'STUDI' DI INTELLIGENCE

NICOLA PEDDE

Una strategia per il Cyber Power

La cultura dell'Intelligence è lo strumento attraverso il quale comprendere il ruolo e l'operato dei moderni Servizi di informazione e sicurezza. Strumento dato dall'approfondimento degli studi e delle analisi dei principali think tank, centri di ricerca, università italiane e straniere.
La cultura dell'Intelligence intende, quindi, selezionare e presentare periodicamente i più significativi studi sulle tematiche relative alle strutture di intelligence, o a queste direttamente connesse, agevolando la comprensione della storia, delle metodologie e delle funzioni delle più moderne strutture di settore.
Un contributo per sfatare i tanti miti e luoghi comuni che da sempre accompagnano l'immagine dei Servizi segreti di tutto il mondo e per acquisirne, al contrario, consapevolezza del ruolo e dell'operato.

Making Strategic Sense of Cyber Power: Why the Sky is not Falling

di Colin S. Gray
U.S. Army War College, Strategic Studies Intitute
Carlisle (PA), aprile 2013, pagg. 82

http://strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1147

Cyberterrorism:
a Survey of Researchers
di Thomas Chen, Lee Jarvis e Stuart Macdonald
Swansea University, The Cyberterrorism Project
Swansea, marzo 2013
http://www.cyberterrorism-project.org/cyberterrorism-report/

Rapporto estremamente interessante, estratto da un progetto condotto da un nutrito team di ricerca della Swansea University (Regno Unito), e finalizzato a raccogliere i risultati della ricerca sul cyberterrorismo nell'ambito della comunità accademica.
Condotto sulla base di una serie di questionari, il documento illustra con chiarezza e grande linearità i tratti comuni della ricerca di settore, evidenziando aspetti spesso trascurati nell'ambito delle ricerche o degli studi specialistici.
Il rapporto rappresenta senza dubbio uno strumento utilissimo di valutazione complessiva fornendo, al tempo stesso, molti spunti di riflessione per ulteriori ambiti di indagine.

Self-defensive Force against Cyber Attacks:
Legal, Strategic and Political Dimension
di Matthew C. Waxman
U.S. Naval War College, International Law Studies
New York, Volume 89, marzo 2013
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2235838

Questo studio risponde essenzialmente ad una domanda: quando un cyber-attacco (o la minaccia di un cyber-attacco) può dar luogo al diritto di autodifesa, inclusa l'autodifesa armata? L'autore risponde alla domanda attraverso l'analisi di tre differenti contesti. Il primo è l'ambito giuridico, che esamina la gamma delle interpretazioni ragionevoli di diritto all'autodifesa dai cyber-attacchi. Il secondo è un punto di vista prettamente strategico e, quindi, di collegamento tra il preteso diritto di autodifesa armata e la politica di lungo termine per il perseguimento degli interessi di sicurezza e di stabilità. Il terzo ambito è, invece, valutato attraverso una prospettiva politica, prendendo in considerazione il contesto situazionale in cui i responsabili dei governi dovranno affrontare il problema.
L'obbiettivo è quello di dimostrare concretamente come lo sviluppo della politica, della strategia e della legge, agiranno in maniera interdipendente nel caso di una minaccia cibernetica traendo, al tempo stesso, alcune conclusioni sull'evoluzione del diritto nello specifico settore.

Una strategia per il Cyber Power

Sulla Gazzetta Ufficiale n. 66 del 19 marzo 2013 è stato pubblicato il testo del Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013 dal titolo "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale".
Con questo Decreto, anche in Italia prende avvio il processo di definizione delle misure di contrasto alla minaccia da attacchi cibernetici, intesi nel più ampio alveo della sicurezza dell'interesse nazionale, al fine di definire i distinti ruoli che le competenti istituzioni devono esercitare per assicurare la sicurezza del Paese e la predisposizione di meccanismi di coinvolgimento di tutti gli attori pubblici e privati. Molta strada dovrà ancora essere percorsa prima di poter realizzare un efficiente sistema di prevenzione nel settore della minaccia cibernetica, ma il Decreto segna un primo significativo passo nella giusta direzione, rispondendo in modo adeguato alla realtà della specifica minaccia.
Per restare quindi in tema, si è scelto, in questo numero, di offrire una panoramica sui principali studi di settore pubblicati nel corso del primo quadrimestre del 2013, dovendo riscontrare ancora una volta, tuttavia, come la gran parte della produzione sia di origine americana e anglosassone, restando assai scarso il contributo europeo.

La premessa al volume è alquanto esauriente. Secondo l'autore, infatti, per troppo tempo è stata sottovalutata la portata della minaccia cibernetica, e alla gran parte di quelli con competenze tecnologiche di settore è mancata una visione strategica, impedendo, di fatto, il determinarsi di una cultura della cybersicurezza adeguata, e perdendo terreno al tempo stesso nei confronti di quegli attori statuali e non che invece, al contrario, ne hanno saputo anticipare la portata e la capacità.

Si rende, quindi, necessaria una complessiva rilettura della materia, partendo dal concetto stesso di minaccia tecnologica e, conseguentemente, di minaccia cibernetica.

Tre ambiti specifici dominano la materia oggetto di interesse: il cyber - spazio, il cyberpotere e la cyberstrategia. È nell'insieme di questi tre ambiti che va creata la soluzione per la definizione di un'adeguata contromisura alla minaccia.

Il primo è l'ambiente globale dove le informazioni e i dati vengono scambiati per mezzo di apparecchi elettronici; il secondo è l'abilità di utilizzare il primo per determinare un vantaggio ed influire sugli eventi; il terzo rappre-

senta la capacità di utilizzare i primi due ambiti in funzione di una visione e di un progetto.

La guerra cibernetica, ci ricorda l'autore, deve essere considerata nell'ambito di tre settori specifici, al fine di comprenderne il complessivo potenziale, e per definire una corretta strategia di utilizzo e prevenzione.

Il primo è rappresentato dalla teoria della strategia. L'autore considera l'ambiente cibernetico semplicemente come una nuova – ma tradizionale – arma e, come tale, deve essere inserita nel più ampio contesto degli strumenti capaci di generare una minaccia da e contro l'avversario. Un'arma di nuova generazione, quindi, con tutte le sue complessità e nuove potenzialità, ma nulla di più di uno strumento tradizionale. La teoria generale degli studi strategici deve, quindi, essere adattata alla cibernetica, senza cercare di concettualizzare nuove e spesso improbabili collocazioni.

Il secondo ambito è quello grafico, dove la cibernetica deve trovare una collocazione nuova e specifica.

Se da un lato è, infatti, innegabile la natura globale, il cyberspazio deve tuttavia poter essere anche ricondotto alla fisicità della tecnologia che ne delimita gli spazi.

In tal modo possiamo individuare le dimensioni spaziali e geografiche attraverso i network di comunicazione e gli impianti per la trasmissione, circoscrivendone gli ambiti e determinandone le vulnerabilità.

Il terzo campo è quello dell'informazione. Il concetto di informazione, oggetto di un'ampia speculazione dottrinale nel corso di tutti gli anni Novanta, costituisce il presupposto all'esistenza del cyberspazio. La cibernetica è, quindi, al tempo stesso informazione e vettore dell'informazione, amplificando rispetto al passato non solo la portata geografica della disseminazione, ma anche e soprattutto le sue modalità. Aumentando, quindi, il valore dell'informazione, ma anche i rischi connessi con la sua protezione.

La guerra e i suoi strumenti sono decisi dalla superiorità della capacità strategica. È partendo da questo assunto che l'autore sottolinea l'importanza della concezione strategica della minaccia cibernetica riconducendo, quindi, la fattispecie alla teoria generale degli studi strategici senza necessità di definire nuovi quanto improbabili modelli interpretativi.

Lo studio insiste, quindi, ancora sull'esigenza di considerare la cyber-minaccia alla stregua di ogni altra forma tradizionale di minaccia, e suggerisce di mutuare per analogia la dottrina sviluppata in passato per la comprensione e la definizione della minaccia nucleare.

Ed è soprattutto la concezione strategica del rischio nucleare, con le sue conseguenze e l'utilizzo dello strumento della deterrenza, a fornire secondo l'autore la migliore chiave interpretativa per lo sviluppo di una adeguata e coerente concezione strategica della minaccia cibernetica. L'analogia non è solo di natura strategica, tuttavia, ma anche nella concezione tattica, stante la particolare architettura del cyberspazio e delle tecnologie che ne delimitano i confini.

Le conclusioni al documento sono, infine, alquanto incoraggianti. Secondo l'autore, infatti, 'il cielo non sta cadendo', nel senso che la minaccia, seppur presente e molto articolata, non è di natura tale da far presagire una rivoluzionaria evoluzione del modo di concepire i rapporti di forza tra Stati.

Sarà certamente necessario adattare le nostre concezioni strategiche attuali alla realtà evoluta della minaccia ma non sussistono, secondo l'autore, elementi per ritenere che quella cibernetica sia in realtà un'evoluzione della minaccia stessa. Attraverso l'adozione di scelte ragionate, e soprattutto spesso mutuate dall'esperienza del passato, sarà possibile configurare una modalità di contenimento del rischio certamente efficace e rispondente alle esigenze del nuovo veicolo di manifestazione del rischio.

La difesa dalla minaccia cibernetica è, quindi, certamente difficile, ma in alcun modo impossibile, richiedendo quindi uno sforzo non solo economico e tecnologico quanto, soprattutto, concettuale nella definizione di un approccio strategico adeguato e commisurato alla reale natura della minaccia.

La riproduzione totale o parziale dell'articolo pubblicato non è ammessa senza preventiva autorizzazione scritta della Direzione.