09|2013

IL RUOLO DEL CYBER WARFARE NEL CONFLITTO IN SIRIA

A cura di
Mario Avantini

CISINT Centro Italiano di Strategia e Intelligence

LIMITAZIONE DELLA RESPONSABILITÀ

Le opinioni espresse nel presente documento, rilasciato a scopo informativo, sono di responsabilità esclusiva dell'autore e non riflettono necessariamente la posizione ufficiale del CISINT - Centro Italiano di Strategia e Intelligence.

www.cisint.org **info@cisint.org**

Sommario

OFFENSIVE CYBER CONTRO LA SIRIA 4

CYBER REPRESSIONE, L'ULTIMA FRONTIERA DELLA CYBER WAR 6

LE MODALITÀ DI ATTACCO DEL SYRIAN ELECTRONIC ARMY 8

ATTI DI CYBER WAR E IL POTERE 10

OFFENSIVE CYBER CONTRO LA SIRIA

L'Arabia Saudita ha dichiarato che la diffusione di informazioni tramite Internet a beneficio di gruppi "terroristici" è fuorilegge, assumendo una posizione in linea con la decisione già adottata dalle monarchie del Golfo Persico.

L'agenzia di stampa ufficiale saudita SPA ha reso pubblica l'approvazione da parte del Gabinetto di una legislazione unitaria contro la criminalità informatica, adottata dal **Consiglio di Cooperazione del Golfo** (CCG) nel mese di dicembre 2012. L'agenzia ha dichiarato inoltre che la normativa mira a perseguire coloro che creano siti e pubblicano informazioni su Internet o in una rete di computer a beneficio di gruppi terroristici, per agevolare contatti tra i vari esponenti di appartenenza, per promuovere la proliferazione di correnti di pensiero o la ricerca di finanziamenti.

Suddetta legislazione vieta anche la diffusione di idee che potrebbero influenzare l'ordine pubblico o il buon costume. Ciò è quanto dichiarato dall'agenzia SPA, senza però fornire ulteriori dettagli. La maggior parte degli Stati appartenenti all'organizzazione GCC (Bahrain, Kuwait, Oman, Qatar, Arabia Saudita e gli Emirati Arabi Uniti) negli ultimi anni hanno rafforzato le proprie leggi contro la criminalità informatica.

Probabilmente, una cyber guerra potrebbe giocare il ruolo più importante in un intervento in Siria piuttosto che in qualsiasi altro conflitto. Tecniche di cyber attacchi anonimi potrebbero essere negabili, poco costose, sempre più efficaci e relativamente prive di rischi, certamente in termini di fatalità da parte di chi lancia l'offensiva. Tali peculiarità rendono questa opzione estremamente appetibile in un panorama così complesso e caratterizzato da una situazione di stabilità precaria.

Come per altre forme di operazioni clandestine, è probabile che da qualche tempo siano state avviate attività preparatorie alla cyber war. Le attività di tipo cyber potrebbero essere utilizzate sia per la raccolta di informazioni, che per la distruzione attiva di obiettivi militari e governativi.

A titolo di esempio, il virus informatico denominato **Flame**, che è stato lanciato in primo luogo contro l'Iran, ha conseguentemente infettato i sistemi informatici appartenenti anche ad altri Paesi del Medio Oriente, tra cui la Siria. Il virus Flame può essere attivato anche per penetrare e controllare sistemi di computer infettati, raccogliendo informazioni riguardo dati di registrazione delle intercettazioni su apparecchiature audio e fotocamere, oppure dati di monitoraggio. Un intervento attivo di tipo cyber potrebbe essere focalizzato allo sfruttamento di eventuali debolezze dei sistemi informatici appartenenti alla Difesa siriana (quasi tutti di provenienza Russa), per agevolare attacchi fisici tradizionali, disabilitando ad esempio i sistemi di Comando e Controllo C2, le reti di difesa aerea, i sistemi d'arma computerizzati e le comunicazioni.

Tali operazioni offensive possono produrre effetti anche sulle dotazioni logistiche dell'esercito siriano, pur risultando meno vulnerabili in quei sistemi moderni che sono prerogativa degli eserciti più avanzati.

Al di là dell'arena militare, un attacco informatico potrebbe essere utilizzato per danneggiare le infrastrutture civili come radio e Tv, reti elettriche, reti finanziarie, linee aeree, trasporti e telecomunicazioni, mettendo in ginocchio l'intero sistema governativo e militare siriano.

In tutti i casi risulta opportuno, infatti, analizzare anche le capacità e le possibilità che sono a disposizione del governo siriano. In prima istanza occorre esaminare il potenziale effettivo di cui dispone il gruppo di attivisti denominato **Syrian Electronic Army**, attualmente tra i più attivi e pericolosi sulla scena dei cosiddetti "**hacktivist**".

Syrian Electronic Army non è un gruppo nuovo ad attacchi contro obiettivi americani e solo negli ultimi mesi ha caratterizzato le proprie azioni con numerose operazioni di hacktivism e di "social engineering" soprattutto ai danni di soggetti governativi, agenzie di stampa americane, come da ultimo, ad esempio, il famosissimo attacco lanciato contro il profilo Twitter dell'Associated Press, in conseguenza del quale, dopo aver annunciato una (finta) esplosione alla Casa Bianca e il ferimento di Obama, il Dow Jones ha avuto un crollo di 150 punti.

In Siria però non sta avvenendo luogo unicamente una sanguinaria repressione ma da settimane è in corso anche una guerra in Rete, che si dipana tra sofisticate campagne di attacchi con malware e attività di hacking, effettuate dal Syrian Electronic Army.

La cyber war in Siria è realtà ed è il volto virtuale della terribile guerra che si combatte per le strade e i quartieri.

CYBER REPRESSIONE, L'ULTIMA FRONTIERA DELLA CYBER WAR

Un articolo intitolato "**Syria's Online Conflict: The Hackers And Their Weapons**", scritto da **Tom Brewster** e pubblicato su Techweek, illustra qual è l'ultima frontiera della cyber war: la cyber repressione.

Esiste un nome che a un cittadino occidentale viene subito in mente appena si parla di cyber conflitto in Siria, ed è quello della Syrian Electronic Army. Ciò avviene perché molti dei suoi obiettivi sono stati media occidentali. Ciò ha colpito l'inconscio collettivo. Tuttavia la guerra online è in realtà vasta e complessa, e non si limita ad azioni di hacking. Alcuni attacchi hanno ramificazioni più profonde dei defacement e degli hijacks dei profili Twitter. Nel mese di luglio, per due giorni, è stato oscurato un sito Internet allestito per fornire ai siriani avvisi sugli attacchi dei missili Scud: il sito è andato in tilt non a causa di un disservizio, in un Paese dilaniato da una guerra civile, bensì è stato messo fuori uso da un massiccio attacco di tipo DDoS (Disributed Denial of Service). Il fondatore del sito, **Dlshad Othman**, ha dichiarato al giornalista di Techweek di aver bloccato manualmente gli indirizzi IP utilizzati come parte dell'attacco fra le 6 del pomeriggio del 9 luglio fino alle 4 della mattina seguente. In seguito ha dichiarato di essersi arreso, non potendo andare oltre.

Sul sito web **www.virtualroad.org**, appartenente a una società che offre servizi sicurezza IT per organizzazioni impegnate nella tutela dei diritti umani, è stato segnalato che sono stati sfruttanti ben 10.000 bot[1] nell'assalto al sito di **Aymta** (termine arabo il cui significato è "quando"), **www.aymta.com**. La maggior parte degli indirizzi IP sono provenuti da Stati che un tempo sono appartenuti all'ex Unione Sovietica, tra essi la Russia e l'Ucraina. Altri indirizzi IP individuati sono risultati ubicati in Iran. Othman ha espresso profonda certezza in merito al fatto che alcune nazioni possano aver sponsorizzato i DDoS. Inoltre sospetta che questi Stati abbiano sostenuto e sostengano tuttora il Presidente siriano **Bashar al-Assad**. Non avendo assistito ad attacchi di proporzioni simili, Othman ha poi sottolineato che, in virtù dell'esperienza acquisita nel settore IT, ha riconosciuto la tipologia di attacchi come provenienti da entità governative e non da piccole organizzazioni private. I DDoS, soprattutto in casi come quelli poc'anzi descritti, hanno un impatto profondo nel mondo reale.

Lanciato a fine giugno 2013, il sito aymta.com permette di selezionare fonti certificate in Siria per condividere informazioni sicure sui potenziali obiettivi dei missili Scud. Missili facilmente intercettabili, gli Scud hanno già causato centinaia di vittime, forse migliaia. I dati rilevati sulla minaccia proveniente dall'utilizzo di tali vettori sono poi inoltrati alla popolazione civile sotto forma di messaggi testuali su supporti telefonici mobili, email, Feed RSS, reti broadcast su canali televisivi satellitari oppure tramite trasmissioni radio-pirata non controllate dallo

[1] Bot: in gergo informatico, programma la cui funzione è di accedere alla Rete attraverso gli stessi canali utilizzati dagli utenti, talvolta simulandone anche le azioni.

Stato. Una mappa, inoltre, evidenzia le aree a rischio SCUD, in modo poter individuare le aree da evacuare poiché pericolose. Se s'interrompesse il servizio questo servizio di allerta, a causa di un DDoS, ciò non rappresenterebbe unicamente un attacco telematico: a fare la differenza è l'innalzamento del rischio di morte che si riverserebbe sulla popolazione. Othman, Ingegnere Sistemista con la passione per i diritti umani, ha rilevato che per ricevere gli aggiornamenti testuali oltre 3.000 cittadini siriani si sono registrati nei primi giorni di funzionalità del servizio web.

In Siria le vittime della guerra civile ammonterebbero a oltre cento mila, dunque è auspicabile che il servizio fornito da Aymta rimanga in funzione ancora a lungo, conservando la propria efficacia preventiva e che, anzi, si espanda quanto più possibile.

Secondo quanto dichiarato da **Tarek al-Jazairi**, consulente di new media per la **National Coalition of Syrian Revolution and Opposition Forces**, anche il sito web appartenente a quest'organizzazione, denominato etilaf.org, è stato oscurato da un attacco DDoS ed è rimasto offline per diversi giorni. Tarek al-Jazairi ritiene che molti indirizzi IP utilizzati negli attacchi siano provenuti da Russia e Iran, inoltre non escluderebbe perfino collegamenti con il DDoS sferrato contro Aymta. Poiché il sito diffonde informazioni per i sostenitori della rivoluzione contro Assad, non stupisce che possa facilmente rappresentare un obiettivo della cyber guerra.

Appare chiaro quindi che nell'era dei bit i DDoS rappresentano un'arma particolarmente efficace.

LE MODALITÀ DI ATTACCO DEL SYRIAN ELECTRONIC ARMY

A proposito invece del Syrian Electronic Army, ai relativi atti di mass defacement e hijack di Twitter, occorre chiarire che non sono solo gli attacchi DDoS a impensierire l'opposizione contro Assad. A metà giungo 2013, Citizen Lab ha rilevato due attacchi, uno di essi consistente in un codice malware inserito in un client VPN legittimo, detto Freegate, che l'opposizione utilizza per evitare lo snooping da parte del regime. Hacker infiltrati in gruppi privati all'interno di social media sono stati individuati mentre diffondevano software "**booby trap**", contenente un Trojan per l'accesso da remoto, in genere utilizzato in operazioni governative di cyber sorveglianza. In grado di effettuare un keylog, il Trojan poteva attivare le webcam delle vittime e trafugare file. Durante altre campagne anti-ribelli sono stati diffusi attacchi tramite email phishing, apparentemente indirizzate a membri dell'opposizione Siriana ma i cui link, una volta selezionati, trasmettevano i malware nei computer degli utenti. Il software era controllato da server situati in Siria, con indirizzo IP appartenente alla società **SyriaTel Mobile Telecom**. SyriaTel è un'azienda di telecomunicazioni posseduta da **Rami Makhlouf**, cugino del Presidente Bashar al-Assad, in precedenza messo in connessione con il Syrian Electronic Army. Altre campagne di attacchi malware sono state individuate nel corso del 2012, come quella operata tramite siti fasulli e finti aggiornamenti software coi quali veniva installato software malevolo nei computer di utenti ignari. Il sito web Syrian Malware attualmente traccia gli attacchi per impedire ai civili siriani e agli oppositori di essere vittima di trappole IT.

Un portavoce del Syrian Electronic Army ha spiegato che talvolta il gruppo utilizza malware tramite i quali inseriscono codice malevolo in alcune pagine web attendendo poi che siano visitate. In questo modo il malware è in grado di rilevare password e altre informazioni memorizzate nel computer dell'utente e provvede a trasmetterle a un sito appartenente al SEA. Tuttavia il portavoce ha negato la responsabilità del SEA per gli attacchi DDoS, che potrebbero invece essere attribuiti a gruppi affiliati. Nel 2011 il gruppo noto come Syrian Hackers School si è avvalso di un noto servizio di social network per disseminare strumenti software in grado di attuare azioni di Denial of Service (DoS), per attaccare siti di media. Il portavoce di SEA ha negato però il coinvolgimento del gruppo, adducendo che le accuse sono mosse da al-Jazairi della coalizione, in merito al fatto che il gruppo sarebbe finanziariamente supportato da Makhlouf, cugino di Bashar al-Assad e proprietario di SyriaTel, con ufficio a Dubai.

Sostenendo di avere base in Siria, un folto numero di volontari siriani appoggia SEA. In effetti non esiste un prova a conferma dell'esistenza di un collegamento tra SEA e il regime del Presidente, sebbene Bashar alAssad abbia espresso sostegno alle azioni del gruppo fin dal 2011. Gli attacchi informatici di SEA sono iniziati contro siti web, e gli account nei social network dell'opposizione, ma poiché apparivano obiettivi fantoccio, hanno iniziato ad attaccare i

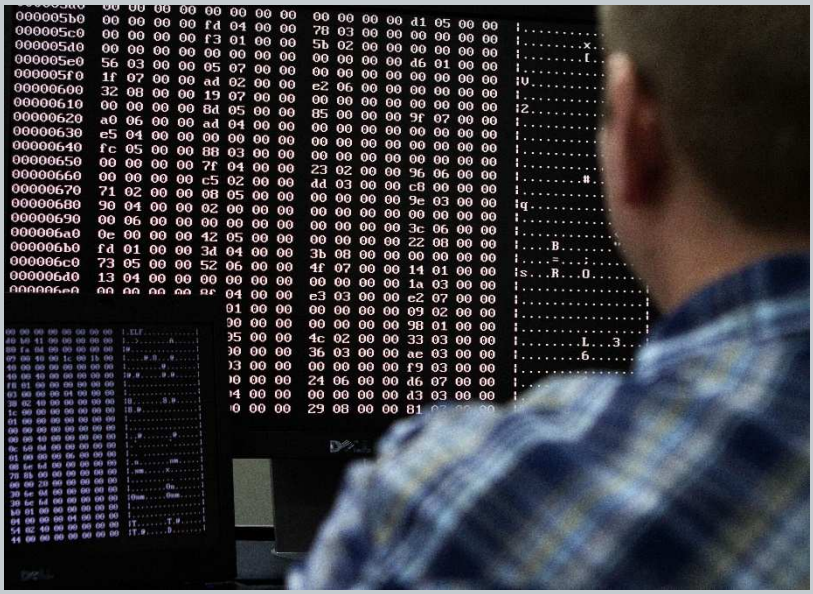
"mandanti", come lo Stato del Qatar, Arabia Saudita e gli Stati Uniti. L'attacco è stato poi condotto contro siti israeliani, a sostegno dei "fratelli palestinesi", e contro i media britannici.

Ogni settimana vengono compromessi account di social media e vengono portate a termine azioni di defacement di siti allo scopo di propagandare messaggi in aperto sostegno al presidente Bashar alAssad.

Il SEA appare favorito dal supporto di altri cyber gruppi (Yemen Hackers, Muslim Hackers, Arab Hackers For Free Palestine al Syrian Hackers School). SEA dice di non aver notato grandi azioni offensive messe in campo da parte degli oppositori. Un gruppo è Elektrony Nusra Front Army, che potrebbe avere affiliazioni con il fronte ribelle Al-Nusra, il quale si suppone sia molto legato ad Al Qaeda. Accusata del defacement ai danni della Syrian Commission on Financial Markets and Securities a inizio agosto 2013, già nel marzo dello stesso anno aveva operato contro il governo Russo.

Un altro gruppo è composto dai **Pirati di Aleppo**, che attualmente opera in Turchia, nei pressi dei confini con la Siria. Fondato da un ex appartenente del SEA, il gruppo lavora in parallelo con il collettivo denominato **Falcons of Damascus**. Leader dei Pirati di Aleppo è **Ahmed Hiedar**, che all'inizio del 2013 ha dichiarato al Global Post di aver disturbato la diretta delle trasmissioni della Tv di Stato per ben 13 volte, tramite attacchi hacker.

ATTI DI CYBER WAR E IL POTERE



Helmi Noman, Ricercatore Senior presso Citizen Lab, ha focalizzato l'attenzione sull'aspetto settario del cyber conflitto. Lo scisma fra Sciiti e Sunniti, nell'Islam, si riflette in Siria con la setta di Alawite Shi'ite del regime che si schiera contro i vari gruppi sunniti. L'identità ideologica dei combattenti è visibile nei messaggi pubblicati tramite i defacement dei siti oggetto di cyber attacchi. Nel settembre 2011, ad esempio, alcuni hacker si sono resi protagonisti di un defacement ai danni di un sito siriano dedicato al Grand Ayatollah Ali Khamenei, capo supremo dell'Iran e figura dell'establishment conservatore sciita. Helmi Noman ha sostenuto che il defacement è stato dedicato ai rivoluzionari del popolo siriano e ai martiri della Siria, ma soprattutto ha affermato che la Siria continua ad appartenere ad Ahl Al-Sunnah (termine arabo con cui si indica la comunità sunnita).

Altro tema chiave è il potere. Finché il regime controlla le infrastrutture critiche del Paese, i disservizi e i tilt saranno frequenti: se è vero che i black-out di Internet guadagnano le prime pagine, è anche vero che bloccano tutte le forme di comunicazioni elettroniche, causando grandi problemi agli oppositori. A tal proposito Noman ha sottolineato che il problema dei black-out elettrici sono gravi e impattano tutte le telecomunicazioni, non solo Internet.

Secondo Othman gli ISP (Internet Service Provider) sono collegati al governo e si comportano da "man-in-the-middle" nell'attività di snooping, mentre altri attacchi a livello di Rete sono frequenti. I governativi detengono il controllo sui contenuti, oltre che su Internet ma in tutti i media pertanto hanno la possibilità di sferrare e pilotare massicce campagne di propaganda contro i ribelli.

Nella cyber guerra in Siria il regime, nella Rete, ha il coltello dalla parte del manico.

Traduzione e adattamento dell'articolo "Syria's Online Conflict: The Hackers and their Weapons" scritto da Thomas Brewster, pubblicato su TechWeekEurope – Agosto 2013.

Fonte originale: http://www.techweekeurope.co.uk/news/syria-online-conflict-125652

L'AUTORE

Mario Avantini

Vicepresidente e membro fondatore del CISINT, è laureato in Scienze Politiche presso la Newark International University LLC, negli Stati Uniti. Inoltre possiede un Master in Sicurezza e Intelligence conseguito presso l'Università Internazionale di Scienze Sociali di Mantova. È analista di Studi Strategici. Ha conseguito la qualifica di consulente esperto CBRN presso la Scuola Interforze del Ministero della Difesa e ha partecipato al 31° corso COCIM in Cooperazione Civile Militare presso il Centro Alti Studi della Difesa. È tra gli autori di "Cyberworld" pubblicato da Hoepli, con il suo saggio "Oltre la grande muraglia: alleanze e tensioni". Ha effettuato docenze presso l'Università di Roma "Tor Vergata" nelle materie di sicurezza cibernetica e infrastrutture critiche. Ha frequentato un Master in Cyber Security organizzato dal Global Cyber Security Center e dalla Royal Holloway University of London. Svolge studi e ricerche nell'ambito della Sicurezza Cibernetica.

CISINT
Centro Italiano di Strategia e Intelligence

Via Clelia 45, 00181 - Roma

Tel/Fax: (+39) 06 7808035

Email: info@cisint.org

www.cisint.org