La guerra di Pechino alla rete

Alessio Casagrande
{alessio.casagrande@studenti.unimi.it}

Lazzaro Labienta
{lazzaro.labienta@studenti.unimi.it}

ABSTRACT - Nel mondo 2.0 in continua evoluzione, il ruolo della tecnologia è sempre più determinante. La libertà di pensiero di parola e di comunicazione sono le basi per un paese libero e democratico. In questo articolo vogliamo prendere in considerazione la situazione della Cina. Uno dei paesi più grandi del mondo, che da molti anni è sotto un sistema di controllo della rete applicato dal suo governo. Nella prima parte dell'articolo analizzeremo la storia di Google in Cina, dal suo ingresso nel 2000 fino alla decisione di dirottare sul motore di Hong Kong, il suo motore cinese. Illustreremo inoltre l'attacco "Operation Aurora" portato a Goggle e ad altre grandi società americane. Nella seconda parte dell'articolo tratteremo le possibili tecniche di censura che possono essere applicate e spiegheremo come poterle bypassare. Infine mostreremo le storie di due dissidenti famosi, il premio nobel Liu Xiaobo e Shi Tao, entrambi condannati ed incarcerati dalle autorità cinesi perchè considerati una minaccia al governo.

Key Words: Cina, Google, Operation Aurora, The Great Firewall, Liu Xiaobo, Shi Tao.

INTRODUZIONE

Tutti noi siamo nati e ci siamo abituati ad un mondo, dove la tecnologia si intreccia fortemente con la vita reale, dove l'espansione della rete ci ha dato la possibilità con l'uso dei Social Media di connetterci con tutti i nostri amici, conoscenti e persone esterne, dove con un click possiamo recuperare notizie, commentarle e criticarle. L'evoluzione radicale della rete ha portato i popoli ad un nuovo modo di comunicare e quindi, allo stesso tempo, messo in guardia molti governi. L'idea di possibili rivolte e insurrezioni hanno spinto molte autorità governative ad intraprendere una vera e propria guerra contro Internet. Un mezzo di comunicazione cosi forte, veloce e dalle potenzialità infinite viene visto come una minaccia da combattere e non come un'opportunità di crescita e di democrazia. Il mezzo più facile da adottare per limitare la rete all'interno della propria nazione è proprio quello del controllo, l'applicazione di regole per censurare contenuti che possono portare danno al governo, nascondendo al proprio popolo le vere ragioni della censura, cercando di alterarne il pensiero comune e far vedere la rete come mezzo per commettere reati, subire torti e trovare materiale illecito.
Il caso più noto alle cronache mondiali è la Cina, dove tutti i contenuti della rete vengono perennemente filtrati e controllati dalle autorità di stato. Un intero paese che vanta ad oggi il maggior numero di utenti connessi alla rete, circa 500 milioni di persone, chiuso dietro un grande firewall, il famoso "The Great Firewall".
Una continua lotta del governo cinese contro notizie, video, blog, siti web che possano essere dannosi al regime. La terna adottata "Sorveglianza globale + firewall + censura", in Cina, da luogo al più sofisticato sistema di controllo presente al mondo. Un sistema studiato per controllare e cercare di manipolare il pensiero del proprio popolo.
Ci piace riportare una citazione di John Draper, tratta dal libro "Hacker - il richiamo della libertà" di Giovanni Ziccardi:

> "*[...] Penso che l'aspetto se sia o meno realmente possibile controllare la tecnologia oggi sia molto interessante:*
> *non penso sia possibile realmente controllare la tecnologia in fondo, internet fu inizialmente disegnata come un sistema aperto, come una porta scorrevole in un sottomarino, con troppi buchi, in ipotesi, da rattoppare per controllarla. Si noti ad esempio, il grande firewall cinese: non sarà certo quello a fermare i dissidenti in quel paese dall'attaccarlo e dall'utilizzare sistemi proxies per superarlo"*

1. GOOGLE vs CHINA

Qualsiasi società che voglia impegnarsi in internet su territorio cinese dovrà applicare ai propri contenuti web filtri di censura, accettando il controllo continuo da parte della Pubblica sicurezza. Non sono escluse da questo regolamento neanche le più grandi Bigcorp americane, una su tutte Google.
Goggle introdusse il suo famoso motore di ricerca in Cina nell'anno 2000, sotto il dominio di google.com. Nei 4 anni successivi molti servizi di Google come Gmail e Google News subirono dei forti rallentamenti, causati

dai controlli effettuati dal governo cinese. Nel 2006 Google decise di fare il suo ingresso ufficiale in territorio cinese, inaugurando la propria sede a Pechino, situata nella torre NSC, aprendo così ufficialmente il suo motore di ricerca www.google.cn. Google applicò al suo motore di ricerca la censura dei contenuti ritenuti dannosi da parte del governo.
Questa mossa da parte di Google ha generato forti discussioni all'interno del mondo occidentale, arrivando ad accusare l'azienda americana di violare i propri principi, riferendosi soprattutto al classico motto pubblicizzato da Google "Don't be evil".
L'ingresso da parte della grossa azienda di Mountain View in Cina non è mai stato visto positivamente anche da parte del governo cinese, considerando Google un forte alleato del governo degli Stati Uniti, accusandoli di lavorare insieme per riuscire a portare la libertà della rete da parte del popolo cinese, boicottando così i provvedimenti e i controlli applicati dal governo.
Come riportato nel cable originale "GOOGLE UPDATE: PRC ROLE IN ATTACKS AND RESPONSE STRATEGY" rilasciato da Wikileaks il 30/08/2011, è possibile trovare la dichiarazione di un contatto cinese dell'ambasciata americana, che rende l'idea del timore del governo cinese verso il colosso di Mountain View:

> "*Baidu sembrava una noiosa e grigia impresa statale mentre Google sembra molto interessante, come il frutto proibito. Al popolo cinese sarebbe sembrato molto chiaro che Google e il governo americano stavano lavorando insieme per la libertà di Internet e per minare i controlli del governo cinese su di esso. Questo avrebbe reso felici alcuni intellettuali, ma ad altri sarebbe stato considerato come un'ingerenza negli affari interni della Cina."*

E' chiaro che l'ingresso di Google in Cina avrebbe potuto destabilizzare il governo, concedendo ai cittadini una grossa possibilità di poter far sentire la loro voce.
Nel 2010 dopo la scoperta di un attacco contro due account di posta Gmail, di Ai Wei Wei, Google decise di togliere tutti i filtri di censura nel suo motore di ricerca, dirottando google.cn sotto il motore di ricerca presente ad Hong Kong, google.com.hk. Il 17 Gennaio 2010 sul suo blog ufficiale Google dichiara la chiusura di google.cn

> "*These attacks and the surveillance they have uncovered—combined with the attempts over the past year to further limit free speech on the web—have led us to conclude that we should review the feasibility of our business operations in China. We have decided we are no longer willing to continue censoring our results on Google.cn, and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all. We recognize that this may well mean having to shut down Google.cn, and potentially our offices in China."*

Dietro questo attacco chiamato "Operation Aurora" si è sempre pensato esserci il governo cinese, desideroso di raccogliere informazioni utili contro i vari attivisti, ufficialmente Google ed il governo americano non hanno mai accusato direttamente il governo cinese dell'attacco, pur lasciando intendere molte volte della presenza di esso dietro quell'operazione di hacking.

1.1 Operation Aurora
Con un comunicato ufficiale comparso sul proprio blog, Google il 12 Gennaio 2010 comunica a tutto il mondo di essere stato vittima di un cyber-attacco. L'inizio dell'attacco risale alla metà del 2009 e si stima sia proseguito fino a Dicembre 2009.
L'attacco viene portato ai server di Google e ad altre grandi società come Adobe System, Junipert Networks, Rackspace. Il nome "Operation Aurora" creato da McAfee che ha redatto un paper contenente l'intera spiegazione dell'attacco, deriva dal fatto che il nome Aurora era contenuto nel path che riconduceva al file che veniva installato all'interno della macchina vittima. La realizzazione di questo attacco è stata ricondotta, seppur non ufficialmente, al governo cinese, accusato di ingaggiare degli esperti per poter scoprire tutte le informazioni utili sugli attivisti, oltre all'acquisizione delle informazioni riguardanti di quest'ultimi, lo scopo degli attaccanti consisteva anche nell'ottenere l'accesso al codice sorgente, cercando così di scoprire i vari segreti custoditi segretamente dietro il codice proprietario. L'attacco sfrutta delle vulnerabilità zero-day presenti all'interno di Internet Explorer e di Adobe. La procedura dell'attacco viene spiegata dettagliatamente all'interno del documento redatto da McAfee "Protecting Your Critical Assets - Lessons Learned from "Operation Aurora".
L'attacco si compone delle seguenti parti:

1. Viene scelto un user o un gruppo di user, essi ricevono in casella mail o tramite istant message da una sorgente considerata trusted, un messaggio contenente un link.
2. L'utente cliccando sul link presente nella casella mail, viene rediretto verso un sito web contenuto in server presenti a Taiwan, in questo sito web è presente il codice javascript maligno che consente di attaccare la vittima. Ovviamente la vittima non si accorge minimamente di visitare un sito web considerato maligno.
3. Una volta che l'utente accede al sito, viene eseguito il codice Javascript maligno, che sfrutta le vulnerabilità trovate nei sistemi.

4. Il codice maligno consente l'apertura di una backdoor verso i server ospitati a Taiwan, consentendo agli attaccanti l'accesso al sistema della vittima.

Dopo una decina di giorni dalla pubblicazione dell'attacco Microsoft ha dichiarato il fix del bug di cui era affetto il browser Internet Explorer. Dopo l'attacco Google decise di non sottostare alla censura governativa spostando il google.cn sotto google.com.hk, una chiara mossa contro il governo cinese. In una nota apparsa il 17 Gennaio 2010 sul suo blog Google dichiara:

> "*[...] we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. Based on our investigation to date we believe their attack did not achieve that objective. Only two Gmail accounts appear to have been accessed, and that activity was limited to account information (such as the date the account was created) and subject line, rather than the content of emails themselves."*

Google afferma che l'attacco "Operation Aurora" non è stato portato a termine con successo, sostenendo che le informazioni che sono state trafugate dai server di Google riguardino principalmente l'oggetto e la data di creazione dei messaggi di due account di posta elettronica di Gmail appartenenti a AI WeiWei.

2. TECNICHE DI CENSURA

Come abbiamo detto nei paragrafi precedenti, le tecniche di censura danno la possibilità di limitare le informazioni che circolano sulla rete, offuscandole con opportune tecniche. Le tecniche principali di censura che vengono utilizzate sono:
- IP BLOCKING
- DNS filtering and redirection
- URL filtering
- Packet Filtering
- Connection Reset

Iniziamo con l'analizzare la prima tecnica quella riguardante l'IP Blocking. L'IP Blocking è una tecnica che permette di oscurare un dato indirizzo IP, rendendo irraggiungibile il sito web o il server di riferimento. Se l'indirizzo IP di un server viene bloccato, ovviamente qualsiasi contenuto presente all'interno di esso non potrà essere visualizzato. Rientra nel blocco anche un qualsiasi sito web che non contiene materiale proibito ma che viene ospitato all'interno del Server bloccato. Questa tecnica è molto facile da implementare e non richiede grossi costi di realizzazione.
La tecnica di DNS filtering and redirection permette ai DNS usati, di risolvere in maniera sbagliata un nome di dominio. In questo modo è possibile dirottare il traffico su un indirizzo IP non corretto, rendendo inaccessibile il sito che desideriamo. In questo modo un qualsiasi utente che utilizza dei DNS "modificati" non sarà in grado di accedere al contenuto ritenuto proibito, ma verrà reindirizzato su una pagina contenente un errore fittizzia, nel più dei casi la pagina con l'errore 404.
La tecnica di URL e Packet filtering, consiste nell'analizzare la stringa URL immessa dall'utente, facendo un'analisi delle parole chiave e bloccando la connessione nel caso in cui vengano trovate delle parole che rientrano nella lista nera delle parole da cercare. Tramite il filtraggio dei pacchetti immessi sulla rete è possibile chiudere una connessione TCP. La chiusura della connessione TCP viene spesso fatta attraverso una TCP Reset. I pacchetti di TCP Reset consentono la chiusura forzata della connessione tra il client ed il Server. In questo modo il browser del client visualizzerà a video una pagina bianca non potendo così accedere ai contenuti desiderati. Un esperimento condotto Richard Clayton, Steven J. Murdoch e Robert N. M. Watson nel loro articolo "Ignoring the Great Firewall of China" mostrano chiaramente il blocco della connessione tramite una TCP Reset. Da una postazione situata a Cambridge gli autori inviano una richiesta ad un server cinese per la visualizzazione di un sito web ritenuto accessibile, dopo la classica procedura di Handshaking viene fatta una Get e senza alcun tipo di problema viene restituita la pagina da visualizzare.

```
cam(53382) → china(http) [SYN]
china(http) → cam(53382) [SYN, ACK]
cam(53382) → china(http) [ACK]
cam(53382) → china(http) GET / HTTP/1.0<cr><lf><cr><lf>
china(http) → cam(53382) HTTP/1.1 200 OK
(text/html)<cr><lf> etc…
china(http) → cam(53382)  … more of the webpage
cam(53382) → china(http) [ACK]
… and so on until the page was complete
```

Diverso invece il discorso quando si tratta di richiedere l'accesso ad una pagina ritenuta proibita.

```
cam(54190) → china(http) [SYN]
china(http) → cam(54190) [SYN, ACK] TTL=39
cam(54190) → china(http) [ACK]
cam(54190) → china(http) GET /?falun
HTTP/1.0<cr><lf><cr><lf>
china(http) → cam(54190) [RST] TTL=47, seq=1, ack=1
china(http) → cam(54190) [RST] TTL=47, seq=1461, ack=1
china(http) → cam(54190) [RST] TTL=47, seq=4381, ack=1
china(http) → cam(54190) HTTP/1.1 200 OK
(text/html)<cr><lf> etc…
cam(54190) → china(http) [RST] TTL=64, seq=25, ack zeroed
china(http) → cam(54190)  …more of the webpage
cam(54190) → china(http) [RST] TTL=64, seq=25, ack zeroed
china(http) → cam(54190) [RST] TTL=47, seq=2921, ack=25
```

Una volta rilevata la parola chiave proibita che si sta cercando, il server invia tre pacchetti di Reset per forzare la chiusura della connessione. Il firewall invia tre diffirenti pacchetti di TCP reset per assicurarsi dell'accettazione da parte del client dei pacchetti. Dalla navigazione in territorio cinese, è stato possibile verificare che quando viene applicata una TCP Reset alla connessione, nei successivi 30 minuti non è più possibile accedere a quel dato contenuto. Questo è possibile tramite una nuova regola che il Firewall adotta, bloccando la connessione verso la macchina incriminata nella fase di Handshake.

```
cam(54191) → china(http) [SYN]
china(http) → cam(54191) [SYN, ACK] TTL=41
cam(54191) → china(http) [ACK]
china(http) → cam(54191) [RST] TTL=49, seq=1
```

3. TECNICHE PER BYPASSARE IL FIREWALL

Se da un lato il governo cinese prova a limitare i contenuti che possono recare danno al regime, dall'altro ci sono molti cittadini che ogni giorno per provare a sfuggire ai controlli di censura provano a mettere in pratica alcune tecniche per bypassare il grande firewall. Le tecniche più usate per evadere il firewall sono:
- Utilizzo di Tor
- Utilizzo di VPN e Proxy

L'utilizzo della rete Tor consente ad un cittadino presente nel territorio cinese di scavalcare il firewall di controllo, mantenendo l'anonimato sulla rete. il fatto che l'indirizzo IP dell'exit node non sia un indirizzo cinese permette all'utente che naviga sulla rete Tor di non subire i controlli. Un altra tecnica molto utilizzata riguarda l'uso di VPN e Proxy, queste tecniche è sono molto utilizzate dai cittadini cinesi, per evadere il firewall.
Un altro interessante progetto è FreedomBox. FreedomBox è stato presentato da Eben Moglen in occasione della New York ISCO il 2 Febbraio 2010, lo scopo di questo progetto consiste nel dare la possibilità a qualsiasi utente di godere completamente della propria privacy, concedendogli una navigazione completa ma anonima, e dando la possibilità di criptare i propri dati all'interno della macchina FreedomBox. Questo sistema consente di avere una privacy completa all'interno di governi che applicano qualsiasi mezzo di censura. FreedomBox è un plug computer, cioè un server molto piccole che una volta attacco alla rete di corrente consente la gestione di dispositivi sulla rete. La connessione anonima sulla rete viene effettuata mediante la rete Tor, la FreedomBox permette di dirottare il traffico di rete sulla rete Tor. Inoltre la FreedomBox permette l'eliminazione dalle pagine dei banner pubblicitari che come spesso accade consentono di acquisire informazioni sul computer che sta navigando. La FreedomBox viene sviluppata usando hardware a basso costo e software libero, basata su una distribuzione Debian.
La conoscenza di queste tecniche in territori ritenuti ostili, dove non sussiste alcuna libertà di stampa può essere reso possibile dal classico passaparola.

4. DISSIDENTI

4.1. LIU XIAOBO

Liu Xiaobo nasce nel 1955 a Changchun (Cina del Nordest): professore universitario di letteratura, quando scoppiò la protesta studentesca del 1989 fu tra gli intellettuali che si schierarono con i giovani. Partecipò in prima persona alla creazione della Federazione autonoma degli studenti, che guidò la mobilitazione di quegli anni.
Quando venne a conoscenza che il segretario del Partito comunista cinese, Deng Xiaoping, aveva scelto la repressione contro gli studenti nella piazza di Tienanmen, Liu si attivò per convincere i giovani a lasciare la piazza

prima dell'intervento dell'esercito. Fu quindi arrestato, con l'accusa di essere una delle "mani nere" che manovravano gli studenti e trascorse 18 mesi in prigione. Nel 1995 scontò tre anni di "rieducazione attraverso il lavoro" e in seguito gli fu vietato di insegnare.
Celebre fu la frase riportata in seguito ad una sua intervista del 1988 rilasciata ad una rivista di Hong Kong:

> *« In 100 anni di* colonialismo *Hong Kong è cambiata fino a diventare ciò che è oggi. Data la grandezza della Cina, ovviamente ci vorrebbero 300 anni per trasformarla in quello che Hong Kong è oggi. E ho dei dubbi che 300 anni siano abbastanza. »*

Nel 2008 nasce Charta08 dove Liu Xiaobo è promotore, manifesto pubblico che inneggia alla libertà di espressione e al rispetto dei diritti umani.
Questo movimento in breve tempo otterrà quasi 10000 adesioni e sarà causa dell'arresto del dissidente con l'accusa di "incitamento alla sovversione del potere dello stato".
Il 25 dicembre 2009 viene condannato a 11 anni di prigione e 2 anni di interdizione dai pubblici uffici.
Il 18 gennaio 2010 gli viene assegnato il premio Nobel per la pace con la seguente motivazione:

> *« Durante gli ultimi decenni la Cina ha fatto enormi progressi economici, forse unici al mondo, e molte persone sono state sollevate dalla povertà. Il Paese ha raggiunto un nuovo status che implica maggiore responsabilità nella scena internazionale, che riguarda anche i diritti politici. L'articolo 35 della Costituzione cinese stabilisce che i cittadini godono delle libertà di associazione, di assemblea, di manifestazione e di discorso, ma queste libertà in realtà non vengono messe in pratica». «Per oltre due decenni, Liu è stato un grande difensore dell'applicazione di questi diritti, ha preso parte alla protesta di Tienanmen nell'89, è stato tra i firmatari e i creatori di* Charta 08*, manifesto per la democrazia in Cina. Liu ha costantemente sottolineato questi diritti violati dalla Cina. La campagna per il rispetto e l'applicazione dei diritti umani fondamentali è stata portata avanti da tanti cinesi e Liu è diventato il simbolo principale di questa lotta».*

Le autorità cinesi cercarono qualsiasi modo per non far trapelare la notizia all'interno dello stato, preoccupate di come potesse reagire il popolo e anche per cercare di non fare sapere a Liu dell'onoreficenza ricevuta, imposero ai media (giornali, tv) di non diffondere la notizia, che però riuscì ad arrivare alla famiglia di Liu Xiaobo. Per evitare che qualche parente del dissidente andasse a ritirare il premio ad Oslo, furono messi tutti agli arresti domiciliari, mentre la moglie in isolamento, per non avere nessun tipo di contatto con media stranieri.

4.2. SHI TAO
Il 20 Aprile del 2004 Shi Tao partecipò ad una riunione tra giornalisti, dove venne trasmesso un comunicato che indicava la linea da seguire da parte di quest'ultimi in occasione del 15°Anniversario della repressione del movimento per la democrazia del 1989. Il governo voleva attuare un'azione preventiva per evitare possibili disordini durante l'anniversario. In particolare questo comunicato, mirava ad istruire la stampa per consentire di indirizzare l'opinione pubblica, evitando di far rilasciare alla stampa pareri che fossero in contrasto con il parere del governo centrale. Shi Tao durante la riunione prese appunti, segnando tutte le linee guida che erano scritte sul comunicato. Intorno alle 22, orario dimostrato dalle informazioni rilasciate da Yahoo, il giornalista inviò una mail ad un suo contatto negli Stati Uniti. Tale mail fu pubblicata sul sito web Minzhu Tongxun (Forum della democrazia) sotto la voce "198.964".
Riportiamo il post 198964 comparso sul sito Minzhu Tongxun:

> Provided by 198964
>
> On April 20, propaganda departments in China distributed to news organizations at various levels a Document 11 issued by the offices of the Communist Party of China and by the offices of the State Council. The content of the document was "A notice concerning the work for maintaining stability". An extract is as follows:
>
> 1: An analysis on the current situation:
>
> (1) This year will see the 15th anniversary of the "June 4th event," and overseas pro-democracy activists have been busy, and are preparing to commemorate the day by adopting very intrusive activities, and preparing to infiltrate China
>
> (2) On the problem of liberalism, its main tenet is to deny the leadership of the Communist Party and the socialist system, and carry on what is known as studying the people; and therefore some antagonistic forces are politicizing criminal cases
>
> (3) Evil "Falun Gong" members are carrying out damaging activities
>
> (4) Various kinds of harmful information are being spread on the Internet.

(5) Mass events have become prominent, such as those that have resulted from resettlement after demolition or relocation of residential housing, and appeals for help from higher authorities

(6) Overseas antagonistic forces are trying to draw young people and teenagers through such channels as religion (printed matter and Internet), or developing academic activities and assistantships to study in schools, and engaging in illegal activities

(7) The Hong Kong problem.

The key points above are about the "June 4th event," "Falun Gong" and about "mass events."

2. Departments at various levels should take widespread preventive measures on the following:

(1) Resolutely stop pro-democratic activities from infiltrating the country
(2) Take strict precautions against all kinds of activities (by this they mean outlawed ones)
(3) Take strict precautions against hostile elements who use the Internet to organize activities
(4) Take strict precautions against mass events taking place
(5) Take strict precautions against the "Falun Gong" evil cult organization sabotaging events
(6) Take strict precautions for the safety of key departments and personnel
(7) Take strict precautions against certain factors that would have adverse influences on stability and unity

Five crucial jobs that must be seriously tackled:

(1) To adhere to correct theories and sense of responsibility
(2) To thoroughly strengthen intelligence information so as to be aware of any activities
(3) To preserve in influencing public opinion in the right way, effectively prevent sabotage by overseas antagonist elements; never say any thing that is not in line with the policies of the central government
(4) Stress the key points, and effectively carry out preventive controls against them
(5) Reduce the number of petitions to higher authorities from the masses

(Also monitor contacts between overseas pro-democratic activists and editors and reporters of mainland media. Report immediately once such contacts are discovered.)

(Originally published on Democracy Info *2004.4.20)*

Shi Tao fu condannato a 10 anni di reclusione, la sua famiglia è stata messa sotto osservazione e maltrattata. Durante il processo Yahoo ebbe un ruolo fondamentale, infatti la mail venne inviata da un indirizzo mail @yahoo.com.cn. La grossa azienda Americana ha fornito al governo cinese l'indirizzo IP della locazione di dove era stata inviata la mail. Si scoprì che la mail fu inviata dalla sede del giornale dove lavorava Shi Tao. Ufficialmente non si hanno delle notizie, ma in molti sostengono che Yahoo per assecondare il governo cinese oltre all'indirizzo IP abbia fornito altri dati personali di Shi Tao.

Bibliografia

[1] G.Ziccardi "*Hacker - il richiamo della libertà*", Marsilio, 2011.
[2] Surya Deva: "*Corporate complicity in Internet censorship in China: Who cares for the global compact or the global onliene freedom act?*", 2007.
[3] Dichiarazione Wang Chen: *"http://usa.chinadaily.com.cn/china/2011-09/29/content_13818683.html".*
[4] Google in China: "*http://googleblog.blogspot.it/2006/01/google-in-china.html*".
[5] Comunicato nuova strategia google in cina: "*http://googleblog.blogspot.com/2010/01/new-approach-to-china.html".*
[6] McAfee Labs, McAfee Foundstone Professional Services "*Protecting Your Critical Assets - Lessons Learned from "Operation Aurora".*
[7] Attacco "Operation Aurora": *http://www.wired.com/threatlevel/2010/01/operation-aurora/.*
[8] Cable dell'Ambasciata Americana *"http://wikileaks.org/cable/2010/01/10BEIJING207.html".*
[9] Testing siti e keyword censurate: *https://en.greatfire.org/*
[10] FreedomBox: "*http://freedomboxfoundation.org/*".
[11] R.Clayton, S.J. Murdoch, R.N. M.Watson: "*Ignoring the great firewall of China*", I/S: A Journal of law and policy for the information society.
[12] Biografia Liu Xiaobo: "*http://en.rsf.org/chine-liu-xiaobo-biography-28-10-2010,38704.html".*
[13] Shi Tao: *http://www.amnesty.it/Cina_Shi_Tao_condannato.*
[14] Contenuto mail Shi Tao: "*http://cpj.org/awards/2005/shi-tao.php#govt".*
[15] Criminal Verdict Shi Tao