Centre Français de Recherche sur le Renseignement
Centro Studi Strategici Carlo De Cristoforis

Problemi e prospettive della Cyberwarfare

Yves-Marie Peyry

2012

CFR2-CESTUDEC

CF2R
Centre Français de Recherche sur le Renseignement

NOTA "CYBER RENS" N° 5

COMUNITÀ HACKER: UNA NUOVA POTENZA NEL CUORE DELLE SFIDE STRATEGICHE MONDIALI

Yves-Marie Peyry

Il termine hacker, molto usato dai mass media, contiene una diversità semantica difficilmente comprensibile per il neofita.

Parliamo volentieri di pirati informatici, di anarchici cibernetici o di ciberdissidenti. Certi hacker si sforzano di presentare una vocazione umanitaria[1], mentre altri si mettono in luce in azioni più imparentate con la cibercriminalità, il ciberterrorismo o addirittura il cibermercenarismo.

Gli Stati stessi, come per esempio l'Iran, la Cina o gli Stati Uniti, sollevano peraltro degli eserciti di hacker (chiamati il "quarto esercito" dopo quelli di terra, d'aria e di mare) per dei colpi informatici. Così, si stima che il "commando cibernetico" dell'esercito americano conti più di 100.000 uomini e donne, che lavorano, nell'ombra delle reti, per sferrare attacchi contro i server nemici.

Dinanzi a questa varietà di generi, un'analisi delle azioni recenti permette di delineare i contorni di numerosi movimenti che si distinguono, al contempo, per il loro modus operandi ma anche per l'ideologia che soggiace al loro comportamento.

Un attivismo al servizio della libertà d'espressione e della difesa delle libertà individuali

L'aiuto apportato da numerose comunità di hacker in difesa della libertà d'espressione durante le rivoluzioni arabe dimostra l'emergere di un hacking etico e militante a scopo umanitario. Il gruppo Télécomix ha dato così la sua assistenza ai ciberdissidenti arabi per aggirare la censura governativa. Attualmente, le comunità Télécomix e Anonymous sono impegnate in azioni volte a permettere il libero accesso a internet in Siria. Su quest'attivismo al servizio della libera espressione, ci dà la sua testimonianza un membro di Télécomix: "*noi non siamo un'organizzazione ufficiale o un'associazione. Noi cerchiamo unicamente di permettere a tutto il mondo di esprimersi. L'accesso a internet è un diritto per tutti, poco importa la sua localizzazione. Noi aiutiamo tutte le persone o i popoli che ne hanno bisogno e*

[1] Cfr. Note d'Actualité n° 249, http://www.cf2r.org/fr/notes-actualite/la-cyber-dissidence-au-coeur-des-revolutions-arabes.php.

che lo desiderano, blogger spagnoli, americani, iraniani. Forniamo dei mezzi di anonimizzazione gratuitamente, aiutiamo in progetti che rientrano nella nostra ottica (hosting, ecc…). Organizziamo seminari di sensibilizzazione (privacy, criptaggio, opendata, ecc.). Mettiamo in primo piano la neutralità della rete così come la libera circolazione dei dati. Internet è un vettore d'informazione e di libertà d'espressione, noi rimaniamo in guardia semplicemente perché resti tale, né più, né meno".

Questa nuova forma di attivismo hacker al servizio della libertà d'espressione si manifesta anche attraverso delle azioni volte a impedire il blocco da parte delle autorità di siti considerati sensibili. Così, quando il Ministero degli Interni francese ha annunciato la sua volontà di bloccare, mediante procedimento giudiziario, il sito internet *Copwatch*, che scheda poliziotti e gendarmi, i gruppi di hacker Anonymous e Télécomix hanno reagito immediatamente informando che avrebbero aiutato ad attivare siti specchio per aggirare qualsiasi tentativo di blocco.

La lotta contro la "schedatura informatica" è anche all'origine di numerose azioni rivendicate dagli hacker. Si può citare, all'inizio di novembre, la pirateria parziale del server del gruppo politico francese UMP. Il gruppo che ha rivendicato quest'intrusione si qualifica come gruppo di volontari "ciberidealisti" e intende dimostrare, mediante quest'attacco, i pericoli della schedatura di identità su server non abbastanza protetti.

Questa difesa della libertà d'espressione sulla rete è inoltre all'origine di lotte intestine all'interno della comunità hacker. In effetti, il 14 novembre scorso, un gruppo denominato *Voxel Project* ha attaccato il sito internet di BFM-TV per dichiararvi la sua ostilità al gruppo internazionale di hacker Anonymous e minacciare di divulgare, per il 25 dicembre, i nomi di molti dirigenti a capo degli Anonymous. *Voxel Project* precisa: "*non possiamo sopportare l'idea che un gruppo, Anonymous, imponga, senza alcun dibattito, il suo modo di pensare e blocchi questo o quel sito (…). Nessuno ha il diritto di imporre una maniera di pensare e di bloccare milioni di persone*".

Come si vede, la comunità hacker non è solidale. Al suo interno si oppongono alcune correnti ideologiche. Se alcuni si attribuiscono la missione di "guardiano" delle libertà individuali e della libera espressione sulla rete, altri vedono nella propria azione un mezzo di contestazione e di comparsa di un contropotere.

Un attivismo impegnato al servizio della comparsa di un contropotere

Dopo alcuni mesi, si osserva una netta radicalizzazione di certe comunità hacker. Così, si assiste alla moltiplicazione di azioni di "ciber-ribellione" caratterizzate dalla volontà di esercitare un contropotere in cui l'hacker non esita a utilizzare la minaccia informatica o addirittura a distruggere o trafugare dati sensibili per la sicurezza degli Stati.

I metodi impiegati per questi attacchi – dove prevalgono l'attacco per negazione di servizio e il defacing – differiscono dai mezzi utilizzati da altre comunità di hacker, come Télécomix, che, dal canto suo, mostra la volontà di non deteriorare le reti informatiche e, soprattutto, di non distruggere i dati che vi sono immagazzinati.

L'attacco per negazione di servizio, ben noto agli ambienti hacker, utilizza software semplici. Uno dei più conosciuti si chiama LOIC (*Low Orbit Ion Cannot*). Questo programma

permette di stabilire un gran numero di connessioni simultanee al fine di provocare una saturazione del server attaccato e, così, bloccarne l'accesso. Contrariamente a quanto si pensa, un membro di una comunità hacker conferma la facilità di compiere un tale attacco: "*i due unici prerequisiti sono avere il programma LOIC, che è facilmente scaricabile, e comunicare ai membri l'indirizzo del sito che si desidera attaccare. Contemporaneamente, dai quattro angoli del pianeta e con qualche click di mouse, sarà sferrato l'attacco*".

Questo tipo di attacco rivela l'impiego di un vero e proprio "esercito di hacker" pronto a far tremare le maggiori istituzioni civili e militari. La cosa più pericolosa è che un computer può essere utilizzato a distanza, a insaputa del suo utente, per partecipare a un attacco. Così, certi gruppi hacker rivendicano il controllo di molte migliaia di computer, detti "macchine zombi". Questa potenza di calcolo fenomenale permette di aumentare l'impatto di un attacco per negazione di servizio o di decifrare un codice in un tempo notevolmente inferiore che con una sola macchina. Una rapidità d'azione che riduce i rischi di una localizzazione dell'attacco. Su scala planetaria, si stima che oggi giorno ci siano 250 milioni di computer "zombi". Una forza d'urto cinquanta volte più potente della rete di computer utilizzata per il programma SETI per la ricerca di segnali extraterrestri. Secondo alcuni esperti, questo "esercito virtuale" potrebbe infliggere dei danni superiori a un attacco militare convenzionale e annientare, in poche ore, l'insieme delle reti di comunicazione di un Paese, o di vari Stati. Nessun server sembra poter sfuggire a tale minaccia. Per gli hacker "qualsiasi oggetto connesso alla rete è vulnerabile".

Questo "potere nocivo" manifesta inoltre la sua forza attraverso l'anonimato. Un anonimato che è diventato il simbolo del gruppo internazionale di hacker Anonymous creato nel 2003. Il suo motto riflette, senza ambiguità, la sua volontà di esercitare un contropotere: "*Noi siamo Anonymous/Anonimi. Noi siamo Legione. Noi non perdoniamo. Noi non dimentichiamo. Preparatevi*".

Utilizzando come simbolo la maschera di Guy Fawkes – l'istigatore della Congiura delle polveri che mirava ad assassinare il re inglese protestante Giacomo I[2] – Anonymous rivendica numerose operazioni mondiali di hacking. Uno dei suoi membri descrive il gruppo come "*una comunità planetaria, socialmente, ideologicamente e culturalmente eteroclita*". E aggiunge: "*non si può tracciare un profilo tipo. Quello che ci unisce è l'idea che la comunità cibernetica possa sfuggire ai controlli dello Stato ed esprimere la sua dissidenza aldilà delle frontiere. È un contropotere che, secondo noi, restaura l'equilibrio tra il debole e il forte. La rete è incontrollabile e deve rimanere tale*".

Anonymous si è messo in luce attraverso degli attacchi che hanno avuto grande eco per quanto i suoi bersagli potevano essere sensibili. Si può citare, nel mese di luglio del 2011, l'attacco della società Booz Allen Hamilton, un'impresa di consulenza che lavora in particolare per il Pentagono. Anonymous afferma di aver cancellato più di 4GB di dati e scoperto informazioni che permettono futuri attacchi contro strutture governative. Ma il gruppo non si presenta come una minaccia rivolta unicamente agli Stati. La comunità hacker Anonymous si è fatta conoscere anche per la sua lotta contro la Chiesa di Scientology, le reti di pedofili o addirittura un cartello della droga, Los Zetas, in Messico.

[2] http://it.wikipedia.org/wiki/Guy_Fakes.

Tuttavia, le azioni di Anonymous non raccolgono l'adesione dell'insieme della comunità hacker. Alcuni vi vedono "*degli pseudohacker che non sanno fare altro che servirsi di software fabbricati da altri*". Un hacker testimonia: "*alcuni si credono dei re della pirateria informatica mentre non sono capaci di scrivere una sola riga di programmazione. Sono pericolosi quanto dei conducenti che guidano senza patente e non sanno nemmeno dove si trovi il pedale del freno*". Anonymous riconosce d'altra parte degli sbandamenti: "*la nostra struttura è aperta, il suo principio è la garanzia dell'anonimato e ciascuno può effettuare un attacco rivendicandolo in nome di Anonymous, anche se la regola da noi non è di tirare l'acqua al proprio mulino. Abbiamo addirittura visto dei servizi ufficiali farsi passare per noi per screditare la nostra immagine*".

Se alcuni consacrano il proprio talento informatico all'affermazione di un contropotere, di una ribellione cibernetica, altri vi trovano l'opportunità di un'arma temibile per portare a termine i piani di imprese criminali.

Un attivismo lucrativo impegnato in una nuova forma di criminalità

Questa forma di hacking è in continua progressione. Essa risponde ai bisogni lucrativi di un individuo o di un'organizzazione criminale. Qui, lungi dal difendere la libera espressione o di cercare di far emergere un contropotere, l'hacker diventa un "cibermercenario" pronto, dietro remunerazione, a compiere delle missioni di ciberspionaggio, di cibercriminalità o perfino di ciberterrorismo.

Il forte aumento del numero di scambi commerciali su internet ha attirato le brame della pirateria informatica. Un hacker confida nel fatto che la vendita di dati confidenziali rubati mediante intrusione informatica nei server di siti di vendita online gli permetta di "arrotondare" lo stipendio di qualche centinaia o qualche migliaia di euro. L'individuo non è assolutamente un asso della pirateria informatica, lo riconosce lui stesso: "*non faccio altro che sfruttare le falle di sicurezza ormai ben note. Ci sono dei software molto accessibili che circolano sulla rete per effettuare questo tipo di intrusione in un server. La remunerazione varia in proporzione all'importanza dei dati rubati*".

Altri attaccano i server di grandi società per rivendere i file trafugati a dei concorrenti. Lo spionaggio industriale o economico mediante intrusione informatica permette di penetrare nel cuore stesso delle imprese per sottrarre rapidamente e senza il bisogno di compromissioni interne, spesso lunghe e fastidiose, i dati confidenziali ambiti. Inoltre, questi attacchi rimangono perlopiù "silenziosi". In effetti, si stima che l'80% delle imprese vittime di spionaggio informatico non sa di esserlo.

Aldilà del furto di informazioni confidenziali, i pirati informatici fanno gravare altre minacce sulle imprese. L'estate scorsa degli hacker sono riusciti a falsificare gli indirizzi di grandi direttori francesi e a inviare delle mail ai servizi di contabilità di grandi imprese con delle richieste di bonifico che andavano dai 90.000 agli 800.000 euro.

Alcune società sono anche vittime di estorsione di carattere informatico. Con la minaccia di attaccare i suoi server, l'hacker chiede all'impresa un riscatto. In generale, la minaccia di hacking si accompagna a un "defacing" (modifica non richiesta della homepage di un sito) come avvertimento. Quest'estorsione informatica può anche prendere la forma del *Ransomware*. In questo caso, l'hacker introduce nel PC o nella rete della sua vittima un virus

informatico che chiede del denaro per non mettere in esecuzione le proprie minacce. Molti internauti giapponesi ne sono stati vittime all'inizio del 2011. Infatti, degli amanti di manga a sfondo pornografico sono stati minacciati da un virus informatico che pretendeva il versamento di una somma di 1.500 yen (pari a circa 12 euro) per non rendere pubblico sulla rete il nome dell'internauta con le schermate dei siti pornografici visitati. Un importo volutamente basso per aumentare le probabilità di percepire la somma richiesta. Questo è anche uno dei vantaggi offerti all'hacker dalla criminalità cibernetica. L'immensità della rete offre una moltitudine di "prede" potenziali. Può accontentarsi, per ogni vittima, di piccole cifre e, così, limitare i rischi di denunce, aumentando le sue possibilità di ricevere il frutto del suo ricatto.

L'attrattiva del guadagno è una delle principali motivazioni della cibercriminalità. Tuttavia, per certi Stati e gruppi radicali, il "terrore informatico" è anche una nuova "arma operativa".

La minaccia ciberterroristica

Il terrorismo, tematica prioritaria nell'ambito della sicurezza in questo inizio di XXI secolo, ha trovato nelle reti informatiche un nuovo mezzo di espressione, affrancandosi dalle costrizioni frontaliere.

Di fronte a questa minaccia, dopo molti anni, gli Stati si esercitano nei ciberattacchi per premunirsi contro un possibile "attentato informatico". Si considerano molteplici scenari: attacchi alle reti telefoniche, ai centri di approvvigionamento dell'acqua o dell'elettricità, alle reti dei trasporti, dei circuiti finanziari, ecc.

Questo terrorismo informatico non ha nulla dello scenario fantascientifico. Recentemente, un'infrastruttura di gestione dell'acqua dello Stato dell'Illinois è stata vittima di un ciberattacco proveniente dalla Russia. Se quest'attacco non ha avuto gravi conseguenze sul funzionamento dell'impianto (sebbene si sia registrato un arresto temporaneo), esso può essere considerato un avvertimento, poiché il pirata è riuscito a penetrare nel cuore stesso del sistema di gestione della sua vittima. Inoltre, un altro impianto americano di trattamento dell'acqua sarebbe stato attaccato nello stesso modo.

Nel 2007, l'Estonia è stata sottoposta a un ciberattacco massiccio in seguito alla rimozione di un monumento commemorativo della Seconda Guerra mondiale nel centro di Tallinn. Questi attacchi, realizzati mediante negazione di servizio, hanno provocato la disconnessione di numerosi siti governativi e dimostrato la fragilità delle strutture statali rispetto alla minaccia informatica.

Secondo un rapporto dei servizi segreti canadesi reso di dominio pubblico, il grande blackout del 2003, che ha privato dell'elettricità decine di milioni di utenti nell'America del Nord e causato dei danni che ammontavano a sei miliardi di dollari, illustra le conseguenze che potrebbe avere un attacco informatico massiccio contro uno Stato.

Su questa minaccia di terrorismo informatico, Nigel Inkster, ricercatore presso l'Istituto Internazionale di Studi Strategici (IISS) di Londra ed ex membro dell'MI 6, il servizio d'intelligence estera britannica, confessa la sua preoccupazione di vedere degli hacker prestare i loro servizi o il loro esercito di computer "zombi" a imprese terroristiche.

Inoltre, se certi attacchi recenti sono stati perpetrati da gruppi che non proclamano un'appartenenza a un movimento terroristico, l'ipotesi di un'infiltrazione di numerose comunità di hacker da parte di gruppi radicali non deve essere scartata. Dopo che il gruppo Anonymous ha rivendicato, lo scorso luglio, di aver sottratto a un'impresa che lavorava per il Pentagono delle informazioni che avrebbero permesso futuri attacchi contro strutture governative, c'è grande timore di vedere questi dati cadere nelle mani di un gruppo terroristico.

L'attualità recente mostra anche che questo tipo d'attacco non è solo appannaggio di gruppi radicali o fondamentalisti. In effetti, numerosi Stati lavorano, nell'ombra delle reti, per costituire il loro "quarto esercito" ed elaborare attacchi informatici contro delle strutture nemiche. Paesi come la Cina, gli Stati Uniti, l'India, l'Iran, Israele, la Corea del Sud e la Corea del Nord sono regolarmente sospettati di essere all'origine di attacchi informatici ai server di Paesi ritenuti ostili. Nel luglio del 2009, vari ciberattacchi sono stati lanciati contro i siti web del governo americano quali il Pentagono e la Casa Bianca, come pure agenzie governative nella Corea del Sud. Questi due governi accusano la Corea del Nord di aver lanciato questi attacchi. Nel 2010, il virus *stuxnet*, che ha infettato 30.000 sistemi informatici in Iran – tra cui dei PC utilizzati dalla centrale nucleare iraniana di Bouchehr – è stato identificato come una ciberarma volta a colpire un bersaglio preciso, un'"infrastruttura di grande valore situata in Iran" e verosimilmente legata al programma di ricerca nucleare. Molti esperti in sicurezza informatica sospettano che l'*Unité 8200*, un'unità d'intelligence elettronica dell'esercito israeliano, specializzata nell'intrusione elettromagnetica e nella decifrazione di codici, sia all'origine del *malware stuxnet*. Questa stessa unità è stata recentemente sospettata di aver attaccato i server palestinesi nel mondo all'indomani dell'ingresso della Palestina nell'UNESCO.

*

Lo spazio cibernetico oggi è diventato indispensabile per i nostri scambi commerciali, politici, sociali o culturali. Quest'universo virtuale ha profondamente sconvolto i nostri comportamenti e modificato la nostra visione del mondo. Mediante le sue azioni e il suo potere d'influenza, la comunità hacker ne è diventata un attore di primo piano il cui impatto sociale e a livello di sicurezza pubblica è da prendere in considerazione nell'analisi delle principali sfide strategiche della nostra epoca.

Yves-Marie Peyry
Membro del comitato di redazione di *RENSEIGNOR*
Dicembre 2011

CF2R
Centre Français de Recherche sur le Renseignement

NOTA DI RIFLESSIONE N° 11

IN FRANCIA È INDIVIDUABILE UNA RIVOLUZIONE CONDOTTA DA CIBERATTIVISTI?

Yves-Marie Peyry

È l'11 febbraio 2012, siamo a Place de la Bastille a Parigi. Diverse centinaia di manifestanti sfoggiano la maschera di Guy Fawkes, la maschera divenuta il simbolo degli hacker informatici *Anonymous* e l'emblema di una lotta contro il potere stabilito, giudicato irrispettoso delle libertà individuali. Sui cartelli alzati dei cibermilitanti si può leggere "*è sotto la protezione dell'anonimato che è nata la rivoluzione*", "*l'insurrezione che cresce – nel 2012 verremo per voi*" o ancora "*noi non dimentichiamo – siamo pronti per il 2012 – temeteci*". Qui, l'MP5 su una stella a cinque punte della banda di Baader è rimpiazzata da una tastiera di computer. Compare anche il pugno serrato dei gruppi anarchici a illustrare il motto di *Anonymous*: "Noi siamo *anonimi*. Noi siamo legione. *Noi non perdoniamo. Non dimentichiamo. Temeteci*". Uno scenario da apparati radicali che, a somiglianza dell'impatto della ciberdissidenza nel cuore delle rivoluzioni arabe, interroga sulla possibilità di veder emergere, in Francia, una corrente rivoluzionaria sostenuta da ciberattivisti.

In questi ultimi mesi, numerose azioni di pirateria informatica hanno messo in evidenza la volontà di esprimere una lotta politica. Dopo la scomparsa del gruppo *LulzSec* lo scorso luglio (lulz: "se moquer", cioè farsi beffe, sec: "securité", cioè sicurezza), assistiamo alla ricomparsa di un gruppo dalla connotazione più radicale, *AntiSec* (contro la sicurezza) e perfino alla creazione di un nuovo gruppo, *DestructiveSec* (distruggere la sicurezza). Così, gli hacker che evolvono nel seno di questi gruppi non si accontentano più di aggirare la sicurezza delle reti ma ormai intraprendono le loro azioni in una lotta destinata a esprimere il loro disaccordo, "contro", e la loro volontà di distruggere queste barriere informatiche, attuali o future, imposte da un potere ritenuto illegittimo. Una radicalizzazione che si esprime anche nei defacing (modifiche della homepage) operati negli attacchi informatici. Così, il 24 dicembre scorso, l'attacco al gabinetto della società che si occupa d'intelligence economica Stratfor, rivendicato dal gruppo *AntiSec*, è consistito, oltre che in dati confidenziali trafugati durante l'azione e messi su internet, in un defacing che faceva riferimento all'"insurrezione che verrà", estratto dal "libro verde" denominato "breviario anarchico" all'epoca dell'affare francese Tarnac. Questa citazione, ripresa da diversi siti internet vicini ai movimenti hacker, segna fortemente l'impronta ideologica che ormai sembra sostenere numerose azioni di pirateria informatica.

Azioni che non esitano più ad attaccare le fondamenta della Repubblica francese. Il 20 gennaio scorso, il sito internet dell'Eliseo è stato vittima di un'azione di pirateria su grande scala. In uno dei defacing di url compiuti in tale occasione, si poteva leggere "*Sarko, il popolo avrà la tua pelle*". Secondo *Anonymous*, in tale occasione sono state mobilitate diverse centinaia di internauti. Una mobilitazione effettuata attraverso le reti sociali e le chat IRC dalle "cellule d'azione" del gruppo *Anonymous* che in Francia, secondo uno dei suoi membri, conterebbe meno di 100 persone.

Alcune settimane prima, *Anonymous* aveva messo su *Youtube* un videomessaggio all'attenzione di Nicolas Sarkozy, nel quale si affermava un po' di più la minaccia diretta rivolta al vertice di Stato francese: "*Noi, cittadine e cittadini del popolo sovrano di Francia, non ammettiamo più il tradimento e l'impostura generale delle nostre istituzioni e dei nostri dirigenti corrotti…*". In un altro messaggio, rivolto al "popolo di Francia", il gruppo aggiungeva: "*popolo di Francia, la crisi che vivete è artificiale, è un'illusione creata con il solo scopo di indebolirci e di mantenerci in una condizione di stress insopportabile e farci accettare il loro nuovo ordine mondiale…*".

Nel 2011, *Anonymous* ha lanciato un "*appello alle armi, un appello ai combattenti della libertà per l'anno 2012*". Secondo un membro francese, il 2012 è un anno cardine per i popoli occidentali, un anno in cui si apre una "rivoluzione virtuale" per esprimere il disaccordo dei popoli nei confronti di "*questi bruti che vi hanno promesso tutte queste cose perché voi deste loro il potere: mentivano. Non hanno mantenuto le loro meravigliose promesse: non lo faranno mai*" (citazione di un video di *Anonymous* accompagnato da immagini di vari leader occidentali tra cui il Presidente francese, Nicolas Sarkozy). Di rimando, Rick Falvinge, il fondatore del Partito pirata svedese, ha dichiarato sul suo blog "*gran parte della popolazione dei Paesi occidentali ha osservato la Primavera araba e si sta preparando a dover fare probabilmente la stessa cosa nel corso della sua vita. (…) La foto che illustra quest'articolo, la pistola e il bersaglio, non è presa da un catalogo come il 99% delle foto di questo blog. Questa foto è stata scattata nel mio ufficio, a cinquanta centimetri da dove sono seduto…*".

Parole e azioni altrettanto tinte di impegni antiglobalizzazione e ecologisti. Il blocco del sito istituzionale dell'EDF, in aprile e giugno 2011, che ha condotto ai recenti interrogatori di presunti membri francesi di *Anonymous*, è stato il risultato di una delle azioni dell'operazione *Green rights*. Un'operazione decisa dal gruppo *Anonymous* in seguito alla catastrofe di Fukushima con l'obiettivo di "prendersela con i giganti dell'energia che arrecano danno al pianeta" (*Anonymous* a proposito dell'azione *Green rights*). Anche due altri fornitori di elettricità, la società italiana Enel e la General Electric, sono stati vittime di attacchi del gruppo mediante DDOS ("denial of service": letteralmente "negazione di servizio"). Un sostegno importante è stato dato anche al movimento detto degli "indignati" o del "99%". D'altro canto, secondo alcuni esperti, l'avvicinamento di *Anonymous* al movimento degli indignati ha provocato un profondo mutamento del gruppo, che è passato risolutamente da un attivismo tecnico a un attivismo politico.

Secondo un membro di una comunità hacker vicina ad *Anonymous*, "*è in atto una rivoluzione virtuale per un riavvio della democrazia*". E aggiunge: "*Riguardo alla situazione politica ed economica attuale, la democrazia partecipativa non ha più legittimità. Ormai bisogna esercitare la democrazia diretta e le reti sociali, internet, la coscienza collettiva che emana dal web ne saranno le armi d'espressione. Il rinvio dei progetti PIPA/SOPA, che*

rappresentano una minaccia reale per la libertà d'espressione sul web, è una prima vittoria della mobilitazione mondiale di migliaia di internauti nel mondo. E, come dice bene il motto di Anonymous, noi siamo legione".

A proposito degli elementi citati, rimane una questione: i mezzi tecnici a disposizione della comunità hacker possono permettere questo "riavvio della democrazia"? Su questa questione, un messaggio di *Anonymous* risulta particolarmente inquietante e informa "*ci siamo infiltrati tra i vostri militari, tra i vostri poliziotti e tra i vostri informatici*" (estratto del videomessaggio rivolto al popolo di Francia). Se si può vedere in questa dichiarazione solo un eccesso di linguaggio, alcuni elementi sconcertanti rinforzano però queste parole. In effetti, all'inizio di febbraio, *Anonymous* ha diffuso online l'intercettazione di un'audioconferenza telefonica non pubblica tra vari servizi di intelligence occidentali, tra cui alcuni membri del Ministero degli Interni francese. Questa riunione era dedicata alle attività proprio di questi "hacker". L'FBI, che aveva organizzato questa conferenza, ha riconosciuto che "*l'informazione era destinata esclusivamente ai responsabili delle forze dell'ordine ed è stata ottenuta illegalmente*". Com'è potuta cadere nelle mani di questi hacker una comunicazione riservata che esponeva elementi d'indagine e le strategie previste dai servizi di intelligence per lottare contro l'attività degli stessi hacker? Inoltre il gruppo *Anonymous* rilancia annunciando "*l'FBI dev'essere curiosa di sapere come siamo capaci di leggere continuamente le loro comunicazioni interne, già da molto tempo*". Complicità interne o pirateria informatica? La questione rimane ma, in ogni caso, quest'azione dimostra la potenza dei mezzi a disposizione di questa comunità hacker. Come corollario, si può inoltre citare la pubblicazione regolare su un sito di scambio di dati confidenziali sulle tecniche d'indagine informatica utilizzate dall'FBI o persino di mail scambiate tra agenti federali americani.

*

Un vivaio contestatario dalle ambizioni rivoluzionarie sembra dunque profilarsi tra questi attivisti informatici, le cui azioni sono quotidianamente riportate dai media. Sostenuti da mezzi tecnici, umani e logistici importanti, questi "ciber-rivoluzionari" possono trovare in Francia un terreno d'azione privilegiato? A questa domanda, un analista politico dichiara "*In Francia c'è un terriccio rivoluzionario costante dal 1789 e, nell'inconscio dei francesi una specie di gusto amaro d'incompiuto. La ragione è semplice: i poteri accordati al Presidente, come il diritto di grazia o il potere di sciogliere l'Assemblea nazionale, sono percepiti da alcuni come un retaggio monarchico. Coniugati a una grossa crisi economica, a rivoluzioni arabe a catena e in pieno periodo elettorale, la Francia presenta una grande vulnerabilità nei confronti di correnti radicali che potrebbero utilizzare, come nei Paesi arabi entrati nella rivoluzione, internet come fonte di mobilitazione e d'azione*".

Yves-Marie Peyry
Membro del comitato di redazione di *Renseignor*
Webmaster del blog *Signal Monitoring* (http://signal-monitoring.blogspot.com/)
Febbraio 2012

CF2R
Centre Français de Recherche sur le Renseignement

NOTA D'ATTUALITÀ N° 249

LA CIBERDISSIDENZA NEL CUORE DELLE RIVOLUZIONI ARABE

Yves-Marie Peyry

Il 12 marzo scorso, davanti a una platea di ONG riunite a Ginevra dall'appello di Reporter Senza Frontiere per la Giornata mondiale contro la cibercensura, il gruppo TELECOMIX ha portato la propria testimonianza su un hacking "etico e militante" a finalità umanitarie.

In effetti, dall'inizio delle rivoluzioni arabe, questo gruppo creato da hacker svedesi e che si definisce una "società cibernetica" non gerarchizzata[3] si è messo in luce con varie azioni destinate a dare assistenza alle rivolte in corso. La principale è stata l'"esfiltrazione cibernetica" di numerosi video girati dagli insorti, con l'aiuto di connessioni via modem attraverso dei numeri di FAI (fornitori di accesso a internet) situati all'estero o la messa a disposizione di strumenti di criptaggio e di "anonimizzazione" delle comunicazioni. Durante la rivoluzione egiziana, TELECOMIX ha anche lanciato un appello ai radioamatori per stabilire delle comunicazioni su onde radioelettriche. Del resto, anche se TELECOMIX riconosce volentieri la sua vocazione primaria di "hacking", l'organizzazione estende ormai le proprie attività all'insieme di tecniche che permettono di aggirare le censure digitali (crittografia, algoritmi, radioelettricità, ecc.)[4].

In occasione della Giornata mondiale contro la cibercensura, TELECOMIX ha anche condotto un workshop destinato a sensibilizzare gli organismi umanitari ai mezzi di intercettazione o di ascolto dei regimi autoritari, alle tecniche per aggirare la censura ma anche alle soluzioni per proteggere e mettere in sicurezza gli scambi digitali.

La nuova potenza delle reti

[3] TELECOMIX è stato creato nel 2009 da un gruppo di hacker svedesi difensori delle libertà digitali e contrari alla sorveglianza intrusiva. I suoi creatori la definiscono come una società cibernetica non gerarchizzata. Essa riunisce hacker, artisti, ma anche intellettuali. TELECOMIX rimane abbastanza vago sul numero esatto dei suoi membri (in teoria 300) e sui propri mezzi finanziari e materiali.

[4] TELECOMIX, come azione principale, mette a disposizione strumenti per contrastare la censura su internet, rendere anonimi gli scambi sul web o criptare i dati trasmessi. L'organizzazione ha anche costituito una rete di server dedicati che propongono servizi internet in tutto mondo col fine di liberare l'informazione e di permettere la neutralità della rete e parità di trattamento di tutto il traffico internet.

L'impatto delle azioni di TELECOMIX rivela l'importanza di internet e delle reti sociali per "esportare" una rivoluzione e influenzare l'opinione internazionale. Chi avrebbe potuto prevedere l'uscita di scena di Ben Ali e di Mubarak? La Tunisia e l'Egitto, che avevano saputo contenere le voci dissidenti per molti anni, non sono riusciti a soffocare le recenti rivolte nonostante la censura imposta. È probabile che l'esito delle rivoluzioni in questi due Paesi non si giochi unicamente sulla strada ma anche sul web.

Dall'inizio delle manifestazioni antigovernative al Cairo, il canale *Al Jazeera* ha coperto ampiamente gli avvenimenti, in diretta e in modo continuato, sulla sua rete satellitare. E, nonostante il divieto di diffusione pronunciato contro di esso dalle autorità egiziane, il canale qatariano è riuscito a mantenere la sua copertura in diretta con l'aiuto di webcam amatoriali piazzate in tutta la città. Le immagini trasmesse con l'aiuto dei mezzi di aggiramento messi a disposizione dalla "ciberdissidenza" – tra cui TELECOMIX – erano poi diffuse sul satellite *Hot Bird* che, contrariamente al satellite egiziano *Nilesat*, sfuggiva alla censura governativa. In effetti, se la diffusione hertziana può rimanere sotto il controllo dello Stato, non c'è alcun modo di censurare la copertura satellitare straniera accessibile su ampie zone (*Hot Bird* è accessibile nel Nord Africa con una parabola da 90 cm). Inoltre, vari operatori – tra cui *Opensky* – propongono delle connessioni a internet via satellite, come *Hot Bird*, *Eutelsat* o *Hispasat*. Un semplice modem collegato tra la parabola e un microcomputer è sufficiente per aprire un accesso a internet senza passare da un operatore nazionale.

I ciberdissidenti arabi hanno anche ricevuto un aiuto importante dall'ONG americana AVAAZ.

AVAAZ – che significa "voce" in diverse lingue – è un'organizzazione non governativa americana, la cui sede si trova a New York, ma che ha anche degli uffici a Londra, Parigi, Washington, Ginevra e Rio de Janeiro. È stata fondata nel 2006 dall'anglo-canadese Ricken Patel, ex consulente all'ONU, ma anche membro delle fondazioni Rockfeller e Bill Gates. AVAAZ è l'emanazione di *ResPublica*, un gruppo che promuove campagne civili transnazionali, e *MoveOn*, un gruppo americano di mobilitazione sociale su internet. Questi due gruppi hanno profondamente ispirato la sua azione, il cui principale obiettivo è raggruppare "cittadini del mondo" per sensibilizzare, condurre azioni volte a influenzare le decisioni mondiali e fare "fronte alle nuove sfide che minacciano il nostro avvenire, come i cambiamenti climatici e l'aumento dei conflitti". Secondo Ricken Patel "è necessario ridurre lo scarto tra il mondo in cui viviamo e quello che sogniamo".

Nell'aprile 2011, AVAAZ rivendicava più di otto milioni di membri in 193 Paesi del mondo. Le sue azioni sono condotte principalmente su internet e sulle reti sociali con la diffusione di petizioni o la sensibilizzazione degli internauti alle principali poste in gioco a livello mondiale. Ciononostante, grazie alle donazioni ricevute (unica fonte di finanziamento secondo AVAAZ), l'organizzazione ha potuto anche inviare delle squadre sul terreno per organizzare manifestazioni tematiche non violente (ambiente, diritti umani, globalizzazione, ecc.), inoltrare materiale informatico per aggirare le censure digitali o finanziare grosse campagne pubblicitarie. Tra le sue azioni sul campo, si possono citare i supporti tecnologici (server, webcam, telefoni satellitari, ecc.) forniti a movimenti democratici e di difesa dei diritti

umani in Birmania, Zimbabwe, Tibet, Iran, Haiti e, più recentemente, alle rivolte in corso nei Paesi arabi.

AVAAZ conta su appoggi celebri all'interno degli ambienti politici. Si possono citare: l'ex Primo Ministro britannico Gordon Brown, che ha dichiarato che essa aveva fatto avanzare gli ideali del mondo; l'ex vicepresidente Al Gore, che considera AVAAZ una fonte d'ispirazione che ha già fatto cambiare molto le cose; o Zainab Bantura, l'ex Ministro degli Affari Esteri della Sierra Leone, che descrive AVAAZ come un alleato e un punto di incontro per le persone svantaggiate in tutto il mondo, per promuovere un vero cambiamento.

AVAAZ, con l'aiuto delle donazioni ricevute per sostenere le contestazioni arabe, ha potuto inviare agli insorti libici e yemeniti dei kit di connessione a internet via satellite a prova di blackout, piccole videocamere, trasmettitori radio portatili e perfino delle squadre di esperti per formare i manifestanti al loro utilizzo. La vocazione di quest'azione è chiaramente ostentata da AVAAZ sul suo sito internet: permettere "di diffondere video in streaming, anche durante i tagli di internet e del telefono, e garantire che l'ossigeno dell'attenzione internazionale alimenti i loro coraggiosi movimenti per il cambiamento".

*

Così, numerosi video delle rivolte in corso in Medio Oriente che ci arrivano su Youtube sono stati inoltrati con l'aiuto dei mezzi digitali messi a disposizione da AVAAZ e degli strumenti di criptaggio e di aggiramento della censura forniti da TELECOMIX.

Con le contestazioni arabe, è nata una nuova forza, da prendere in considerazione nelle nostre analisi, quella della ciberdissidenza che segnerà una svolta nella Storia delle Rivoluzioni.

Yves-Marie Peyry
Membro del comitato di redazione di *Renseignor*
Webmaster del blog *Signal Monitoring* (http://signal-monitoring.blogspot.com/)
Maggio 2011