Information Warfare 2012

Armi cibernetiche e processo decisionale

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 2012

Armi cibernetiche e processo decisionale

a cura di Umberto Gori
e Serena Lisi

FrancoAngeli

La Conferenza, svoltasi per la prima volta presso l'Aula Magna dell'Università "La Sapienza" di Roma, è stata ideata dal Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali dell'Università degli Studi di Firenze (CSSII), dalla Link Campus University, dal Centro Studi "Gino Germani" e dall'Istituto di Studi di Previsione e le Ricerche Internazionali (ISPRI), d'intesa con Maglan Europe, realtà leader internazionale nell'auditing e consulting per la difesa delle informazioni in ambito civile, militare e governativo.

Indice

Indirizzo di saluto

di *Antonello Folco Biagini*[*]

Discutere nel cuore scientifico di Roma - l'Università degli Studi "La Sapienza" - di un tema "caldo" come "Armi cibernetiche e processo decisionale", nonostante le criticità che l'argomento potrebbe sollevare, mi sembra importante per almeno due ordini di ragioni.

La prima è che testimonia la volontà del nostro Ateneo di impegnarsi direttamente nell'opera di rilancio della riflessione sulle relazioni internazionali a Roma. La Capitale, pur essendo il luogo dove vengono fisicamente compiute le scelte da cui dipende la proiezione dell'Italia nel Mondo, in passato ha visto dedicare minore attenzione alla riflessione accademica sulla politica internazionale rispetto ad altre piazze politicamente meno importanti. Negli ultimi anni, tuttavia, abbiamo cercato di invertire questa tendenza invitando alla Sapienza grandi attori delle relazioni internazionali ed esperti di geopolitica, che hanno attirato l'attenzione non solo di studenti e ricercatori, ma anche di un pubblico di esperti esterno al mondo universitario.

La seconda ragione è che "La Sapienza" si vuole fare promotrice di un dibattito di tipo nuovo, soprattutto rispetto ad argomenti che ritiene costituiscano parte integrante di un concetto decisivo, ma non ancora compiutamente declinato e condiviso, come quello di "interesse nazionale". Una delle parole chiave delle riforme degli ultimi venti anni è stata l'evoluzione in senso "multidisciplinare" dell'Università e, quindi, per dare un riscontro concreto dell'adozione di tale concetto abbiamo sostenuto fortemente l'organizzazione di un incontro, come l'Information Warfare Conference 2012, in grado di mettere intorno ad uno stesso tavolo un gruppo eterogeneo di

[*] Prorettore per la Cooperazione e i Rapporti internazionali

relatori composto da diplomatici, storici, politologi, militari, ingegneri e rappresentanti del settore privato.

Al di là di ragioni il cui risvolto pratico appare molto evidente, tuttavia, la IWC 2012 stimola anche la riflessione teorica intorno ad un settore rilevante per la nostra contemporaneità. Parlare di armi cibernetiche e processo decisionale nel mondo occidentale, d'altronde, significa trattare un tema politico nevralgico come il rapporto tra guerra e democrazia soprattutto sulla definizione del concetto di "difesa" e in qualche modo la riproposizione dell'antico dibattito sulla guerra giusta e su quella ingiusta. È comunque fuori discussione che alla democrazia si associ una sola possibilità di conflitto e cioè quello relativo alla necessità della difesa di tutto ciò che – attualmente – si coniuga alle tematiche relative al rispetto dei diritti umani. Il conflitto in senso "classico" – quello con gli eserciti in divisa che si fronteggiano sul campo di battaglia – è ormai tramontato in quanto Stati e/o gruppi non statali sono in grado di sferrare colpi dalle conseguenze altrettanto drammatiche attraverso mezzi non convenzionali, come le armi cibernetiche e l'utilizzo del cyberspazio, contro i sistemi di sicurezza nazionali, delle grandi imprese e delle banche. Per salvaguardare la democrazia è necessario fronteggiare tali minacce, comprendendo appieno la difficoltà di arginare una dimensione che supera la distinzione politica tradizionale di interno/esterno e individuare i mezzi sia giuridici che di intelligence imprescindibili per un sistema di difesa da azioni evidentemente ostili, ma non ancora classificate come veri e propri atti di guerra.

Prefazione

di *Vincenzo Scotti*[*]

1. Tema centrale e obiettivi culturali della conferenza

Un numero crescente di Stati si sta dotando di armi cibernetiche, alcune delle quali ad elevata potenza distruttiva. Anche molti attori privati o "non-statali" si stanno dotando di cyber weapons sia difensive che offensive. L'interesse ad acquisire armi cibernetiche non riguarda soltanto le entità illecite o devianti (mafie, gruppi terroristici, movimenti "cyber-anarchici", criminali informatici o singoli hackers malintenzionati), ma anche attori non-statali leciti, come imprese, istituti bancari e finanziari, lobbies, gruppi politici, movimenti religiosi.

Lo sviluppo di armi cibernetiche, e la loro diffusione a una molteplicità di attori, statali e non, stanno trasformando la geopolitica globale e creando nuove forme di conflittualità e nuovi problemi di sicurezza e stabilità sia all'interno degli Stati sia a livello del sistema internazionale nel suo complesso.

Inoltre, la caratteristica peculiare che contraddistingue le cyber weapons è che esse colpiscono il processo decisionale e la capacità di reazione dello Stato o organizzazione bersaglio dell'aggressione. Gli attacchi cibernetici, infatti, mirano a influenzare o a paralizzare il processo decisionale dell'avversario.

In considerazione di ciò il comitato organizzatore di questa conferenza ritiene particolarmente opportuno porre al centro dell'evento due obiettivi culturali di fondo:

[*] Presidente Link Campus University

- Il primo obiettivo è aumentare la consapevolezza, tra i decisori politici ed economici del sistema-Italia, dell'emergere delle armi cibernetiche , nonché dei problemi inediti che esse creano per i processi decisionali nel campo della sicurezza nazionale e nel settore privato.
- Il secondo obiettivo è dare un contributo innovativo di idee e proposte utili all'elaborazione di una strategia italiana di sicurezza cibernetica nazionale e alla riforma della struttura decisionale in materia di difesa e sicurezza nazionale. Nell'era delle armi cibernetiche occorre potenziare sempre di più le capacità decisionali del sistema-paese per quanto riguarda sia la prevenzione sia la reazione efficace e tempestiva a eventuali attacchi cibernetici.

La Link Campus University , in collaborazione con gli altri Enti promotori di questa conferenza (il CSSII, il Centro Studi Gino Germani) e insieme alla Maglan Information Defense and Intelligence e altre importanti aziende, intende promuovere un programma di formazione universitaria avanzata sulle tematiche centrali di questa conferenza.

2. Le ripercussioni delle armi cibernetiche sulle relazioni internazionali e sulla sicurezza globale.

È ancora limitata la nostra conoscenza delle implicazioni delle cyber weapons per la sicurezza e la stabilità internazionale. Tuttavia, è possibile individuare alcune linee di tendenza che caratterizzeranno le relazioni internazionali nell'era cibernetica:

- gli Stati – non solo le grandi potenze ma anche potenze medie e piccole – utilizzeranno con crescente frequenza armi cibernetiche offensive per conseguire vantaggi strategici e politici.
- Un numero sempre maggiore di attori non-statali acquisiranno cyber weapons e se ne serviranno per sfidare, minacciare o influenzare gli Stati. Le armi cibernetiche, pertanto, sono destinate a favorire una crescente diffusione e frammentazione del potere nel sistema internazionale.
- Gli Stati continueranno a essere gli attori preminenti della politica internazionale, ma la loro centralità verrà sempre più messa in discussione da una molteplicità di entità e poteri non-statali dotati di armi cibernetiche offensive. Inoltre, la diffusione di tali armi tenderà a indebo-

lire la capacità degli Stati di esercitare la sovranità e mantenere l'ordine e la stabilità all'interno dei propri territori.

- Lo sviluppo e la proliferazione di armi cibernetiche accentuerà i fenomeni di conflittualità e d'instabilità nelle relazioni internazionali. Diversi fattori spiegano l'impatto potenzialmente destabilizzante delle cyber weapons sui rapporti strategici fra Stati. Vanno menzionati l'assenza di un quadro normativo internazionale relativo all'uso della forza nel cyberspazio, nonché l'inefficacia delle strategie di sicurezza cibernetica fondate sul concetto di deterrenza.

3. Ripensare le strategie di sicurezza a livello globale e nazionale

Le cyber weapons ci obbligano a ripensare sia il concetto di "sicurezza" sia le strategie di sicurezza adottate a livello sovranazionale e dei singoli Stati.

Una delle maggiori sfide intellettuali e politiche del futuro per la comunità internazionale è l'elaborazione di una visione strategica nuova atta a contrastare e contenere, a livello globale, le conseguenze potenzialmente destabilizzanti delle armi cibernetiche offensive.

Inoltre, diversi Stati, per fronteggiare le crescenti minacce provenienti dal cyberspazio, hanno elaborato una propria strategia di sicurezza cibernetica nazionale e costituito una struttura centrale di direzione e pianificazione strategica in materia di cyber-security.

In vari Paesi dell'area euro-occidentale (tra cui Stati Uniti, Gran Bretagna, Francia, Olanda) le innovazioni nel campo della cyber-security si inseriscono in uno sforzo più ampio di superamento delle politiche tradizionali di tutela della sicurezza, che appaiono sempre meno adeguate per contrastare minacce complesse, multidimensionali, interdipendenti e in continua evoluzione.

Negli ultimi anni detti Paesi hanno adottato un nuovo approccio alla gestione della sicurezza che comprende due importanti innovazioni:

- l'adozione di una propria "strategia di sicurezza nazionale": un disegno strategico di ampio respiro che identifica gli interessi vitali del sistema-paese e il suo ruolo nel sistema internazionale, individua i rischi e le minacce alla sua sicurezza, e indica le linee-guida strategiche di risposta a tali sfide.
- La creazione di una struttura governativa, per alcuni aspetti simile al National Security Council americano, preposta alla pianificazione

strategica delle politiche di sicurezza. Tale struttura dovrebbe permettere un'elevata integrazione e coerenza tra i processi decisionali nei vari settori attinenti alla sicurezza nazionale (politica estera, difesa, sicurezza interna, sicurezza cibernetica, stabilità finanziaria).

4. Implicazioni per l'Italia

Uno scenario più insidioso e complesso di rischi e minacce al sistema-Italia rende sempre più necessaria l'elaborazione di una visione strategica nazionale chiara e coerente, nonché il potenziamento delle capacità di pianificazione e decision-making dell'apparato governativo nazionale.

Noi ci auguriamo che questa conferenza non solo contribuisca a elevare la consapevolezza delle minacce cibernetiche e delle loro profonde implicazioni politico-strategiche, ma anche ad avviare una riflessione più ampia circa la necessità di adottare una strategia di sicurezza nazionale per l'Italia e di creare, nell'ambito della Presidenza del Consiglio dei Ministri, un "consiglio di sicurezza nazionale".

In Italia, la gestione dei vari aspetti della sicurezza nazionale è ancora frammentata tra diversi dicasteri. Per poter contrastare minacce multidimensionali e interdipendenti occorre non solo rafforzare il coordinamento inter-ministeriale, ma promuovere una sempre maggiore integrazione tra i vari apparati governativi coinvolti nelle attività di tutela della sicurezza . Alla luce di questa esigenza appare opportuno creare una struttura centrale di direzione e pianificazione strategica in materia di sicurezza nazionale: un National Security Council italiano.

Una tale struttura, composta dal Presidente del Consiglio e dai Ministri competenti nei vari settori della sicurezza nazionale (Esteri, Difesa, Interno, Economia e Finanza), dovrebbe disporre di un apparato permanente preposto ad attività di pianificazione strategica e di supervisione dei processi di attuazione delle politiche di sicurezza.

Per concludere, vorrei sottolineare il ruolo importante che dovrà svolgere il mondo universitario e della ricerca nel processo di elaborazione di una nuova visione strategica per il sistema-Italia. Ciò richiederà la creazione di nuove sinergie fra Università, apparati istituzionali, e settore privato. Il sistema universitario potrà affrontare questa sfida solo superando la diffidenza culturale con cui il mondo accademico italiano spesso percepisce gli studi strategici e le problematiche della sicurezza nazionale.

Riconoscimenti

Adesione del Presidente della Repubblica

Patrocini

Senato della Repubblica
Camera dei Deputati
Presidenza del Consiglio dei Ministri
Ministero della Difesa
Ministero dello Sviluppo Economico

Promotori

Link Campus University
Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII)
Centro Studi "Gino Germani"
Istituto per gli Studi di Previsione e le Ricerche Internazionali (ISPRI)

Ideata d'intesa con Maglan - Information Defense & Intelligence

con il contributo di ELT - Elettronica
con la sponsorship di Finmeccanica, Beta 80 Group, IBM, HMS

Medaglia di Rappresentanza, con firma del Presidente della Repubblica Giorgio Napolitano, inviata al Prof. Umberto Gori, direttore scientifico della Conferenza, in segno di apprezzamento per l'iniziativa

Cyberspazio e relazioni internazionali: implicazioni geopolitiche e geostrategiche

di *Umberto Gori*[*]

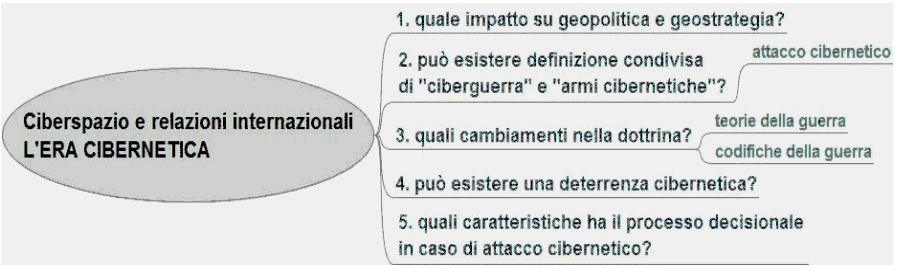
Questa relazione ha l'ambizione di fornire un contesto ai ben più importanti contributi di questa terza Conferenza nazionale sull'Information Warfare, dedicata quest'anno al tema innovativo *Armi cibernetiche e processo decisionale.* A tal fine cercherò di dare una risposta - ovviamente aperta a discussione – ai seguenti quesiti:

1. Quale impatto ha l'era del cyberspazio sulla geopolitica e sulla strategia ?
2. È possibile una definizione condivisa del concetto di cyber guerra e di 'armi cibernetiche' (*cyber weapons*) ?
3. Quale deve essere la dottrina d'impiego delle armi cibernetiche ? In particolare, subiscono mutamenti le teorie e codificazioni della guerra ?
4. Può esistere una deterrenza cibernetica ?
5. Quali caratteristiche ha il processo decisionale di fronte alla minaccia di attacchi cibernetici ?

Risponderò a ciascuna di queste domande nei seguenti paragrafi.

[*] Professore Emerito, Università degli Studi di Firenze – Presidente del Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII), Direttore, Istituto per gli Studi di Previsione (ISPRI).

La fine della geografia



Se è vero che la geopolitica studia gli effetti della geografia sulla politica, che è storia *in fieri* e da fare, che guarda al futuro, che non è mai neutrale e che è la rappresentazione delle relazioni internazionali in funzione dei propri interessi, la domanda che si pone è se essa non muti natura con l'avvento dell'era digitale.

Molti ritengono infatti che le tecnologie dell'informazione abbiano causato la «fine della geografia» su cui la geopolitica tradizionalmente si appoggia, così come Fukujama, per altri versi, aveva teorizzato la «fine della storia».

Così come Mackinder aveva salutato l'avvento della ferrovia come lo sblocco del potenziale dell'*Heartland* a danno delle Potenze marittime, così i sostenitori dell'IW hanno visto l'avvento delle reti come il declino della geopolitica e della strategia continentale.

L'idea non è nuova. Infatti De Seversky, agli inizi degli anni Cinquanta, aveva parlato della *nuova geopolitica del Potere aereo* che aveva spazzato via i tradizionali limiti geografici imposti alla strategia.

Più recentemente, sostenitori della RMA, come Libicki e altri, hanno sostenuto che la rivoluzione informatica ha alterato del tutto la natura del tempo, dello spazio e della distanza nelle interazioni moderne. In sintesi estrema, si sostiene insomma che la geopolitica di Mahan, Mackinder, Spykman, Kissinger e Brzezinski è diventata, tutta d'un colpo, obsoleta.

Alcuni affermano che il cyberspazio è un *non-luogo*. Ma un *non-luogo* può avere effetti sulle relazioni internazionali? e se sì, come? Se i confini spariscono nel cyberspazio, può esserci una geopolitica, sia pure virtuale?

La nostra era, basata sulla conoscenza e sulla tecnologia, ha drammaticamente ridimensionato, e talora annullato, fattori fondamentali quali lo spazio e il tempo. Tutto, oggi, si muove verso l'*intangibile*. Una tendenza,

questa, che è una costante nella storia dello sviluppo umano. In altre parole, in natura tutti i progressi appaiono andare dal materiale all'astratto.

Anche la guerra, da azione reciproca di forza materiale che produce distruzioni fisiche e spargimento di sangue, è diventata *virtuale*. L'evoluzione del fenomeno bellico dipende anche dai processi di globalizzazione e dalla nascita della politica *post-internazionale*, una politica, cioè, che non si svolge più soltanto fra «nazioni», ma piuttosto con e fra sottosistemi di queste. Ed ecco le «nuove guerre» o «guerre post-moderne», come le chiama Mary Kaldor, guerre asimmetriche, a bassa intensità (si noti il procedere a un sempre minor impiego della forza fisica), che non consentono una chiara distinzione fra «interno» e «internazionale», basate su rivendicazioni di identità piuttosto che di territorio (anche qui si va dal concreto all'astratto). In questa categoria possono rientrare anche le guerre virtuali, le guerre nel cyberspazio che, dopo la terra, il mare, il cielo e lo spazio, costituisce la quinta dimensione della conflittualità.

Una *cyber war* totale, secondo i maggiori esperti, può modificare l'equilibrio strategico e alterare profondamente le relazioni politiche ed economiche fra gli Stati. Nello stesso tempo, la cyber war potrebbe realizzare l'ideale, antico di 2.500 anni, di Sun Tzu: sottomettere il nemico senza combattere. L'annientamento dell'avversario sarà quello strategico piuttosto che quello fisico. Gli attori non statali giocheranno ruoli importanti in queste guerre, ruoli che , da secoli, appartenevano solo agli Stati.

A fronte di questa evoluzione sorge un problema e la risposta non è semplice. Dopo il periodo della geopolitica «binaria» (terra contro mare, MacKinder e Mahan), della geostrategia dei tempi della guerra fredda, della geoeconomia (Luttwak) e geofinanza (Savona, Jean), della geopolitica dello spazio extra-atmosferico (Collins) stiamo vivendo il periodo della *geopolitica virtuale*? Il prefisso *geo*, la terra, lo spazio, sta anch'esso subendo un processo di *efemeralizzazione*? Questa strana parola fu coniata nel 1938 dallo scienziato e filosofo statunitense Buckminster Fuller che si riferiva all'uso delle risorse tecnologiche per ottenere il miglior risultato con il minimo sforzo, per «fare sempre di più con sempre meno peso, tempo ed energia per ogni dato livello di prestazione funzionale ». Con il processo di *efemeralizzazione*, in una parola, si può ottenere sempre di più con un uso sempre più limitato di risorse. È l'effetto «crisalide».

In realtà, allo spazio fisico, orizzontale, si è progressivamente sostituito uno spazio progressivamente dematerializzato, verticale, come risulta chiaro dalla denominazione di geoeconomia, geofinanza, geocultura, ecc.. Lo *spazio cibernetico*, in particolare, è unico perché costruito dall'uomo e soggetto quindi a mutamenti tecnologici molto più rapidi di qualsiasi altro spa-

zio. Come qualcuno ha osservato, la geografia del cyberspace è molto più mutevole di ogni altro spazio. Non si possono spostare montagne e oceani, ma porzioni del cyberspazio possono essere aperte o cancellate con un semplice *click*.

Così le caratteristiche del cyberspazio, fruibile da chiunque (ed è per questo che fa parte dei *global commons*), riducono il differenziale di potere fra gli attori, statuali e non, contribuendo in tal modo alla diffusione di potenza che caratterizza la politica post-internazionale.

La situazione appena descritta fa sorgere il problema di sapere se si vada o meno verso un mondo caratterizzato dalla sparizione delle limitazioni prodotte dalla geografia e dallo spazio fisico e se si possa quindi parlare di una geopolitica virtuale e delle sue nuove peculiarità.

Anche se le metafore geografiche e spaziali sono impiegate utilmente per interiorizzare un nuovo mondo complesso fatto di impulsi elettronici e quindi invisibile ai nostri occhi, già da molti anni è aperto un dibattito sul declino, e addirittura sparizione, della geografia e dello spazio, visto come ostacolo allo scambio delle comunicazioni e alle relazioni politiche ed economiche internazionali.

Si è parlato della fine della geopolitica, ma anche della «geopolitica nascosta del cyberspazio» (Ron Deibert, 2010). Anche se apparentemente suggestiva, però, la tesi della fine della geografia e della geopolitica appare alquanto esagerata. È vero che spazio e tempo sono stati drasticamente ridimensionati, ma è altrettanto vero che il territorio resta un basilare principio organizzativo che definisce sia le relazioni sociali che quelle umane.

Ciò che semmai è innovativo è il ruolo dell'informazione istantanea che agisce come un «facilitatore» rispetto alla geografia fisica e alle forme, militari e non, del potere.

In altre parole, l'era dell'informazione non libera improvvisamente l'arte della conflittualità e della guerra dalle realtà geografiche e logistiche del mondo fisico (Collins, Gray, Mearsheimer). Alcuni analisti (Robert D. Kaplan) hanno addirittura parlato di *revenge of geography*. Colin Gray, in particolare (*The Continued Primacy of Geography*, p. 251), afferma che:

> all politics is geopolitics, and (…) all strategy is geostrategy.

Per esempio, l'emergere della Cina come potenza mondiale non può essere compresa solo in termini di ciberspazio e di tecnologia informatica, ma come dimensione, popolazione, accesso al mare, geografia e crescita economica e — aggiungo io — una particolare cultura.

La geografia, insomma, rappresenta «la grammatica della strategia», laddove la logica di quest'ultima è data dalla politica.

Vero è che la geografia condiziona, ma non determina, la strategia. La geografia è una costante, ma la creatività politica ne può fare una variabile nel calcolo strategico (magari attraverso la stipula di un'alleanza).

È Joseph Nye che ha affermato che il «ciberspazio non rimpiazzerà lo spazio geografico e non abolirà la sovranità dello Stato, ma (…) coesisterà con loro, complicando non poco ciò che significa essere uno Stato sovrano o uno Stato potente » (Nye, *The Information Revolution and American Soft Power*, p. 68).

La guerra cibernetica

Vediamo cioè di chiarire che cosa sia in realtà una guerra cibernetica (*cyber war*) e cosa siano le armi cibernetiche (*cyber weapons*). Secondo Scott Borg, direttore della US Cyber Consequences Unit, finora è stata creata molta confusione intorno al concetto di *cyber war* soprattutto a causa dell'«idea errata che gli attacchi informatici riguardino principalmente i sistemi di telecomunicazioni». Finora — sostiene questo A. — «non vi è stata alcuna guerra informatica».

Una ricerca della nota azienda di sicurezza informatica McAfee mette in evidenza tre dati interessanti a proposito della *cyber war*:

— alcuni Stati cercano segretamente di studiare *cyber weapons* sempre più sofisticate. Non si è ancora in presenza di una hot cyber war, ma certo viviamo già l'era della *cyber guerra fredda*;

— se dovesse scoppiare un *cyber conflitto* di vaste dimensioni fra Stati, il settore privato ne subirebbe tutte le conseguenze: le infrastrutture critiche sarebbero vulnerabili ad attacchi condotti tramite Internet;

— il dibattito sulle problematiche relative alla *cyber war* avvengono troppo spesso a porte chiuse e addirittura molti Stati considerano queste questioni classificate. Secondo la classica definizione ispirata da Clausewitz, il concetto di guerra implica l'uso della forza fisica *organizzata*. Oggi, ciò non è più necessariamente vero. Allora, per determinare se un attacco cibernetico è cyber war quali fattori dovremmo logicamente prendere in considerazione? Anche ammettendo che l'analisi potrebbe di solito non essere così semplice, la mia opinione è che dovremmo innanzi tutto individuare la fonte, e cioè valutare: