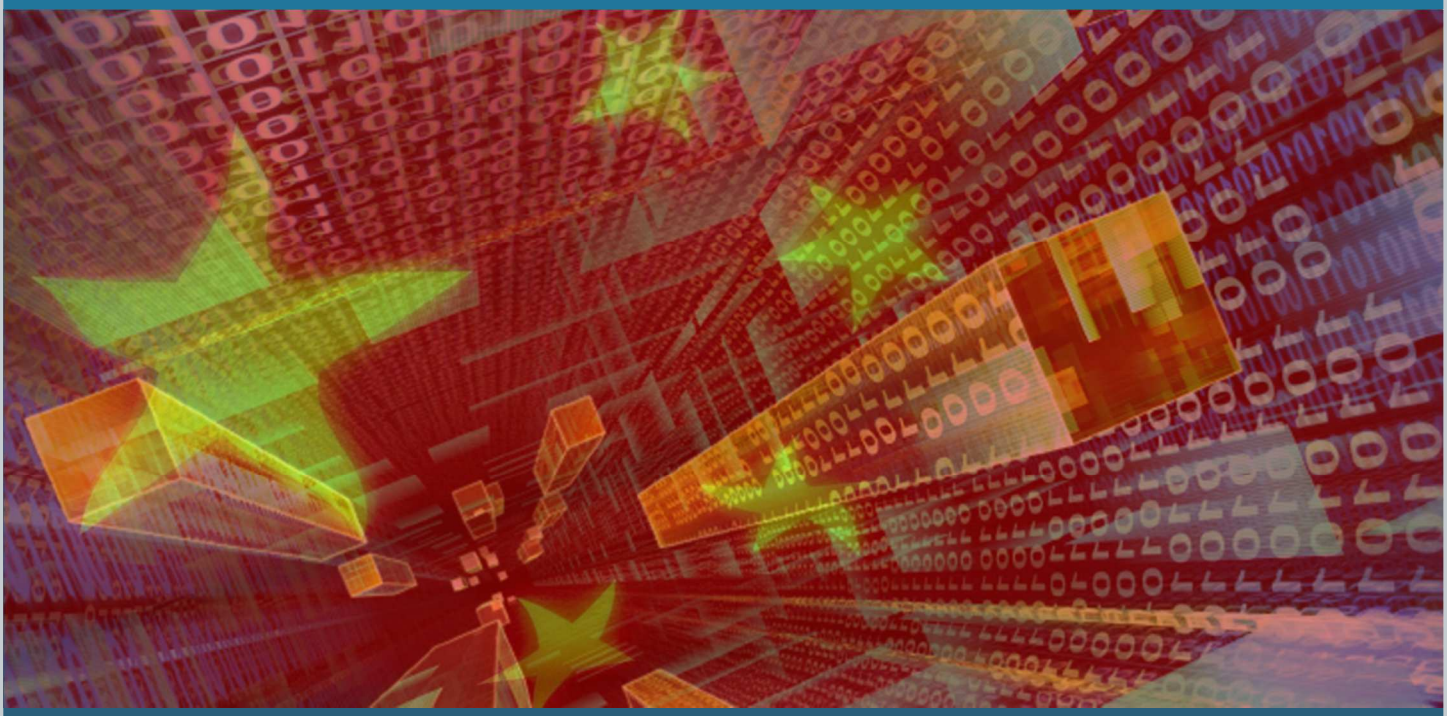
05|2012



LA CINA E IL PENSIERO STRATEGICO DEL CYBERSPACE

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

L'APPROCCIO DELLA CINA AL CYBERSPACE

L'ultimo decennio è stato caratterizzato dal moltiplicarsi di minacce informatiche o, almeno, come un periodo di crescente timore e crescente convinzione per quanto riguarda l'insicurezza informatica. Il cyberspazio è diventato un panorama importante: esperti e governi ammettono che le infrastrutture critiche, nelle quali sono compresi i sistemi di distribuzione acqua, elettricità, petrolio e gas per citarne alcuni, sono soggetti ad attacchi informatici. Alcune più sorprendenti questioni emerse sono quelle riferite a infiltrazioni cinesi e russe nella rete elettrica degli Stati Uniti.

- Nel 2009 le compagnie petrolifere americane Marathon Oil, Exxon Mobil e Conoco Philips sono state gli obiettivi di attacchi informatici. Da indiscrezioni raccolte tali eventi risultano essere stati atti di spionaggio compiuti da hacker cinesi;

- Nel febbraio 2010, la EU ETS - Emission Trading Scheme dell'Unione Europea è stata vittima di attacchi informatici fraudolenti. I registri di 13 Paesi europei sono stati costretti a chiudere;

- Nel 2003, ad esempio, un worm è penetrato in un computer della centrale nucleare Devis Besse ad Oak Harbor in Ohio, riuscendo a disabilitare il sistema di monitoraggio della sicurezza.

Altre tipologie di attacchi possono consistere in **intrusioni nei sistemi di rete**, **attacchi DDoS (Distributed Denial of Service)**, **Botnet** (una rete composta da molteplici computer infettati da malware e collegati a Internet, controllati da un'unica entità, per scagliare attacchi informatici), **sabotaggio di apparecchiature attraverso il cyberspazio**, **furti di dati personali** ecc.

In reazione a tali episodi, sempre più frequentemente i sospetti che emergono si concentrano sulla Repubblica Popolare Cinese (l'Esercito di Liberazione Popolare, Pechino, il governo e i suoi hacker) la quale è accusata di essere l'origine da cui sono provenuti gli attacchi informatici più importanti. La Cina ha dimostrato la propria intenzione di assurgere al ruolo di player dominante a livello internazionale nei settori dell'informazione e della cyber war. L'information war comporta l'attuazione di azioni volte a conquistare una posizione di superiorità in virtù delle informazioni ottenute, rispetto all'avversario. Tali azioni possono essere rivolte verso processi informativi, sistemi informativi e reti basate su computer, ostacolando al contempo gli avversari, eventualmente impegnati nel porre in atto le medesime procedure di raccolta informativa.

Più di 20 anni fa, la Cina ha iniziato a pubblicare le proprie teorie, le politiche e le strategie in materia di utilizzo sia difensivo che aggressivo nel cyberspazio.

Recentemente uno studente della Facoltà di Ingegneria dei Sistemi, presso la DUT - Dalian University of Technology in Cina, ha pubblicato un documento di ricerca dal titolo "Cascade-Based attacco alle vulnerabilità della rete elettrica degli Stati Uniti"[1], nel quale è proposta una comparazione degli effetti risultanti da due differenti attacchi al network elettrico statunitense.

Diversi esperti e giornalisti americani hanno analizzato il documento, interpretandolo come una nuova dimostrazione delle motivazioni offensive della Cina contro le infrastrutture critiche e anche come prova del coinvolgimento della Cina stessa in una nuova corsa agli armamenti nel cyberspazio.

Va specificato che in questo contesto i termini "cyber" e "cyberspazio", esattamente come avviene in Russia, ad esempio, non sono molto utilizzati nella Repubblica Popolare Cinese, nella quale si predilige il suffisso "info-" per "informatico" (mentre in Russia si tende a utilizzare l'aggettivo "electronic").

L'approccio della Cina alla guerra informatica consiste nell'attività di "controllo" che rimane una parte principale della filosofia cinese. Controllare la rete Internet ha un duplice vantaggio: **militare** e **civile**.

[1] http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/wang.pdf

LA DIMENSIONE MILITARE

Il successo folgorante degli Stati Uniti nella prima Guerra del Golfo è stato interpretato da esperti militari internazionali come la vittoria delle nuove tecnologie. Secondo questo modello, il possesso di una posizione dominante nell'ambito delle tecnologie dell'informazione ha permesso di ottenere il controllo totale sul campo di battaglia. Ciò ha rappresentato la chiave per il successo militare, la vittoria e il potere. L'epilogo di quest'evento militare ha indotto le forze armate cinesi a intraprendere una trasformazione radicale al proprio interno. Un tale processo, seguito da una trasformazione della dottrina cinese, ha guidato gli affari militari di questo Paese verso nuove strategie. Già dal 1990 l'esercito cinese ha attuato un programma di modernizzazione guidato dal concetto di "***Informatization***" (traducibile nel dominio sulle tecnologie dell'informazione e il cyberspazio).

Tenendo conto della sostituzione del suffisso "cyber" con "information", nel marzo 2006 la Cina ha rilasciato una pubblicazione intitolata "The State Informatization Development Strategy (2006-2020)"[2], ovvero una strategia per lo sviluppo di un cyberspazio nazionale, da compiersi in un periodo di quattordici anni. Tra gli obiettivi principali che compongono questa strategia vi sono:

1. La creazione di una struttura cibernetica nazionale;
2. Il rafforzamento delle capacità per l'innovazione indipendente di tecnologie informatiche;
3. L'ottimizzazione della struttura relativa all'industria informatica;
4. Il miglioramento della cybersicurezza nazionale;
5. Il compimento di progressi effettivi nel costruire una società e un'economia nazionale orientata al cyberspazio;
6. L'accelerazione della "informatizzazione" sociale, fattore questo molto importante col quale si ridurrebbe drasticamente il fenomeno del cosiddetto "digital divide", ovvero il gap tecnologico e di capacità informatiche all'interno della società.

[2] http://www. gov.cn/gongbao/content/ 2006/content_315999.htm

Nel 1995 il **Generale Wang Pufeng**, considerato il padre della dottrina cinese per la guerra dell'informazione ne aveva illustrato alcuni concetti chiave:

- L'information war può essere condotta in tempo di pace, crisi e guerra;
- L'information war consiste in operazioni offensive e difensive;
- Le componenti principali dell'information war sono Comando e Controllo (C2), Intelligence, Guerra Elettronica, Guerra Psicologica, Cyber War e Guerra Economica.

Nel febbraio 1999 i **Colonnelli Qiao Liang** e **Wang Xiangsui**, con la pubblicazione del loro libro "La guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione"[3], sottolineano che "... il processo tecnologico ci ha dato i mezzi per colpire direttamente il centro nevralgico del nemico senza danneggiare le altre cose, dove il modo migliore è quello di controllare e non di uccidere".

Questa forma di guerra moderna, denominata "guerra senza restrizioni", rappresenta il fatto che le armi e le tecniche sono molteplici e che il campo di battaglia ormai è ovunque. In breve essi sottolineano che "... il campo di battaglia è accanto a noi e il nemico è in rete", inoltre aggiungono che "... la guerra dell'informazione è la guerra in cui viene utilizzato il computer per ottenere o distruggere le informazioni".

Dalla metà degli anni novanta, in Cina diversi centri di addestramento militare forniscono programmi di formazione sulla cyber war rivolti al personale già attivo. Dal 1997 i media internazionali hanno segnalato un gran numero di esercitazioni di cyber war condotte dalle forze militari di questo Paese. Suddette esercitazioni dimostrano il passaggio dalla teoria della information war alla pratica. Le reali capacità di information war e di cyber war rimangono attualmente sconosciute.

Qualsiasi siano le capacità acquisite, la Cina ha conquistato superiorità e potere nella dimensione cibernetica, ambito questo divenuto strategico per il Paese. L'obiettivo è quello di essere in grado di prevalere sull'avversario con l'ausilio delle informazioni (information warfare, cyber war) prima del 2050.

Internet diventerà il luogo in cui si verificherà una corsa agli armamenti. Nel 2003 il Comitato appartenente alla Commissione Centrale Militare del Partito Comunista Cinese ha approvato il concetto di "***Three Warfares***" che appartiene all'ambito delle "information operations" e comprende:

[3] Testo originale: "Unrestricted Warfare", Qiao Liang e Wang Xiangsui - Beijing: PLA Literature and Arts Publishing House, febbraio 1999

1. La guerra psicologica;

2. La guerra dei media (che influenza l'opinione pubblica sia a livello nazionale che internazionale);

3. La guerra legale (con la quale si utilizzano gli strumenti del diritto nazionale e internazionale per ottenere il sostegno delle comunità internazionali)[4].

Per quanto riguarda quest'ultimo aspetto, la Cina è stata accusata di aver condotto attacchi informatici, ad esempio, contro le reti elettriche degli Stati Uniti (2009), come precedentemente indicato. Tuttavia Pechino nega ogni accusa di illecito e utilizza i media internazionali per divulgare la propria versione dei fatti, appellandosi alla cooperazione internazionale per il contrasto alle minacce informatiche. Ulteriormente, la Cina utilizza il cyberspazio per proclamarsi "vittima", denunciando la divulgazione di tali accuse contro il proprio Paese e ricordando alla Comunità Internazionale che la Repubblica Popolare Cinese dispone di un quadro legale contro la criminalità informatica.

[4] "The Chinese Army Today: Tradition and Transformation for the 21st Century", Dennis J. Blasko – Routledge, febbraio 2012

LA DIMENSIONE CIVILE

La Cina sviluppa le proprie capacità militari in stretto rapporto con l'industria privata e il mondo accademico, attuando politiche finalizzate alla promozione di un collegamento tra il settore pubblico e privato, oltre che tra quello civile e militare. Questo fenomeno può essere osservato in un gran numero di altri Paesi industrializzati.

Alcune fonti suggeriscono l'esistenza di legami tra sostenitori dell'Esercito di Liberazione Popolare e la comunità di hacker. La "Relazione annuale sulla potenza militare della Repubblica Militare Cinese" del 2003 fa riferimento ai pericoli inerenti alla pirateria informatica nazionalista (***hacktivism***) durante i periodi di crisi.

Tra le numerose azioni attribuite agli hacker cinesi, si possono citare: le ondate di attacchi informatici che si sono verificate a seguito del bombardamento dell'Ambasciata Cinese da parte delle forze appartenenti alla NATO a Belgrado nel 1999, gli attacchi contro gli interessi di Taiwan, le aggressioni contro i siti web ufficiali degli Stati Uniti in segno di protesta contro la collisione tra un caccia cinese e un aereo spia statunitense avvenuta nel 2001, gli attacchi contro i siti web tibetani. Ancora, nel 2008 è avvenuta la violazione del sito Internet dell'Ambasciata francese in Cina, successivamente all' incontro tra il Dalai Lama e il Presidente francese Nicolas Sarkozy.

L'elenco degli attacchi degli ***hacktivisti*** è esteso. La guerra dell'informazione cinese è principalmente dedicata alla gestione dei rapporti di potere con il mondo esterno ma tutto ciò può essere applicato anche nell'ambito dei propri confini: le informazioni e la superiorità nel cyberspazio è una questione di potere in Cina. Tuttavia, negli ultimi anni il progresso tecnologico ha svolto il ruolo di "guastafeste". I social network (in particolar modo Twitter e

Facebook) sono diventati i nuovi attori e strumenti nel panorama politico nazionale e internazionale. Nell'agosto 2009 un articolo pubblicato sul sito web cinese CE News, ha descritto Twitter e altri social network come una nuova arma utilizzata per la sovversione culturale e per l'infiltrazione politica del Paese.

RIFLESSIONI CONCLUSIVE

Occorre volgere un'attenta riflessione sulle infrastrutture critiche, proprio dove la risoluzione delle relative criticità rappresenta una questione di primaria importanza. Con il crescente utilizzo di energia elettrica, telefono, benzina, gas e prodotti alimentari importati, il fattore di dipendenza da una tecnologia sconosciuta è molto ampio. Il cyber spazio è diventato un sistema vulnerabile, un sistema che la Cina ha dimostrato di saper utilizzare abilmente anche in tempo di pace, per acquisire maggior potere nel mondo globalizzato.

Le politiche sviluppate dal Governo cinese ufficialmente sono a carattere difensivo e non suggeriscono alcuna linea offensiva in tempo di pace (come un attacco informatico che potrebbe essere interpretato come un vero e proprio atto di guerra da parte di chi ne è rimasto vittima).

Le autorità di Pechino condannano ufficialmente tutte le forme che può assumere il crimine informatico ma sono altrettanto note le grandi capacità offensive tecnico/teorico/dottrinali possedute dalla Cina nell'ambito della cyber war. Tuttavia, l'esistenza di una evidente strategia non fornisce sufficienti elementi schiaccianti per attribuire attacchi informatici al gigante asiatico. Ciò si riflette anche nel modo in cui nelle sedi internazionali la RPC affronta la questione della cybersecurity e, soprattutto, l'internet governance, tentando di creare un ombrello internazionale di norme e regole per gestire meglio il cyberspazio globale. Però allo stesso tempo il Paese utilizza, come già detto, un vocabolario unico e un regime di censura e controllo dei contenuti su tutto il proprio territorio.

In ogni caso la difficile individuazione dei responsabili delle aggressioni informatiche rende altrettanto ostico attribuire l'azione a un Paese piuttosto che a un altro. E anche basandosi su fattori di analisi rilevanti, occorre tenere in considerazione che la Cina è solo uno fra i molti Paesi dotati di capacità di cyber war e modelli teorici per l'information war. Diversi rapporti affermano che più di 120 Paesi possiedono tali peculiarità: **un attacco informatico rilevante potrebbe essere perpetrato da un attore all'interno di uno Stato, da qualsiasi hacker ma anche da qualsiasi Paese del mondo**.

Citando quanto ha affermato un alto funzionario dell'Intelligence americana, in un articolo pubblicato nel 2009, "i cinesi hanno cercato di mappare infrastrutture elettriche di alcuni Paesi, lo stesso hanno fatto i russi. Occorre avere molta cautela, concentrando la nostra attenzione sulla fonte cinese, riguardo attacchi informatici, ciò potrebbe impedire la visualizzazione del nuovo ambiente strategico globale. Il rischio è quello di ignorare le minacce provenienti da altre nazioni. Di due cose però possiamo avere la certezza: da una parte vi sono Stati come l'Iran che si ispirano alla Cina per quanto riguarda la politica interna e nella strategia dell'attacco a sorpresa come strumento per far percepire le proprie capacità, dall'altra ci sono Paesi come gli Stati Uniti che invece vogliono abbracciare la volontà internazionale della Repubblica Popolare per evitare di avere un nuovo nemico nel cyberspazio".

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