositamente per gli affari digitali, assicuratevi di potervi fidare di questa persona come nessun altro. In uno scenario ideale, nominate per questo incarico un membro della vostra famiglia o un vecchio amico che morirebbe piuttosto che voltarvi le spalle. La stessa regola si applica a chiunque gestisca i fornitori di servizi Internet (ISP) nel paese, perché dovrà lavorare quotidianamente sugli affari digitali con il funzionario nominato da voi. Assicuratevi che queste persone siano affidabili e leali, concedetegli tutte le risorse di cui hanno bisogno, ed assicuratevi di estirpare ogni dissidenza, corruzione interna o altre fonti potenziali attrito con queste organizzazioni. Come sostiene Philip N. Howard, la defezione da parte delle elite di solito segna la fine di un regime autoritario.[50] Assicuratevi che questo regime non sia il vostro.

Assieme al comando del vostro esercito, questa è certamente una delle ultime aree di controllo che vorrete cedere. Molti ISP, per ragioni storiche, si sono sviluppati a partire da fornitori di telefonia (spesso, adattare le infrastrutture telefoniche ad infrastrutture Internet non è un grosso problema), che sono spesso aziende fondate e controllate dallo Stato. Quindi sono una linea diretta con ciò che la vostra popolazione sa, come vengono a saperlo, dove vanno per ottenere informazioni e come si organizzano. Mantenere una salda presa sugli ISP e e sui fornitori di telecomunicazioni è fondamentale per il vostro successo, poiché la storia ci ha insegnato che essere i detentori di un grosso e violento randello può funzionare bene, ma essere il guardiano della coscienza collettiva di solito è un male molto più sostenibile.

Se non siete in condizione di soddisfare questi prerequisiti...

La via che è più saggio seguire è quella di bandire il libero accesso ad Internet più aggressivamente possibile, e stare semplicemente fuori dalla rete come sta facendo correntemente la Corea del Nord [5]. Comunque, è importante adattarsi rapidamente a questa nuova realtà e mettere in opera i cambiamenti necessari per realizzare questi requisiti. Anche la Corea del Nord alla fine dovrà aprirsi. La sua ossessione di rimanere nel XX secolo non può durare indefinitamente, mentre il resto del mondo dispotico marcia in avanti verso la vittoria tecnologica.

3. Creare condizioni di sorveglianza ottimali

ci sono due cose che semplicemente non sono compatibili col regime che gestite: gli strumenti per l'anonimato e gli strumenti per la criptazione dei dati. Con gli strumenti per l'anonimato, potete forse controllare e monitorare l'attività di Internet, ma non potete correlare queste attività ad un determinato individuo. L'anonimato perciò fa evaporare la responsabilità. Con gli strumenti per la criptazione dei dati, non potete nemmeno vedere o capire i dati che viaggiano lungo i cavi Internet che voi controllate, poiché sono alterati in maniera specifica per evitare di essere riconoscibili. La proliferazione di dissidenza politica on-line, negli Stati non democratici, di solito dipende dalla disponibilità degli strumenti per l'anonimato e per la criptazione dei dati. Se non potete smantellare con efficacia l'uso di questi strumenti, spesso è questione di (poco) tempo prima che l'opposizione politica si organizzi contro di voi.

3.1 sopprimere l'anonimato (chi)

3.1.1 I proxy

È cruciale capire come funzionano gli strumenti per l'anonimato e per la criptazione, al fine di accertarvi che non raggiungono mai i vostri cittadini. Ci sono numerose applicazioni che possono rendere un utente anonimo quando è connesso ad Internet, ma il loro funzionamento è per lo più simile. I proxy Internet costituiscono la minaccia maggiore in quest'area, e verranno trattati in questa sezione, con particolare attenzione per un progetto chiamato "Tor".

È un compito semplice collegare le attività di un individuo al suo account sul suo ISP [nota 1]. Ma se questo individuo vuole connettersi in maniera anonima ad un sito senza il vostro onorevole consenso, può chiedere ad un altro computer di farlo per lui - mascherando la sua identità. Questo server intermedio è chiamato un proxy, perché permette alle persone di connettersi ad un computer intermedio per mantenere il loro anonimato. Questo computer intermedio trasmetterà le informazioni richieste e le rispedirà indietro come un messaggero. Recuperare documenti attraverso un proxy e un'attività popolare nei circoli dissidenti perché permette loro di funzionare sotto il vostro attento radar.

Cosa si può fare contro tali vili tecniche di aggiramento? In primo luogo, i buoni proxy cadono spesso vittime della loro stessa popolarità. Se un proxy è efficace, apparirà un picco evidente nel traffico di un computer sconosciuto, sul quale si dovrebbe investigare prontamente. State in guardia contro tali picchi e aggiungete ogni nuovo proxy alla vostra lista nera. In secondo luogo, create i vostri server proxy! La maggior parte delle persone che si collegano ai proxy non sono tecnologi, ma semplicemente vogliono accedere a risorse che per loro sono proibite. Molti danno per scontato che i proxy possano essere solo il prodotto di una mente "libera", "democratica", e suppongono di non essere monitorati. Lasciate che il vostro proxy gestito dallo Stato passi attraverso i filtri e raccolga tutte le informazioni su coloro che se ne avvantaggiano. Poi abbattetevi su di loro (per allora ne avrete ottenuto gli indirizzi fisici) e fate della cosa un caso pubblico importante. Fate in modo che i vostri cittadini sappiano che siete esperti di tecnologia e che state impostando i vostri server proxy, cosa che dovrebbe scoraggiarli dall'usarli mai più.

3.1.2 Il progetto Tor

una seconda minaccia da cui guardarsi, più recente e più pericolosa, è chiamata "Tor". Tor è un dispositivo composto da una vasta rete di nodi gestiti dagli utenti - che essenzialmente fungono da proxy - e da un software apposito costruito per avvantaggiarsi di questa rete. Il modo in cui Tor si distingue da un normale proxy è piuttosto semplice. Tor è più o meno una vasta rete di molti proxy intelligenti che possono comunicare fra di loro. Tor rende possibili collegamenti proxy multipli fra questi "relays", ognuno dei quali trasporta solo una parte dei dati che devono tornare indietro. Questo rende molto più complicato individuare chi stia richiedendo cosa, poiché nessun singolo nodo sulla rete mostrerà grossi picchi di traffico e ciascun nodo è a conoscenza solo dei suoi collegamenti e di nessuno degli altri. Inoltre, i nodi Tor possono essere aggiunti o eliminati dalla rete rapidamente, a differenza dei proxy monolitici.

La sofisticatezza di Tor ha reso nervosi molti colleghi dittatori negli ultimi anni (e non senza ragione), ma non c'è bisogno di agitarsi. Ancora una volta, ci sono soluzioni per gestire questo problema. In primo luogo, assicuratevi di filtrare, bandire, rimuovere, cancellare qualsiasi riferimento a Tor sulla vostra rete. Questo è il primo passo, ed è il più importante per garantire che Tor sia semplicemente invisibile alla vostra popolazione. Secondo le statistiche di Tor, nessun paese autoritario, a parte l'Iran, ha una base di utenti significativa [23]. Premesso che questa soluzione non è esattamente una "soluzione" ma semplicemente una precauzione, dovete prepararvi a combattere il fuoco con il fuoco se Tor entra nel vostro paese. Poiché Tor è decentralizzato e fa affidamento su volontari sconosciuti per espandere la sua rete, dovreste creare i vostri nodi Tor, ed analizzare cautamente il traffico che scorre attraverso essi. Mobilitate il vostro cyber-esercito e assoldate nuovi combattenti digitali più rapidamente possibile. Secondo il progetto, Tor ha lo scopo di proteggere il trasporto di dati all'interno della sua rete, ma non sarà mai in grado di controllare i punti di ingresso e di uscita di questi dati [nota 2]. Focalizzatevi su queste due aree

per raccogliere dati [nota 3]; facendo questo, potreste imparare abbastanza da identificare con precisione chi sta facendo cosa [24]. Infine, imparate di più sul progetto: come funziona, chi contribuisce, quali sono i suoi meccanismi interni. È gratuito ed open source, e questo significa che qualunque dei vostri abili programmatori può capire come funziona.

Infine una cosa più generale e forse più importante da ricordare: mentre queste tecniche possono dare l'impressione di richiedere investimenti pesanti di tempo ed energia, vi permetteranno di mantenere un innegabile vantaggio col creare complicazioni, introdurre nuovi passi procedurali ed imporre questo carico sugli utenti di proxy e Tor per accedere anonimamente a semplici risorse. Tor è nato dalla necessità di proteggere la privacy degli utenti, ed ha rappresentato un grosso passo in avanti in questo campo, ma ha anche aggiunto un nuovo livello di complessità per i non tecnologi che vogliono usare Internet in maniera anonima. Nel corso del tempo, è stato necessario aggiungere a Tor molte estensioni necessarie per soddisfare necessità particolari [nota 4]. Man mano che combattete queste iniziative, gli strumenti diventano sempre più complessi da usare, cosa che, alla fine dei conti, scoraggerà l'utente medio che potrebbe semplicemente desiderare di dare un'occhiata a del materiale vagamente sensibile.

3.2 Sopprimere la sicurezza (cosa)

Probabilmente un problema più serio dell'anonimato è la criptazione dei dati, poiché potete vedere che qualcuno sta richiedendo "qualcosa", ma non potete determinare cosa. Dall'altro lato, è un problema più semplice da risolvere. Ci sono molti tipi di traffico su Internet, incluso il peer to peer, l'HTTP, le VPN, l'FTP, la posta elettronica, eccetera. Ognuno usa un diverso protocollo per comunicare dati, e tutti possiedono diversi livelli di sicurezza nel trasportare questi dati. Per esempio le VPN (reti private virtuali) sono progettate in maniera specifica per criptare i dati, l'HTTP può contare sull'HTTPS per la criptazione, e così via.

Bandite o disabitate ogni forma di contenuto criptato. Questa include certamente le VPN ed altre tecnologie di tunneling. Semplicemente non potete permettervi di essere ciechi a ciò che i vostri cittadini stanno facendo in rete. L'Iran ha agito con saggezza su questo fronte, bloccando efficacemente il traffico https nel febbraio 2012.[25] Ogni qualvolta è possibile, prendete gli utenti di sorpresa e monitorate il loro comportamento, dandogli allo stesso tempo la sensazione di essere al sicuro. Per esempio, esistono dei sistemi per violare il protocollo https mentre gli utenti stanno semplicemente controllando la loro posta elettronica o trasmettendo informazioni di login a vari siti (banche, reti sociali). [nota 5] Avere accesso alla loro posta elettronica, ai loro account sulle reti sociali o sui servizi di home banking estende le vostre possibilità ad ovunque la vostra immaginazione vi porti. Inoltre, costringete i costruttori di apparecchi elettronici e le compagnie che fabbricano hardware ad includere degli accessi "back-door" nei componenti per computer, in modo da poterli

violare quando ne avete bisogno. La prossima raccomandazione esprime questa strategia in maniera più dettagliata.

Ricordatevi, lo scopo non è quello di bloccare tutti i protocolli usati per la trasmissione di informazioni su Internet. L'ideale invece è di bloccarne solo una minoranza scelta, e permettere a tutti gli altri di badare ai loro affari usando connessioni in chiaro.

3.3 Offrire servizi gestiti da voi

Nel caso di un regime più totalitario, si raccomanda la tecnica dell'offrire i vostri servizi. Questa richiede un controllo solido dei canali di distribuzione on-line ed una interferenza pesante sulla Rete, ma vi dà in cambio una supervisione quasi perfetta sulle attività dei vostri cittadini. In collaborazione con gli sviluppatori di hardware e software, imponete un accesso "back door" esclusivo al computer venduti nel vostro paese (tema trattato nel prossimo capitolo), e create del software su misura per le vostre necessità. Per esempio, un browser Web che rispetta la vostra lista nera di URL, un antivirus che rileva le minacce digitali (per esempio browser Web non autorizzati), o un client di posta elettronica che analizza i testi mentre spedisce o riceve e-mail. Questa strategia include anche il distribuire software come Tor attraverso canali non ufficiali (il sito Web originale deve essere bloccato), aggiungendo al pacchetto del codice maligno, permettendovi così di monitorare le persone e le loro attività. Dovreste anche creare un sistema operativo nazionale, che viene preinstallato su ogni personal computer, eliminando probabilmente la necessità di creare pacchetti software particolari. Naturalmente questo sistema operativo potrebbe inviare rapporti dettagliati sull'uso o sulle attività illecite, e raccolte di altre informazioni utili, al vostro ente centrale di sorveglianza.

Una volta che sapete chi fa cosa...

Non dovrebbero esserci più segreti per voi. Con il potere politico completo ed abbastanza risorse umane, potete monitorare tutti i dati che passano per i vostri cavi Internet e gestire quello che le persone vedono e fanno senza fatica. Come ha fatto l'Iran, costruite un semplice punto di passaggio obbligato sulla vostra rete Internet e mettete in atto una ispezione profonda dei pacchetti su tutto il traffico che ci passa attraverso [55]. Il prossimo capitolo della guida si occupa di "tattiche variabili" per controllare con efficacia la vostra popolazione nell'uso di Internet, dopo che avete sconfitto l'anonimato e la sicurezza. Ma in primo luogo, una discussione sull'imbrigliare tutte le capacità dell'industria privata vi spiegherà come una forte e docile industria tecnologica può assistervi ulteriormente nella vostra battaglia contro l'anonimato e la sicurezza, ed allo stesso tempo permettervi di delegare molto del vostro lavoro al settore privato.

3.4 Imbrigliare l'innovazione nel settore privato

È possibile isolare completamente il vostro Paese da tutta la nuova tecnologia ed essere rigidi senza compromessi nella vostra strategia di controllo - in questo

caso, ancora una volta, l'esempio guida è la Corea del Nord. Comunque, non raccomandiamo questo approccio a meno che non siate mettendo insieme i blocchi di costruzione per la vostra Internet futura. Una tale strategia diventerà meno efficace nel tempo, per poi fallire. Al confine nord della Corea con la Cina, il segnale dei cellulari può essere usato per comunicare con dispositivi portatili. Man mano che la tecnologia migliora e migliorano i dispositivi capaci di condividere il segnale wireless, questo potrà solo peggiorare. Sono stati catturati coreani del Nord che contrabbandavano audiocassette della Corea del sud e altri beni attraverso il confine,[6] ed è solo questione di tempo prima che queste crepe si allarghino abbastanza perché la gente voglia conoscere la verità di cui sono stati tenuti all'oscuro.

A seconda delle dimensioni e della potenza del vostro regime, è possibile sviluppare un'infrastruttura Internet allo stato dell'arte come servizio per i vostri cittadini, e tuttavia filtrare pesantemente i dati che scorrono attraverso di essa, come viene fatto in alcune repubbliche islamiche e in alcune monarchie costituzionali islamiche.[61] Molti di questi regimi non si preoccupano di frenare lo sviluppo economico in cambio di capitale culturale, ma non tutti gli Stati sono ricchi di petrolio come l'Arabia Saudita, per la quale tali investimenti sono insignificanti. Tuttavia, è anche possibile coltivare una fiorente industria privata della tecnologia e tenere invece le compagnie strettamente al guinzaglio, come ha fatto Singapore.[62]

3.4.1 L'industria privata

Questo può non essere ovvio per molti dittatori che gestiscono Stati comunisti o socialisti a partito unico, ma una fiorente industria privata può fornire strumenti di valore incalcolabile per aiutare ad implementare un'Internet controllabile. La ragione è piuttosto semplice: le tecnologie che trasformano le applicazioni Internet in esperienze più personalizzate, efficienti e gradevoli di solito sono le stesse che aumentano la capacità di monitorare i loro utenti. Se i cookies di Internet hanno risolto il problema dei servers senza stato, sono perfetti anche per tracciare gli utenti (e qualche volta perfino per violare i loro sistemi).[8] Anche se il protocollo fondamentale di Internet (TCP/IP) ignora ciò che trasporta e quale sia la sua destinazione nel mondo reale, dei programmatori intelligenti hanno rapidamente costruito degli strumenti che possono "rivestire" questo protocollo per fornire informazioni più dettagliate. Il risultato è un'esperienza molto più personalizzata (siti Web mostrati nella lingua dell'utente, la valuta locale quando si fanno acquisti on-line, i risultati delle ricerche personalizzati per adattarsi alle realtà locali, pubblicità personalizzate, eccetera) ma possiede anche una impressionante capacità potenziale di tracciare quali dati stanno viaggiando, quando e dove.[67]

Le tecnologie di trattamento dei dati ci possono dare solo degli indirizzi IP (ciò che i computer usano per comunicare fra di loro), che però corrispondono a un particolare computer (o una rete di computer), non ad una persona o una localizzazione fisica affidabile. Ma se avete completato il prerequisito #3, questo non è più un problema. La chiave, qui, è avere il controllo completo dei

vostri ISP, poiché sono loro che attribuiscono ai diversi abbonati (clienti) i loro indirizzi IP. Come dimostrato in precedenza (nota 1) è un gioco da ragazzi far corrispondere l'identità del titolare di un account legato ad un indirizzo IP con la sua attività on-line.

Ancora una volta, rendere più efficiente la vostra Internet attraverso l'innovazione del settore privato comporta vantaggi incredibili: 1) date una maggiore impressione di imparzialità, cioè di non stare interferendo nello sviluppo di tecnologie importanti correlate alla privacy; 2) queste innovazioni vi forniscono un potente arsenale di strumenti di sorveglianza; 3) fornite ai vostri cittadini un'esperienza Internet più ricca e più gradevole; e 4) ottenete dei vantaggi economici significativi creando una nuova industria dei servizi. Come direbbe Lawrence Lessig, "questi cambiamenti [al design di Internet] non vengono architettati dai governi. Piuttosto vengono richiesti dagli utenti e forniti dal commercio. [...] Ancora una volta, il commercio è venuto in soccorso della regolazione."[9]

I vantaggi ottenibili da un'industria tecnologica in espansione adesso dovrebbero essere più chiari. Se l'industria cresce troppo rapidamente, usate i vostri muscoli del controllo. Massaggiate con attenzione vostri interessi nell'ecosistema industriale con tutti i mezzi a vostra disposizione. Le tecniche morbide - come sovvenzionare le compagnie e i nuovi sviluppi che permettono una sorveglianza o un tracciamento migliore (mettendo la concorrenza in condizione di non competere), oppure creare leggi che favoriscono queste stesse compagnie (bonus fiscali, privilegi speciali, eccetera) - sono spesso facili da implementare. Potete anche costringere determinati produttori a includere meccanismi di sorveglianza, come si è scoperto che faceva il governo tedesco nel 2011 con il suo "staatstrojaner", un virus per computer rilasciato per controllare gli "individui sospetti."[31] Negli anni 70 e 80, la Libia ha richiesto che ogni computer fosse registrato dal governo.[60] Inoltre, nel febbraio 2012, il Pakistan ha pubblicato una gara d'appalto "per lo sviluppo l'installazione e la gestione di un sistema a livello nazionale per il filtraggio ed il blocco degli URL ,"[44] chiedendo alle compagnie private di inviare le loro proposte. Valore totale del progetto: 10 milioni di dollari. Si preoccupavano dell'opinione pubblica o di nascondere le loro intenzioni? Apparentemente no - comprarono persino spazio pubblicitario sui giornali per reclamizzare il loro bando. Fate la stessa cosa: incoraggiate la crescita dell'industria della sorveglianza tramite prodotti consumer, e vantatevi con regolarità di quanto i vostri cittadini siano tecnologicamente avanzati. Le cosiddette tecnologie a "scatola nera" in questo momento stanno fiorendo, mentre diventa chiaro che gli utenti della tecnologia in tutto il mondo desiderano sacrificare la trasparenza per una migliore esperienza utente.

I vostri cittadini hanno bisogno di essere controllati, ma potete fare in modo che l'industria svolga per vostro conto molto del lavoro pesante. Invece di creare leggi draconiane che sicuramente risveglieranno le ire di alcuni cittadini, limitatevi ad incoraggiare un fabbricante di tecnologia per ottenere risultati simili. Gli esempi di ciò, da ogni parte del mondo, sono troppo numerosi per poterli elencare, poiché questa è stata una pratica standard fin dagli esordi di Intenet. Ogni aspetto della tecnologia è stato oggetto di questo tipo di

"trattamento selettivo preferenziale" da parte dei governi, inclusi una miriade di pacchetti software, routers, centri dati, imprese del settore della sicurezza, strumenti per la condivisione dei media e molto altro. Questa strategia è già stata sperimentata e verificata per decenni, da parte di ogni tipo di regime, fino ad oggi. E' una miniera d'oro per le pubbliche relazioni ed un piano di sorveglianza imbattibile.

3.4.2 Localhost

Secondo Facebook, ci sono più utenti del suo servizio ad Ottawa, la tranquilla capitale del Canada e patria di circa un milione di persone, che in tutta la Cina, un Paese di oltre un miliardo di abitanti.[10] Anche se questo può suonare improbabile, avrà senso per le persone che hanno familiarità con l'avversione della Cina per i servizi Internet sviluppati dai Paesi occidentali. Facebook è stato bandito nella Cina continentale (mentre è molto popolare ad Hong Kong) dal 2009 [11] ed il governo censura o condanna pesantemente gli altri (il sito cinese di Google, ad esempio, ora ridirige il traffico alla sua controparte di Hong Kong). La sua strategia è stata di proibire gli strumenti che sfidano la legittimità del governo, creando allo stesso tempo degli equivalenti nazionali per i cittadini ordinari. Il popolo cinese non può usare Google, ma hanno Baidu. Facebook è bandito, ma RenRen offre servizi simili. Twitter è introvabile, arriva Weibo. Tutti questi spinoffs non possono rivaleggiare da un punto di vista ingegneristico con le loro controparti originali; ma non importa, non ne hanno bisogno. Finché l'esperienza è sufficientemente vicina all'originale, non c'è molto da lamentarsi per gli utenti (tutti questi servizi sono gratuiti). Può sembrare un modo di sostituire un male con un altro, ma c'è una differenza fondamentale che è spesso invisibile all'utente: coloro che governano la Cina possono (e lo fanno) creare una legislazione che sostenga le loro dure politiche censorie, alla quale le compagnie cinesi devono adattarsi. Inoltre, i capi della Cina possono dormire molto più tranquillamente, sapendo che i dati Internet della loro enorme popolazione risiedono dentro i confini del Paese, e non da qualche parte vicino alle spiagge sabbiose della California, soggette alla legislazione americana.

Avvantaggiatevi del fatto che, spesso, i fornitori di servizi online sono goffi nell'adattarsi ai nuovi mercati globali. Sfruttate le differenze di religione, lingua ed abitudini locali per fornire loro un'esperienza personalizzata nel connettersi – sicuramente avranno più fiducia in questa, piuttosto che in un modello insapore progettato per le masse. Finché il sistema generale si basa su infrastrutture che voi controllate, ed è soggetto a leggi su cui avete potere, più gente usufruisce di sevizi Internet e sociali nazionali e meglio è. Uno dei sevizi email più popolari attualmente in Cina è Yahoo!, in parte perché fu fondato dall'imprenditore cinese Jerry Yang, ma anche perché ha firmato l'"Impegno pubblico per l'autodisciplina per l'industria Internet Cinese". A volte, non è nemmeno necessario clonare un servizio occidentale popolare perché le stesse compagnie faranno, una volta tanto, tutto il lavoro sporco per voi. Nella migliore delle

ipotesi, i servizi online dovrebbero servire come un altoparlante morbido per sostenere in maniera gentile la politica del governo.

Alla data di questo scritto, la Russia, un campione mondialmente riconosciuto nell'anestetizzare i suoi utenti Internet con "media da intrattenimento"[68] sta lottando contro una crisi politica che dipende in parte dall'uso di un sito web americano chiamato LiveJournal." Poiché "i suoi servers erano negli Stati Uniti nel periodo in cui il governo Russo imponeva un giro di vite sui media privati, è stato visto come una garanzia di libertà di parola".[34]

Le lezioni da imparare dalla Cina e dalla Russia sono importanti: lasciare che la gente chiacchieri sui servizi di microblogging e sulle reti sociali è innocuo, se voi controllate queste reti e monitorate il loro contenuto. Meglio ancora, fate che questi servizi dipendano da risorse del governo, avvicinandovi di un ulteriore passo ai dati dei loro utenti.

3.4.3 Strumenti ed intenzioni

Nell'estate del 2010, si è tenuta a NYC la Conferenza degli Hackers sul Pianeta Terra (Hackers On Planet Earth, HOPE), con Julian Assange – il fondatore di Wikileaks, un sito Web che permette agli informatori di pubblicare documenti segreti – in lista per l'intervento principale. Questo succedeva appena due mesi dopo che Wikileaks aveva rilasciato il video "Omicidio Collaterale" che mostrava soldati americani che sparavano contro giornalisti a Baghdad, e poco prima che centinaia di migliaia di altri documenti di guerra trapelassero (il Diario di Guerra Afgano ed i Log della Guerra Irachena). Assange non si è mostrato per il discorso, probabilmente per ragioni di sicurezza, perché la copertura dell'evento da parte dei media mondiali era al massimo. Al suo posto, il ricercatore nel campo della sicurezza Jacob Appelbaum è salito sul podio per un discorso sulla sicurezza, l'anonimato ed il progetto che lo teneva occupato al momento, Tor. Come già detto, Tor "permette di difendersi contro una forma di sorveglianza in rete che minaccia la libertà personale e la privacy".[13] Naturalmente, la sicurezza ai massimi livelli gioca un ruolo fondamentale per Wikileaks – almeno, se vuole proteggere le sue fonti. Tor guadagnò in conseguenza molta pubblicità, ed il lavoro di Appelbaum certamente fece di lui una persona in evidenza negli Stati Uniti. I suoi aggiornamenti su Twitter testimoniano le difficoltà che la polizia di confine e doganale gli ha creato quando entrava nel Paese o lo lasciava, come per esempio confiscargli l'equipaggiamento o sottoporlo a numerosi interrogatori. Uno stato tweetato da lui il 19 gennaio 2011 dice: "Spero in un futuro in cui non sarò in una lista segreta di sorveglianza, perquisizione, vessazione, detenzione, interrogazione, ostacolamento, infastidimento e stress [12]". Il governo americano stava puntando ogni arma a sua disposizione contro Appelbaum. Ovviamente qualcuno che lavorava duramente per rendere anonime le identità degli informatori (che in questo caso rilasciavano dati che erano molto imbarazzanti per il governo) doveva essere sorvegliato con cura.

Durante i pochi mesi successivi abbiamo assistito allo scontento delle popolazioni dell'Africa centro-orientale e settentrionale, che chiedevano stati più

democratici e domandavano ai loro leaders di cedere quote di potere o semplicemente di farsi da parte. Queste richieste sono germogliate da un misto di processi lenti (politicizzazione, per nominarne uno), insoddisfazione accumulata (per le limitazioni costanti alla libertà di parola, per esempio) e momenti intensi (l'immolazione di Mohamed Bouazizi in Tunisia, per esempio). Qui non approfondirò l'argomento di questi elementi catalizzatori (più in là discuterò come (de)politicizzare la vostra popolazione), ma è importante considerare come la tecnologia di Internet possa aver contribuito ad organizzare, sincronizzare ed informare queste popolazioni sul loro regime, gli eventi locali in corso, e così via. Perfino in paesi come l'Iran, l'Egitto e l'Arabia Saudita, dove la censura è rapida e spietata, le popolazioni hanno imparato ad evitare alcuni filtri governativi ed a conservare l'anonimato, grazie a software come Tor! Il discorso fondamentale di Hillary Clinton nel 2010 sulla libertà in Internet ed il suo ruolo nella democraticizzazione echeggiava le richieste delle popolazioni di questi Stati: "La libertà di informazione sostiene la pace e la sicurezza che forniscono una base per il progresso globale. Abbiamo bisogno di mettere questi strumenti nelle mani delle persone in tutto il mondo, che li useranno per l'avanzamento della democrazia e dei diritti umani".[14] Si da' il caso, quindi, che lo stesso pacchetto software che il governo degli Stati Uniti condanna severamente per la sua capacità di rendere anonimi i suoi utenti potrebbe anche essere la pietra angolare di nuove rivoluzioni nei paesi non democratici.

Questa breve storia su Tor, Wikileaks e la politica estera americana dovrebbe servire come un racconto educativo per tutti i dittatori seri. Ha lo scopo di illustrare come le tecnologie, messe in un contesto diverso, possono rivelare poteri incredibili, capaci di attivare o disattivare la vostra strategia di controllo. Vi mostra anche che azzittire gli esperti che correntemente lavorano contro di voi non è sempre l'atteggiamento migliore. Rimodellando in modo creativo gli scopi degli strumenti prodotti dalla vostra industria tecnologica locale, potete nascondere le vostre vere intenzioni e controllare più efficacemente i vostri cittadini. Inoltre, valutate le vostre scelte con cura quando lavorate con hackers di talento ed ingegneri brillanti (che siano ideologicamente con voi o meno), perché potrebbero credere in determinati ideali (libertà di informazione, sicurezza, anonimato eccetera) che a volte si allineano con le politiche del vostro governo ed a volte no. Quando si sviluppano nuove tecnologie per minare il vostro regime, prendetevi il tempo necessario per decompilarle, analizzarle, e provate ad immaginarle per altri usi, in altri contesti, combinate con altri fattori (sui quali potete avere maggior controllo). Inoltre, le intenzioni del creatore sono in primo luogo politiche o tecnologiche? Con l'assistenza di ingegneri competenti, un atteggiamento di questo genere migliorerà enormemente sia il vostro attacco (l'implementazione di una strategia di controllo) che la vostra difesa (l'anticipare gli oppositori e liberarsi di loro).

4. La scelta di una strategia di controllo

4.1 Tattiche variabili

Sopprimendo l'anonimato e la sicurezza vi siete posti in una situazione invidiabile. Ora Internet è un libro aperto e trasparente. Il prossimo passo? Raccogliere più informazioni possibile: a cosa è interessata la vostra popolazione? Come stanno usando Internet? I cittadini stanno guardando in streaming serie TV brillanti per rilassarsi dopo una lunga giornata di lavoro forzato? Leggono le notizie su uno dei vostri siti web statali? Si impegnano in discussioni sulla storia della nazione sui forum online? Più probabilmente tutte queste cose, ma in quali proporzioni? Che rapporto c'è tra i consumi di banda in collegamenti nazionali ed internazionali? Chi sono i dissidenti nel vostro Paese e dove vivono? Chi sono i loro amici? Quale scuola hanno frequentato? A questo punto dovrebbe essere facile rispondere a queste domande.

4.1.1 Il dilemma del dittatore

Una volta che avete raccolto questi dati, la chiave è sviluppare una strategia di controllo su misura per le vostre particolari esigenze, adatta alle qualità specifiche del vostro regime corrente. Se gestite un regime più repressivo (come la Cina o l'Iran),[69] è necessario investire più energia nella propaganda. Spesso, questo riduce perfino la quantità di monitoraggio necessaria per sorvegliare i cittadini, poiché le voci dissidenti vengono annegate nel mare di chiacchiere digitali.

Qualsiasi sfumatura di controllo digitale decidiate andar bene per il vostro Paese, aderite alla strategia scelta ed applicatela a qualsiasi costo. Potreste essere costretti a scegliere tra benefici economici e rischio politico. Un approccio più liberale stimolerà la vostra economia con lo sviluppo di un'industria di servizi e del commercio online, ma aumenterà anche il rischio che la vostra popolazione sviluppi un maggior senso di autonomia politica.

In molti casi, una combinazione di diverse modalità di interferenza otterrà i risultati migliori. Una possibile configurazione comprende una ciber-polizia sofisticata che bandisca i contenuti selezionati rapidamente e con efficacia, una potente artiglieria propagandistica, una volontà politica forte di fare rispet-

tare le leggi ed un'industria privata brillante per produrre strumenti per la centralizzazione che facilitino la sorveglianza.

E' importante notare che non abbiamo certamente elencato in maniera esaustiva tutte le possibilità di controllo sul cyberspazio (i regimi non democratici si innovano in continuazione su questo fronte), e vi incoraggiamo a sperimentare nuove tecniche adatte alle vostre necessità per anticipare i tempi. Il numero delle opzioni a vostra disposizione di solito è proporzionale alla complessità di queste tecnologie, ed alla velocità con cui emergono e vengono sviluppate nell'industria privata.

4.1.2 Politicizzare e depoliticizzare

La prossima serie di raccomandazioni, purtroppo, non può essere offerta come un'insieme preimpostato di regole universali da seguire. Lo scopo è di aiutare il leader di un Paese a decidere se, e fino a che punto, i cittadini devono essere coinvolti nella vita politica, ed in quali casi. Tratterò brevemente le due possibilità principali che dovrebbero essere disponibili a seconda del tipo di regime non democratico che gestite: autoritario o totalitario. Per rimanere coerenti con le loro politiche correnti, i dittatori degli stati autoritari che solitamente permettono l'esistenza di istituzioni sociali ed economiche indipendenti (ad esempio Singapore), potrebbero preferire depoliticizzare pesantemente la loro popolazione; mentre l'approccio più olistico di un totalitarismo (la Russia stalinista o la Germania nazista per esempio) suggerirebbe che trasformare ogni cosa in un atto politico potrebbe essere una scelta più saggia. Inoltre, è importante ricordare che l'approccio totalitario sarà più difficile da realizzare con successo, perché richiede un controllo perfetto delle attività online dell'utente. Se vi trovate in questa situazione, sarebbe consigliabile migrare lentamente verso la depoliticizzazione della vostra popolazione, più sottile ed efficace nell'offuscare le coscienze.

Politicizzare o depoliticizzare una vasta utenza richiede tempo. Non si può realizzare nello spazio di una notte.

Quando lavorate allo scopo di instillare un'opinione collettiva in un vasto gruppo di persone, non ci sono soluzioni rapide ed è necessario fare piccoli passi incrementali per evitare false partenze. È anche importante sottolineare che se iniziate questo processo mentre le persone sono in strada a protestare e ad organizzarsi per mezzo delle reti sociali, siete destinati a fallire. Se siete arrivati a questo punto, sfortunatamente avete altri problemi da risolvere e dovreste o saltare direttamente all'ultima parte di questa guida, che tratta di controllo dei danni e di tattiche per i social media, oppure ricominciare daccapo. Come ha scritto Ethan Zuckerman, direttore del Centro per i Media Civici del Mit, nel suo popolare articolo su Internet "La prima rivoluzione di Twitter?", "Qualsiasi tentativo di attribuire un cambiamento politico importante ad un fattore singolo - tecnologico, economico o altro - è semplicemente una falsità. I tunisini si sono riversati nelle strade a causa di decenni di frustrazione, non in reazione ad un cablo pubblicato su Wikileaks, un attacco denial-of-service, o un aggiornamento su Facebook".[15]

Quando iniziate il processo di (de)politicizzazione, siete metodici e costruite il vostro capitale politico lentamente.

Strategia A: depoliticizzazione significa intrattenimento.

Nelle "Lettere" satiriche di Screwtape di C. S. Lewis, Screwtape, un demone anziano che lavora per il Diavolo, all'inizio spiega a suo nipote che "il problema del discutere è che sposta l'intera lotta sul terreno del Nemico. [...] Con l'atto stesso del discutere, risvegli la ragione della vittima; ed una volta che sia desta, chi può prevedere il risultato?" [16] Ciò che Screwtape sta essenzialmente suggerendo è di stare alla larga dalla polemica, dalla discussione e dal confronto. Il miglior modo per non risvegliare la mente di qualcuno è di distrarla ed assicurarsi che rimanga annebbiata.

Dovreste seguire questo esempio, dato che l'intrattenimento è probabilmente la migliore valvola di sfogo per pacificare una popolazione che vive sotto la vostra guida. Il libro di Lewis è un'altra lettura raccomandata, poiché descrive molte tattiche utili per la coercizione psicologica. A questo scopo, i mezzi di intrattenimento vi possono aiutare a conseguire i vostri obiettivi. Se gestite uno Stato autoritario e tollerate una sfera privata nella società, i talk-show, i siti Web di immagini buffe, i siti Web di video e le piattaforme di blogging possono essere degli alleati estremamente potenti. Perfino le piattaforme più "pericolose" come Wikipedia o i media sociali possono essere degli ipnotizzatori terribili, se censurate e gestite con cura. L'unica regola importante da seguire in questo contesto è di bloccare qualsiasi contenuto sensibile. Rendete gli argomenti sociali e politici non visibili o fateli apparire banali. Lo show di David Letterman è ok, i forum di discussione sulla vostra storia nazionale no. I documentari sulla conservazione della natura sono ok, quelli sulle condizioni di vita in altre nazioni no. La copertura degli eventi sportivi dovrebbe essere incoraggiata, si possono reclamizzare i libri di auto-aiuto e si può permettere che il gioco d'azzardo sia estremamente popolare, ma l'argomento della libertà di stampa non dovrebbe trovarsi da nessuna parte su Internet. In pratica, questo si traduce spesso nel bandire il contenuto nazionale nelle lingue locali e permettere il contenuto internazionale in inglese. Seguite l'esempio dell'Iran che attualmente censura più contenuto in lingua persiana che contenuto in lingua inglese. [64]

Mentre filtrate ed ispezionate i pacchetti Internet dei vostri cittadini (con l'aiuto dell'amico che avete nominato per gestire questi affari), disabitate e reprimete qualsiasi riferimento ad argomenti "caldi" ma assicuratevi di aprire i gateway allo scaricamento illegale di serie e show televisivi popolari. Mentre voi limitate le libertà, è importante che il vostro popolo sia capace di rilassarsi, ridere un po' e provare una gioia superficiale. Fornite loro abbastanza materiale di pettegolezzo per il giorno venturo. Bisogna trovare un equilibrio tra soppressione efficace e intrattenimento benigno. Senza tale equilibrio, rischiate di alimentare un sentimento di disperazione, che alla fine produrrà delle masse infuriate. Lasciare che i cittadini visitino i siti delle reti sociali, come viene fatto in Cina, significa che l'intrattenimento benigno occupa tempo e spazio

mentale che diversamente potrebbe essere usato da molti giovani per la riflessione critica, che può essere pericolosa per il vostro regime. Lasciateli flirtare sulle reti sociali, lasciateli discutere l'uscita della notte precedente, lasciateli postare frequentemente le loro foto, lasciate che mandino link a video buffi l'uno all'altro via e-mail. Date ai contestatori la sensazione di essere liberi di esprimersi quanto desiderano, perché non c'è niente di pericoloso in una popolazione narcisista e assorbita in se stessa. È poco probabile che gente di questo genere scateni una rivoluzione.

Indubbiamente, se gestite un regime autoritario più liberale, permettere ai media per l'intrattenimento di diffondersi sulla vostra Internet può essere una strategia di ottundimento efficace, senza parlare dei benefici economici(il suo costo è nullo se fate in modo che siano altri a produrre contenuti per voi). Nel loro studio recente "Oppio per le masse: come i media stranieri gratuiti possono stabilizzare regimi autoritari" Kern ed Hainmueller hanno dimostrato che "i media stranieri hanno effettivamente aiutato a stabilizzare uno dei regimi comunisti più oppressivi dell'Europa orientale, la Repubblica Democratica Tedesca". Le loro scoperte, per quanto poco intuitive, sono importanti. I tedeschi dell'est avevano accesso alla televisione occidentale che "offriva una via di fuga dall'opaca realtà socialista almeno per un paio di ore al giorno". Infatti, "i tedeschi dell'est che si sintonizzavano sulle televisioni della Germania occidentale divennero più e non meno soddisfatti del regime della Germania orientale. invece di stimolare la resistenza alla dittatura comunista, l'effetto narcotizzante della televisione servì a stabilizzare invece che a minare il regime comunista."[18] Apparentemente, il governo russo ha imparato molto da queste tecniche. Come sottolinea Morozov: "Dal punto di vista dei governi, è molto meglio tenere i giovani russi completamente lontani dalla politica, permettendo loro di consumare video divertenti sulla versione russa di YouTube, RuTube (di proprietà di Gazprom, il gigante statale dell'energia), o su Russia.ru, dove è ugualmente raro che siano esposti a messaggi ideologici. Molti russi sono felici di adattarsi, e non poco merito di questo va all'alta qualità di tali distrazioni on-line." [33]

Come dice Screwtape il Demone descrivendo i mortali, "Non essendo mai stato un umano, non puoi capire quanto siano schiavi della pressione dell'ordinario."[17]

Strategia B: politicizzare significa pressione costante.

In alternativa, potete scegliere la seconda opzione, cioè di trasformare ogni pensiero ed azione, comprese quelle su Internet, in atti politici. Questo approccio tipicamente va a braccetto con qualsiasi sfumatura di totalitarismo e suggerisce un controllo molto più stretto dell'attività su Internet. Essenzialmente, non dovete lasciare alcun margine d'errore e dovete cercare di distruggere in maniera compulsiva qualsiasi segno di discorsi contrari al regime. Usate Internet per trasformare ogni utente in un fanatico che eventualmente denuncerà per voi le persone con cui ha rapporti. Ogni informazione reperibile in formato digitale dovrebbe riferirsi in qualche maniera alla grandezza del regime, o altrimenti

essere filtrata. Assicuratevi di organizzare e promuovere discorsi nazionalisti nei forum, nei (micro)blog, nelle chat, nei notiziari, nei film gratuiti ed a pagamento, nei podcast, nella musica, nei siti di immagini e qualsiasi altra possibile applicazione basata sul TCP/IP. Per evitare di avere troppe persone che abbandonano ed ignorano la vostra Internet perché la giudicano troppo estrema, pubblicate on-line informazioni importanti per i cittadini, rendendo difficile farne a meno (per esempio, orari dei servizi pubblici, informazioni sui giorni nazionali di vacanza, discorsi nazionali importanti, stampa di buoni pasto, eccetera). Essenzialmente, dovete semplicemente trasporre le regole principali che governano il vostro regime nei loro equivalenti digitali. A prima vista questo può sembrare più semplice, in virtù del fatto che non dovete concepire una nuova strategia, ma ricordate che controllare il cyberspazio non è la stessa cosa che controllare lo spazio fisico. Se avete soddisfatto con attenzione i requisiti di questa guida, la vostra crociata digitale non dovrebbe essere troppo difficile. Dall'altro lato, se non controllate adeguatamente la vostra infrastruttura fisica e non avete accesso diretto ai dati grezzi di Internet tramite i politici sotto il vostro completo controllo, questo si può rivelare molto più rischioso che non usare la strategia A.

L'esempio più ovvio di un'implementazione di questo tipo sarebbe la politica Internet della Corea del Nord, che ha aderito a questi principi così seriamente, che effettivamente non sappiamo molto sulla loro misteriosa Internet interna - che è in realtà una intranet specifica della loro nazione. A proposito di questo argomento, Jonathan Zittrain ha detto che "In una situazione di questo genere, il trapelare di qualsiasi informazione dal mondo esterno potrebbe essere devastante, e l'accesso ad Internet per la cittadinanza dovrebbe essere così controllato da diventare inutile". [21] Secondo ogni apparenza, la Corea del Nord è riuscita a mettere insieme una strategia di controllo a tenuta stagna, e la ha adattata meticolosamente al suo spazio Internet. Sue Lloyd-Roberts, nelle sue corrispondenze della Corea del Nord e parlando del suo cyberspazio regolato, ha osservato che "alle persone comuni qui l'accesso ad Internet è proibito. Il caro Leader fornisce loro tutto ciò che hanno necessità di sapere".[22]

Sarebbe una menzogna affermare che questo approccio potrebbe essere sostenibile a lungo termine, poiché piccole crepe in un sistema di questo tipo - che sono molto difficili da evitare in un mondo completamente globalizzato - potrebbero essere catastrofiche. È un azzardo giocare su una strategia così ad alto rischio, ma vi può decisamente mantenere in pista per alcuni anni mentre preparate la transizione verso un modello simile alla strategia A.

4.2 Creare una casa di vetro: procedure ottimali

4.2.1 Usate i vostri simpatizzanti

Immaginate l'improbabile scenario in cui il vostro governo abbia problemi di popolarità. I vostri cittadini stanno lentamente diventando infelici, e si può percepire una viraggio nell'opinione pubblica. Questo scontento si manifesta

poi on-line in piccole esplosioni, e infine arrivate a rendervi conto che solo una minoranza crede ancora nella vostra autorità.

Se avete realizzato le tre condizioni essenziali di questa guida, potete dare la sensazione del controllo e del consenso. Usate la minoranza dei fanatici, fateli lavorare per voi. Assumendo che possiate influenzare la topologia dei siti Web nazionali più usati, create dei moduli on-line per denunciare traditori. Create campagne di consapevolezza per denunciare il comportamento "sospetto". Create gruppi di milizie on-line che pattugliano i forum su Internet, le chat room, gli spazi on-line ed altri angoli oscuri di Internet. Date loro un compenso ed incoraggiate queste spie volontarie, perché spesso riescono a raggiungere spazi on-line cui voi non avreste mai accesso. Cercate di scoprire immediatamente i membri scontenti dei partiti di opposizione (se c'è un'opposizione). Conducendo queste campagne pubbliche e creando delle schede on-line per la denuncia sui siti Web, la popolazione di Internet sa di essere sorvegliata non solo da voi, lo Stato, ma anche da chiunque altro.

Se cercate ispirazione, guardate l'Arabia Saudita dove "[i cittadini] stessi possono nominare parole e siti Web che vorrebbero fossero bloccati dal firewall governativo".[57]

4.2.2 Usate i vostri oppositori come esempio

In un documento pubblicato quest'anno, Pearce e Kendzior hanno dimostrato che "il governo [dell'Azerbaijan] ha dissuaso con successo gli utenti frequenti di Internet per sostenere la protesta che gli utenti medi di Internet dall'usare i media sociali per scopi politici".[46] L'atteggiamento del governo può essere riassunto come segue: "puniscono alcune persone e fanno in modo che tutti gli altri assistano. Cioè, 'Questo è ciò che può succedervi".[47] Il documento ha studiato l'attivismo sui media sociali tra il 2009 e il 2011, un periodo durante il quale è stato osservato che "gli utenti frequenti di Internet sono diventati significativamente meno disposti a sostenere le proteste contro il governo, indicando che le campagne governative contro l'attivismo on-line hanno avuto successo."[48] Sorprendentemente, durante gli stessi anni, è stato notato che gli utenti di Facebook aumentavano costantemente e che era in aumento in generale l'uso dei media sociali.

Gli Stati dell'ex Unione Sovietica possiedono un arsenale di trucchi da cui potete imparare; ma anche sul lato opposto del pianeta, intelligenti funzionari governativi hanno creato ricette brillanti per scoraggiare le attività "illegali" spaventando le loro popolazione. La prima decade del nuovo millennio è stata negli Stati Uniti un'enorme campo di battaglia per schermaglie legali, con l'industria musicale (schierata a difesa dei detentori di copyright) contro le compagnie tecnologiche, gli ISP e singoli individui. Questi ultimi sono stati spesso accusati sia di facilitare che di effettuare personalmente lo scaricamento illegale e la condivisione di file (solitamente musica o film). Entrambi gli schieramenti hanno vinto grandi battaglie e sofferto perdite pesanti lungo il cammino, ma il risultato di questa battaglia non è di grande interesse per lo scopo di questa guida. Invece, è indispensabile guardare le tattiche usate dalla RIAA (Record

Industry Association of America, Associazione Americana delle Industrie della Registrazione Musicale) per terrorizzare una popolazione scegliendo come bersaglio individui innocui e portandoli davanti a una corte. Per la fine del 2008, la RIAA aveva sporto almeno 30.000 denunce contro individui nella speranza di creare un potente deterrente per fare in modo che le persone ci pensassero due volte prima di condividere materiale coperto da copyright.[27] Il numero può sembrare elevato, ma considerando il numero di casi che sono stati abbandonati o risolti tramite accordi extragiudiziali, ed in paragone ai milioni di file trasferiti in peer to peer usando i siti di file sharing (gli indicizzatori di torrent, per esempio), in effetti questo numero costituisce una frazione molto ridotta. Ma lo scopo della RIAA e di altre grandi corporazioni non era quello di guadagnare denaro - per esempio chiedendo cifre come $ 80.000 o 2 milioni di dollari, come diverse corti hanno ordinato di pagare a Jammie Thomas-Rasset, una donna di trent'anni che guadagna $ 36.000 all'anno. Sanno che perseguire chiunque abbia condiviso almeno un file coperto da copyright non è solo irragionevole ma semplicemente impossibile, così cercano invece di spaventare gli utenti ordinari di Internet. La strategia non ha veramente funzionato bene, in gran parte perché la RIAA non è riuscita a provare maniera inequivocabile la colpevolezza degli accusati e costringerli a pagare completamente le cifre richieste. Alla fine perciò si è rivolta contro gli ISP, desiderando "collaborare" con loro per bloccare e filtrare i contenuti.[30]

Voi potete fare molto meglio di questo. Dando per scontato che nel vostro Paese ci sia una stretta integrazione della sfera politica e di quella giudiziaria, dovrebbe essere molto più facile fare di tali ridicole sentenze una realtà, proprio come nell'Azerbaijan. Un sondaggio successivo alle campagne della RIAA contro gli individui ha mostrato che oltre il 25% degli interrogati che ha smesso di scaricare musica l'ho fatto per la ragione seguente: "ho paura di mettermi nei guai/ ho sentito delle cause legali della RIAA".[30] Anche se questo sondaggio è stato eseguito su un piccolo campione, tuttavia permette di capire il livello di efficienza che può essere conseguito anche da una campagna piuttosto fallimentare. Immaginate se la grande maggioranza di quelle 30.000 cause si concretizzasse in indennizzi a sei cifre più alcuni anni di prigione. Non è difficile immaginare quel 25% saltare ad un 50%, ad un 75% o perfino di più. Considerate quanto segue: nel luglio 2009, "il parlamento iraniano ha iniziato a discutere una misura per aggiungere i siti Web ed i blog che promuovono 'la corruzione, la prostituzione e l'apostasia' alla lista dei crimini punibili con la morte."[56] Che ne pensate di questo come deterrente?

Dovreste trarre ispirazione dalla RIAA, dato specialmente il costo molto basso di queste spettacolari repressioni. I vostri soldati digitali probabilmente possono trovare al giorno 10.000 "criminali di Internet" colpevoli di pubblicare discorsi di odio. In tutti i tipi di Stati persone sono state arrestate, picchiate, detenute, mandate in prigione, se non incontro alla pena di morte (come Hossein Derakhshan nell'Iran) per crimini come "insultare i servizi di sicurezza", "violare le norme culturali" e "insultare l'Islam".[63] A volte non è stata data alcuna ragione ed alcuni di questi criminali rimarranno in prigione per molti anni per semplici commenti pubblicati on-line.[64]

Rendete questi casi pubblici, fateli personali. Trattateli in maniera tale che ogni cittadino possa facilmente immaginare se stesso al posto dello sfortunato poveraccio che è stato appena beccato a scrivere on-line un'affermazione politicamente ambigua. Inoltre, enfatizzate le implicazioni ideologiche e moralistiche: questi processi ed accuse dovrebbero avere pesanti sottintesi morali e servire come una lezione sul bene ed il male. Modellate il comportamento dei vostri cittadini usando dei raid sporadici come questi ed alla fine i vostri oppositori non saranno in grado di sopportare la pressione psicologica. Se questo riduce la quantità di dissidenza politica on-line del 50%, avrete la metà di dati pericolosi da trovare bandire e filtrare. Siate estremamente scrupolosi nelle tecniche con cui applicate le leggi. Se le usate assieme alla prima pratica (stimolare la cooperazione dei maggiori fanatici del vostro regime per aiutarvi a scoprire le mele marce), inevitabilmente fra i vostri utenti di Internet emergerà un comportamento di efficace auto-repressione.

4.2.3 Tattiche di controllo dei danni

Se le persone riescono a mantenere la sicurezza dell'anonimato, a condividere on-line materiale politicamente sensibile ed iniziare a richiedere un cambiamento, potreste avere fra le mani un problema serio. Questo è successo di recente in Tunisia, in Egitto ed in Iran. Spesso, il processo di (de)politicizzazione funzionerà come desiderato, ed in tal caso conseguirà un altro problema inevitabile: i cittadini iniziano ad organizzare la dissidenza usando i media sociali, poiché nessun equivalente del mondo reale arriva nemmeno vicino alla loro efficacia. Essere in questa situazione non è l'ideale, ma mentre vi ci trovate dovreste cercare di sfruttarla a vostro vantaggio. Se i vostri oppositori hanno fretta e dimenticano alcuni dettagli importanti, potete sfruttare la potenza e la portata dei media sociali per monitorare sorvegliare facilmente gli individui. Potete farvi avanti e soffocare il movimento con prontezza se necessario. I social media, come scoprirete, aprono certe porte che vi sono sempre state chiuse. Mentre i vostri cittadini stanno protestando con rabbia per le strade e si organizzano usando i social media, considerate quanto segue:

- Come citato nell'esempio precedente riguardante l'Azerbaijan, non è molto difficile frenare l'entusiasmo dei vostri attivisti mostrando loro quanto potete essere spietati anche per i reati più piccoli. Rendete evidente che mentre i social media possono essere tollerati, qualsiasi forma di dissidenza politica è completamente inaccettabile.

- Stimolare la rivoluzione è una cosa, rovesciare un governo è un'altra, e rimpiazzarlo con un nuovo governo è una cosa diversa ancora. Ci sono molti passi graduali che la maggior parte delle rivoluzioni devono compiere, ed i social media, lo strumento Internet favorito dei dissidenti, sono d'aiuto solo in due di questi passi - precisamente l'organizzazione e la chiamata a raccolta. I media sociali come strumento non sono molto efficaci per politicizzare un pubblico, e non vanno neanche molto bene per esercitare pressione sui politici o implementare una richiesta di cambiamento. Sono uno strumento efficace per diffondere l'informazione e a volte per organizzarsi in gruppi (anche se quando

una struttura è troppo orizzontale, i social media servono più a confondere che ad aiutare). "La tecnologia in sé e per sé non causa cambiamento politico - non l'ha fatto nel caso dell'Iran. Ma fornisce nuove capacità ed impone nuove limitazioni agli attori della scena politica. Le nuove tecnologie dell'informazione non rovesciano i dittatori, ma vengono usate per prendere i dittatori di sorpresa."[38]

- Non c'è da temere i social media per altre due ragioni. La prima è che, anche se potete assistere a numerosi attacchi ideologici contro il vostro regime da parte degli utenti dei social media, gli unici che importano sono quelli che vengono dall'interno del vostro paese. Anche se milioni di tweet vengono spediti dall'esterno del vostro paese dagli oppositori esiliati o dai loro sostenitori, che differenza fa, se vostri cittadini non li vedono mai? Questo aumenta la pressione sui vostri politici da parte dei leader di altri paesi, ma lo si può gestire con facilità con le tattiche della politica tradizionale. Concentratevi su quello che succede all'interno del vostro Paese: lì è dove l'attività dei social media dovrebbe essere sorvegliata attentamente. La seconda ragione è che i social media sono molte chiacchiere, ma poca azione. Pare che Tweeter e Facebook siano i posti di ritrovo migliori per i narcisisti disimpegnati, come hanno mostrato degli studi. [35][36] È piuttosto divertente esaminare i preferiti e l'elenco delle cause e dei gruppi sostenuti dell'utente medio di Facebook e confrontarli con il sostegno effettivo, economico o sul campo, che le stesse cause recente ricevono dall'utente. "Grazie alla sua granularità, l'attivismo digitale fornisce troppe facili vie d'uscita. Molte persone scelgono il sacrificio meno doloroso, decidendo di donare un penny dove potrebbero donare un dollaro."[37]

- Se decidete veramente di entrare in questa arena, siate preparati. Abbiate un esercito di guerrieri digitali imponente e in servizio 24 ore su 24. Non potete abbassare la guardia per un singolo attimo perché un assembramento spontanep on-line di oppositori può esplodere nel giro di minuti. Inoltre, siate pronti ad abbandonare le strategie che potreste aver usato nel passato. A questo punto avrete bisogno di osare, e la peggiore cosa che possiate fare è rivolgervi a vecchie strategie mediatiche per combattere problemi di natura diversa. Parlando della rivoluzione su Internet in Iran, Howard sostiene che "da alcuni punti di vista la risposta del regime è stata decisamente vecchio stile: espellere i corrispondenti stranieri, bloccare le linee telefoniche, evitare la pubblicazione dei quotidiani, e accusare i governi stranieri di diffondere disinformazione."[39] Con l'eccezione dell'ultima tattica, quella dell'incolpare (che è meno correlata ai media) queste strategie hanno un effetto molto modesto sulle crisi che viaggiano sui nuovi media.

4.2.4 Un'ipotesi di linea di comportamento

In pratica, ecco alcune cose che potete fare:

- Accusate gli altri regimi di stare tentando di creare agitazione. Simultaneamente, approfittate di questa opportunità per rinforzare il discorso nazionalistico e accusate specifiche compagnie straniere che comunque desideravate bandire dal vostro territorio.

- Assicuratevi di sottolineare gli stretti rapporti tra le agenzie governative americane ed i presidenti di diverse compagnie, e la loro tendenza a scambiarsi personale. Un esempio ridicolmente chiaro di questo potrebbe essere Regina Dugan, Direttrice del DARPA (Defense Advanced Research Projects Agency, l'Agenzia della Difesa per i Progetti di Ricerca Avanzata) che è entrata a lavorare alla società Google nel marzo 2012. Sottolineate il fatto che molti social media hanno una chiara vocazione politica. Nel febbraio 2012, Mark Zuckerberg, il presidente di Facebook, ha pubblicato una lettera per spiegare quali sono le posizioni di Facebook, poiché intendeva quotare Facebook in Borsa. La sua lettera di intenti dice: "Crediamo che costruire strumenti per aiutare le persone a condividere possa portare ad un dialogo più onesto e trasparente sui governi che potrebbe causare un coinvolgimento più diretto delle persone, ed una maggiore responsabilità per i funzionari pubblici[...]"[40] Questo mostra apertamente le intenzioni di Facebook di entrare nell'arena politica e dovrebbe essere denunciato come un'interferenza nei vostri affari nazionali.

- Non c'è niente di peggio che Facebook e Twitter senza restrizioni. Parallelamente, non c'è niente di meglio che Facebook e Twitter sotto il vostro controllo:

una volta che usano i social media per collegarsi fra di loro, avrete accesso ad una ricca messe di informazioni sui vostri oppositori. L'Iran si è avvantaggiato di questo durante le proteste che hanno seguito le elezioni del 2009, "mentre questo contenuto fluiva, il governo ispezionava strettamente il traffico digitale per cercare di identificare il leaders del movimento di rivolta sociale." In seguito, staccò persino la spina per 45 minuti allo scopo di inizializzare il suo "sistema di ispezione profonda dei pacchetti".[54] Spesso, queste informazioni sono perfino pubbliche. Se tali gruppi ed organizzazioni sono privati, usate semplicemente il potere che avete sugli ISP ed esercitate la vostra influenza per accedere a queste informazioni (questo il motivo per cui il prerequisito #3 è così importante). I benefici così ottenibili sono eccezionali, e comprendono, ma non si limitano a, quanto segue:

- I nomi e le informazioni di contatto dei leader della vostra opposizione
- La struttura interna dei gruppi degli attivisti
- informazioni riguardanti le risorse sia monetarie che di intelligence
- informazioni private come per esempio fotografie, indirizzi, numeri di telefono, e-mail, eccetera
- informazioni sulla loro personalità e profili (dove fanno shopping, cosa mangiano, eccetera).

Ovviamente, incrociando questi dati potete estrarne un'immagine molto accurata dei vostri oppositori e predire con facilità la loro prossima mossa. Potete anche usare questi dati per arrestare, incriminare e distruggere i vostri oppositori. Sfruttate i vostri ingegneri ed estraete l'immenso valore contenuto in questi dati grezzi, forniti dagli stessi servizi che starete accusando di creare agitazione e di intervenire nei vostri affari nazionale.

Avete una vasta schiera di strumenti a vostra disposizione: scaricate del software di riconoscimento facciale, che è gratuitamente disponibile on-line, e poi personalizzatelo per adattarsi alle vostre esigenze. I motori di ricerca delle

immagini vi permetteranno di trovare la fonte di determinate immagini. Ci sono perfino servizi cloud di violazione delle password WPA (che di solito è lo standard per i router domestici), come CloudCracker,[41] se avete necessità di entrare nelle reti locali private delle persone. Questi strumenti di solito sono gratuiti o molto economici, ma appena vi è possibile dovreste creare i vostri propri o appaltarene all'industria privata la creazione per conto vostro.

Sfruttate la potenza delle applicazioni di terze parti per raccogliere più dati possibile sulla vostra popolazione. Create applicazioni di terze parti che chiedono all'utente di connettersi con loro account sui social media (questo è molto comune), e di autorizzare l'accesso ai suoi dati. Per esempio, il sito Web per la Campagna 2012 di Barack Obama permette agli utenti di registrarsi usando Facebook, cosa che dà accesso a "nome, immagine del profilo, sesso, reti, ID utente, lista degli amici, e qualsiasi altra informazione che avete reso pubblica" [42] - un'autentica miniera d'oro. Per non parlare del fatto che questi permessi sono il minimo, ma la maggior parte degli utenti non si lamenterebbe se ne venissero richiesti degli altri. Sembrerebbe che Facebook abbia la responsabilità di proteggere i dati degli utenti, ma non è così. Una volta che un utente permette l'accesso dall'applicazione, chiunque può facilmente raccogliere ed immagazzinare qualsiasi cosa che rientri nei parametri di quei permessi. Forse tra questi il bene di maggior valore è la lista degli amici, alla quale dovreste prestare un'attenzione particolare quando state monitorando dissidenti. Non sembra che ci siano tentativi documentati di fare questo prima d'ora, ma qualsiasi dittatore intelligente, sotto pressione per un'ondata di contestazione sui social media, dovrebbe costruire l'applicazione mobile più efficace da usare per i dissidenti, e costringere a passare attraverso i social media per il processo di autenticazione. Tutto quello che avete mai desiderato di sapere a riguardo di ogni persona che rappresenta una minaccia per il vostro regime sarebbe a portata di mano.

- Se avete seguito passi precedenti, dovreste avere più dati disponibili sui vostri dissidenti di quanti non ne servano, per rendere inattivi ed arrestare i protagonisti di un movimento. Ricordatevi, i tweet non fanno una rivoluzione, ma le persone si.

Come Appelbaum ricordava mentre parlava sull'uso di telefoni cellulari per organizzare movimenti di protesta, "[in Iran], ti danno abbastanza corda per potertici impiccare"[43]

Assicuratevi di fare altrettanto.

Bibliografia

[0] The University Of North Carolina. Commentary and Analysis. Retrieved from http://www.unc.edu/depts/diplomat/archives_roll/2004_01-03/palmer_axis/palmer_axis.html

[1] TED. Rebecca MacKinnon: Let's take back the Internet!. Retrieved from http://www.ted.com/talks/rebecca_mackinnon_let_s_take_back_the_internet.html

[2] Washington Post. In Face of Rural Unrest, China Rolls Out Reforms.

Retrieved from:

http://www.washingtonpost.com/wp-dyn/content/article/2006/01/27/AR2006012701588.html

[5] The New York Times. The Internet Black Hole That Is North Korea.

Retrieved from http://www.nytimes.com/2006/10/23/technology/link.html

[6] BBC News. Life inside the North Korean bubble. Retrieved from http://news.bbc.co.uk/2/hi/programmes/newsnight/8701959.stm

[8] Sectheory. Clickjacking. Retrieved from http://www.sectheory.com/clickjacking.htm

[9] Lessig, L. (2006). Code V2. New York: Basic Books. p57.

[10] By using Facebook's ad creation platform (https://www.facebook.com/advertising/), it is possible to estimate the number of users in a geographical area.

[11] Jacobs, K. (2012). People's Pornography: Sex and Surveillance on

the Chinese Internet. Chicago: The University Of Chicago Press. p.28.47

[12] ChirpStory. Collection of Tweets from @ioerror. Retrieved from http://chirpstory.com/li/526.

[13] Tor Project. Retrieved from http://www.torproject.org

[14] Morozov, E. (2011). The Net Delusion. New York, Public Affairs. p34.

[15] Foreign Policy. The First Twitter Revolution? Retrieved from:

http://www.foreignpolicy.com/articles/2011/01/14/the_first_twitter_revolution?page=0,1

[16] Lewis, C.S. (2009). The Screwtape Letters: Letters from a Senior to

a Junior Devil. HarperCollins Publishers. Letter 1.

[17] Lewis, C.S. (2009). The Screwtape Letters: Letters from a Senior to a Junior Devil. HarperCollins Publishers. Letter 1.

[18] Kern, H & Hainmueller, J. (2009). Opium for the Masses: How Foreign Media Can Stabilize Authoritarian Regimes. Political Analysis, Vol. 17, No. 4. Chapter 1. p2.

[19] Reuters. China's effort to muzzle news of train crash sparks outcry. Retrieved from http://www.reuters.com/article/2011/07/25/us-china-train-censorship-idUSTRE76O1IG20110725

[20] Morozov, E. (2011). The Net Delusion. New York, Public Affairs. p137.

[21] The New York Times. The Internet Black Hole That Is North Korea. Retrieved from http://www.nytimes.com/2006/10/23/technology/link.html

[22] BBC News. Life inside the North Korean bubble. Retrieved from: http://news.bbc.co.uk/2/hi/programmes/newsnight/8701959.stm

[23] Tor Project. Tor Metrics Portal: Users. Retrieved from: https://metrics.torproject.org/users.html

[24] Tor Project. "One cell is enough to break Tor's anonymity". Retrieved from: https://blog.torproject.org/blog/one-cell-enough

[25] Tor Project. Iran partially blocks encrypted network traffic. Retrieved from https://blog.torproject.org/blog/iran-partially-blocks-encrypted-network-traffic

[26] Thoughtcrime. sslstrip. Retrieved from: http://www.thoughtcrime.org/software/sslstrip/index.html

[27] Overbeck, W & Belmas, G. (2012). Major Principles of Media Law, Boston: Cengage Learning. p277

[28] Overbeck, W & Belmas, G. (2012). Major Principles of Media Law, Boston: Cengage Learning. p278

[29] Overbeck, W & Belmas, G. (2012). Major Principles of Media Law, Boston: Cengage Learning. p279

[30] Jaishankar, K. (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. Boca Raton: CRC Press. p169.

[31] Chaos Computer Club. Chaos Computer Club analyzes government malware. Retrieved from http://ccc.de/en/updates/2011/staatstrojaner

[32] Morozov, E. (2011). The Net Delusion. New York, Public Affairs. p58.

[34] BBC. LiveJournal: Russia's unlikely internet giant.

http://www.bbc.co.uk/news/magazine-17177053

[35] Mashable. STUDY: Social Media Is for Narcissists.

http://mashable.com/2009/08/25/gen-y-social-media-study/

[36] http://www.eurekalert.org/pub_releases/2011-08/apa-sng072711.php

[37] Morozov, E. (2011). The Net Delusion. New York, Public Affairs. p190.

[39] Howard, P. (2010).

The Digital Origins of Dictatorship and Democracy.

New York: Oxford University Press. p.8

[40] Techcrunch. Facebook's S-1

Letter From Zuckerberg Urges Understanding Before Investment. Retrieved from

http://techcrunch.com/2012/02/01/facebook-ipo-letter/

[41] CouldCracker. Retrieved from https://www.wpacracker.com/

[42] The Guardian.

Obama, Facebook and the power of friendship:

the 2012 data election. Retrieved from

http://www.guardian.co.uk/world/2012/feb/17/obama-digital-data-machine-facebook-election?INTCMP=SRCH

[43] The Bureau Of Investigative Journalism.

In Video – Jacob Appelbaum on phone tracking. Retrieved from

http://www.thebureauinvestigates.com/2011/12/21/in-video-jacob-appelbaum-on-phone-tracking/50

[44] The New York Times. Pakistan Builds Web Wall Out in the Open.

Retrieved from

http://www.nytimes.com/2012/03/03/technology/pakistan-builds-web-wall-out-in-the-open.html

[45] Packard, A. (2010). Digital Media Law. Malaysia : Blackwell Publishing. p.26

[46] Pearce1 K. E. & Kendzior S. (2012). Networked Authoritarianism

and Social Media in Azerbaijan. Journal of Communications. Vol 62. Issue 2.

[47] Pearce1 K. E. & Kendzior S. (2012).

Networked Authoritarianism and Social Media in Azerbaijan.

Journal of Communications. Vol 62. Issue 2.

[48] Pearce1 K. E. & Kendzior S. (2012). Networked Authoritarianism

and Social Media in Azerbaijan. Journal of Communications. Vol 62. Issue 2.

[49] Baloyra E. A. & Morris, J. A. (1993). Conflict and change in Cuba, University Of New Mexico Press. p182

[50] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.11

[51] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.4

[53] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.6

[54] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.651

[55] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.8

[56] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.10

[57] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.44

[58] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.44

[59] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.212 (Appendix A)

[60] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.57

[61] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.80

[62] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.80

[63] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.114

[64] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.115

[65] Howard, P. (2010). The Digital Origins of Dictatorship and Democracy. New York: Oxford University Press. p.11952

[66] Lessig, L. (2006). Code V2. New York: Basic Books. p61.

[67] Lessig, L. (2006). Code V2. New York: Basic Books. p73.

[68] Morozov, E. (2011). The Net Delusion. New York, Public Affairs.

p57.

[69] The Economist. The Democracy Index 2011: Democracy under stress. Taken from https://www.eiu.com/public/topical_report.aspx?campaignid=DemocracyIndex2011 (China rated 141st, Iran 159th, Singapore 81st and Russia 117th)

Note

1. Sappiamo che il signor XYZ ha un indirizzo IP (un indirizzo Internet per ogni computer connesso alla rete) di 111.111.1.1 ad un determinato momento, poiché l'ISP gli ha assegnato questo indirizzo. Di conseguenza è possibile vedere quali risorse l'indirizzo IP 111.111.1.1 sta richiedendo e capire cosa stia facendo il signor XYZ. Per maggiori dettagli vedi [66].

2. Questo si potrebbe paragonare a possedere controllare un'autostrada ma non i caselli di ingresso e uscita. I dati che scorrono attraverso la rete sono difficili da raggiungere, ma il modo in cui entra ed esce dalla rete è a discrezione dell'utente.

3. Per un punto d'ingresso, sfruttate la pigrizia degli utenti quando loro usano applicazioni più veloci e meno sicure, assieme al controllo che avete sugli ISP, per rivelare i dati del richiedente. Per il punto d'uscita, assicuratevi di controllare molti nodi di uscita da Tor, e di registrare diligentemente tutti i dati.

4. Alcuni utenti non erano capaci di collegarsi direttamente alla rete Tor, così sono stati sviluppati dei "ponti". I dittatori avevano realizzato come bloccare il traffico di Tor riconoscendone il tipo, così fu creato "Obfsproxy" per fare sembrare il traffico Tor qualcos'altro.

5. Come ha dimostrato Moxie Marlinspike con il suo strumento SSLSTRIP durante la conferenza degli Hacker Black Hat DC 2009, si può agire come un "uomo in mezzo" per intercettare le richieste HTTP che contengono nella risposta collegamenti HTTPS, ingannando molti utenti (nel piccolo test condotto, il 100%) facendo loro pensare di stare usando una connessione sicura.[26]

7. Nota dall'autore.

Io credo nella democrazia come uno strumento potente per l'uguaglianza la trasparenza e la sicurezza in tutto il mondo. Dovrebbero esserci più paesi democratici e tutti noi dovrebbero vivere in uno stato che salvaguarda questi valori. Sono completamente d'accordo con Mark Palmer, che lavorò in Europa Orientale come ambasciatore degli Stati Uniti durante gli ultimi anni del comunismo, ne-

gli anni 90, quando dice "penso che l'obiettivo dovrebbe essere la democrazia universale per l'anno 2025".[0]

Non mi dispiacerebbe nemmeno se succedesse nel 2020 o nel 2015, ma so che è poco probabile che questo si avveri.

Mentre scrivo, il mondo occidentale è spazzato da un'ondata di ottimismo senza precedenti sul ruolo indiscusso giocato dalla tecnologia nel rovesciare regimi non democratici. Nei libri di anni come cittadino digitale, non riesco a ricordare un periodo di tempo in cui i miti sulla tecnologia digitale siano stati più esagerati e stravaganti di adesso. C'è un'idea pericolosa che circola in Occidente, che Internet abbia un'inclinazione naturale a produrre una marca specifica di democrazia Occidentale e spruzzare libertà dalla punta della sua bacchetta magica di fibra ottica. Se dobbiamo raggiungere l'obiettivo di Palmer, abbiamo bisogno di pensare in maniera critica ad affermazioni come "se vuoi liberare una società, devi solo dare loro Internet" dell'attivista Internet Wael Ghonim.[1] Queste asserzioni sono semplicistiche e spesso pericolose.

Abbiamo bisogno di un approccio più raffinato di quello che propongono i media occidentali, se vogliamo liberarci degli Stati autoritari - ed anche di più immaginazione. Io spero che questo saggio aiuterà con quest'ultima, che, sperabilmente, può portare al primo.

Vorrei aggiungere la mia voce al coro degli stati che domandano maggiore democrazia, maggiore libertà e maggiore trasparenza imposti come l'Iran, la Cina, la Siria e la Corea del Nord. Ma la nostra strategia Internet e la nostra politica estera per quanto riguarda questi stati spesso incoraggiano i sistemi totalitari di questi regimi.

Ancora non sappiamo abbastanza su come le dittature usano la tecnologia per opprimere i loro cittadini in molti paesi. Dall'altro lato, sappiamo molto più di quanto ci piacerebbe credere sulle tecnologie di cui speriamo che rovescino i leader dispotici per virtù della loro semplice esistenza.

Abbiamo bisogno di rovesciare tavoli e chiederci, anche solo per un breve istante, quale danno potremo fare alla causa della democrazia considerando Internet uno scopo piuttosto che un mezzo.

Infine, vorrei sottolineare che io non sono un esperto di affari internazionali, politica estera o perfino semplicemente di politica. Ho scritto questo saggio come un tecnologo ed uno studente di belle arti con esperienza di sviluppo di software ed un semplice interesse per l'umanità.