CESTUDEC CENTRO STUDI STRATEGICI CARLO DE CTISTOFORIS

Infowar : la potenza dell'informazione

Mario Avantini

2012

CESTUDEC

Infowar : la potenza dell'informazione

di Mario Avantini

L'informazione è sempre potenza. Propaganda e contropropaganda, disinformazione e mascheramento delle proprie intenzioni sono state sempre praticate in guerra, in politica e in economia. Occorre però approfondire come l'informazione si trasformi in potere capace di conseguire obbiettivi strategici, politici, economici, di influenza o di destabilizzazione. La sua strategia comporta componenti difensive e offensive. Queste ultime sono necessarie anche per porre a disposizione dello Stato una certa capacità dissuasiva. In relazione alle nuove ICT (Information Comunication Tecnology), alla diffusione dei media audiovisivi in tempo reale e alla copertura globale, nonché agli sviluppi della semantica e della semiotica, il settore dell'infowar sta conoscendo uno sviluppo notevole. La comunicazione e utilizzata per manipolare le percezioni, e quindi, il comportamento dell'avversario, del concorrente o del mercato. Le capacità di manipolazione si accresceranno con la diffusione dei media interattivi. Essi consentono di suddividere l'audience in segmenti omogenei, che dispongono della medesima griglia di lettura della realtà e di effettuare comunicazioni mirate a penetrare ciascuno di essi. Con i media tradizionali tutta questa segmentazione non era possibile. Ogni individuo è portato a credere in ciò che conferma i suoi valori, i suoi preconcetti e convinzioni. Il fenomeno della dissonanza cognitiva, ben conosciuto anche ai Servizi di Intelligence. Una volta infowar (propaganda, disinformazione, ecc.) si rivolgeva alle classi dirigenti politiche più che alle popolazioni. Con la trasformazione dei sudditi in cittadini, anche l'infowar si è democratizzata, dirigendosi soprattutto alle opinioni pubbliche. Si è esaltata la necessità dei dirigenti politici di reagire con immediatezza agli stimoli dei media, anche in assenza di informazioni sufficientemente attendibili e valutabili nelle loro conseguenze. In tal modo, i responsabili politici ed economici rimangono

spesso prigionieri di reazioni estemporanee, che hanno dovuto fare per non perdere di credibilità, nascondendo il fatto di essere stai colti di sorpresa. Ne discende un ulteriore importanza dei Servizi di Intelligence pubblica e privata. Essi non devono solo analizzare le notizie e cercare di ricostruirne l'origine e gli impatti degli eventi, ma anche, unitamente ai responsabili della comunicazione Istituzionale o aziendale, fornire ai responsabili opinioni circa le iniziative da adottare per riprendere il controllo della situazione, soprattutto se pilotata da intenzioni ostili, genera un escalation emotiva che può provocare rapidamente fenomeni di panico. L'infowar comunicativa comporta come ogni operazione componenti offensive e difensive, che seguono logiche analoghe a quelle a cui obbedisce qualunque strategia in situazioni conflittuali. La tempestività delle risposte è spesso più importante del contenuto. L'analisi delle notizie rende necessaria la disponibilità di capacità professionali specifiche, di cui devono dotarsi i Servizi di Intelligence. Il settore informatico - comunicativo richiede una continua sorveglianza (vigilanza comunicativa), perché caratterizzato da improvvise accelerazioni, specie in caso di avvenimenti drammatici che ben si prestano a spettacolarizzazioni e manipolazioni. Mentre l'infowar si svolge a livello "soft" delle percezioni, la cyberwar si svolge "hard" delle reti. La cyberwar include tutte le forme di attacco e di difesa nel cyberspace. E' un estensione della guerra elettronica nei suoi aspetti più offensivi (contromisure, intercettazioni ecc.) che difensive (crittografia, firebreak, ossia sbarramenti per impedire l'accesso alle reti e alle banche dati) e va strettamente coordinata con essa. Ha finalità sia politico – strategiche che economiche. In entrambe i settori, le reti informatiche agiscono da moltiplicatori – e anche come generatori – di potenza economica e militare. La cyberwar è estremamente dinamica, rapida e imprevedibile, annulla il valore della distanza, del tempo e delle frontiere. I "guerrieri cibernetici" possono essere organizzati spontaneamente ma anche dai governi. Quando organizzata da governi o da gruppi terroristici

hi – tech, la cyberwar puo includere aspetti hard, ad esempio l'attacco a computer, ai server, ai cavi in fibra ottica, alle banche dati, disturbi alle comunicazioni satellitari ecc. Può includere anche la preventiva installazione di "Trojan horse" (cavalli di troia) o di "worm" (e-mail contaminati) che si diffondono nelle reti e nelle banche dati diminuendone l'efficienza e, a limite, bloccare il sistema. Nel campo della cyberwar, il diritto internazionale è estremamente carente. Lo è anche quello italiano. Si è accresciuta la pericolosità di un settore divenuto indispensabile per le funzionalità delle istituzioni, dell'economia e dei servizi sociali e pubblici. Tutti i principali Stati stanno sviluppando capacità di attacco contro le reti informatiche di potenziali avversari e di difesa delle proprie, quest'ultima non può mai essere completa. Potrebbe esserlo solo rinunciando alla connessione con le reti globali come Internet. L'isolamento significherebbe però declino, come dimostra la storia di tutte le società che si sono chiuse su loro stesse, come quella sovietica. Un cyberattacck è effettuabile da chiunque e da tutti i luoghi del mondo, mentre la difesa può essere organizzata solo localmente, dai governi degli utilizzatori delle reti cibernetiche e, e a livello territoriale da parte degli Stati. Negli USA la responsabilità della cybersecurity è stata affidata alla NSA e in Cina al 7° Dipartimento dello Stato Maggiore generale della PLA (People Liberation Army). In Italia, esiste una pluralità di organismi. Ciò rende più importante che i Servizi si interessino al settore e svolgano un ruolo trainante sia nella strategia di riduzione delle vulnerabilità, sia in quella di risposta, a partire dall'allertamento per giungere alla valutazione dei danni. Beninteso, anche in questo settore, i Servizi non possono fare tutto da soli, devono collegare in rete i vai operatori del settore. Con L'avvento della cyberwar accrescerà anche lo spionaggio tecnologico e industriale, molte informazioni verranno acquisite con le intercettazioni o con la penetrazione nelle banche dati. La protezione delle informazioni riservate diventa una priorità anche per l'economia. La crittografia aumenterà di importanza, ma al tempo stesso

diverrà più difficile creare sistemi non penetrabili. Basti ricordare il caso "Echelon" e quello recente di "Google" per comprendere le ragioni della competizione prevalgano sulla quelle della cooperazione. Il nuovo caso, per molti aspetti simile a Echelon, e quello di Google. Avvalendosi di rilevatori mobili posti a bordo di furgoni, Google ha rilevato le comunicazioni Wi Fi in tutti i continenti, effettuandone una mappatura dettagliata. Non si conoscono ancora le finalità dell'iniziativa e, soprattutto se sia stata attuata per motivi economici o politici. Certamente lo è stata con metodi illegali, se non altro per evidenti violazioni alla Privacy che ha comportato. Probabilmente, il rilevamento è stato fatto per incarico dei Servizi di Intelligence americani, che anche n questo caso, avrebbero effettuato illecite ingerenze nella sfera di sovranità degli Stati alleati. L'Europa è la più colpita, ma non può reagire, le sue divisioni la paralizzano. Nell'era dell'informazione, la potenza riguarda più gli aspetti "soft" che quelli "hard". Il mondo delle "cose pesanti" sta trasformandosi in quello delle "cose pensanti". I Servizi di intelligence hanno un loro preciso ruolo da svolgere nel settore. Esso comporta mutamenti profondi di approcci, di professionalità e anche di cultura istituzionale dell'intelligence. Comporta anche contatti strutturali con opinion maker e giornalisti realizzabili con la diffusione della "cultura della sicurezza", dell'intelligence e degli interessi nazionali.

Riferimenti

G. Tremonti, C. Jean, Guerre stellari: società ed economia nel cyberspazio, Franco Angeli

A. Woodrow, information e manipolation, Le felin Paris

F e M. Pierantoni, la Guerra incruenta Cemiss- Franco Angeli

P. Savona C. Jean Intelligence Economica - Rubettino

C. Jean Geopolitica Strategia e Sicurezza – Franco Angeli