Cyber Warfare 2017

Information, Cyber e Hybrid Warfare: contenuti, differenze, applicazioni

a cura di Umberto Gori

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.

Cyber Warfare 2017

Information, Cyber e Hybrid Warfare: contenuti, differenze, applicazioni

a cura di Umberto Gori

FrancoAngeli

L'evento, articolato anche quest'anno in due edizioni, ha avuto luogo a Roma il 6 luglio 2017, presso la Nuova Aula del Palazzo dei Gruppo Parlamentari – Camera dei Deputati, e a Milano il 28 novembre 2017, al Centro Congressi Palazzo delle Stelline. La conferenza è stata promossa dal Centro universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSII), Centro Studi Difesa e Sicurezza (CESTUDIS), CIS Università La Sapienza, Istituto per gli Studi di Previsione (ISPRI), European Center for Advanced Cyber Security (EUCACS), Centro studi Grande Milano, d'intesa con InTheCyber – Intelligence & Defense Advisors.

Il curatore del volume sente l'obbligo di ringraziare Daria Vernon De Mars, esprimendo il più alto compiacimento per la sua intelligente, paziente e costante collaborazione alla revisione dei testi e all'editing dei presenti Atti.

Indice

Questo volume annuale esce per la prima volta da molti anni senza il contributo del Sen. Gen.Cd'A. Luigi Ramponi, scomparso il 5 maggio 2017.
Il Generale Ramponi, pioniere della promozione della cyber security in Italia, sia a livello parlamentare che attraverso l'attività del CE-STUDIS (Centro Studi Difesa e Sicurezza), oltre ad essere stato membro eminente del nostro Comitato scientifico, è stato anche Presidente di EUCACS (European Center for Advanced Cyber Security), titolo che mantiene post mortem *per volontà unanime del Centro.*
Gli Enti organizzatori e sostenitori, il V. Presidente esecutivo di EUCACS e il curatore del volume dedicano con reverente affetto questi Atti dell'ottava Cyber Conferenza alla Sua memoria.

Prefazione

di *Paolo Lezzi*[*]

Il mio carissimo amico prof. Umberto Gori ha immediatamente sposato il tema della CWC 2017 "Cyber Warfare vs Information Warfare". I relatori delle due edizioni di Roma e Milano hanno con professionalità e precisione delineato ed esemplificato, nel tempo a disposizione, molte delle sfaccettature di queste realtà. Sicuramente nessuno poteva prevedere la profondità e la rapida escalation che l'Information Warfare avrebbe preso, ma che già nel corso del 2016 aveva dato seri segnali. Al tempo della scrittura di queste note sta emergendo in maniera eclatante un fatto grave in sé, ma che evidenzia ben altri pericoli: la manipolazione di decine di milioni di account di uno dei più grandi social media.

Siamo arrivati alla paradossale situazione nella quale il potere dell'informazione, nonché il modus operandi e "comunicandi" di centinaia di milioni di persone, quasi tutto il mondo occidentale (ma non solo), è nelle mani di poche entità private. Il controllo del fenomeno sfugge o è stato fatto sfuggire dal controllo dei singoli Stati.

Il potere economico nelle mani di queste realtà è superiore a quello di storici Stati della vecchia Europa, che possono solo abbozzare qualche tentativo di giurisdizione di scarso successo.

Da ciò deriva, quindi, anche un potere "politico" non secondario, che deve essere attentamente valutato e previsto nelle sue intrinseche ed estrinseche possibili conseguenze.

Fenomeni di tale portata si ascrivono a pieno titolo nella difesa nazionale e sovra nazionale.

Abbiamo quindi la responsabilità di cimentarci anche nella CWC 2018 con il connubio "Informazioni e Potere".

La Hybrid Warfare, come sottolinea sempre il prof. Gori, è ciò con cui dobbiamo fare i conti ormai quotidianamente. Non abbiamo più davanti qualcosa di ben identificato e di cui si possano prevedere le mosse o le cui mosse

[*] Vicepresidente Esecutivo EUCACS, CEO & Founder InTheCyber Group.

stesse siano evidenti nel primo accadere. Un attacco cyber nasce e può persistere silente e coperto per tutto il tempo che ne ha l'abilità e/o la volontà. Più l'attore è di alto livello, dalla criminalità internazionale, al terrorismo, financo all'ambiente statuale, più la volontà di essere "*stealth*" prevale. Tutto ciò ha poco a che fare con gli attacchi "automatici" che tanto agitano i media. Questo è il motivo per cui è sempre più necessaria la crescita di una capacità di "*detection & response*", sia a livello della singola azienda sia a livello del sistema Paese. Parimenti si richiede una fortissima collaborazione pubblico-privato, volta a raggiungere il massimo livello di preparazione, difesa e reazione. La condivisione istantanea di segnali anche deboli, ma soprattutto di ogni forma di tentativo di attacco riduce drasticamente la capacità di azione e propagazione del nemico.

Lo scenario in cui viviamo e la sua evoluzione a breve e medio termine fa emergere in modo ormai ineluttabile il compito e la responsabilità del Paese intero verso un quasi ciclopico sforzo per la creazione ad ogni livello ed età di una consapevolezza diffusa rispetto alla minaccia cibernetica in tutte le sue forme. Uno sforzo che deve convogliarsi anche nello sviluppo a pieno ritmo di un piano nazionale coordinato per la formazione di decine di migliaia di "operatori cyber civili e militari" con competenze multidisciplinari e capaci di lavorare in squadra.

In un momento di profonda incertezza politica per il Paese l'allerta deve essere massima, perché le vulnerabilità di imprese ed istituzioni non siano sfruttate per infiltrarsi nei gangli vitali in maniera permanente. Allo stesso modo deve essere massimo l'impegno del sistema Paese per l'individuazione e rimozione delle vulnerabilità stesse.

Tutte le azioni previste dagli ultimi decreti della Presidenza del Consiglio devono trovare rapida e certa attuazione.

Le entità preposte alla difesa cyber del Paese, così come avviene per la difesa militare e l'intelligence, devono poter operare in maniera continuativa, indipendentemente dai processi di ricambio/avvicendamento istituzionale tipici delle democrazie occidentali.

I Piani Cibernetici Nazionali, tanto voluti dal nostro mai dimenticato e caro gen. Sen. Luigi Ramponi, devono essere quindi di lungo respiro, in modo da recuperare rapidamente i gap con i Paesi più avanzati, se non – proprio in virtù della brillantezza delle giovani menti e dei nuclei di competenza già presenti sul territorio a livello accademico, militare e privato – addirittura far distinguere il Paese tra i leader in campo cyber.

Riconoscimenti

Patrocini

Presidenza del Consiglio dei Ministri
Ministero dell'Interno

Patrocini aggiuntivi per l'edizione di Milano

Regione Lombardia
Comune di Milano

Promotori

Centro universitario di Studi Strategici, Internazionali e Imprenditoriali (CSSII) – Università degli studi di Firenze
Centro Studi Difesa e Sicurezza (Cestudis)
CIS Università La Sapienza
Istituto per gli Studi di Previsione (ISPRI)
European Center for Advanced Cyber Security (Eucacs)
Centro studi Grande Milano

Ideato d'intesa con InTheCyber- Intelligence & Defense Advisors

Con la sponsorship di

Trend Micro

Con la collaborazione di

CLUSIT
CERSA


Clusit
Associazione Italiana
per la Sicurezza Informatica


CERSA

Edizione di Roma

6 luglio 2017

Oltre l'ambiguità concettuale: significato e contenuti della Information Warfare, Cyber Warfare e Hybrid Cyber Warfare

di *Umberto Gori*[*]

Minacce cyber e misure di contrasto comunitarie

È evidente, ormai, che la sicurezza dei cittadini, la difesa del Paese e la competitività economica delle imprese possono essere assicurate in grandissima misura solo nel cyberspazio. A questo fine – come è noto – sono stati emanati a livello comunitario due strumenti, la Direttiva NIS (Network and Information Security) ed il Regolamento sulla Protezione dei Dati (GDPR), tesi ad uniformare la normativa e ad innalzare il livello della cyber security. Si ricorda, senza entrare nei particolari, che fra le previsioni è presente anche come obiettivo la creazione di un mercato digitale dell'Unione Europea, che sottragga a Paesi esterni la produzione di hardware e soprattutto di software, e cioè dell'*infrastruttura della sicurezza*. Non sarà facile, considerando la sterminata quantità degli oggetti IoT, oggetti interconnessi dai quali possono provenire minacce e pericoli senza fine.

In Italia il cyber crimine colpisce 1 azienda su 5 (calcoli del 2016) e continua a crescere in misura esponenziale, parafrasando le parole del Presidente di Leonardo-Finmeccanica. Secondo uno studio di Trend Micro l'Italia è il settimo Paese al mondo e il secondo in Europa più colpito dai *ransomware*; il quarto più colpito in Europa per numero di *app* maligne scaricate. Il numero totale di malware scaricati nella prima metà del 2017 raggiunge la cifra di 19 milioni contro i 22 milioni di tutto il 2016. Nel settore dell'*Home Banking* sono stati oltre 1500 i malware che hanno colpito il nostro Paese. Il settore finanziario è particolarmente soggetto a incursioni malevole (*Banking Trojan* e potenziale manipolazione degli algoritmi di *trading*, combinata con attività di speculazione sui mercati).

A quanto riporta Europol in Europa sono stati rubati nel 2016 ben 2 miliardi di dati. Bastano questi numeri a sintetizzare la gravità del problema.

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

Senza contare, inoltre, l'Industria 4.0 che, oltre ai benefici, causerà anche ulteriori complicazioni.

Tre sono i "pilastri" indicati dall'Unione per gestire la cyber sicurezza: la resilienza, che può essere assicurata con dei *penetration test* o a mezzo di strutture "in parallelo", la Direttiva NIS, che dovrà essere recepita nell'ordinamento nazionale entro il mese di maggio 2018, e il Regolamento Europeo per la protezione dei Dati sopra evocati. È del Governo Gentiloni, poi, la proposta al G7 di un codice di condotta internazionale sul comportamento degli Stati nel cyberspazio, che dovrebbe in un secondo momento avere, tramite le Nazioni Unite, una vigenza mondiale.

In Italia non si riscontra una grande consapevolezza delle cyber minacce e dei relativi rischi, ma fortunatamente oggi abbiamo una consolidata architettura istituzionale, dovuta alla preveggenza del Senatore Generale Luigi Ramponi (alla cui cara memoria è dedicato questo libro). La cosiddetta "mozione Ramponi" del 2011 ha posto le basi per questa struttura, dando in seguito vita al DPCM 24/1/2013 sulla protezione cibernetica e la sicurezza informatica nazionale, detto Decreto Monti, recentemente aggiornato dal Presidente Gentiloni (DPCM 17/2/2017).

La Direttiva NIS si sviluppa dal presupposto riguardante l'insufficienza di un approccio nazionale per far fronte alle sfide della sicurezza, e prevede quindi un minimo standard di sicurezza comune, puntando molto, fra l'altro, sul criptaggio dei dati.

La Direttiva, inoltre, prevede l'istituzione di una (o più) Autorità nazionale NIS e di un punto unico di contatto nazionale per la ricezione delle notifiche di incidenti e la cooperazione alla loro risoluzione, prevedendo specifici obblighi di sicurezza informatica per gli operatori di servizi essenziali (nei settori dell'energia, del trasporto, bancario e finanziario, sanitario, idrico e delle infrastrutture digitali) e i fornitori di servizi digitali (come i motori di ricerca on-line, i negozi on-line, i servizi di *cloud computing*), tra cui l'obbligo della tempestiva notifica all'Autorità nazionale NIS.

Il GDPR (Art. 83, par.4), già in vigore, ma applicabile a partire dal 25 maggio 2018, a sua volta prevede sanzioni pesanti, con multe fino al 2% o 4% del fatturato annuo dell'azienda che non ottemperi all'obbligo di comunicare tempestivamente una fuga di dati (*Data Breach*). Sanzioni amministrative riguardano anche le Amministrazioni pubbliche.

Da qui l'esigenza sempre più avvertita di assicurarsi contro attacchi e incidenti vari. Negli USA, all'avanguardia nel settore, quasi 1 azienda su 3 possiede una polizza sul rischio cibernetico. Ovviamente al momento non esistono sufficienti dati storici per determinare matematicamente il premio da pagare, ragion per cui è ancora ipotizzabile e consentita una trattativa fra azienda e compagnia assicurativa, lasciando chiaramente all'azienda l'eventuale selezione degli asset da assicurare. La copertura, infatti, può riguardare i costi di ripristino, il danno alla reputazione, il lucro cessante, etc. Da notare

il recente forte incremento della richiesta di assicurarsi da parte delle imprese, come confermano importanti operatori del settore. In Italia, tuttavia, devono essere superate alcune difficoltà legislative per quanto riguarda in particolare la copertura dei danni procurati dai *ransomware*.

La necessaria precisione dei concetti: dalla Information Warfare alla Cyber e Hybrid Warfare

La rapidissima evoluzione degli attacchi cibernetici e delle modalità con le quali essi vengono attuati ha comportato alcuni problemi di interpretazione concettuale.

Quando alcune idee e discipline si sviluppano in fretta per tenere il passo, come nel nostro caso, con l'inarrestabile e impetuoso sviluppo della tecnologia accade che i concetti, ossia i mattoni logici sui quali si erge ogni costruzione scientifica, abbiano connotazione e denotazione diversificata e imprecisa, tanto più che questi vengono interpretati in funzione delle varie culture e ambienti relativi ad essi. È il caso, dunque, dei concetti di Information Warfare, Cyber Warfare e Hybrid (Cyber) Warfare. L'imprecisione concettuale è tipica del linguaggio comune, ma è noto che il linguaggio scientifico non tollera concetti plurisenso. Ogni termine deve avere un solo significato per tutta la comunità scientifica. Solo così si sviluppa il linguaggio tecnico di ogni disciplina, *condicio sine qua non* al progresso della medesima.

I concetti, inoltre, sono come dei "contenitori" sintetici che riferiscono a "contenuti" diversificati (i cd referenti empirici). Lungi dalla pretesa di risolvere una volta per sempre il problema, ciò che abbiamo ritenuto di dover tentare consiste, sulla scorta anche della letteratura più accreditata, nell'arrivare a delle definizioni sulle quali sia possibile un confronto e, auspicabilmente, un'adesione almeno a livello nazionale.

A premessa del processo di disambiguazione è opportuno osservare che esiste una relazione inversamente proporzionale fra denotazione, o estensione di un concetto, e connotazione, o intensione del medesimo. In altre parole: quanto maggiore è il numero degli "oggetti" cui il concetto si riferisce, tanto minore è la precisione del suo contenuto e viceversa.

In sostanza de-finire è creare un confine e questo – come è stato detto – (Enzo Colombo, Univ. di Milano) – «è un atto generatore di realtà, un atto che dà forma al mondo introducendo una discontinuità dove prima c'era omogeneità».

Detto ciò, esaminiamo innanzitutto una (provvisoria) definizione dei concetti qui pertinenti, per passare successivamente all'analisi dei loro rispettivi contenuti. Solo dopo l'esplicitazione di questi ultimi si potranno prendere in considerazione definizioni eventualmente più precise e si avranno, comunque, idee più chiare in materia.