LA CINA E IL PENSIERO STRATEGICO DEL CYBERSPACE

di Mario Avantini

L'ultimo decennio è stato caratterizzato dal moltiplicarsi di minacce informatiche o, almeno, come un periodo di crescente paura e crescente convinzione per quanto riguarda l'insicurezza informatica. Il cyberspazio è diventato un panorama importante; esperti e governi ammettono che le infrastrutture critiche, che comprendono i sistemi di distribuzione acqua, elettricità, petrolio e gas - per citarne alcuni -, sono soggetti ad attacchi informatici. Alcune questioni più sorprendenti 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 tali azioni risultano essere spionaggio compiute da hacker cinesi.

- Nel febbraio 2010, la 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, a esempio, un worm penetrò in un computer della centrale nucleare Devis Besse e disabilitando il sistema di monitoraggio della sicurezza.

Altri attacchi includono intrusioni nei sistemi di rete, attacchi DDoS (Distributed Denial of Service), Botnet (rete formata da computer collegati ad Internet e infettati da malware, controllata da un'unica entità per scagliare attacchi), sabotaggio apparecchiature attraverso il cyberspazio, furti di dati personali ecc.

Sempre più spesso, i sospetti che stanno emergendo si concentrano sulla Cina (l'Esercito di Liberazione Popolare, Pechino, il governo, i suoi hacker) accusandola di essere l'origine degli attacchi informatici più importanti. La Cina ha dimostrato la sua intenzione di diventare un player leader a livello internazionale nei settori dell'informazione e della *cyber war*. L'*information war* comporta l'intraprendere azioni per ottenere la superiorità delle informazioni rispetto all'avversario, azioni rivolte verso processi informativi, sistemi informativi e reti basate su computer, negando nel contempo, la capacità degli avversari di fare lo stesso.

Più di 20 anni fa, la Cina ha iniziato a pubblicare le sue teorie, le politiche e le strategie in materia di utilizzo sia difensivo che aggressivo nel cyberspazio. Recentemente uno studente presso l'Istituto di Ingegneria dei sistemi di Dalien della University of Tecnology in Cina ha pubblicato un documento di ricerca dal titolo " Cascade-Based attacco alle vulnerabilità della rete elettrica degli Stati Uniti". Diversi esperti americani e giornalisti hanno analizzato il documento come una nuova dimostrazione delle motivazioni offensive della Cina contro le infrastrutture critiche e anche come prova del coinvolgimento della Cina in una nuova corsa agli armamenti nel cyberspazio. Premetto che in questo caso, la parola "cyber" o "cyberspazio", esattamente come avviene in Russia, ad esempio, non sono molto usate nella Repubblica Popolare, nella quale si predilige il suffisso "info-" per "informatico" (mentre in Russia si tende ad usare l'aggettivo *electronic*).

L'approccio della Cina alla guerra informatica è "il controllo" che rimane una parte principale della filosofia cinese. Controllare la rete internet ha un duplice vantaggio: **civile** e **militare**;

LA DIMENSIONE MILITARE

Il successo folgorante degli Stati Uniti nella prima guerra del golfo è stata interpretata da esperti militari nel mondo come la vittoria delle nuove tecnologie. Secondo questo modello, la posizione dominante delle tecnologie dell'informazione ha fornito il controllo totale sul campo di battaglia ed è stata la chiave per il successo militare, la vittoria e il potere. Questa conclusione ha richiesto una trasformazione radicale all'interno delle forze armate cinesi. Tale concetto e la seguente trasformazione della dottrina cinese ha guidato gli affari militari cinesi a nuove strategie. Già dal 1990 l'esercito cinese ha attuato un programma di modernizzazione guidato dal concetto "Informatization" (che si traduce come un dominio sulle tecnologie dell'informazione e il cyberspazio). Tenendo conto della sostituzione del suffisso "cyber" con "information", nel 2006 la Cina pubblicò la "2006-2020 State Informatization Development Strategy", ovvero una strategia per lo sviluppo di un cyberspazio nazionale, da compiersi in un periodo di quattordici anni. Tra i punti 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 dell'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 e soprattutto (6) l'accelerazione della "informatizzazione" sociale, chiudendo il cosiddetto "digital divide", ovvero il gap tecnologico e di capacità informatiche all'interno della società.

Nel 1995 il Generale Wang Pufeng, considerato il padre della dottrina cinese di guerra dell'informazione aveva illustrato alcuni concetti chiave di tale dottrina :

- 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, intelligence, guerra elettronica, guerra psicologica, *cyber war* e guerra economica.

Nel 1999, i Colonnelli Qiao Liang e Wang Xiangsui nel loro libro " La guerra senza restrizioni" 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 chiamata "guerra senza restrizioni" significa che le armi e le tecniche sono ormai molteplici e che il campo di battaglia è ormai dappertutto. In breve essi sottolineano che "il campo di battaglia è accanto a noi e il nemico è in rete", e aggiungono, "la guerra dell'informazione è la guerra in cui viene utilizzato il computer per ottenere o distruggere le informazioni".

Diversi centri di addestramento militare in Cina forniscono programmi di formazione sulla *cyber war* per il personale militare già attivo ~~e~~ dalla metà degli anni novanta. Dal 1997 i media internazionali hanno segnalato un gran numero di esercitazioni di *cyber war* condotte dalle forze militari. Le 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 divenuto strategico per il Paese. L'obiettivo è quello di essere in grado di vincere l'avversario con l'ausilio delle informazioni (*information war*fare, *cyber war*) prima del 2050.

Internet diventerà il luogo di una corsa agli armamenti. Nel 2003, il Comitato della Commissione Centrale Militare del Partito Comunista Cinese ha approvato il concetto di "Three warfare" che comprende 1 _ la guerra psicologica; 2_ la guerra dei media (che influenza l'opinione pubblica sia a livello nazionale che internazionale); 3_ la guerra legale (che è quella di utilizzare gli strumenti del diritto nazionale e internazionale per ottenere il sostegno delle comunità internazionali).

Per quanto riguarda quest'ultimo aspetto, la Cina è stata accusata di aver condotto attacchi informatici, per esempio, contro le reti elettriche degli Stati Uniti (2009); tuttavia Pechino nega ogni accusa di illecito e utilizza i media internazionali per dare la propria versione dei fatti e appellandosi alla cooperazione internazione per il contrasto alle minacce informatiche. Di più: la Cina utilizza il cyberspazio per proclamarsi come "vittima" denunciando la fabbricazione 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.

LA DIMENSIONE CIVILE

La Cina sviluppa le sue capacità militari, in stretto rapporto con l'industria privata e il mondo accademico, mettendo in pratica politiche di promozione per il collegamento tra il settore pubblico e privato e tra quelli civili e militari. 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. Molte azioni sono attribuite agli hacker cinesi; ondate di attacchi informatici si sono verificate a seguito del bombardamento dell'Ambasciata Cinese da parte delle forze della Nato a Belgrado nel 1999; gli attacchi contro gli interessi di Taiwan; 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; attacchi contro i siti web tibetani; nel 2008 la violazione del sito dell'Ambasciata francese in Cina avvenuta successivamente all' incontro tra il Dalai Lama e il Presidente francese Nicolas Sarkozy. L'elenco degli attacchi degli hacktivisti è lungo. 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 suoi 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 (Twitter, Facebook) sono diventati i nuovi attori e strumenti nel panorama politico Nazionale e Internazionale. Nell'agosto del 2009 un articolo pubblicato sul sito web cinese Cenews, ha descritto Twitter e altri social network come una nuova arma utilizzata per la sovversione culturale e per l'infiltrazione politica del Paese.

Un'attenta riflessione va fatta sulle infrastrutture critiche dove la risoluzione delle loro 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 grande. Il cyber spazio è diventato un sistema vulnerabile, sistema che la Cina ha dimostrato di saper ben usare in tempo di pace, gestendo abilmente lo strumento ai fini di acquisire maggior potere nel mondo globalizzato. Le politiche sviluppate dal Governo cinese sono ufficialmente quelle difensive e non suggeriscono alcuna offensiva in

tempo di pace come un attacco informatico che potrebbe essere considerato come un atto di guerra da parte di chi ne è rimasto vittima.

Le autorità di Pechino condannano ufficialmente tutte le forme di crimine informatici, ma è sono altrettanto note le grandi capacità offensive tecnico/teorico/dottrinali della Cina nel campo della *cyber war*. Tuttavia, l'esistenza di una evidente strategia, non fornisce sufficienti argomenti per attribuire attacchi informatici al gigante asiatico. Questo si riflette anche nel modo in cui la RPC affronta nelle sedi internazionali la questione della cybersecurity e, soprattutto, per quanto riguarda l'internet governance, tentando di creare un ombrello internazionale di norme e regole per gestire meglio il cyberspazio globale. Ma allo stesso tempo utilizza, come già detto, un vocabolario unico e un regime di censura e controllo dei contenuti a livello nazionale.

In ogni caso la difficile individuazione dei responsabili delle aggressioni informatiche rende altrettanto ostico l'attribuire l'azione a un Paese piuttosto che a un altro. E anche basandosi su analisi la Cina è solo una fra i molti Paesi che hanno capacità di *cyber war* e modelli teorici per l'*information war*. Diversi rapporti affermano che più di 120 paesi hanno tali capacità, un attacco informatico rilevante potrebbe essere perpetrato da un attore all'interno, da qualsiasi hacker, da qualsiasi paese del mondo. Secondo un alto funzionario dell'intelligence americana, citato in un articolo pubblicato lo scorso 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".

Riferimenti :

Brian M. Mazanec - "The Art of Cyber War"

Benjamin A. Shobert - "China's capacity for cyber-war"

Daniel Ventre – "Infowar"