Oltre la grande muraglia, alleanze e tensioni.

di Mario Avantini

In questo periodo il Cyber spazio è in pieno fermento: l'attenzione internazionale si concentra sulla politica iraniana, soprattutto per ciò che concerne le relazioni con il mondo occidentale. È opinione degli analisti che l'Iran potrebbe rappresentare una seria minaccia nel Cyber spazio, un dominio in cui Teheran ha grandi possibilità di affrontare il «nemico» americano. Un tema, questo, che potrebbe distogliere l'attenzione interna dalle sanzioni e dal crescente dissenso contro l'amministrazione centrale. I conflitti interni hanno creato numerosi problemi all'Iran che nell'ultimo anno ha investito molto nel web e in particolare nei sistemi di monitoraggio con l'intento di controllare e isolare le infiltrazioni esterne. La sorveglianza del web è diventata in breve tempo una priorità per l'Iran che potrebbe contare sulla collaborazione della Cina, una delle nazioni ad avere una maggiore esperienza nel campo del monitoraggio dei media. Con la comparsa della Cyber arma «stuxnet», che ha colpito il programma nucleare iraniano, improvvisamente Teheran si è resa conto di essere vulnerabile a questo tipo di attacchi i quali, per essere arginati, hanno richiesto un immediato impegno nel Cyber spazio di investimenti cospicui in tecnologie e la creazione di un «Cyber esercito» composto da esperti addestrati alla guerra informatica.

Ma nel mondo globalizzato altre battaglie sono emerse. Nell'ultimo mese è stata registrata un attività sorprendente che oppone la Cina e le Filippine con continui e reciproci attacchi a suon di byte. L'impegno cinese nel Cyber spazio non è una novità, la nuova sorpresa è l'approccio aggressivo del Cyber esercito filippino, che ha deciso di misurare le proprie capacità con il gigante Cinese. L'origine della battaglia sarebbe una disputa territoriale sull'isola Spratlys e Shoal Scarborough. La Cina, con il pretesto di proteggere i suoi pescatori e rivendicare l'esclusività della pesca nelle zone vicine al paese, cela il suo vero interesse, sconfinare nei campi petroliferi *off-shore*. Prima dello scorso 20 aprile non si erano mai registrati attacchi, improvvisamente un gruppo di hacker cinesi hanno preso di mira l'Università delle Filippine deturpando il sito web con una mappa con caratteri cinesi, che riproducevano il Shoal Scarborough. L'evento ha scatenato una serie di attacchi reciproci, il governo di Manila è convinto che aggressioni simili potrebbero avere un effetto critico sul rapporto difficile con la Cina compromettendo ogni dialogo diplomatico. Proprio l'Asia Pacifc è tra quelle regioni dove ci sono le principali preoccupazioni per una guerra militare e Cyber. La tensione storica è tra le due Coree, nonostante la corsa agli armamenti, non sfocerà in un conflitto sul campo: gli esperti sono convinti che la Corea del Nord adotterà una strategia diversa contro la Corea del Sud, non utilizzerà armi convenzionali, ma aumenteranno le operazioni offensive nel Cyber spazio.

Kim Jong Dae capo redattore della rivista *Defense 21* ha riferito che «*la Corea del Nord potrebbe provocare la Corea del Sud attaccando le isole del mare ad ovest, o potrebbe lanciare un attacco informatico tale da disturbare la società civile sudcoreana*». Tale opinione potrebbe collegarsi ai recenti attentati che hanno colpito la Corea del Sud e delle sue strutture satelliti del paese nel settore delle telecomunicazioni, che hanno causato interferenze, il blocco dei segnali GPS nei voli

commerciali, nel sistema di navigazione di navi e del trasporto su gomma. Fortunatamente nessun incidente è stato attribuito ai segnali di navigazione bloccati a bordo dei voli commerciali dentro e fuori gli aeroporti internazionali sudcoreani. Questa non è la prima volta che la Corea del Sud si trova di fronte allo stesso tipo di attacco (agosto e dicembre 2010 e marzo 2011). Non è chiaro chi stia fornendo la tecnologia di disturbo alla Corea del Nord, ma indiscrezioni portano a sospettare di Cina e Russia. Secondo fonti di *intelligence* americane il governo di Pyongyang sta investendo grandi risorse per il potenziamento delle capacità offensive informatiche, reclutando e formando un team esperto di *hacker*. Un'attenta analisi degli eventi fa risultare abbastanza chiaramente ~~è~~ che la situazione in quella scenario stia diventando difficile da gestire ed è necessario l'intervento dei principali paesi, come Stati Uniti e Cina. Per questo motivo, il Segretario della Difesa degli Stati Uniti Leon Panetta e il Ministro della Difesa cinese Liang Guaglie, si sono recentemente incontrati.

Tuttavia, alcuni punti sono ancora da chiarire: gli Stati Uniti vorrebbero comprendere per quale motivo i cinesi stiano investendo ingenti risorse per una rapida modernizzazione delle forze armate, soprattutto in un momento di pace di cui gode l'aria asiatico – pacifica; la Cina si preoccupa della strategia degli Stati Uniti e dell'interferenze nella regione.
Stati come la Cina e l'Iran continueranno a perseguire i mezzi asimmetrici per contrastare le capacità di proiezione di potenza di altri Paesi, mentre la proliferazione di armi sofisticate e tecnologiche si estenderà anche ad attori non statali. E un documento americano del 2010 specificamente dedicato alla nuova strategia "***AirSea-Battle***", a proposito della potenziale minaccia cinese **A2/AD** "Denial Anti-Access/Area" ovvero di "negazione dello spazio" ad eventuali nemici attorno al proprio territorio.
A2 Anti-Accesso – inteso come strategie che mirano a evitare che le forze militari degli Stati Uniti possano fare ingresso in un teatro operativo, mentre *AD Area-Denial* - operazioni che mirano a impedire la loro libertà d'azione nei confini più stretti della zona. Il termine non si riferisce solo alla capacità di negare lo spazio nella zona circostante il territorio cinese: al contrario, riguarda lo sviluppo di una capacità militare in grado di disarmare l'avversario prima che questi possa colpire. Da tempo gli analisti militari cinesi hanno identificato nell'eccessiva dipendenza dall'alta tecnologia la debolezza principale della struttura militare a stelle e strisce. Il forte livello di dipendenza dall'information technology determinata dalla rivoluzione degli affari militari renderebbe possibile un "attacco accecante" nei confronti del cosiddetto C4isr (Command control communication computer intelligence surveillance and reconnaissance) americano. Questo tipo di attacco si svolgerebbe con diverse modalità. In modo diretto con il tentativo di colpire i satelliti situati nello spazio e in modo indiretto attraverso attività di cyberwarfare.
L'America e l'intero Occidente hanno sottovalutato lo sviluppo militare delle nazioni come Cina e l'India e i rischi connessi a un possibile scontro militare che potrebbe avvenire in un futuro non molto lontano; questo è già accaduto sia nel settore militare convenzionale, sia nella guerra informatica. Una situazione non facile da affrontare in quanto i precedenti conflitti in cui gli Stati Uniti e buona parte dell'occidente hanno partecipato, come Iraq e Afghanistan e l'attuale crisi economica, hanno richiesto e richiedono un pesante apporto di risorse economiche.

Ad aumentare la complessità della situazione contribuisce anche la dualità di comportamento dei principali contendenti: infatti, mentre ufficialmente la questione è affrontata per via diplomatica, nel Cyber spazio, le ostilità non cessano. A ciò si aggiungano le accuse rivolte dagli USA alla Cina ritenendola responsabile dei principali attacchi sulle loro reti informatiche, e dei massicci investimenti per la produzione di nuove armi informatiche; la Cina, invece, continua a perseguire

una politica di «copertura» dei nemici storici degli Stati Uniti, come Iran e la Corea del Nord, sostenendoli tecnologicamente. Il tessuto sociale delle nazioni come gli Stati Uniti è ormai permeato dalla presenza della moneta cinese, le aziende occidentali lavorano ogni giorno con quelle in Asia nella realizzazione di nuovi progetti, scambio di informazioni sulle tecnologie sensibili. È chiaro ormai che analizzando il Cyber spazio è ora possibile capire le reali intenzioni politiche di un Paese.