

L'analisi di C. Lepère, F. Droz, F. Langlet, J.-C. Marcoux, P. Bauer, intitolata *Stratégie de contre-offensive de Siemens suite a la crise politique iranienne de juin 2009* (Strategia di controffensiva di Siemens in seguito alla crisi politica iraniana del giugno 2009), illustra i diversi aspetti di una complessa guerra informativa, che ha avuto luogo tra i mesi di marzo e luglio del 2009, volta a destabilizzare il fornitore europeo di infrastrutture delle telecomunicazioni Nokia Siemens Networks (NSN).

Nokia Siemens Networks occupava allora il 2° e il 3° posto rispettivamente nei mercati delle infrastrutture telefoniche e della telefonia mobile. Il fatto che l'ha esposta agli attacchi informativi è rappresentato dalla vendita all'Iran nel 2007 di una rete a bande larghe, alcune stazioni d'ascolto e di decodifica dei contenuti e un sistema centralizzato di intercettazione e di sorveglianza delle comunicazioni telefoniche, internet, SMS e altri canali, che permetteva di controllare tutto il traffico delle comunicazioni in entrata e in uscita dal Paese oltre che all'interno del Paese stesso. Il destinatario e beneficiario di questo sistema era la Telecommunication Infrastructures Company, l'operatore nazionale iraniano detentore del monopolio del settore.

Nel periodo in questione, infatti, nel quadro delle elezioni iraniane e di feroci repressioni contro gli oppositori politici e i giovani nel Paese, la NSN e i suoi stakeholder sono stati pesantemente attaccati dai media occidentali come presunti alleati del regime iraniano, a causa della vendita della loro fornitura di una rete sofisticata e di tecnologia di monitoraggio.

Gli attacchi alla NSN, una joint-venture creata nel 2006, vanno visti in una prospettiva molto più ampia, ossia quella delle pesanti battaglie commerciali per la supremazia nel mercato delle infrastrutture delle telecomunicazioni. In questa lotta globale, dominata da aziende americane, gli europei si sono molto avvicinati al livello degli Stati Uniti e questo settore è diventato particolarmente sensibile alle pressioni politiche. Pertanto, le azioni contro Nokia sono state ampiamente sfruttate e amplificate da alcune istanze statunitensi.

L'azienda tedesca Siemens di fatto è stata oggetto di un attacco informativo organizzato, basato su un contesto storico e una congiuntura (la crisi iraniana) particolarmente favorevoli per gli aggressori. Tale orchestrazione è stata avviata in seguito al superamento di una soglia di tolleranza da parte di Siemens, in grado di

nuocere in maniera duratura agli interessi americani negli ambiti economico, geopolitico e geostrategico. Questa campagna offensiva è stata sostenuta dalla convergenza di azioni di diverse lobby, americane e non, che difendevano gli interessi economici americani e che, soprattutto, operavano a favore della strategia globale americana. Gli attori dell'operazione erano organismi associativi, di attivisti (sia gruppi organizzati sia singoli individui) tra i quali potevano militare anche gli oppositori iraniani in esilio.

La crescita di Siemens nel mercato internazionale è stata caratterizzata da una strategia di globalizzazione e dallo sviluppo di tecnologie avanzate, al pari di quelle degli Stati Uniti. Tuttavia, Siemens e Nokia Siemens Networks (NSN, una joint-venture tra Siemens e Nokia) sono state segnate da un'immagine sociale degradata e si sono trovate in un feroce contesto di rivalità economiche nel campo delle tecnologie sensibili, all'interno del quale, negli ultimi anni, Siemens è diventata uno degli attori principali, attirandosi l'invidia degli americani che hanno visto compromessi i propri interessi. In particolare, l'insediamento dell'azienda negli Stati Uniti, gli orientamenti assunti da NSN e la partnership con Microsoft hanno costituito una minaccia alla sicurezza degli Stati Uniti. Durante la crisi iraniana, la posizione di Siemens, attraverso NSN, è diventata il pretesto e l'elemento catalizzatore degli attacchi contro quest'azienda.

La guerra dell'informazione, scoppiata nel giugno 2009, è stata preceduta l'anno prima dalla comparsa sulla stampa austriaca di una notizia che riferiva l'esistenza di trattative tra la NSN e l'Iran, che si erano concluse con la vendita di tecnologie a Iran Telecom. Nell'aprile 2009 in un articolo del *Washington Times* emergeva il primo tentativo di destabilizzare le aziende europee presenti in Iran e negli Stati Uniti. Il 22 giugno 2009, dieci giorni dopo le elezioni presidenziali iraniane, scoppiò l'attacco mediatico sul *Wall Street Journal*, amplificato dalle reti sociali come Facebook, Twitter, ecc.

Tra gli attori che presero parte all'attacco informativo contro Siemens si trova innanzitutto l'Open Net Initiative (ONI), un gruppo di ricercatori delle università di Harvard, Oxford, Cambridge e Toronto, che nella primavera del 2009 annunciò in un rapporto che il sistema di Nokia Siemens Networks era pienamente operativo in Iran. Il gruppo di ricercatori aveva reso noto già nel 2005 che la rete

internet iraniana era stata sottoposta a un'azione di sorveglianza per mezzo di soluzioni tecniche prodotte dalle società Cisco Systems e Secure Solutions Corp. L'ONI sosteneva che queste tecnologie fossero state impiantate in Iran nel 2004-2005, sebbene fosse in vigore un embargo sulla loro esportazione.

Nell'aprile 2009 il giornale americano *Washington Times* rivelava per la prima volta il fatto che il regime iraniano aveva la possibilità di scovare gli oppositori del regime, in vista delle imminenti elezioni presidenziali, utilizzando la sofisticata attrezzatura venduta da Nokia Siemens Networks. Inoltre, l'articolo denunciava che un'azienda che possedeva numerosi contratti con il governo americano e dava lavoro a più di 70.000 persone negli Stati Uniti stava collaborando anche con regimi repressivi permettendo loro di spiare e incriminare i propri cittadini. L'articolo criticava anche il fatto che i governi europei non avessero il controllo sull'esportazione di materiale tecnologico a uso sia civile che militare.

Un altro attore importante nella vicenda è costituito dai cyber-attivisti europei, tra cui si distinse Erich Möchel, giornalista austriaco specializzato in nuove tecnologie. Quest'ultimo nell'aprile 2008 veniva citato in un articolo pubblicato dal *Jerusalem Post*, intitolato "German firm helps Iran monitor Israel" ("Un'impresa tedesca aiuta l'Iran a monitorare Israele"), in cui si sosteneva che Siemens e Nokia Siemens Networks avevano venduto le tecnologie per l'intercettazione all'Iran. Lo stesso Möchel, il 22 giugno 2009, rese accessibile sul suo sito *quintessenz.org* tutta la documentazione su Siemens e pubblicò articoli che la incriminavano, i quali furono poi ripresi dalla stampa tradizionale americana.

Lo stesso giorno, il 22 giugno, fu sferrato un ulteriore attacco a livello mediatico dal *Wall Street Journal*, che pubblicò un articolo accusatorio nei confronti del rapporto tra la NSN e l'Iran, seguito quattro giorni dopo da un'altro articolo in cui si presentava un progetto di legge americano volto a impedire alle imprese che fornivano tecnologie di sorveglianza all'Iran di entrare in affari con il governo americano. Questi articoli sono stati diffusi dalle reti sociali come Facebook, Twitter e YouTube.

Sempre il 22 giugno la CCIA (Computer & Communications Industry Association) reagiva all'articolo del *Wall Street Journal* denunciando l'utilizzo da

parte dell'Iran di sistemi di intercettazione del traffico su internet, fattore che minacciava la libertà di comunicare in rete. La CCIA, organizzazione internazionale senza scopo di lucro con sede negli Stati Uniti, rappresenta una buona parte degli industriali nel campo delle comunicazioni e dell'informatica, tra cui Google, Microsoft, Oracle Corporation, Yahoo e Sun Microsystems, e ha lo scopo di preservare il libero mercato, la competizione corretta e la libertà di navigazione su internet. La CCIA, molto attiva all'interno del Congresso in cui esercita azioni di lobbying per promuovere i propri obiettivi, ha anche chiesto al Dipartimento di Stato americano di includere la libertà di navigazione su internet tra i diritti umani.

Il giorno dopo l'articolo del *Wall Street Journal*, il 23 giugno 2009, l'ONG francese Reporters sans Frontières impegnata a favore della libertà di stampa, diffuse un articolo in cui si evidenziava la necessità di adottare una legislazione che permettesse alle imprese di informatica sia americane sia europee con sede in Paesi con regimi repressivi di eludere le misure che erano loro imposte dai governi locali. L'ONG denunciava che sia l'Iran sia la Cina potevano bloccare l'accesso all'informazione grazie al ricorso a tecnologie occidentali: il governo iraniano poteva farlo tramite i sistemi di Nokia e Siemens per filtrare il web e intercettare gli scambi di messaggi, mentre il Ministero cinese dell'Industria e della Tecnologia dell'informazione ricorreva all'installazione obbligatoria di un software di filtraggio su tutti i computer per contrastare la pornografia. L'unica azienda americana che si preoccupò degli effetti sulla libera circolazione dell'informazione provocati dal software del Ministero cinese fu Microsoft.

A due giorni di distanza dall'articolo del *Wall Street Journal*, Charles E. Schumer e Lindsey Graham, due senatori americani, proposero un progetto di legge che denunciava i traffici delle imprese occidentali con l'Iran nell'ambito del controllo delle telecomunicazioni. Il testo mirava a impedire alle imprese che commerciano con l'Iran di ottenere o di rinnovare i contratti esistenti con il governo americano.

Anche l'Unione Europea, per tramite di Viviane Reding, commissario responsabile dell'informazione e dei media, metteva in atto nel maggio 2009 una strategia volta a rinforzare la sua presenza a livello mondiale nel campo delle tecnologie dell'informazione nei confronti dell'America del Nord e dell'Asia.

Un altro fattore di attacco contro Siemens e NSN è rappresentato dal Global Online Freedom Act (GOFA), una proposta di legge studiata negli Stati Uniti che si ispirava al Foreign Corrupt Practices Act e mirava a impedire alle imprese americane di collaborare con Paesi retti da regimi repressivi che cercano di trasformare internet in un mezzo di censura e di controllo, ad assicurare il ruolo del governo americano di promozione della libertà di espressione su internet e a ristabilire la fiducia del pubblico nell'integrità delle imprese americane. Su iniziativa del senatore repubblicano Christopher Smith, questa proposta di legge è stata introdotta nella Camera americana dei rappresentanti con la nuova versione del 6 maggio 2009. Una versione europea del GOFA era stata presentata già nel luglio 2008 al Parlamento Europeo per iniziativa dell'eurodeputato olandese Jules Maaten (ALDE). Ispirata al modello americano, questa proposta di direttiva chiedeva alle imprese di assumersi le proprie responsabilità nei confronti dei principi della Dichiarazione universale dei diritti dell'uomo e le incitava in particolare a porre i propri server fuori dai Paesi con regimi repressivi.

Per uscire da questa situazione e lanciare la propria controffensiva Siemens e NSN avrebbero dovuto puntare a spostare l'attenzione dal proprio caso particolare e modificare lo scacchiere internazionale, sollevando su scala mondiale la problematica della regolamentazione delle vendite da parte delle imprese (occidentali e non) di sistemi sensibili verso Paesi non democratici. Dunque avrebbero dovuto presentarsi come alleato anziché come rivale degli Stati Uniti nella promozione di una regolamentazione comune volta a limitare la proliferazione degli strumenti di censura delle tecnologie dell'informazione e della comunicazione, soprattutto per gli Stati non democratici e/o che non rispettano le libertà individuali, e neutralizzare i vettori satellitari, salvo quelli istituzionali statunitensi, attraverso i cyber-libertari che in genere si oppongono a Siemens.

Per realizzare tale obiettivo una delle leve possibili cui ricorrere sarebbe stato il contrattacco sfruttando le contraddizioni della CCIA (vettori indiretti), in particolare la parzialità dell'azione di quest'ultima, obbligandola a rispettare i valori che è chiamata a difendere, indipendentemente dagli attori coinvolti. A tale proposito, si sarebbe potuta evidenziare la sua indifferenza di fronte alle due vicende che diedero luogo al dibattito sulle libertà individuali nell'utilizzo delle

telecomunicazioni e nella navigazione internet, ovvero l'installazione obbligatoria su tutti i computer cinesi del software di filtraggio imposta dal Ministero cinese dell'Industria e della Tecnologia dell'Informazione (intenzione notificata dal MIT cinese nel maggio 2009) e l'azione di sorveglianza a cui era sottoposta la rete internet iraniana grazie a soluzioni tecniche messe a punto da Cisco Systems e Secure Solution Corp (come aveva messo in evidenza l'Open Net Initiative già nel 2005).

La posizione della CCIA in questa vicenda è stata, infatti, di non-reaione. L'Associazione non si è mossa a sostegno del progetto di legge GOFA, sostenuto invece da alcuni senatori statunitensi e da deputati europei e diffuso da alcune organizzazioni come Reporters sans Frontières. Inoltre è stata criticata per non essersi impegnata a favore della necessità di protezione delle imprese occidentali (ovvero democratiche) contro l'obbligo implicito ma reale di consegnare avanzate tecnologie di sorveglianza ai regimi non democratici. Non si è impegnata, poi, a sviluppare gli interessi comuni a tutte le imprese occidentali e americane, al fine di fissare un quadro legale su scala mondiale, né a esercitare delle pressioni su Paesi stranieri che non rispettavano le regole del gioco per obbligarli a sottostare alla regolamentazione, in modo da fissarne una internazionale, con un'autorità di riferimento (come l'ONU o l'OMC).

Siemens, inoltre, nella propria controffensiva, avrebbe potuto fare leva sulla propria posizione negli Stati Uniti, ricorrendo al lobbying e a vettori diretti e indiretti, in particolare puntando sul suo legame con Microsoft e sui 70.000 posti di lavoro in territorio statunitense.

Diversi sarebbero stati i vettori o le casse di risonanza disponibili per Siemens/NSN: senatori americani promotori o comunque favorevoli alla legge GOFA; deputati europei sostenitori della stessa legge; il commissario europeo per la società dell'informazione e dei media; i governi europei; Microsoft e il suo impatto sulla CCIA e i rappresentanti americani; Reporters sans Frontières, movimenti associativi e blogosfera; i media tradizionali e specializzati.

Dunque, di fronte all'evidente orchestrazione dell'offensiva ai danni di Siemens a vari livelli (media, reti sociali e politica) che ha messo a repentaglio il successo dell'azienda con potenziali gravi conseguenze economiche e finanziarie,

rischio di danno dell'integrità della sua immagine e rischi di boicottaggio, sarebbe stato utile individuare i bersagli e i canali per un contrattacco che spostasse l'attacco subito su altri temi e altri target. In particolare, il bersaglio principale poteva senz'altro essere la CCIA, seguita dagli attivisti, dall'opinione pubblica mondiale e dal gruppo Murdoch per quanto riguarda l'informazione.

L'attacco alla CCIA sarebbe potuto avvenire costringendo quest'ultima ad adottare una posizione netta e chiara in merito alla recente legislazione sui sistemi IT di controllo venduti a governi stranieri. Con una tale controffensiva, probabilmente sarebbe stato possibile porre fine alla discriminazione nei confronti degli attori europei quali Siemens e ottenere una situazione più equilibrata, con le stesse normative valide per tutti, americani ed europei, e proteggere le imprese europee dalle richieste di governi non democratici, soprattutto per quanto riguarda i sistemi di monitoraggio. Come conseguenza di tutto ciò, i difensori delle cyber-libertà e i cyber-attivisti che sferrano continue campagne contro Siemens sul web sarebbero stati neutralizzati e il flusso di attacchi informativi contro Siemens si sarebbe arrestato sul breve, medio e lungo periodo.