Information Warfare 2015

Manovre cibernetiche: impatto sulla sicurezza nazionale

a cura di Umberto Gori
e Serena Lisi

FrancoAngeli

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con

La versione completa dell'e-book (a pagamento) è leggibile con Adobe Digital Editions. Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta cliccando qui le nostre F.A.Q.

Collana di Scienza Politica e Relazioni Internazionali, diretta da Umberto Gori

Il progresso delle scienze sociali è strettamente legato alla ricerca interdisciplinare. Tale indirizzo non ostacola però l'applicazione di un approccio e di un metodo rigorosamente unitari. L'approccio è quello dei sistemi, il metodo è quello della scienza politica più avanzata. L'uno e l'altro mirano a conoscere il reale nella sua complessità, a partire da dati e variabili fattuali, con l'ausilio, anche, di discipline diverse, teorie empiriche e quindi previsioni aventi valore probabilistico.
C'è una fortissima domanda, oggi, di strumenti aggiornati atti ad interpretare fenomeni complessi e talora privi di precedenti ed a consentirne la previsione, data l'accelerazione dei tempi storici.
A questa domanda la «Collana di Scienza Politica e Relazioni Internazionali» si propone, ambiziosamente, di rispondere, cercando anche di rimuovere, in misura progressiva, le resistenze, ancora vive nel nostro Paese, dovute al tradizionale convincimento che il campo sociale non sia coltivabile con gli strumenti euristici che hanno determinato lo sviluppo eccezionale delle scienze della natura.
La denominazione della collana si giustifica per due aspetti: primo, perché di solito quando si parla di scienza politica si pensa al quadro interno e qui invece si vuole accreditare la tesi che anche il sistema internazionale è analizzabile in tale prospettiva; secondo, perché anche per l'analisi corretta del sistema interno è ormai impensabile non fare un sistematico riferimento al contesto internazionale (e viceversa).
La collana svilupperà sia una parte di metodologia e di tecniche analitiche, sia una parte teorica e di ricerca sugli aspetti di sostanza del vasto campo preso in considerazione. Contribuiranno all'una e all'altra metodologi e scienziati politici, sociologi della politica e studiosi dell'amministrazione, comparatisti e cultori di relazioni internazionali.
La collana ha essenzialmente un taglio operativo. I suoi naturali destinatari saranno quindi, oltreché gli specialisti, anche tutti coloro che, ai diversi livelli, sono detentori di responsabilità decisionali. Scopo ultimo è infatti la progressiva «modernizzazione» dell'Italia nel campo della valutazione scientifica dei fatti politici, interni ed internazionali, che è premessa insieme di razionalizzazione dei processi decisionali e di un corretto funzionamento delle istituzioni e della vita democratica del Paese.

Information Warfare 2015

Manovre cibernetiche: impatto sulla sicurezza nazionale

a cura di Umberto Gori
e Serena Lisi

FrancoAngeli

L'evento, articolato anche quest'anno in due edizioni, ha avuto luogo a Milano il 3 giugno 2015, presso l'Auditorium G. Testori Palazzo Lombardia, e a Roma, il 14 ottobre 2015, presso la Sala Gruppi della Camera dei Deputati. La Conferenza è stata ideata dal Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII) dell'Università di Firenze, dall'Istituto per gli Studi di Previsione e le Ricerche Internazionali (ISPRI), dal Centro Studi Difesa e Sicurezza (CESTUDIS) e dal Centro di Ricerca di Cyber Intelligence and Information Security (CIS) da "La Sapienza" di Roma, d'intesa con InTheCyber - Intelligence & Defense Advisors.

Un ringraziamento particolare va a Jacopo Losi, laureando dell'Università di Firenze, per la collaborazione all'editing del volume.

Indice

Prefazione

di *Paolo Lezzi*[*]

Il nostro ciclo di conferenze è giunto alla sua settima tappa e così, come di consueto, abbiamo il piacere di pubblicare gli Atti dell'anno precedente che ha visto affrontato il tema delle Manovre Cibernetiche impattanti sulle Aziende (edizione di Giugno a Milano) e sulla Sicurezza Nazionale (edizione di Ottobre a Roma).

Le *Manovre Cibernetiche* includono tutte quelle attività offensive e difensive nei confronti dei sistemi IT dedicati alla Difesa Cyber, dalle operazioni di Cyber Intelligence alle pratiche di attacchi intrusivi di qualsivoglia genere (logici, fisici, man-made) e/o malware.

Il termine *"manovra"* caratterizza una mossa od una serie di mosse tattiche volte a migliorare, mantenere o almeno non peggiorare la propria situazione strategica in un ambiente competitivo. I teorici militari utilizzano il termine *"manoeuvre warfare"* (guerra di manovra) per indicare un tipo di offensiva volta a sconfiggere l'avversario inibendone le capacità decisionali, attraverso shock ed azioni di disturbo.

In gergo tecnico, *"Cyber Maneuver Expo"* indica un dibattito fra esperti sulle manovre cibernetiche offensive e difensive. In tal senso la nostra Conferenza è sempre stata un'occasione unica nel suo genere per apprendere, ascoltare e scambiare punti di vista di carattere tecnico e approfondito sulla tematica affrontata, così da dissipare incertezze e dubbi.

Oggi le tecniche difensive e offensive cambiano così rapidamente da obbligare gli operatori del settore a rivedere pressoché ogni giorno le contromisure per affrontare le minacce future, ancora sconosciute. Le minacce hanno un nuovo volto e mescolano gli strati fisici, logici e umani: da semplici codici malevoli e defacement di siti ad attacchi globali, furto di dati, DDoS, attacchi di business intelligence o infrastrutturali.

L'ambiente commerciale ed economico è strettamente correlato a quello cibernetico e alle sue capacità difensive, in un rapporto di dipendenza.

[*] Chairman CWC. Founder & CEO InTheCyber – Intelligence & Defence Advisors.

Nonostante vengano fatti investimenti per milioni nella difesa e sicurezza cibernetica, i tre strati (logico, fisico e umano) sono costantemente sotto attacco.

Le manovre cibernetiche offensive e difensive sollevano molti quesiti e riflessioni che, speriamo la Conferenza Nazionale sulla Cyber Warfare del 2015, nelle sue due edizioni, abbia contribuito a chiarire, ma soprattutto a far crescere la consapevolezza che solo una reale, fattiva ed efficace collaborazione ed assunzione sinergica di responsabilità e consapevolezza da parte di tutti gli attori pubblici e privati, civili e militari possono far accrescere il livello di Sicurezza Nazionale.

Fondamentale è lo spostamento di risorse dalla Difesa tradizionale alla Difesa Cyber sia in termini di tecnologie sia di formazione di operatori Cyber nazionali.

Riconoscimenti

Patrocini

Presidenza del Consiglio dei Ministri
Ministero degli Affari Esteri e della Cooperazione Internazionale
Ministero dell'Economia e delle Finanze

Patrocini aggiuntivi per l'edizione di Milano

Regione Lombardia
Comune di Milano

Promotori

Centro universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSI)
Centro Studi Difesa e Sicurezza (CSD)
Cyber Intelligence and Information Secuirity (CIS Sapienza)
Istituto per gli Studi di Previsione e le Ricerche Internazionali

Sponsor

Trend Micro
Fortinet
Biz Empowerment
BV Tech

Con la collaborazione di

CERSA
CLUSIT

Ideata d'intesa con Maglan – Information Defense & Intelligence

Edizione di Roma svoltasi durante il Mese Europeo per la Sicurezza Informatica


CERSA


Clusit
Associazione Italiana
per la Sicurezza Informatica

Edizione di Milano

3 Giugno 2015

Manovre nel ciberspazio: prospettive

di *Umberto Gori*[*]

Gli argomenti che quest'anno la sesta Cyber Warfare Conference vuole passare in rassegna riguardano in particolare le tendenze riscontrabili nello spazio cibernetico e, di conseguenza, le prospettive che se ne possono ragionevolmente trarre.

Prospettive che devono essere viste alla luce dei profondi rivolgimenti che sta subendo il sistema internazionale il quale sta visibilmente ritornando alle logiche di Westfalia che sembravano ormai ricordi di un passato che aveva visto i suoi esordi nel XVII secolo.

Le teorizzazioni degli studiosi di relazioni internazionali, all'indomani della guerra fredda, si erano per lo più concentrate sulle magnifiche sorti e progressive della globalizzazione, sul declino degli Stati nazionali riscontrabile sia sul piano politico che su quello economico, su un nuovo ordine internazionale che avrebbe favorito l'instaurarsi di norme di condotta propiziatrici di cooperazione e di pace internazionale.

Purtroppo, il sogno si è rivelato di breve durata. Partendo dai cerchi più interni della nostra collocazione nel mondo fino a quelli più esterni e addirittura lontanissimi nello spazio geografico, riusciamo a scorgere solo tensioni, crisi, controversie, conflitti armati, aberrazioni terroristiche. Dall'Artico all'Europa orientale, dal Medio Oriente all'Africa, dall'Asia centrale fino all'Oriente estremo, il mondo presenta forti criticità, alcune delle quali difficilmente sanabili.

Tale situazione fa prevedere che lo spazio cibernetico sarà sempre più conflittuale più che uno spazio di cooperazione. I conflitti che si avranno in tale dominio, avranno natura politica, economica, finanziaria, con conseguenze tutt'altro che virtuali.

In un documento del Dipartimento della Difesa USA del 13 gennaio 2013, Resilient Military Systems and the Avanced Cyber Threats, si legge che le minacce cibernetiche sono un problema estremamente serio, con conseguenze potenziali simili a quelle delle minacce nucleari. Nello stesso documento si afferma che ci vorranno anni affinché il DoD metta in piedi

[*] Emerito Università di Firenze, Presidente CSSII e Direttore ISPRI.

un'efficace risposta alle minacce cibernetiche sempre più sofisticate. Con le risorse e tecnologie attuali una difesa non sarebbe più possibile. Se questo è vero per gli Stati Uniti, figuriamoci quale possa essere il livello della preparazione in Italia, livello che riflette il grado di scarsa consapevolezza delle élites, delle imprese e dell'opinione pubblica.

Se il paragone fatto fra le conseguenze delle armi cibernetiche e quelle nucleari è da considerarsi appropriato, emergono però subito almeno due differenze: la prima riguarda l'invisibilità dell'attuale minaccia, il che comporta una minore comprensione del pericolo; la seconda riguarda l'istantaneità, senza preavviso, del possibile attacco cibernetico, diversamente da quanto accadeva nell'ipotesi di attacco nucleare con segnali e tempi calcolabili almeno in minuti. Conclusione: siamo in una situazione ben peggiore oggi. Ciò che può salvarci è la difficoltà psicologica delle parti contrapposte, come è sempre accaduto in epoca nucleare, a superare il punto di "non ritorno". Ma, attenzione: il sistema di guerra fredda era caratterizzato da attori razionali, il sistema cibernetico è popolato da attori irrazionali o, meglio, di diversa razionalità. Mi riferisco, in particolare, al terrorismo di matrice radicale.

Ciò premesso vengo subito ad elencare le tendenze più rilevanti in campo cibernetico.

Innanzitutto, è bene avere chiaro in mente che non esiste una soluzione tecnologica assoluta alle cyber minacce. Dato il ritmo esponenziale dello sviluppo tecnologico, le manovre difensive, le *white manoeuvres*, resteranno sempre indietro rispetto a quelle offensive, le *black manoeuvres* del titolo della Conferenza, almeno nel prevedibile futuro. Sul punto vorrei però osservare che, più spesso che non si creda, manovre difensive possono essere usate per scopi offensivi e che manovre offensive possono essere impiegate per finalità difensive.

In un recentissimo libro di Marc Goodman, edito quest'anno (2015) – *Future Crimes – A Journey to the Dark Side of Technology, and How to Survive It* – ho letto quanto segue (traduco liberamente):

> *è difficile rendersi conto di cosa significhi esattamente "sviluppo esponenziale". Forse solo un esempio concreto può rendere l'idea. Immaginiamo di fare trenta passi "lineari": al massimo attraverseremo il nostro salotto. Ma se i passi sono "esponenziali" la distanza percorsa equivarrà a quella fra la terra e la luna. Il che significa che i progressi che sarà possibile sperimentare nel XXI secolo non saranno quelli di un secolo, ma, al ritmo attuale, quelli di almeno duecento secoli. Provate a immaginare le conseguenze di tutto ciò.*

In questi termini di linguaggio corrente il discorso fa venire il capogiro. In realtà, quando si parla di crescita esponenziale di un fenomeno dal punto di vista matematico, s'intende che esso è esponenziale in funzione del tem-

po, ma siccome ciò che chiamiamo tempo continua inesorabile, implicitamente diciamo che il fenomeno tende a diventare infinito. E ciò non è né vero né possibile nella nostra esperienza umana. Tali fenomeni, ad esempio le epidemie, seguono curve di crescita logistiche ad S. In realtà, esistono solo fenomeni di crescita che "*per un certo loro tratto* possono essere approssimati bene con un esponenziale" (Roberto Vacca). Anche così ridimensionata, la prospettiva resta comunque inquietante.

Continuiamo con le quantità. Il numero dei malware è impressionante. La McAfee ne ha identificati nel 2011 due nuovi milioni al mese. Il Karspesky lab, nel 2013, ne ha identificati e isolati duecentomila ogni giorno, pari a tre volte tanto.

Attualmente, le difese si limitano, per lo più, a individuare le intrusioni e a monitorare le comunicazioni. Per fare passi avanti, occorre creare delle strutture che favoriscano la condivisione delle informazioni in modi sicuri.

S'impone una nuova strategia di difesa basata sull'analisi delle minacce, sia tentate che riuscite, al fine di avere a disposizione indicatori che consentano di intravedere tendenze e modelli d'azione.

Si ritiene pertanto, da parte degli esperti, che si cercherà di creare sistemi di monitoraggio dei comportamenti in rete capaci di evidenziare attività anomale alla stessa stregua, ad esempio, di ciò che fanno le compagnie emittenti di carte di credito per contrastare le frodi. Tale attività dovrà essere continua. Il problema della cyber security, infatti, è di per sé dinamico, non statico. E non va mi dimenticato che quando tutto è connesso tutto diventa vulnerabile.

Altro grande problema destinato purtroppo a durare a lungo è il comportamento degli utenti della rete che resistono alla necessità di utilizzare robuste parole di passo, firewall multistrato, trasmissioni criptate, etc., rimedi – questi – realizzabili a basso costo. La prima linea di difesa dovrà dunque essere assicurata da un intenso addestramento e istruzione permanente degli

utenti. Ma dovranno anche essere escogitati sistemi di resilienza sempre più efficaci per le infrastrutture critiche.

Gli sviluppi di base che muteranno la natura del ciberspazio e di conseguenza quella delle minacce saranno l'affermarsi del *Cloud Computing* e la riprogettazione dei sistemi d'informazione. Per quanto riguarda i sistemi sulla "nuvola", essi possono funzionare su diverse macchine e ciò significa che sarà sempre più difficoltoso creare malware che possano avere effetti deleteri a livello di macchina. Infatti, quando un malware cerca di agire in un contesto "cloud", esso, in effetti, lo fa su un software che imita un dispositivo hardware. E ciò limita o modifica la sua capacità di nuocere.

L'utilizzo della "nuvola" sarà sempre più intenso sia per ragioni economiche che per una maggiore resilienza della struttura, oltre che per una maggiore facilità di anonimato, il che renderà ancora più difficile la soluzione del problema dell'attribuzione. Le vulnerabilità saranno certamente meno frequenti ma anche potenzialmente catastrofiche.

Le caratteristiche della "nuvola" sono in ogni caso rilevanti. Esse sono: possibilità di disporre in autonomia sia di risorse computazionali che di spazio virtuale; utilizzazione del servizio in qualsiasi momento; assegnazione dinamica delle risorse a seconda del carico e delle esigenze del cliente; allocazione automatica e rapida di maggiori eventuali funzionalità; controllo e ottimizzazione in automatico delle risorse utilizzate. Una delle conseguenze dell'utilizzo della "nuvola" sarà una maggiore cooperazione internazionale per contrastare le minacce.

Di converso, i punti di debolezza sono, fra gli altri: la difficoltà di migrazione dei dati, dal momento che ogni operatore di servizi "cloud" progetta l'ambiente operativo secondo determinate caratteristiche; possibili violazioni della riservatezza degli spazi virtuali, *private clouds*, dei singoli clienti dovute anche a scorrettezze dei *cloud providers*, spesso situati all'estero.

Per quanto riguarda la gestione dell'informazione, la tendenza che si profila è quella di stabilire delle priorità alla documentazione da proteggere, evitando di pretendere, anche perché costoso, la sicurezza per materiali non essenziali.

Gli attacchi saranno sempre più numerosi e sofisticati con la conseguenza che le misure di contrasto saranno sempre più difficili da attuare. Fra quelli che interessano le imprese, si segnalano sempre più probabili le intrusioni nei *device* personali e nel *cloud*, le e-mail sempre più ingannevoli e il blocco dei computer con richiesta di riscatto, *ransomware*. È l'ammiraglio Sanfelice di Monteforte che giorni fa mi ha segnalato come gli attacchi con richiesta di riscatto siano iniziati anche nel settore della marina mercantile le cui navi sono ormai controllabili da remoto. C'è solo da sperare che ciò non accada con le navi militari.

Agli attacchi non sfugge nessuno, neanche i capi di Stato e di governo. La vulnerabilità delle industrie, poi, dipende da molti fattori, quali il tipo di settore e di localizzazione in cui l'azienda opera, la natura del suo business, l'adeguatezza della sua tecnologia e dei sistemi di sicurezza, la validità delle sue procedure, l'affidabilità della sua *supply line*, la lealtà del suo personale, etc.

Tali sfide, insieme alla difficoltà di arrivare presto ad una efficiente cooperazione internazionale, potrebbero dar luogo a delle comunità chiuse, *gated communities*, alla stregua di SIPRNET e JWICS, sistemi governativi USA che gestiscono materiale *secret* e *top secret*. Ciò può accadere anche nel settore privato, soprattutto in assenza di efficienti meccanismi statali di tutela.

Un'altra tendenza che si va delineando è la ricerca di modalità automatiche di reazione alle minacce che hanno tempi di attuazione di millisecondi. Le risposte manuali, infatti, non possono competere con la velocità della luce.

Importante appare inoltre la tendenza a movimentare i dati in modalità criptata.

Non pretendo di essere esaustivo, ma non posso certo evitare di esprimere alcune considerazioni sull'importanza che va progressivamente assumendo la rivoluzione dei *Big Data* causata da un abnorme e velocissimo aumento dei dati e delle informazioni non più gestibili dai sistemi di analisi e dalla memoria dei computers. Da qui l'origine di nuove tecnologie come *MapReduce* di Google e dell'equivalente open-source *Hadoop* di Yahoo, ed altre ancor più avanzate, capaci di processare quantità di dati esprimibili in Exabyte, 10^{18} o in valori ancora più grandi, cifre, cioè, letteralmente astronomiche. È stata infatti l'astronomia, insieme alla genomica, che ha coniato l'espressione "Big Data".

Ma quando le quantità crescono in misura esponenziale si producono anche mutamenti qualitativi di significativo rilievo, come ad esempio accade nel campo delle tecniche di previsione, un tema a me caro, come ben sanno i miei colleghi.

A monte della previsione c'è la spiegazione che consiste nell'individuare le cause di eventi che ne sono l'effetto.

Oggi, però, con i *Big Data*, non è più necessario, a fini pratici e previsionali, conoscere le cause: è sufficiente sapere "che cosa". Se A è spesso correlata con B, occorre solo tener d'occhio B per restringere il campo d'incertezza ai fini della previsione di A. Del resto, anche le previsioni scientifiche sono valutabili in termini di probabilità, non sono profezie. In altre parole, le correlazioni non ci dicono il "perché" degli avvenimenti, ma ci informano su ciò che sta accadendo, e possono farlo in "tempo reale". Dalla previsione causale si passa, alla previsione a-causale. Lasciar parlare i dati evita di testare un certo numero di ipotesi determinate *ex ante*.