RESEARCH ANALYSIS
GIUGNO 2013

LA QUINTA DIMENSIONE DELLA CONFLITTUALITÀ. LA RILEVANZA STRATEGICA DEL CYBERSPACE E I RISCHI DI GUERRA CIBERNETICA

LUIGI MARTINO

UNIVERSITÀ DEGLI STUDI FIRENZE

Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

LA QUINTA DIMENSIONE DELLA CONFLITTUALITÀ. LA RILEVANZA STRATEGICA DEL CYBERSPACE E I RISCHI DI GUERRA CIBERNETICA

Luigi Martino

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

Giugno 2013

RIGUARDO ALL'AUTORE

Si è laureato cum Laude in Relazioni Internazionali e Studi Europei presso la Facoltà di Scienze Politiche "Cesare Alfieri" di Firenze, con una Tesi sulla rilevanza strategica del cyberspace e i rischi di guerra cibernetica. si interessa, oltre che di Studi Strategici e Politica Internazionale, anche di Intelligence e Processi Decisionali. Attualmente, sempre alla "Cesare Alfieri", è Cultore della Materia in ICT Policies e insegna *Cyber Security and International Relations*. E' Phd Candidate alla Scuola Superiore Sant'Anna di Pisa, con un progetto di tesi sul miglioramento della Cyber Security per la protezione delle infrastrutture critiche dagli attacchi cyber, ed è consultant in Cyber Security del gruppo BV-Tech S.p.A. Dal 2016 è project manager del progetto di ricerca OSCE: "Enhancing the Implementation of Conflict Stemming From the Use of ICT's." un progetto di ricerca congiunto tra OSCE e Università di Firenze. È membro del Research Advisory Group of the Global Commission on the Stability of Cyberspace e del gruppo di esperti ENISA per l'implementazione della Direttiva Europea NIS. Dal 2017 e' membro del gruppo di lavoro Ise-shima G7 Cyber Group e del Forum for Cyber Expertise, dove rappresenta il Center for Cyber Security and International Relations Studies. Autore di numerose pubblicazioni in italiano, inglese e spagnolo su temi legati alla cyber security, cyber warfare, cyber intelligence e cyber diplomacy, ha curato, con Umberto Gori, il libro *Intelligence e Interesse Nazionale*, Aracne Editrice 2015

LA QUINTA DIMENSIONE DELLA CONFLITTUALITÀ. LA RILEVANZA STRATEGICA DEL CYBERSPACE E I RISCHI DI GUERRA CIBERNETICA

INTRODUZIONE

Questa ricerca si pone l'obiettivo di evidenziare la crescente rilevanza strategica assunta dal dominio cibernetico nelle dinamiche della politica internazionale. Lo spazio cibernetico, ambiente artificiale e frutto per eccellenza dell'attività umana, è divenuto cruciale per il potere nel XXI secolo. Dopo terra, mare, aria e spazio extra-atmosferico, il *cyberspace* rappresenta la quinta dimensione della conflittualità. La natura antropica dello spazio cibernetico accentua il nichilismo alienante di una *guerra civilizzata* senza alcuna connotazione militare, trasformandola in una violenza *senza limiti* condotta attraverso minacce *trasversali*. La pervasività delle *Information Technology* e il rilevante impatto delle *Information Communication Telecomunication* (ICT), nonché la crescente interconnessione e interdipendenza raggiunta a vari livelli (politico-economico-sociale-finanziario-militare) dei Paesi intensamente informatizzati, fa emergere un intrinseco *trade-off* tra informatizzazione e sicurezza. In altre parole, i punti di forza dei Paesi tecnologicamente avanzati rischiano di trasformarsi nella più perniciosa delle vulnerabilità. Il tipo di *armi-non militari* utilizzate per combattere, così come gli obiettivi presi di mira, rende i sistemi civili i nuovi *centri di gravità* da dover proteggere contro un nemico che il più delle volte "agisce nelle ombre", favorito da un ambiente sfumato e asimmetrico. Lo stesso scenario internazionale, sotto la spinta propulsiva della rivoluzione informatica (che ha facilitato la "democratizzazione delle informazioni") sta radicalmente evolvendosi da unipolare (a guida americana) verso una architettura pressoché multipolare. La struttura stessa del potere si sta trasformando da piramidale a reticolare dove gli Stati nazionali, retaggio della pace westfaliana, si vedono erodere le loro prerogative (monopolio della violenza e delle informazioni) da nuovi attori (sub-nazionali, transnazionali, non-statali, individui) capaci di influenzare e modellare i processi decisionali. Lo studio condotto parte

dall'assunto archetipo che la guerra, essendo un fenomeno sociale, difficilmente può essere estirpata dalla natura "umana" delle relazioni internazionali, che – come spiega Raymond Aron – si differenziano dalle altre attività sociali proprio per la presenza intrinseca della guerra[1]. Questa, come un *camaleonte*, assume le caratteristiche del contesto socio-culturale e tecnologico nel quale è immersa. Il *cyberspace*, una volta inglobato nei domini della conflittualità, si piega al suo carattere minaccioso e distruttivo. L'interesse per lo studio del dominio cibernetico, dunque, è motivato perlopiù dal suo carattere di ambiente artificiale, dinamico e ubiquo, i cui rischi intrinsechi risiedono nella sua natura virtuale. In questo ambiente strategico le teorie classiche della deterrenza devono essere ripensate per poter ottenere una difesa efficace. Durante la ricerca si è considerato il limite relativo alla difficile reperibilità delle fonti ufficiali causato, in larga misura, dalla reticenza dei governi e degli attori privati (primi obiettivi delle minacce cibernetiche) di divulgare i dati ufficiali sugli effetti e sui danni provocati dagli attacchi cibernetici. L'attualità del campo di ricerca non ha permesso, al momento della stesura, di rintracciare una condivisione diffusa a livello internazionale sulle definizioni di base. Per sopperire a questi ostacoli si è scelto di utilizzare i documenti reperiti da fonti militari ufficiali quali, ad esempio, quelli dati in dotazione all'esercito americano (U.S. *DoD*), nonché le direttive presidenziali statunitensi. Per la parte analitica della tesi si è fatto affidamento sulla letteratura accademica e scientifica perlopiù anglosassone. È doveroso citare la valenza e l'importanza in materia, degli studi condotti in Italia dalla *Cyber Warfare Conference*, ciclo di conferenze annuali che si prospetta il compito di coinvolgere nel campo della difesa cibernetica, il settore pubblico e privato; e le cui pubblicazioni annuali dei vari contributi di esperti hanno come scopo quello di sensibilizzare l'opinione pubblica sui rischi reali derivanti dallo spazio cibernetico. La lettura dei vari studi condotti e pubblicati dal prof. Umberto Gori, emerito dell'Università di Firenze, nonché presidente del Centro interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII), ha fornito un contributo fondamentale per la ricerca.

[1] Cfr. R. Aron, *La politica, la guerra, la storia*, Il Mulino, Bologna 1992

1. DEFINIZIONI

1.1 Lo spazio cibernetico

Fin dalla metà degli anni '90, numerosi esperti hanno proposto svariate definizioni per spazio cibernetico, meglio noto con il termine anglosassone *cyberspace*[2]. Tra questi vi è Daniel T. Kuehl che descrive lo spazio cibernetico come:

"Un dominio globale all'interno dell'ambiente informatico il cui carattere distintivo e unico è caratterizzato da un uso dell'elettronica e dello spettro elettromagnetico per creare, memorizzare, modificare, scambiare, e sfruttare le informazioni attraverso sistemi interdipendenti e interconnessi che utilizzano le tecnologie delle informazioni e delle comunicazioni".[3]

La peculiarità del *cyberspace* è essenzialmente dovuta al fatto che il dominio cibernetico non è un *global common* puramente naturale come tutti gli altri, ma una realtà ibrida. Ne consegue che alla sua formazione concorrono sia elementi naturali che virtuali[4]. Questa natura "spuria" riflette l'incertezza e l'incapacità da parte degli "addetti ai lavori" di circoscrivere una cornice strategica e operativa, dentro la quale far rientrare le azioni e le operazioni condotte "nel e tramite" il *cyberspace*[5]. Secondo Martin C. Libicki il *cyberspace* è un *medium* virtuale e intangibile a differenza degli altri domini quali: la terra, l'acqua, l'aria e lo spazio extra-atmosferico[6]. Un modo utile per comprendere la natura "ibrida" del dominio cibernetico – continua Libicki – è rappresentare questa realtà su tre livelli: quello fisico, sintattico e semantico[7]. Nel dettaglio, Libicki spiega che: **Il livello fisico**: è costituito dagli elementi "materiali" del cyberspace, i cavi a

---

[2] Secondo F. D. Kramer esistono 28 differenti definizioni del termine *cyberspace*. Cfr. Id., *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, in *Cyberpower and National Security*, ed. by F.D. Kramer, S. Starr, L.K. Wentz, National Defense University Press, Washington (D.C.) 2009

[3] Cfr. D.T. Kuehl, *From Cyberspace to Cyber-power: Defining the Problem, in Cyberpower and National Security*...op. cit., cit. pp. 26-28. [T.d.A.]

[4] Sulla diatriba legata alla concezione del *cyberspace* come un *global common* o viceversa come un dominio esclusivamente artificiale e quindi ritenuto uno strumento creato dall'uomo piuttosto che una risorsa naturale e godibile dall'intera umanità anche esulando dagli ordinamenti giuridici nazionali si rinvia al paragrafo interamente dedicato in questo lavoro dal titolo " *global common o dominio antropico*?" .

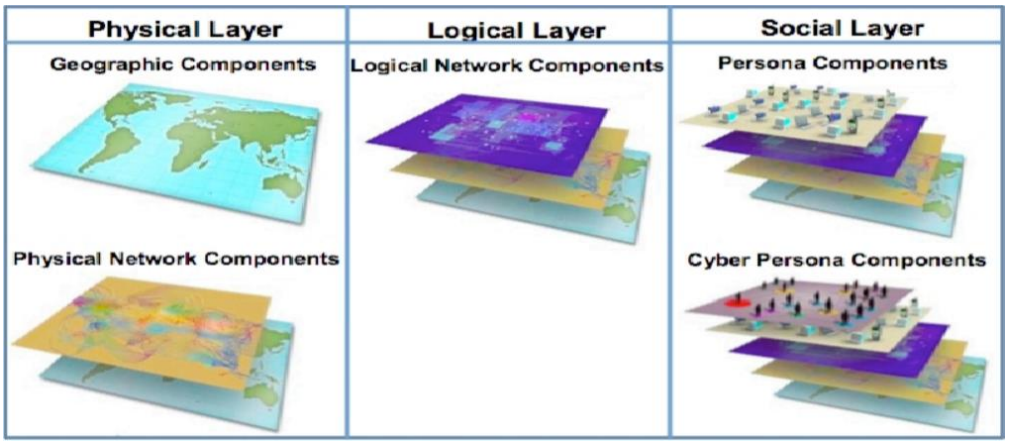
[5] Cfr. J. S. Nye, *The Future of Power*, PublicAffairs, New York, 2011.

[6] Cfr. M. C. Libicki, *Cyberdeterrence and Cyberwarfare*, RAND, Santa Monica (CA) 2009. In riferimento a questo passaggio si legga: "Chapter Two: A Conceptual Framework" pp. 11-37.

[7] *Ibidem*

fibra ottica, i satelliti, i router, le antenne, ecc. Tale livello può essere interrotto o rimosso attraverso classiche operazioni cinetiche[8]. **Il livello sintattico**: in posizione superiore rispetto a quello fisico, è costituito dalle informazioni e dalle istruzioni che i progettisti e gli utenti danno allo strumento informatico; si tratta in particolare, dei protocolli operativi per mezzo dei quali i computer o le "macchine" interagiscono con le infrastrutture di riferimento e con altri dispositivi. In questo strato del cyberspace si possono verificare azioni c.d. hacking ovvero, individui outsider possono introdursi nel sistema per affermare la propria autorità ai danni di progettisti e di utenti[9]. **Il livello semantico**: rielabora i dati contenuti nelle macchine[10]. L'esercito americano, analogamente a Libicki, raffigura il *cyberspace* attraverso una triplice stratificazione: fisica, logica e sociale così come riportato nella figura 1.1[11]

Figura 1.1: Triplice stratificazione dello spazio cibernetico secondo l'US *Army*



Fonte: *Department of the Army Headquarters, United States Army*[12]

Da un punto di vista ambientale, il domino cibernetico si distingue dagli altri ambiti di esercizio del potere militare, non solo perché rappresenta una realtà artificiale e ibrida, ma soprattutto perché "la

[8] Ivi, p. 12
[9] *Ibidem*.
[10] *Ibidem.*
[11] Cfr. Department of the Army Headquarters, United States Army Training and Doctrine Command (2010), *The United States Army's Cyberspace Operations Concept Capability Plan 2016–2028*, TRADOC Pamphlet 525-7-8, URL: http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf [consultato il 14-06-2013]
[12] *Ibidem*

geografia del *cyberspace* è molto più mutevole rispetto ad altri ambienti; a differenza delle montagne e degli oceani statici, le parti del *cyberspace* possono essere attivate e disattivate con un semplice click"[13]. Questa caratteristica "geografica" dello spazio cibernetico ha reso necessaria una più attenta riflessione e ha destato nuovi interrogativi in relazione all'evoluzione degli scenari bellici.

1.2 La guerra cibernetica, il potere militare e il nonsense di una cyber-strategy

Lo spazio cibernetico, come si è visto, possiede di per sé due caratteristiche peculiari: può essere inteso come un mezzo tecnologico attraverso il quale si sviluppano le interazioni umane; esso agendo come una grande via di transito per gli utenti (*users*), riesce a garantire collegamenti planetari. La rappresentazione qui riportata relega il *medium* cibernetico a un ruolo "puramente" civile[14]. Allo stesso tempo però, il *cyberspace* con la sua pervasione globale non è immune dal produrre minacce per la sicurezza nazionale. Già nel 2001, il Dipartimento della Difesa degli Stati Uniti (U.S. *DoD*) tramite la pubblicazione del *Quadrennial Defense Review Report* (QDR) avvertiva che alla luce degli enormi progressi compiuti negli ultimi anni nel campo della tecnologia informatica e satellitare, e soprattutto in riferimento alla continua evoluzione verso la creazione di un sistema congiunto di forze armate "netcentriche", il dominio cibernetico diventava un potenziale "moltiplicatore" delle minacce per la sicurezza e gli interessi americani[15]. Lo spazio cibernetico, unito all'esercizio del potere, diventa dunque il nuovo *centro di gravità clausewitziano*[16], che coinvolge non solo l'apparato

[13] Cfr. G.J. Rattray, *An Environmental Approach to Understanding Cyberpower, in Cyberpower and National Security*...op. cit.

[14] 4Cfr. L. Floridi, *La rivoluzione dell'informazione*, Torino, 2012; P. Lévy, *Il virtuale*, Raffaello Cortina Editore, Milano, 1997

[15] Department of Defense, *2001 Quadrennial Defense Review Report*, Washington DC, September 30, 2001, URL: http://www.defense.gov/pubs/qdr2001.pdf. [consultato il 18-06-2013]

[16] Il centro di gravità, *Schwerpunk*, è secondo Clausewitz "l'attacco al cuore del nemico", ovvero: "Si trova sempre là dove è concentrata la maggior parte della massa, ed ogni urto contro tale centro ha la massima efficacia sull'insieme, così deve avvenire in guerra e perciò l'urto più forte deve avvenire contro il centro di gravità", cfr. C. von Clausewitz, *Della guerra*...op. cit., cit. p. 641. Per una disamina sulla ricezione del concetto clausewitziano nella dottrina militare americana si rinvia a A.J. Echevarria, *Clausewitz's Center of Gravity: Changing our Warfighting Doctrine – Again!*, Strategic Studies Institute, Carlisle Pennsylvania, September 2002.
URL: http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB363.pdf. [consultato il 13-06-2013]

militare, ma tutto il sistema di Comando e Controllo (C2) delle società intensamente digitalizzate[17]. La consapevolezza della rilevanza strategica dello spazio cibernetico emerge nel documento approvato dalla Casa Bianca nel 2003 e intitolato *National Strategy to Secure Cyberspace*[18], nel quale si paragona lo spazio cibernetico:

"A un sistema nervoso – il sistema di controllo del paese – composto da centinaia di migliaia di computer interconnessi, server, router, cavi in fibra ottica che permettono alle nostre infrastrutture critiche di lavorare. Così, il sano funzionamento dello spazio cibernetico è essenziale per la nostra economia e la nostra sicurezza nazionale"[19]

Il concetto di guerra cibernetica (*cyber warfare*) stando a quanto scrive Libicki, altro non è che una delle sette forme assumibili dalla *Information Warfare* (*IW*)[20]. Anzi, è la summa di tutte le tipologie che la precedono e utilizza le scoperte tecnologiche in campo elettronico, informatico e satellitare per compiere atti bellici tramite l'utilizzo di tali tecnologie[21]. Parlare di guerra cibernetica non equivale ad amalgamare in un *unicum* generale le azioni illecite condotte tramite il *cyberspace*; infatti, come vedremo nelle pagine che seguiranno, non tutte le operazioni illecite e lesive seppur condotte anche contro un *target* statale, possono essere ritenute alla stregua di atti rientranti nella categoria della *cyber warfare*, ovvero azioni militari e quindi ricadenti nello *jus ad bellum*[22]. È altresì vantaggioso specificare sin da subito che i termini *cyber war* e *cyber warfare*, entrambi traducibili in italiano con la parola "guerra cibernetica" e quindi apparentemente

[17] Cfr. U. Gori e L.S. Germani, *Information Warfare 2010. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana*, a cura di Id., FrancoAngeli, Milano, 2011.
[18] Cfr. The White House, *The National Strategy to Secure Cyberspace*, Washington DC, February 2003, URL: https://www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf [consultato il 12-06-2013]
[19] Cfr. The White House, The National Strategy to Secure Cyberspace, Washington DC, February 2003, URL: https://www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf [consultatoil13-06-2013]
[20] Cfr. M. C. Libicki, *What Is Information Warfare?, Center For Advanced Command Concept and Technology*, Institute for National Strategic Studies, National Defense University, Washington DC, August 1995. Si rinvia anche al cap. 3.
[21] *Ibidem.*
[22] Nel diritto internazionale con il termine *Jus ad bellum* si fa riferimento all'uso legittimo della forza da parte degli Stati; mentre con *Jus in bello* si rinvia alle modalità con le quali tale uso della forza deve essere messo in atto, in altre parole, lo scontro armato seppur legittimo non deve mai contrastare con i diritti umani che determinano la condotta delle ostilità. Cfr. L. Claude, Jr *Just Wars: Doctrines and Institutions*, in Political Science Quarterly, Vol. 95, No. 1 (Spring, 1980), pp. 83-96, Published by The Academy of Political Science. URL: http://www.jstor.org/stable/2149586. [consultato il 13-06-2013]

identici, esprimono invece due concetti profondamente differenti sul piano della dottrina militare. La definizione di *cyber war*, in linea di massima, rappresenta le operazioni militari condotte tramite il *cyberspace*:

"Al fine di negare all'avversario – statuale o non – l'uso efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati. Include anche attività di difesa e "capacitanti" (volte cioè a garantirsi la disponibilità e l'uso del *cyberspace*). Può assumere la fisionomia di un conflitto di tipo "tradizionale" – quando coinvolge le forze armate di due o più stati – ovvero "irregolare", quando si svolge tra forze ufficiali e non ufficiali. Può rappresentare l'unica forma di confronto ovvero costituire uno degli aspetti di un conflitto che coinvolga altri dominii (terra, mare, cielo e spazio); in entrambi i casi, i suoi effetti possono essere limitati al *cyberspace* ovvero tradursi in danni concreti, inclusa la perdita di vite umane"[23]

Per *cyber warfare*, oltre a quanto già scritto, si intende anche:

"L'insieme della dottrina, dell'organizzazione, del personale, della logistica e delle attività militari svolte dalle Forze Armate nel e tramite il cyberspazio, in tempo di guerra o di crisi, allo scopo di garantire e sfruttare il cyberspazio ai propri fini e, contemporaneamente, negando tale capacità all'avversario"[24]

Per suddetti motivi, si è scelto in questo lavoro di far rientrare il termine guerra cibernetica nel più ampio concetto di *cyber warfare* non solo perché esprime una nozione più ampia e completa, ma soprattutto perché è un termine apprezzato dalla dottrina militare internazionale e in generale dagli autori di Studi Strategici esperti del

[23] Cfr. Dipartimento delle Informazioni per la Sicurezza, *Il linguaggio degli organismi informativi. Glossario di Intelligence*, in "Gnosis. Rivista Italiana di Intelligence. Quaderni di Intelligence", De Luca Editori, Roma, 2012. URL: http://www.sicurezzanazionale.gov.it/web.nsf/pagine/glossario-intelligence#details-100 [consultato il 6-04-2013]

[24] Cfr. P. Scotto di Castelbianco, *La cyber minaccia: attori, mutamenti e sfide al sistema Paese. Il ruolo della cyber intelligence , in Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, a cura di U. Gori e L. S. Germani, FrancoAngeli editore, Milano, 2012, cit. p. 67. L'Autore riporta nel suo contributo un utile glossario, in parte citato anche nelle pagine del presentelavoro

tema[25]. Una volta assodato che il *cyberspace* possiede anche caratteristiche puramente militari (strategiche, tattiche e operative), è lecito chiedersi se è possibile poter formulare una strategia autonoma applicabile al dominio cibernetico ovvero prevedere una *cyberstrategy*[26]. Secondo Colin S. Gray parlare di "strategia cibernetica" è un *nonsense* in quanto, non esiste un mezzo militare (quali sono le armi cibernetiche) che da solo sia capace di risolvere i conflitti autonomamente, così come non esiste un *ambiente* (naturale o artificiale) che possa essere concepito distaccato da tutti gli altri ambienti bellici[27]. A tal proposito Gray telegraficamente scrive:

"If you say cyber strategy you risk implying that the strategy is somehow distinctive as strategy because it is owned by its cyber tools. In fact, boringly, one must recognise that strategy is just strategy, regardless of the geographical domain to which it relates or the military or other agents that it employs. Although the military capabilities by and large unique in kind to each of war's five geographical domains (land, sea, air, Earth-orbital, and cyberspace), must work in harmony towards a common goal, it is quite proper to develop domain-specific strategies as contributing sub-sets of the whole endeavour".[28]

È chiaro che il *cyberpower* non può essere inteso come un potere militare *tout court* e quindi "decisivo in solitaria" per una guerra, tale consapevolezza – avverte Gray – serve per mettere in guardia la struttura decisionale da coloro che, presentandosi come i *deus ex machina* delle minacce cibernetiche, propongono soluzioni dannose e allarmistiche. Alle parole di Gray si potrebbero accostare gli

[25] In lingua inglese guerra si traduce con due termini: *war*, che indica più generalmente il concetto, lo stato, la condizione; *warfare* si riferisce invece oltre a ciò anche alla condotta della guerra e alle operazioni militari

[26] Per una disamina sulla "definizione di strategia" si rinvia all'eminente lavoro di E. N. Luttwak, Strategia. *La logica della guerra e della pace*, Rizzoli, Milano, 2001. L'Autore definisce il termine strategia in ambito militare come la capacità dell'uomo di comando a intraprendere le scelte guidato dalla genialità e dall'istinto; non a caso secondo Luttwak la strada maestra da seguire nelle scelte militari è dettata dalla logica del paradosso, infatti Luttwak scrive: " Io affermo invece che la strategia non implica soltanto questa o quella proposta paradossale, palesemente contraddittoria eppure considerata valida, ma anche che *l'intero regno della strategia è pervaso da una logica paradossale tutta sua*, in netto contrasto con la logica "lineare" comune, in base alla quale viviamo in tutte le altre sfere della nostra esistenza". cit. p. 21. Inoltre si segnala il recente lavoro a cura di L. Bozzo, *Studi di strategia. Guerra, politica, economia, semiotica, psicoanalisi, matematica*, EGEA, Milano, 2012.

[27] Cfr. C. S. Gray, "*Another Bloody Century*?", in Infinity Journal, Issue No 4, Fall. 2011, pp. 4-7.

[28] Ivi, cit. p. 7

avvertimenti che già Clausewitz dettava nel suo *Vom Kriege*: "mai il mezzo può essere concepito senza lo scopo"[29], a proposito della distinzione tra i ruoli che in un conflitto devono avere la guerra (e i suoi strumenti) e la politica (e i suoi obiettivi strategici). Se oggi dunque il mezzo militare è diventato anche (ma non solo) *cyber*, lo scopo rientra pur sempre nella più ampia categoria della strategia la quale, come amano definirla gli anglosassoni, altro non è che "the *servant of politics*"[30]. Sarebbe dunque un errore, da non poco conto, quello di pensare di poter estrapolare una strategia univoca e onnicomprensiva dello strumento cibernetico in modo indipendente dalla sua collocazione unitaria all'interno del più ampio concetto di *warfare*.

2. AMBIENTE OPERATIVO, GEOGRAFIA E GEOPOLITICA DEL CYBERSPACE

2.1 Premessa

Cercare di descrivere un ambiente virtuale attraverso le dinamiche e i concetti degli spazi "reali" sarebbe un compito alquanto arduo, ma soffermarsi solo all'apparenza a causa di una miopia strategica, significherebbe in ambito politico-militare, esporre a seri rischi la sicurezza e la difesa nazionale[31]. In effetti, l'ascesa del dominio cibernetico a dimensione bellica delle relazioni internazionali non è stata valutata da tutti gli osservatori con gli stessi *standard* in termini di rilevanza strategica, potenza militare e letalità delle minacce. Secondo alcuni analisti, Thomas Rid in particolare, la *cyber warfare* non sarebbe altro che una montatura pubblicitaria poiché il rischio di una guerra cibernetica, così come i disastri ipoteticamente paventati, non solo non si sono mai palesati nel passato e nel presente, ma certamente – chiosa Rid – nel futuro: "*cyber war will not take place*". [32]In queste pagine, contrariamente al pensiero critico appena riportato, si cercherà di analizzare lo spazio cibernetico

[29] Cfr. C. von Clausewitz, *Della guerra*…op. cit
[30] Cfr. P. Cornish (et.al.) *On Cyber Warfare, A Chatham House Report*, The Royal Institute of International Affairs, London, 2010.
[31] Cfr. C. S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*, Strategic Studies Institute, Carlisle PA, April 2013
[32] Cfr. T. Rid, *Think Again: Cyber War. Don't Fear the Digital Bogeyman. Virtual Conflict is Still More Hype Than Reality*, in Foreign Policy, March/April 2012. Da questo articolo l'Autore ha preso spunto per il suo recente libro *Cyber War Will Not Take Place*, C. Hurst & Co. Publishers Ltd., London, 2013.

partendo dal presupposto che esiste una rilevante pervasività delle infrastrutture informatiche denominate *Information Communication Technology* (*ICT*)[33] nelle interazioni sociali, politiche, economiche e militari del XXI secolo[34]. Ne consegue che, il crescente "peso" strategico assunto dalle ICT in termini di sviluppo economico e di potere militare (insieme all'intero dominio cibernetico) non si sottrae a tutte quelle dinamiche geo proprie dell'attività umana concernenti a modellare e a influenzare il mondo reale[35]. Il *cyberpower*, come accennato, influisce sulla politica internazionale su due piani differenti: sul piano geografico la struttura fisica del *cyberspace* costituita da elementi tangibili rende questo "strato" uno dei punti di snodo più suscettibili e vulnerabili in caso di azioni malevoli (cinetiche o cibernetiche); in egual misura, la militarizzazione dello spazio cibernetico genera un superamento del concetto di localizzazione della minaccia a causa della *deterritorializzazione* del potere che modifica profondamente i concetti di luogo, tempo e spazio geografico[36]. Sul piano geopolitico invece, con l'avvento della rivoluzione dell'informazione è stato introdotto nelle relazioni internazionali odierne il concetto di *intangibilità* che genera sia una

[33] Non esiste una definizione univoca di ICT, una summa di varie definizioni viene tentata da A. Caperna, *Integrating ICT into Sustainable Local Policies*, Handbook of Research on E-Planning: *ICTs for Urban Development and Monitoring*. IGI Global, 2010, pp. 340-364, l'Autore tra l'altro scrive: "Se da un lato è possibile identificare gli elementi che costituiscono le ICT, dall'altro non risulta facile fornirne una definizione univoca, poiché non esiste una generale e condivisa definizione.
L'OECD opera una classificazione legata più che altro ai settori dove opera la ICT e, cioè:
- quello manifatturiero, ad esempio la fabbricazione di macchine per ufficio o di elaboratori e sistemi informatici; oppure la fabbricazione di apparati riceventi radio TV, per registrazione e riproduzione di suoni od immagini e prodotti connessi;
- il settore dei beni legati ai servizi, ovvero quelli legati alla distribuzione e al commercio all'ingrosso di macchinari per telecomunicazioni, apparati elettrici, computer etc.;
- il settore legato ai servizi immateriali, ovvero attività di radio e telecomunicazione, consulenze software e hardware, database activities, servizi di telematica o robotica, etc.;
- il settore legato all'industria dei contenuti, ad esempio pubblicazione di libri, supporti sonori, proiezioni cinematografiche, etc.
Nel corso degli ultimi anni ha acquisito sempre più rilevanza strategica l'aspetto legato all'utilizzo della ICT come strumento atto a produrre informazioni, nuova conoscenza e nuovi contenuti.
In tal senso possiamo dire che nella ICT si fondono differenti componenti, quali la computer technology (CT), le telecomunicazioni, l'elettronica e i media. Esempi in tal senso sono rappresentati dai PC, internet, telefonia mobile, TV via cavo, sistemi di pagamento elettronico, etc.
Quindi possiamo dire che la ICT ha finito con il legare sempre più la componente Information Technology (IT) con quella relativa alla Communication Technology (CT). In particolare quando quest'ultima ha assunto vesti nuove, cioè con l'avvento delle tecnologie a rete, l'informazione ha finito con il perdere quella caratteristica rappresentata dall'elaborazione su macchine stand alone per divenire una componente condivisa con altre macchine di una rete (sia LAN che quella globale di internet)".

[34] Cfr. C. Jean, *Geopolitica del XXI secolo*. Edizioni Laterza, Roma-Bari, 2004.

[35] Cfr. S. Mele, *Cyberwarfare. Danni ai cittadini*, in www.stefanomele.it [consultato il 13-06-2013]

[36] Cfr. C. Jean, *Geopolitica, sicurezza e strategia*, FrancoAngeli , Milano, 2007

diffusione del potere a favore di attori deboli ma, favorisce soprattutto l'accesso alle informazioni a soggetti prima subordinati alla censura delle gerarchie statali[37]. Nel campo militare queste innovazioni hanno rivoluzionato lo stesso concetto di arma e di propagazione delle minacce e hanno favorito, allo stesso tempo, un *modus operandi* all'incirca anonimo[38]. Le "nuove sfide" costringono i *policymakers* a porre l'accento non tanto sui rischi provenienti dai fronti tradizionali o da eserciti convenzionali quanto, piuttosto, sulle c.d. "minacce ibride"[39]. Come argutamente ha osservato Nye, il salto di qualità rispetto alle precedenti minacce di tipo tradizionale è avvenuto a causa di un abbassamento della soglia di accesso agli strumenti militari capaci di infrangere il monopolio della violenza che, insieme all'informazione, costituivano un tempo le prerogative degli stati nazionali[40]. A tal proposito, Nye scrive: "Le barriere all'entrata nello spazio cibernetico, [rispetto agli altri domini N.d.A.] sono così basse che gli attori non statali e i piccoli Stati possono giocarvi un ruolo significativo a costi relativamente contenuti"[41]. Infatti, proprio la *National Security Strategy* del 2002, coerentemente con la mutata percezione statunitense sulla sicurezza nazionale (o meglio sulla vulnerabilità del suolo americano all'indomani degli attacchi terroristici), pragmaticamente riporta: "*We are menaced less by fleets and armies than by catastrophic technologies in the hands of the embittered few*"[42].

[37] Cfr. J.S. Nye, *The Future of Power*...op.cit.

[38] Cfr. National Defense University – Institute for National Security Studies, *Global Strategic Assessment 2009*, in particolare si rinvia al capitolo III, *The Information Revolution*.
URL: http://www.ndu.edu/inss/index.cfm?type=section&secid=181&pageid=8 [consultato il 13-06-2013]

[39] Cfr. *Ibidem*. In particolare a proposito delle guerre ibride Jean così scrive: "L'espressione "guerra ibrida" venne introdotta perché, nella realtà dei conflitti odierni, non si combatte un solo tipo di guerra, ma guerre di varie categorie (o "generazioni") convergono e si sviluppano in contemporanea. [...] Laddove il termine "asimmetrico" è riferito ai conflitti irregolari, "ibrido" sottolinea il fatto che oggi è necessario preparare le forze per fronteggiare l'intera gamma delle possibili minacce. Occorre farlo anche per evitare che tali minacce da potenziali divengano reali. Le armi, infatti, servono non solo quando vengono impiegate, ma soprattutto, quando non lo sono; anzi, in tal caso si rivelano persino più utili, perché costi e rischi sono inferiori e gli effetti virtuali, potenziali", cit. p. 59.

[40] Cfr. J. S. Nye JR., *The Future of Power*...op.cit

[41] Ivi, cit. p. 148.

[42] Cfr. *The National Defense Strategy of the United States of America*, Washington D.C., September 2002, cit.p. 1. URL: http://www.state.gov/documents/organization/63562.pdf [consultato il 13-06-2013]

2.2 Global commons o dominio antropico?

Secondo la *World Conservation Strategy*, per *global commons* si deve intendere quanto segue:

"A tract of land or water owned or used jointly by the members of a community. The global commons includes those parts of the Earth's surface beyond national jurisdictions - notably the open ocean and the living resources found there - or held in common - notably the atmosphere. The only landmass that may be regarded as part of the global commons is Antarctica"[43]

Dalla definizione qui sopra citata se ne deduce che per *global commons* devono intendersi quelle risorse naturali che, seppur ricadenti nelle giurisdizioni statali, è fatto divieto di imporre su di esse qualsiasi limitazione o riserva giuridica. Servendoci del lessico del diritto internazionale si evince che: i principi che tutelano i *global commons* sono norme che pongono obblighi *erga omnes*[44]. A questo punto sorge una domanda: è possibile far rientrare il *cyberspace* nella definizione di *global common*? In altre parole: lo spazio cibernetico può essere rappresentato come una risorsa ambientale a tutti gli effetti, nonostante la sua duplice caratteristica di "*manmade environment*" e di "intangibilità"? Le posizioni sulla classificazione

[43] Cfr. *World Conservation Strategy*, Chapter 18 "The Global Commons". Relazione pubblicata nel 1980 dall'Unione Internazionale per la Conservazione della Natura e delle Risorse Naturali (IUCN) in collaborazione con l'UNESCO e con il sostegno del Programma delle Nazioni Unite per l'ambiente (UNEP) e il World Wildlife Fund (WWF).
URL:http://data.iucn.org/dbtwwpd/edocs/WCS-004.pdf [consultato il 13-04-2013] [citazione ripresa da Wikipedia: URL:http://en.wikipedia.org/wiki/Global_commons#cite_note-WCS-3]

[44] Per una definizione dettagliata del principio giuridico delle norme con valore c.d. erga omnes si rinvia a A. Cassese, *Diritto Internazionale*, a cura di P. Gaeta, Il Mulino, Bologna, 2006. In tale manuale è possibile leggere: "Le norme [...] *erga omnes*, [...] presentano le seguenti caratteristiche: 1) sono obblighi che proteggono *valori fondamentali* per la comunità internazionale nel suo insieme (pace, diritti umani, autodeterminazione dei popoli, protezione dell'ambiente); 2) sono obblighi di *natura solidale*, nel senso che essi incombono su ogni membro della società internazionale nei confronti di tutti gli altri membri (o, nel caso essi discendano da trattati, nei confronti di tutte le altre parti contraenti); 3) ad essi corrisponde un diritto sostanziale che appartiene ad *ogni membro della comunità internazionale* (o ad ogni parte al trattato); 4) l'azione a tutela di tale diritto è esercitata *per conto dell'intera comunità internazionale* o dell'insieme delle parti contraenti) per salvaguardare gli interessi fondamentali di quella comunità", inoltre, a piè di pagina alla nota (6) è possibile comprendere il contesto storico relativo alla norma presa in questione dove si legge: "In un certo senso, quest'insieme di norme internazionali costituisce ciò che Francisco de Vitoria (1483-1546), giurista spagnolo neo-giusnaturalista, denominava *bonum commune totius orbis*, il bene comune dell'intera umanità, ossia i beni e i valori propri all'umanità tutta intera, davanti ai quali devono cedere gli interessi e le pretese individuali di ciascuno Stato", cit. p. 25

dello spazio cibernetico quale *global commons* sono varie[45]. *In primis*, vi è la tesi contraria alla classificazione del *cyber global commons* secondo la quale, il carattere meramente artificiale del *cyberspace* contrasta con la conformazione naturale delle altre risorse "geografiche" ricadenti nell'alveo della definizione data dalla *World Conservation Strategy*, questa a sua volta pone come *conditio sine qua non* l'elemento naturale per far rientrare una risorsa nel novero dei domini usufruibili dall'umanità. Il secondo elemento di opposizione dei "refrattari" alla concezione del "*cyberspace as global common*" è più pragmatico; a discapito di quanto si voglia far credere, l'accesso e l'utilizzo degli strumenti cibernetici (soprattutto in relazione alle infrastrutture e alla diffusione di Internet) non è garantito a livello globale[46]. Difatti, il carattere artificiale dello spazio cibernetico renderebbe questo ambiente più "materiale" e sensibile agli interventi dei decisori (pubblici o privati) capaci di gestire, limitare o estromettere l'utilizzo ogni qualvolta venga ritenuto necessario in

[45] Uno dei più accattivanti ed elevati dibattiti scaturito attorno al tema "geografico e geopolitico" preso in esame in queste pagine è rappresentato dallo scambio d'idee intercorso tra due dei massimi esperti a livello internazionale in questo settore ovvero tra gli studiosi Martin Libicki e Colin Gray rintracciabile in: C. S. Gray, *The Continued Primacy of Geography*, Orbis, Vol. 40, No. 2, Spring 1996, pp. 247-259; M. C. Libicki, *The Emerging Primacy of Information*, Orbis, Vol. 40, No. 2, Spring 1996, pp. 261-274; e *Rejoinder by Colin S. Gray*, pp. 274-276.

[46] Molti sono gli Autori inclini a considerare il *cyberspace* soggetto alle dinamiche degli interessi di parte. In questo lavoro si è deciso di citarne solo alcuni tra i più diffusi che non mancano di sottolineare i tre principali punti di contrasto con la tesi che avvalora il dominio cibernetico come *global commons*, ovvero: 1) è un dominio artificiale; 2) è soggetto alla *governance* dei privati che gestiscono le infrastrutture fisiche; 3) vi è una preminenza degli interessi economici e finanziari rispetto a quelli politici. Cfr. R. J. Deibert and R. Rohozinski, *Under Cover of the Net. The Hidden Governance Mechanism of Cyberspace, in Ungoverned Spaces. Alternatives to State Authority in an Era of Softened Sovereignty*, edited by A. L. Clunan and H. A. Trinkunas, Stanford University Press, 2010, pp. 255-272, in particolar modo gli Autori in tale lavoro sottolineano che Internet e lo spazio cibernetico sono sottoposti a dei veri e propri meccanismi di governance soprattutto in merito alla gestione delle Infrastrutture fisiche, tra l'altro è possibile leggere: "*The thesis of this chapter is that, contrary to the myths above, the Internet is very much a governed space. At the most basic level, it is governed by rules of physics as well as code, which give it predictability and finite characteristics. It is governed by consensual practices among the network's providers and operators that have their basis in norm without which the Internet could not function*" cit. p. 256; dello stesso avviso sono J. Goldsmith e T. Wu, *I padroni di Internet*, trad. it. a cura di B. Parrella, Unwired Media, 2006. Per quanto riguarda invece una critica sui pericoli di un'eccessiva enfasi sulle catastrofiche conseguenza di una guerra cibernetica si rinvia a T. Rid, *Cyber War Will Not Take Place*, C. Hurst & Co. Publishers Ltd., London, 2013, l'Autore in questo caso parte da alcune domande sarcastiche per poi giungere a delle conclusioni alquanto nette e perentorie: "*But is it? Are the Cassandras on the right side of hystory? Has cyber conflict indeed entered the "fifth domain" of warfare? Is cyber war really coming? This book argues that cyber war will not take place, a statement that is not necessarily accompained with an ironical Girandouxian twist. It is meant rather as a comment about the past, the present, and likely future: cyber war has never happened in the past, it does not accour in the present, and it is highly unlikely that it will disturb our future*", cit. p. xiv.

base ai propri interessi politici, economici o sociali[47]. È pur vero che i c.d. *commons* non sono altro che dei beni o delle risorse modellate dall'uomo in base alle esigenze del gruppo sociale e dunque frutto di un artefatto umano. Non a caso Barry R. Posen rettifica in parte la definizione della *World Conservation Strategy* adattando il concetto di *global commons* al contesto della politica internazionale[48]. Posen, nel suo celebre saggio "*Command of the Commons. The Military Foundation of U.S. Hegemony*"[49] sin dal titolo non lascia equivoci: seppur il termine "*global commons*" nella politica ambientale rinvia ad aree geografiche e a risorse usufruibili da tutta l'umanità che non appartengono a nessuno Stato, tuttavia, – scrive Posen – nelle relazioni internazionali lo sparti acque basilare per il godimento di una risorsa risiede nel determinare chi detiene la capacità di accesso, comando e di estromissione in queste aree globali[50]. Posen, per avvalorare la propria tesi, legge in chiave "realista" la natura dei domini globali, riportando l'esempio dell'aria; in linea di principio – spiega l'autore – questo elemento/dominio geografico rientra nella categoria di "risorsa globale", ma se a tale ambiente si affiancano scopi politici, il dominio aereo assume tutt'altro significato[51]. Infatti, Posen mette in correlazione la nozione di "*commons*" con il concetto di "*command*" e vi legge la militarizzazione dei *global commons* che, in ultima istanza, fungono da moltiplicatori della potenza militare, in particolare di quella statunitense[52]. Di fatto, il discrimine

[47] Si pensi ad esempio quanto riporta uno studio pubblicato dal mensile Wired a proposito della "battaglia per il controllo della rete": secondo tale indagine, condotta sull'analisi dei dati forniti dall'Agenzia ONU International Telecommunication Union (ITU) e dalle previsioni CISCO, emerge che "Gli utenti internet nel mondo 2012 sono 2,4 miliardi, le previsioni pongono che gli utenti nel 2016 diventino 3,4 miliardi e le macchine collegate a internet nel 2016 saranno 22 miliardi"; invece sul versante del valore dell'internet economy si legge che "in base ai dati e le previsioni del Boston Colsunting Group si prevede che per il 2016 tale fetta di mercato varrà 4,2 milioni di miliardi di dollari". Cfr. J. Kiss, La guerra sulla Rete, in WIRED, Anno 4, n. 46, dicembre 2012, pp. 95-100.

[48] Cfr. B. R. Posen, Command of the Common. The Military Foundation of U.S. Hegemony, International Security, Vol. 28, Issue 1, Summer 2003, pp. 5-46.
URL: http://belfercenter.ksg.harvard.edu/files/posen_summer_2003.pdf . [consultato il 13-01-2013]. In realtà, il primo Autore a sottolineare l'importanza dei *global commons*, da un punto di vista strategico per la proiezione della potenza militare e il consolidamento dell'egemonia, fu l'ufficiale della U.S. Navy Alfred Thayer Mahan che attraverso la sua prestigiosa opera *The Influence of Sea Power Upon History (1660-1783)* pubblicata nel 1890 rivoluzionò il concetto di potere militare, di sicurezza e di influenza economica. Secondo Mahan infatti solo le nazioni in grado di assicurarsi il pieno controllo delle rotte navali riescono a garantirsi una posizione egemonica rispetto agli altri contendenti.

[49] *Ibidem.*

[50] *Ibidem.*

[51] *Ibidem.*

[52] *Ibidem.*

fondamentale per il "godimento" di un *commons* è rappresentato dalla capacità fattuale di un determinato attore di preservare i propri interessi vitali, servendosi del suo *status* di superiorità militare in modo tale da negare (*to deny*) ai contendenti l'accesso alla risorsa[53]. D'altronde – come scrive Kenneth N. Waltz – nella politica internazionale il potere è: "La misura in cui un attore è in grado di influenzare gli altri più di quanto questi influenzino lui"[54]. È evidente dunque, che tutto ciò vale anche per i *global commons*, nonostante il principio universalmente riconosciuto prescriva per essi la caratteristica di risorse "usufruibili dall'intera umanità". Di conseguenza, l'elemento centrale per "classificare" una risorsa usufruibile dall'intera umanità sul piano della politica internazionale risiede, *de facto*, nella reale capacità di accesso, comando ed estromissione di altri attori concorrenti dalle c.d. "aree globali"[55]. Dello stesso avviso è Daniel T. Kuehl che partendo dall'assunto: "il *cyberpower* è un fatto fondamentale della vita globale"[56], critica fortemente coloro che si ostinano a porre l'accento sulla natura artificiale del *cyberspace* per ridimensionarne il valore strategico di questo dominio, senza accettare l'idea – spiega Kuehl – che in realtà tutte le dimensioni della conflittualità si muovono lungo il *continuum* delle scoperte tecnologiche[57]. D'altronde, negli ultimi anni si è diffusa, *a priori*, l'idea che è conveniente da un punto di vista politico-strategico, considerare lo spazio cibernetico non solo come un dominio con caratteristiche e dinamiche puramente civili, ma soprattutto come un nuovo e rilevante teatro bellico dal quale prendono vita le minacce del XXI secolo[58]. Colin S. Gray ad esempio, in un *paper* edito dallo *Strategic Studies Institute* s'interroga sulla questione spinosa relativa alla "natura" da dover conferire a questo nuovo elemento delle odierne relazioni internazionali[59]. Gray per onestà intellettuale sottolinea come, ancora oggi, sia in corso un lavoro cognitivo per la caratterizzazione del *cyberspace*, ma – aggiunge Gray – alla luce delle recenti evoluzioni in campo militare e tecnologico:

[53] *Ibidem.*
[54] Cfr. K. N. Waltz, *Teoria della politica internazionale*, Il Mulino, Bologna, 1987, cit. p. 349
[55] Cfr. B. R. Posen, *Command of the Common*…op. cit.
[56] Cfr. D.T. Kuehl, *From Cyberspace to Cyber-power: Defining the Problem*…op. cit.,
[57] *Ibidem.*
[58] Cfr. C. Jean, *Geopolitica, Sicurezza e strategia*…op. cit.
[59] Cfr. C. S. Gray, *Making Strategic Sense of Cyber Power*…op. cit

"It is convenient to regard cyberspace, which should really be cyberspaces, as a fifth geographical domain for war, peace, defense preparation, and strategy. It is somewhat counterintuitive to attempt to think of cyberspace in geographical terms, given its essential placelessness"[60]

Secondo Gray, dunque, lo spazio cibernetico pur essendo un ambiente "*placelessness*"[61], è costituito da elementi fisici e digitali che concorrono a renderlo allo stesso tempo reale e virtuale. Nondimeno, conviene (*It is convenient*) ai fini di una seria "pianificazione strategica" considerare questo dominio come la quinta dimensione del warfare in quanto, anche al suo interno interagiscono le dinamiche della guerra e della pace[62]. Lo sottolinea anche la *National Defense Strategy* quando nel 2005 scrive: "*cyberspace is a new theater of operations*"[63]. In questo modo il dominio cibernetico non solo viene incluso nei *global commons*, ma *ipso facto*, è adattato alle dinamiche militari. Il significato profondo della rilevanza strategica dei *global commons* si può estrapolare dallo studio edito dal *Center for a New American Security* a cura di Abraham M. Denmark e James Mulvenon, dal titolo quanto mai significativo per il tema trattato in questa ricerca: "*Contested Commons: The Future of American Power in a Multipolar World*"[64]. Il loro studio parte da un assunto tanto semplice quanto perentorio: se gli Stati Uniti intendono garantirsi la continuità del loro dominio preservando lo *status quo* nel panorama internazionale devono, per ragioni strategiche, concentrare tutti gli sforzi (politici, diplomatici, militari, economici, finanziari, tecnologici) per il mantenimento del monopolio dell'accesso ai *global commons*[65]. Proprio per questo – attraverso la loro dettagliata ricerca – avanzano degli "*advices*" se non

[60] Ivi, cit. p. 15.

[61] Non esiste, in italiano, una traduzione letterale di tale termine, si è ritenuto, in questo lavoro, che il sostantivo *ubiquità* rappresenti l'esempio più contiguo da un punto di vista rappresentativo (o quantomeno linguistico) nell'assonanza con il termine anglosassone *placelessness*. Infatti, per Ubiquità si deve intendere: "la facoltà di essere contemporaneamente in ogni luogo, propria di Dio [...] Nella filosofia scolastica, il modo di essere nello spazio che consiste nell'occupare per intero sia tutto lo spazio, sia qualsiasi parte dello spazio" cfr. *Il Devoto-Oli. Vocabolario della lingua italiana. 2007*, a cura di L. Serianni e M. Trifone, Le Monnier, Firenze, 2006, cit. p. 2996.

[62] Cfr. C. S. Gray, *Making Strategic Sense of Cyber Power*...op. cit.

[63] Cfr. *The National Defense Strategy of the United States of America*, Washington D.C., Department of Defense, March 2005, cit. p. 16. URL: http://www.defense.gov/news/Apr2005/d20050408strategy.pdf [consultato il 14-06-2013]

[64] Cfr. A. M. Denmark e J. Mulvenon (ed.), *Contested Commons: The Future of American Power in a Multipolar World, Center for a New American Security*, January 2010, Washington DC.

[65] *Ibidem.*

dei veri e propri "*warnings*" utili a mantenere immune il potere americano dalle crescenti minacce eterogenee provenienti dal sistema internazionale contemporaneo[66]. Risulta interessante anche lo studio condotto da Gregory Rattray, Chris Evans e Jason Healey dal titolo: "*American Security in the Cyber Commons*"[67]. Soprattutto perché gli autori includono una tabella per analizzare in chiave comparata i quattro *global commons* (marittimo, aereo, spaziale e cibernetico) da un punto di vista delle dinamiche militari[68], e per evidenziare un duplice aspetto che riguarda la dottrina militare, cioè porre l'accento sull'evoluzione postuma della dottrina rispetto alle scoperte scientifiche e tecnologiche, e sottolineare il cammino intrapreso dalle forze militari statunitensi verso una progressiva integrazione delle dimensioni del *warfare* in una visione *joint*[69]. Prendendo in analisi il "lato" *cyber* della tabella si può notare che, a differenza degli altri *commons*, questo dominio introduce delle novità rispetto al passato nella conduzione dei conflitti armati:

piano strategico: a) la possibilità di trasferire e/o trasmettere informazioni in tempo reale; b) operazioni militari coordinate; c) la capacità per gli attori non statali di utilizzare questo dominio come un moltiplicatore di potenza; **livello operativo:** a) operazioni militari istantanee ed economiche di portata globale; b) un sistema di comando e controllo automatico e autonomo; **caratteristiche peculiari:** a) poggia sull'utilizzo di Infrastrutture fisiche (cavi sottomarini, centri di stoccaggio ed elaborazione dati, punti di scambio dati come antenne e satelliti, router di Internet, ecc.); b) ha una dimensione virtuale costituita da elementi digitali come possono essere i siti web o i Protocolli IP.

È evidente, che da un lato il dominio cibernetico garantisce una propagazione dello spettro militare a livello globale in modo istantaneo e allo stesso tempo assicura una maggiore e più rapida capacità operativa. All'opposto, il "prezzo da pagare" in termini strategici è la grave minaccia alla sicurezza nazionale, dovuta alla capacità da parte degli attori più deboli di sfruttare le aporie presenti nelle barriere di accesso al *cyber global commons* per volgere a

[66] *Ibidem.*
[67] G. Rattray, C. Evans e J. Healey, *American Security in the Cyber Commons*, in A. M. Denmark e J. Mulvenon (ed.) Contested Commons…op. cit., pp. 137-176.
[68] *Ibidem.*
[69] *Ibidem.*

proprio vantaggio le abilità operative garantite dal *cyberspace* il quale, a sua volta riduce il differenziale di potere fra attori (statali e non)

In definitiva, poco importa ai fini della politica internazionale costatare che lo spazio cibernetico rientri nel novero di risorsa naturale (terra, acqua, aria e spazio cosmico) o artificiale. Il vero elemento selettivo per assoggettare un "ambiente" alle dinamiche della conflittualità, risiede nella "rilevanza strategica" che la politica riconosce ai propri interessi e ai propri obiettivi in termini sistemici, piuttosto che in termini di equità e di legalità[70]. Se la politica internazionale valuta la rilevanza assunta dal *cyberspace* vitale per la sicurezza e la difesa dei propri interessi, questo ambiente si piega, di fatto, alle dinamiche dettate dai fini preposti dai *policymakers*. In effetti, secondo un'interpretazione "realista" delle Relazioni Internazionali, il nucleo dell'ordine internazionale (anarchico ma non caotico) va ricercato nei rapporti di forza tra i vari attori[71]. Di conseguenza, l'inclusione nella categoria di *global commons* del dominio cibernetico ad opera *in primis* della dottrina militare statunitense inaugura, a tutti gli effetti, l'avvento della quinta dimensione del *warfare*, con tutto ciò che ne consegue, sia in termini

[70] Tucidide ne *La guerra del Peloponneso* (431-404 a.C.) pone l'accento sulla "filosofia realista" della politica internazionale e sui rapporti di forza tra gli stati, infatti, a proposito dell'altrettanto famoso "dialogo" tra gli ambasciatori Ateniesi e i Meli prima dell'assedio da parte dei soldati Ateniesi, Tucidide riporta alcuni passaggi ritenuti fondamentali dalla teoria realista della politica internazionale in quanto, racchiudono la vera natura delle relazioni internazionali. Scrive Tucidide: "Ché noi siamo certi – dicono gli ateniesi – di fronte a voi, persone informate, che nelle considerazioni umane il diritto è riconosciuto in seguito a una eguale necessità per le due parti, mentre chi è più forte fa quello che può e chi è più debole cede. [...] Noi crediamo infatti che per legge di natura chi è più forte comandi: che questo la faccia la divinità lo crediamo per convinzione, che lo facciano gli uomini, lo crediamo perché è evidente. E ci serviamo di questa legge senza averla istituita noi per primi, ma perché l'abbiamo ricevuta già esistente e la lasceremo valida per tutta l'eternità, certi che voi e altri vi sareste comportati nello stesso modo se vi foste trovati padroni della nostra stessa potenza", cfr. Tucidide, *la guerra del Peloponneso*, Volume Secondo (libri III-IV-V) testo greco a fronte, trad. it. a cura di F. Ferrari, cit. [V-89; V-105] pp. 937-945.

[71] Per la teoria sull'egemonia ed equilibrio di potere cfr. J. J. Mearsheimer, *The Tragedy of Great Power Politics*, Norton, New York, 2001, trad. it. *La logica della potenza*, Università Bocconi Editore, Milano, 2003. Secondo Mearsheimer, esponente del filone realista delle RI, gli Stati attori protagonisti della politica internazionale si trovano a far parte di un sistema anarchico che è governato non solo dai rapporti di forza tra i contendenti ma che "costringe gli stati a competere tra loro in termini di potere, [...] essi ambiscono all'egemonia [...]. L'obiettivo di un paese come gli Stati Uniti è quello di acquisire una posizione di predominio sull'intero sistema, perché solo così può confidare che a nessun altro stato o aggregazione di stati verrà mai la tentazione di muovergli guerra" citazione ripresa da R. Jackson e G. Sørensen, *Relazioni Internazionali*, a cura di M. Weber, Egea, Milano, 2008, cit. p. 99. Per una lettura alternativa si rinvia a, R. O. Keohane, *Hegemony and After*, Foreign Affairs. 1 July 2012. URL: http://www.foreignaffairs.com/articles/137690/robert-o-keohane/hegemony-and-after [consultato il 15-06-2013]

politico-strategici che di influenza sugli equilibri del sistema internazionale[72].

2.3 Ambiente operativo dromologico

Secondo la *National Military Strategy for Cyberspace Operations* (NMS-CO) del 2006, l'ambiente cibernetico può essere descritto secondo l'acronimo *VUCA: Volatility, Uncertainity, Complexity, Ambiguity*[73]. Dunque, le caratteristiche peculiari dell'ambiente operativo del *cyberspace* sono essenzialmente due: la velocità di propagazione e l'abbattimento dei confini[74]. Queste sono saldamente legate alla natura "antropica" del *cyberspace*, infatti, in questo ambiente tutto si evolve in base alle scoperte tecnologiche e scientifiche. La staticità degli elementi naturali è pressoché annullata da una volubilità continua, che permette di espandere e mutare la "geografia" dell'etere in modo praticamente istantaneo. Vi è anche lo spettro elettromagnetico (EMS), che rappresenta: "il prodotto delle possibili frequenze delle radiazioni elettromagnetiche le quali, a loro volta, sono onde elettromagnetiche caratterizzate da una lunghezza d'onda e da una frequenza"[75]. Proprio per questo motivo le attività legate all'uso di questo elemento naturale si propagano in modo istantaneo, ovvero, alla velocità della luce[76]. Tutte le operazioni scaturenti dal *cyberspace* (siano esse diffuse tramite dispositivi *hardware*, *software* finanche attraverso la "manipolazione" dello spettro elettromagnetico) seguono un'andatura pressoché istantanea e soprattutto insensibile a qualsiasi attrito di tipo ambientale, diversamente da quanto avviene per le azioni condotte negli altri domini naturali[77]. In altre parole, il dominio cibernetico si distingue dagli altri ambiti di esercizio del potere perché è artificiale e soggetto a cambiamenti tecnologici rapidi; in aggiunta a ciò, vi è l'economicità degli strumenti operativi e la relativa mancanza di

[72] Su questo argomento specifico si rinvia al paragrafo *la militarizzazione del cyberspace*.
[73] Cfr. J.H. Sherrer e W.C. Grund, *A Cyberspace Command and Control Model*, Air War College, Maxwell Paper, No 47, August 2009
[74] *Ibidem.*
[75] Per una definizione dello spettro elettromagnetico, generica e non esaustiva da un punto di vista scientifico, si rinvia a Wikipedia.org
URL: http://www.wikipedia.org/wiki/Spettro_elettromagnetico [consultato il 15-04-2013]
[76] *Ibidem.*
[77] A tal proposito, solo a titolo di esempio, si pensi alla forza di attrito e alla resistenza prodotta dall'acqua salata nei confronti delle navi che hanno una notevole lentezza di movimento rispetto agli aerei e questi ultimi rispetto alla velocità dei dati digitali.

barriere per l'accesso e il movimento[78]. Dunque, la natura *dromologica* (dinamica) dell'ambiente cibernetico[79], insieme all'economicità degli strumenti operativi, condiziona il rapporto di reciprocità tra territorio, violenza e politica; mentre l'assenza di barriere sia di accesso che di movimento, inclina in modo del tutto innovativo il senso spaziale delle attività militari[80]. Non a caso la *dromologia* insegna che:

"Il territorio è lo spazio-tempo costituito dalle tecniche di spostamento e dalle tecniche di comunicazione, e ne deduce che il potere si concentra nelle mani di chi dispone di tecniche di spostamento e comunicazione più efficienti e veloci".[81]

2.4 Geografia fisica e geopolitica virtuale

La percezione superficiale sembrerebbe suggerire che con l'affermazione della rivoluzione informatica, bisogna decretare la fine della geografia e della geopolitica nelle dinamiche delle relazioni internazionali[82]. A tal proposito, Carlo Jean e Giulio Tremonti avvertono che con l'avvento dell'era informatica: "I paradigmi tradizionali della geopolitica – il *raum*, cioè lo spazio, il *lage*, cioè la posizione, e la distanza – sono stati sostituiti" da una serie di strumenti tecnologici che favoriscono la nascita di un nuovo schema cognitivo per le questioni rilevanti da un punto di vista politico-strategico[83]. Nonostante questi cambiamenti – avvertono Jean e Tremonti – non si assiste né alla fine della geografia né tantomeno della geopolitica, perché anche le dinamiche dell'ambiente cibernetico, pur essendo legate a un dominio virtuale, riversano i propri effetti nel mondo reale[84]. Secondo Umberto Gori, l'era dell'informazione, pur affermando un drastico ridimensionamento del tempo e dello spazio, non implica un superamento del valore del territorio, il quale rimane pur sempre un principio organizzativo chiave nelle relazioni umane; nonché un elemento fondamentale e

[78] Cfr. J.S. Nye, *The Future of Power*…op.cit.
[79] Questa definizione è stata suggerita da Paul Virilio in *La macchina che vede*, Milano, 1989, è stata ripresa dalla postfazione di C. Formenti, all'opera di P. Virilio, *La bomba informatica*…op.cit.
[80] Cfr. U. Gori, *Cyberspazio e relazioni internazionali*…op. cit
[81] Ivi, cit. p. 139
[82] Cfr. M.C. Libicki, *The Emerging Primacy of Information*, in Orbis, 1996, pp. 261-274
[83] Cfr. C. Jean e G. Tremonti, *Guerre stellari*…op. cit., cit. p. 50
[84] *Ibidem.*

logistico per le azioni militari[85]. Da queste premesse se ne deduce che, nonostante il *cyberspace* sia stato definito un luogo intangibile e senza barriere, anche questa "dimensione della conflittualità" è soggetta a quelle dinamiche del dispiegamento del potere proprie della politica internazionale[86]. Dello stesso avviso è Nazli Choucri la quale, riferendosi all'influenza trasmessa dall'avvento dell'era dell'informazione nelle odierne relazioni internazionali, parla appunto di *cyberpolitics*, laddove le interazioni umane si plasmano e producono i propri effetti politici attraverso l'utilizzo di uno spazio virtuale, il *medium* cibernetico, divenuto la nuova arena della conflittualità[87]. Analogamente, Carlo Jean nell'opera *Geopolitica del XXI secolo*, osserva che pur essendoci una "complessità" sistemica nelle odierne relazioni internazionali, ciò non equivale alla sovversione delle dinamiche classiche dei rapporti di forza tra i vari attori[88]. David Clark sottolinea che il piano fisico costituisce le fondamenta sulle quali poggiano gli altri strati del *cyberspace*, ma soprattutto, in termini geografici, questo livello presenta rispetto agli altri, un *sense of location* che gli concede un grado di tangibilità prettamente "materiale"[89]. Inoltre, essendo fisicamente ubicate all'interno di giurisdizioni nazionali, le imprese che operano nel settore informatico sono soggette alle normative e direttive dei paesi nazionali (democratici o meno)[90]. Un'altra entità fondamentale sono le c.d. *Information Communication Technology* (ICT). Queste infrastrutture "geneticamente" legate al dominio cibernetico concorrono a produrre i suoi effetti in termini geopolitici[91]. Come sottolineato in un documento previsionale edito dall'*European Union Institute for Security Studies* (EUISS) e intitolato: "*Citizens in an Interconnected and Polycentric Word*"[92], lo sviluppo delle ICT e la loro pervasività nelle società odierne, nel lungo periodo, faciliterà un processo di *empowerment* (crescita dei poteri) individuale[93]. Nel lavoro dell'EUISS, tra le varie analisi sugli "scenari futuri" prodotti

[85] Cfr. U. Gori, *Cyberspazio e relazioni internazionali*...op.cit.
[86] Cfr. C. Jean, *Geopolitica del XXI secolo*...op. cit
[87] Cfr. N. Choucri, *Cyberpolitics in International Relations*, MIT Press Cambridge, Massachussetts, 2012.
[88] Cfr. C. Jean, *Geopolitica del XXI secolo*....op. cit.
[89] *Ibidem.*
[90] *Ibidem.*
[91] Cfr.J.S. Nye, *The Future of Power*....op. cit
[92] Cfr. Institute for Security Studies European Union, *Global Trends 2030- Citizens in an Interconnected and Polycentric World*, ESPAS, Paris, 2012. In particolare si rinvia al paragrafo *The information age: Empowerment but threats to privacy*, pp. 32-37.
[93] *Ibidem.*

dall'ascesa delle tecnologie informatiche, da un punto di vista delle ripercussioni sulle dinamiche del potere, viene evidenziato un pericolo sempre più diffuso di attacchi di guerra cibernetica[94]. Questi rischi provengono perlopiù da attori che scontando un'inferiorità operativa negli armamenti convenzionali volgono a proprio vantaggio le vulnerabilità presenti nell'ambiente cibernetico[95]. Secondo gli Autori del documento previsionale, con l'incremento delle minacce cibernetiche si rischia, nel lungo periodo, una vera e propria *balcanizzazione* di Internet, a causa della scelta di attori (statali e privati) di istallare reti Intranet[96] (per motivi di sicurezza esterna e di propaganda interna) andando in questo modo a sottrarre parti di *cyberspace* alla collettività; questo comporterebbe, in termini pratici, un'alterazione dell'indole globale di Internet[97]. Da un punto di vista più strettamente militare, come si è sottolineato finora, l'avvento delle c.d. tecnologie *dual-use capability*[98] ha indotto i dispositivi militari a dipendere in misura sempre maggiore da mezzi commerciali[99]. La conseguenza di ciò è stata un vero e proprio processo di *spin-in* dal civile al militare, all'opposto di quanto avveniva prima, dove vigeva uno *spin-off* dal militare al civile. Infatti, il forte legame che intercorre tra le ICT e le varie attività (economiche, finanziarie e militari) svolte dagli Stati, dalle Organizzazioni Internazionali, dalle aziende private, rende queste infrastrutture il nuovo *centro di gravità* delle società tecnologicamente più avanzate[100]. Risulta evidente, pertanto, che proprio da questa consapevolezza della vulnerabilità intrinseca all'ambiente dove operano le infrastrutture ICT, ne derivi la necessità di costruire una dottrina di difesa, che abbia appunto, come *focus* principale la *cyber-security*, con la consapevolezza che le azioni, seppur prodotte in un ambiente intangibile, generano effetti concreti nel mondo reale[101]. Non è un caso dunque, se nella relazione semestrale sulla politica

[94] *Ibidem.*
[95] *Ibidem.*
[96] Rete Locale (LAN) o un raggruppamento di reti locali, usata all'interno di una organizzazione per facilitare la comunicazione e l'accesso alle informazioni, che può essere ad accesso ristretto, limitato o riservato per gli utenti.
[97] Ivi, pp. 36-37.
[98] *Dual-use* si riferisce alle tecnologie che possono essere usate per scopi pacifici e militari; di solito riguarda la proliferazione delle armi nucleari, ma anche tecnologie pensate a scopi pacifici o civili che vengono utilizzate come mezzi distruttivi
[99] Cfr. C. Jean e G. Tremonti, *Guerre stellari*...op. cit.
[100] Cfr. G.J. Rattray, *Strategic Warfare in Cyberspace*, MIT Press, Cambridge Mass, 2001. Sul punto della sicurezza si rinvia al prossimo capitolo la guerra cibernetica e in particolare al paragrafo *dalla deterrenza nucleare alla resilienza cibernetica*.
[101] Cfr. U. Gori, *Cyberspazio e relazioni internazionali*...op. cit.

dell'informazione per la sicurezza del 2010[102], redatta dai servizi di *intelligence* italiani, a proposito delle minaccia cibernetica viene sottolineato che:

"Si tratta di una minaccia che, sebbene riferita al mondo intangibile del cyberspace, presenta ormai tratti di estrema concretezza. Il settore ICT ha infatti assunto negli anni un peso crescente per l'economia e la società, registrando una crescita esponenziale sia delle apparecchiature fisse e mobili che si connettono ora alla rete in wireless, sia del volume e della sensibilità delle informazioni scambiate. Tale settore ha la peculiare caratteristica di costituire un'infrastruttura critica in sé e di rappresentare, al contempo, il nervo portante delle altre infrastrutture critiche"[103].

Un classico esempio di infrastruttura ICT sono i c.d. *data center*[104]. Queste strutture di stoccaggio ed elaborazione dati sono collocate all'interno di un determinato territorio nazionale e il più delle volte sono soggette all'amministrazione di aziende private che gestiscono il flusso di informazioni e dei dati in modo del tutto autonomo e con meccanismi volti al profitto; nonostante ciò, ci sono casi in cui in cui (per motivi di sicurezza interna o esterna) prestano il loro servizio per monitorare le informazioni e i dati che transitano nell'etere[105]. Di conseguenza, la loro difesa da intrusioni esterne, così come la salvaguardia da "fughe inattese" dei dati immagazzinati al loro interno, nonché la possibilità di controllare il traffico dei dati con sistemi quali *Deep Packet Inspection*[106], diventa di vitale importanza per il mantenimento di una superiorità strategica in relazione alle informazioni assimilate[107]. Infatti, la quantità (e la qualità) dei dati immagazzinati permette di creare una "nuova linea del potere" che a ragione è stata definita la *geopolitica dei dati*[108]. È il caso ad esempio

[102] Relazione sulla politica dell'informazione per la sicurezza 2010.
[103] Ivi, cit. p. 30
[104] Per *Data Center* si intende una struttura fisica, normalmente un edificio compartimentato, progettato per ospitare e gestire un numero elevato di apparecchiature e infrastrutture informatiche e i dati ivi contenuti, allo scopo di garantirne la sicurezza fisica e gestionale.
[105] Cfr. F. Vitali, *La geopolitica economica dei dati e il futuro del dominio. Dal controllo alla previsione. Il potere tra social media e manipolazione dell'azione sociale*, in Nomos & Khaos. *Rapporto Nomisma 2011-2012 sulle prospettive economico-strategiche*, Osservatorio Scenari Strategici e di Sicurezza, Nomisma Spa, A.G.R.A., Roma, 2012, pp. 207-231.
[106] Modalità di analisi del contenuto dei pacchetti di dati che transitano all'interno di una rete
[107] Cfr. F. Vitali, *La geopolitica economica dei dati e il futuro del dominio* … op. cit.
[108] *Ibidem.*

dei c.d. *Big Data*[109], porzioni di dati misurati in *petabyte, exabyte, zettabyte,* ovvero quantità gigantesche di dati che non possono essere memorizzati e gestiti dai *database* standard[110]. Questi dati (dalle semplici foto ai documenti riservati) vengono trasferiti dagli utenti ai sistemi del fornitore (perlopiù operatori privati) che a sua volta li memorizza sui propri *data center* attraverso i sistemi di trasferimento a distanza con il c.d. *Cloud Computing*[111]. Dalle osservazioni riportate sopra, se ne deduce che la sfida aperta per il controllo e la difesa delle informazioni da intrusioni malevole, nonché l'incessante raccolta di informazioni, sono il nuovo campo di battaglia nel quale il labile confine tra civile e militare viene meno, un campo dove gli Stati Uniti mantengono un'elevata soglia di eccezionalità[112]; come scrive Vitali:

"Francia e Cina possono controllare la trasmissione dei dati, [...] dispongono anche di centri di ricerca in grado di incrociare algoritmi *Pattern-based-Aggregation*, di *Sentiment Classification*, *algoritmi genetici e reti neurali*; hanno capacità statistiche avanzate, ma non hanno una sufficiente rete di "sensori" a livello globale per poter studiare in tempo reale quello che avviene nel mondo. Non hanno la base dati e la capacità di calcolo tale da poter trasformare con efficacia tali informazioni in azione strategica con valore geopolitico e geoeconomico. Possono fare azioni di *data mining* specifico su informazioni liberamente accessibili su Internet, azioni avanzate di *Open Source Intelligence* ma mancano di capacità computazionali di previsione equiparabili a quella dello Stato e delle società private statunitensi"[113].

D'altronde, se si osserva la mappa della distribuzione dei principali *data center* a livello mondiale, questo *gap* "geografico" e tecnologico tra Stati Uniti e gli altri attori della politica internazionale nel settore dei *Big Data* appare evidente.

---

[109] Cfr. Ibm.com, What Is Big Data?,
URL: http://www-03.ibm.com/software/products/it/it/category/SWP10 [consultato il 15-06-2013]
[110] Cfr. K. Cukier e V. Mayer-Schoenberger, *The Rise of Big Data*, in Foreign Affairs, Volume 92, Number 3, May/June 2013, pp. 28-40.
[111] *Ibidem.*
[112] *Ibidem.*
[113] Ivi, cit. p. 225.

Posizione geografica *Data Center*

Luigi Martino (2013)
Fonte: Elaborazione dati datacentermap.com su immagine *google-maps.com*

I risultati –come suggerisce Francesco Vitali– sono chiari; infatti, siamo di fronte alla "nuova linea del potere"[114]; questa è una geopolitica dei dati che scaturisce dalla consapevolezza che:

"Il predominio, nel prossimo futuro, non si giocherà sui *media*, sui *new media*, o sui *social media*, come poteva apparire da una prima lettura degli ultimi eventi internazionali. Certamente, il ruolo di questi modelli di informazione nella costruzione della società non sarà depotenziato, ma la loro capacità di azione sarà collegata e, probabilmente, conseguente a una diversa forma di potere, più profonda e sottile: il controllo dei dati"[115].

Il "controllo" di cui parla Vitali, rappresenta il salto di qualità nella raccolta dati iniziata con ECHELON[116] (creato in *jointventure* tra Stati Uniti, Canada, Regno Unito, Australia e Nuova Zelanda) e scaturita nelle tecniche più perniciose di raccolta informazionale passiva[117]. Vitali, a tal proposito, avverte che: "La maggior parte delle informazioni sono rese accessibili, quasi sempre in modo

[114] *Ibidem.*
[115] Ivi, cit. p. 207.
[116] ECHELON è il sistema mondiale di intercettazione delle comunicazioni private e pubbliche, divenuto di dominio pubblico nel 1997 dopo che il Parlamento Europeo ha reso noto il famoso rapporto "*Report on the existence of a global system for the interception of private and commercial communications*" nel quale è possibile ritrovare un paragrafo apposito dal titolo "*ECHELON interception system*".
[117] Cfr. F. Vitali, *La geopolitica economica dei dati e il futuro del dominio*...op. cit

inconsapevole, dall'utente stesso o trasmesse in automatico dalle macchine"[118]. Con la pervasività raggiunta dalle c.d. "tecnologie abilitanti" la raccolta dati appare sempre più facilitata dall'avvento dei sistemi *machine-to-machine*, dove sembra profilarsi una maggiore autonomia degli oggetti *smart* rispetto ai comandi forniti dall'utente umano[119]. Un altro aspetto indotto dall'era cibernetica è la caratteristica creazione di nuovi centri di gravità geopolitici, nei quali si assiste ad un radicale mutamento delle traiettorie globali legate all'utenza (ed economia) di Internet[120]. In questo settore emerge un vero e proprio *pivot* asiatico (cinese in particolare) che va a surclassare la tradizionale *leadership* occidentale nel comparto della c.d. *Internet Economy*[121]. Infatti, come sottolinea il già citato studio dell'EUISS le cifre di Internet (e non solo) dimostrano un vero e proprio cambiamento dei centri di gravità geopolitici[122]. Gli Autori del documento mettono in evidenza che, se finora la *cybersfera* è stata dominata dall'Occidente, i numeri degli attuali utenti (consumatori) dimostrano che il "peso demografico" asiatico è in netta ascesa: all'incirca il 42% dell'ammontare degli utenti a livello mondiale; di contro, nel Nord America si registra un calo del 14% rispetto al 2000, il dato riporta dunque un *gap* tra numero di utenti cinesi maggiore rispetto a quelli americani[123]. Il grafico 2.4 fotografa la situazione attuale degli *user* di Internet sul totale della popolazione mondiale; se ne deduce che il "peso" asiatico è evidente.

[118] Ivi, cit. p. 209

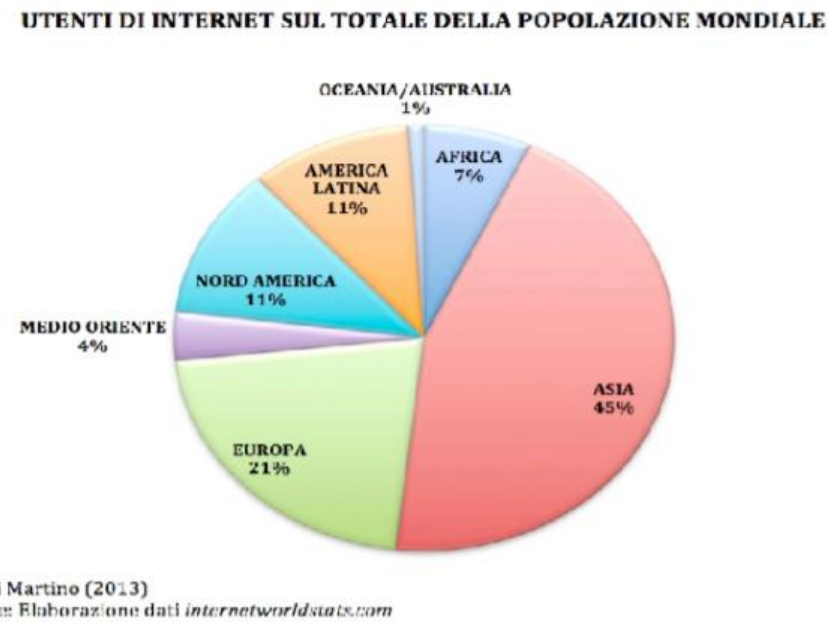
[119] Si pensi a tal proposito alla capacità delle *webcam* di scansionare le espressioni del volto dell'utente in modo da scansionare il suo stato d'animo. È il caso del brevetto *Targheting Advertisements Based on Emotion* depositato nel 2010 dalla Microsoft e registrato nel 2012. Cfr. US Patent Application 20120143693, *US Patent and Trademark Office*, URL: http://patft.uspto.gov/ [consultato il 16-12-2012].

[120] Cfr. European Union Institute for Security Studies, *Global Trends 2030*...op. cit.

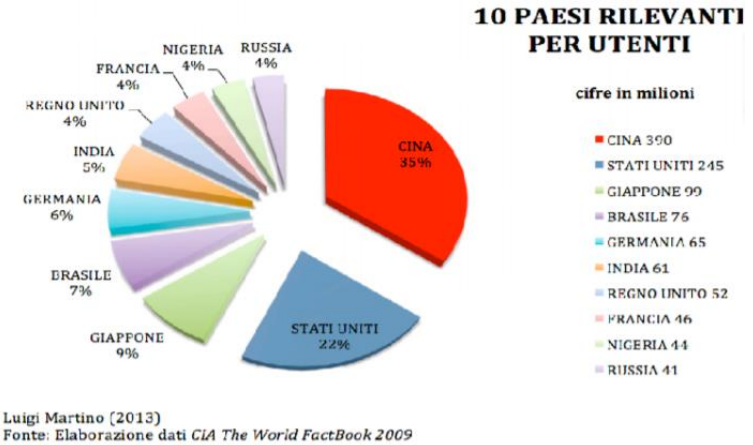
[121] *Ibidem.*

[122] *Ibidem.*

[123] *Ibidem.*

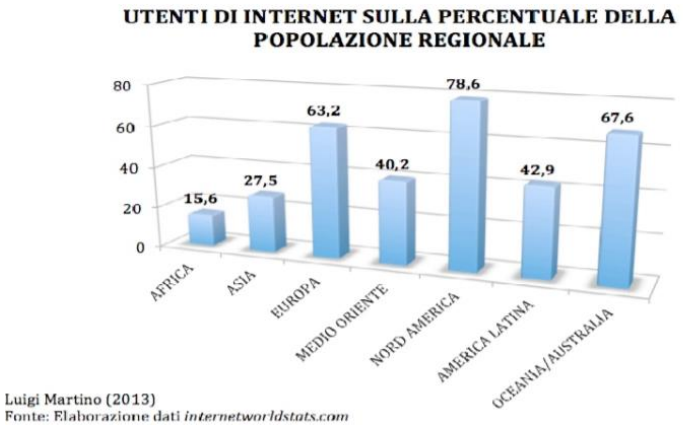


In termini geopolitici, ciò equivale nel lungo periodo a una maggiore "domanda" di Internet da parte delle popolazioni asiatiche (cinesi in particolare) rispetto ai paesi occidentali[124]. Questo dato induce a prevedere uno scenario in cui si assisterà all'avvio di una serie di competizioni commerciali e politiche nel settore dei c.d. *Internet services*, come dimostrano i numeri in ascesa degli utenti di Sina e RenRen equivalenti cinesi di Google e Facebook[125]. Tale competizione, avvertono gli Autori, avrà conseguenze tali per cui: "*Could challenge the universal integrated use of the internet and favour the proliferation of fragmented and even closed communities*"[126].
Il grafico 2.4.1, ritrae i 10 Paesi più rilevanti a livello globale in base alla percentuale degli utenti di Internet.



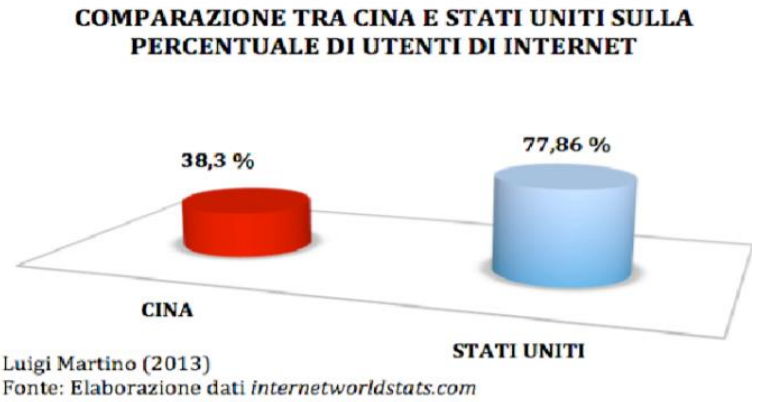
[124] *Ibidem.*
[125] *Ibidem.*
[126] Ivi, cit. p. 33

Se si osserva il grafico si può notare che le "porzioni" di utenti a livello globale sono perlopiù distribuite tra Stati Uniti e Cina; ciò rispecchia fedelmente il *trend* profilato dagli analisti dell'EUISS[127]. Di conseguenza, è facile capire che la posta in palio per la *governance* di Internet racchiude degli scenari che avranno ripercussioni sull'intero sistema internazionale[128]. Tuttavia, osservando il grafico 2.4.2 che riporta la percentuale degli utenti di Internet in base alla popolazione a livello regionale, si nota una maggiore "penetrazione" di Internet nei Paesi Occidentali (Nord America, Europa, Oceania/Australia) mentre l'aria Asiatica rimane marcatamente indietro anche rispetto ai Paesi mediorientali.



Luigi Martino (2013)
Fonte: Elaborazione dati *internetworldstats.com*

Lo stesso *trend* emerge dalla comparazione tra la "penetrazione" di Internet in Cina e negli Stati Uniti, dove i secondi si assestano a un 77,86% sul totale della popolazione statunitense, rispetto al solo 38,30% dei cinesi.



Luigi Martino (2013)
Fonte: Elaborazione dati *internetworldstats.com*

[127] *Ibidem.*
[128] 8 Cfr. H. Kwalwasser, *Internet Governance*...op.cit.

D'altronde, come già sottolineato in precedenza, questo dato rispecchia il sempre più marcato *gap* tra Occidente e resto del mondo, principalmente in termini di *digital-divide*[129] nelle capacità innovative e tecnologiche per quanto riguarda le infrastrutture e le tecnologie di stoccaggio ed elaborazione dati, dove lo Stato e le società private statunitensi registrano un netto vantaggio in questo settore industriale e strategico[130]. Infatti, se si riporta l'attenzione sul valore dei *data center* sui dieci paesi al mondo con maggior numero di presenza di *data center*, emerge un distacco lampante: il primo paese sono gli Stati Uniti con 1046 centri di stoccaggio ed elaborazione dati, segue il Regno Unito 161 e la Germania con 127, mentre la Russia 28 e la Cina ne ha solo 9[131]. Non sorprende dunque la diatriba "solo all'apparenza virtuale", tra Cina e Russia da una parte e Stati Uniti dall'altra, nello specifico settore della *governance* di Internet[132]. I cinesi e i russi accusano gli americani di detenere un controllo monopolistico sul sistema di assegnazione dei c.d. *Internet Protocol* (IP), mentre gli americani lamentano ai cinesi la continua censura delle informazioni presenti sul *Web*[133]. Al di là delle contrapposte tesi propagandistiche per un etere più "democratico", molto realisticamente la disputa cela la posta in palio per il controllo, la *governance* e la sicurezza nel *cyberspace*[134]. In conclusione, emerge a chiare lettere, una vera e propria geopolitica del *cyberspace*; una dimensione che, come tutti gli altri *habitat* dell'attività umana, si conferma essere sottomessa alle azioni della politica, giacché detiene interessi (anche economici) rilevanti dove, pur essendo gli Stati gli attori con maggiore capacità di influenza, si profila un'elevata autonomia degli intermediari privati[135].

---

[129] Il *digital divide*, o divario digitale, è il divario esistente tra chi ha accesso effettivo alle tecnologie dell'informazione e chi ne è escluso in modo parziale o totale

[130] Cfr. F. Vitali, *La geopolitica economica dei dati*...op. cit.

[131] I dati si riferiscono al giugno 2012, per un approfondimento si rinvia a http://www.datacentermap.com/datacenters.html. [consultato il 15-05-2013]. È da sottolineare che questi dati presentano dei limiti in quanto non includono i c.d. centri *cloud* o i centri di elaborazione polifunzionale, non confrontano la capacità di memorizzazione ed elaborazione dei singoli *data center*, e non includono parte di quei centri legati alle varie agenzie governative. Per un'analisi dettagliata si rinvia a F. Vitali, *La geopolitica economica dei dati e il futuro del dominio*...op.cit.

[132] Cfr. L. Mainoldi, *I padroni di Internet*...op. cit.

[133] *Ibidem.*

[134] *Ibidem.*

[135] Cfr. D. Clark. Control Point Analysis, MIT CSAIL, September 2012. Documento gentilmente fornito da http://www.silendo.org.

3. LA GUERRA CIBERNETICA

3.1 Premessa

Dopo aver analizzato l'impatto dell'era cibernetica sulle odierne relazioni internazionali, e posto l'accento sulle varie sfaccettature della natura geopolitica e geografica del *cyberspace*, è giunto il momento di approfondire le implicazioni del *medium* cibernetico dal punto di vista più strettamente militare. Prima di iniziare la dissertazione è utile anticipare qui di seguito, alcune ipotesi plausibili risultanti dalla ricerca condotta:

- La guerra cibernetica può consentire agli attori di raggiungere i loro obiettivi politici e strategici senza la necessità di un conflitto armato;

- Il cyberpower concede un potere sproporzionato ad attori minori e relativamente deboli nei rapporti di forza del sistema internazionale;

- L'azione condotta mediante sistemi informatici virtuali (dietro indirizzi IP fittizi, server stranieri, false identità) favorisce almeno nel breve periodo, l'anonimato e una relativa impunità; · Nel cyberspace i confini tra il militare e il civile, e tra il fisico e il virtuale, sono labili;

- Il cyberpower può essere esercitato in tempo di pace e in guerra da Stati o attori non statali, anche attraverso forme di proxy war o guerre per procura;

- Sul piano giuridico le operazioni di cyber warfare ricadono in linea di principio nella c.d. plausible deniability o negazione plausibile;

- La guerra cibernetica rappresenta un modello strategico di Indirect Approach, perché mira all'annientamento strategico dell'avversario piuttosto che a quello tattico;

- La guerra cibernetica deve essere intesa come una nuova componente, ma non separata del concetto poliedrico di

warfare;

- Lo spazio cibernetico deve essere inteso come la "quinta dimensione della conflittualità" accanto ai domini più tradizionali: terra, aria, mare e spazio extra-atmosferico.

Una volta ristretto il campo delle principali caratteristiche risultanti dall'azione del *cyberpower* e della *cyber warfare*, è altresì utile ai fini di questo lavoro, porsi le seguenti domande[136]: **Cosa** si intende per guerra cibernetica? **Quando** è possibile classificare un'azione virtuale, un atto di guerra? **Chi** sono gli attori principali? **Come** agiscono? **Perché** agiscono? **Dove** colpiscono? **Quali** sono i principali strumenti operativi? Infine, è possibile una deterrenza efficace? Domande che, senza la pretesa di esaustività, serviranno come linee guida per identificare, lungo il nostro breve *exursus*, la "grammatica" della guerra cibernetica[137].

3.2 Alla ricerca di una definizione

Non esiste una definizione condivisa e univoca su ***cosa*** debba intendersi per guerra cibernetica, soprattutto perché questo campo di ricerca è relativamente nuovo rispetto alle dinamiche della conflittualità consolidatesi nel tempo[138]. Si può però giungere ad alcune classificazioni; nello specifico: mentre un atto di *Hacker Warfare* può nascondere delle mire prettamente economiche e quindi criminali, la *Cyber Warfare* pur costituendo la *summa* di tutte le altre "opzioni", per essere definita "guerra" necessita quantomeno di determinati elementi distruttivi e/o coercitivi[139]. A tal proposito, come giustamente fa notare Umberto Gori: se il primo caso di *IWar* è possibile farlo rientrare nell'attacco contro l'Estonia tramite sistemi

[136] A porsi queste domande è anche N. Choucri, *Cyberpolitics in International Relations*…op. cit.

[137] In questo lavoro si condivide l'idea di E. N. Luttwak secondo cui le guerre hanno una loro grammatica, mentre la logica rimane pur sempre la grande strategia ovvero lo scopo politico della guerra; cfr. E.N. Luttwak, *Strategia. La logica della guerra e della pace*…op. cit.

[138] Si pensi ad esempio che negli Stati Uniti "guerra cibernetica" richiama più elementi operativi consoni per la classificazione di azioni condotte nell'alveo della *Electronic Warfare*. Cfr. U. Gori, *Dai DDoS allo Stuxnet: la dinamica esponenziale degli attacchi informatici*, in *Information Warfare 2010. Le nuove minacce provenienti dal cyberspazio alla sicurezza nazionale italiana*, a cura di Id. e L.S. Germani, FrancoAngeli, Milano, 2011, pp. 31-38.

[139] Cfr. U. Gori, *Cyberspazio e relazioni internazionali*…op. cit.; R.A. Clarke e R. K. Knake, *Cyber War. The Next Threat to National Security and What to do About It*, HapperCollins Publishers, New York, 2010.

di *Distribiuted Denial-of-Service* (*DDoS*); a sua volta il primo vero atto acclarato di *cyber war* è possibile farlo risalire all'attacco condotto con il *worm Stuxnet* contro l'Iran[140]. Stando a quanto si legge nel rapporto della *National Defense University*: "La guerra cibernetica include tutte le forme di attacco e di difesa nello spazio cibernetico"[141]. Secondo Richard Clarke e Robert Knake per guerra cibernetica si deve intendere: "Un'azione da parte di uno Stato atta a penetrare i sistemi informatici o le reti di un altro Stato con la finalità di causare danni o distruzione"[142]. È evidente dunque, che il "ventaglio" delle opzioni di impiego possibile è troppo ampio per un settore di ricerca relativamente nuovo. Secondo Scott Borg, Direttore della *U.S. Cyber Consequences Unit*, gli errori di valutazione sono dovuti in parte alle definizioni fuorvianti di politici inesperti e giornalisti compiacenti che hanno diffuso: "L'idea errata che gli attacchi informatici riguardino principalmente i sistemi di telecomunicazioni"[143]. Sempre secondo Borg ha contribuito a questo *misunderstanding* la volontà di usare termini quali "guerra cibernetica" o "informatica", dando per scontato che la guerra non avesse più a che fare con "un gran numero di vittime e gravi danni materiali ed economici"[144]. In realtà, spiega l'autore la guerra si diffonde *anche* attraverso il *medium* cibernetico, (ad esempio tramite sistemi informatici) però con l'obiettivo reale di causare danni alle infrastrutture fisiche e ai sistemi d'arma[145]. Dello stesso avviso è Cordula Droege, consulente legale del Comitato Internazionale della Croce Rossa (CICR), secondo cui la guerra cibernetica: "Si riferisce ai mezzi e metodi di guerra basati sulle tecnologie dell'informazione e che si utilizzano nel contesto di un conflitto armato nel senso del diritto internazionale umanitario"[146]. Anche secondo Colin S. Gray, la mancanza di una definizione univoca è dovuta a una serie di errori di valutazione che non concorrono a rendere giustizia "all'affare *cyber*"[147]. Valutazioni distorte che – come spiega Gray – prendono piede se il promotore è più specializzato in modo tecnico nel settore

[140] *Ibidem.*
[141] National Defense University – Institute for National Security Studies, *Global Strategic Assessment 2009*...op.cit.
[142] Cfr. R.A. Clarke e R. K. Knake, *Cyber War*...op. cit., cit. p. 6.
[143] Cfr. S. Borg, *Logica della guerra cibernetica*, in LiMes, Quaderno Speciale, aprile 2012, pp. 47-53, cit. p. 47.
[144] Ivi, cit. p. 48.
[145] *Ibidem.*
[146] Cfr. Comitato Internazionale Croce Rossa (CICR), *Intervista a Cordula Droege* del 16.08.2011. [On line] URL: http://www.icrc.org [consultato il 12-06-2013]
[147] Cfr. C. S. Gray, *Making Strategic Sense of Cyber Power*...op. cit

informatico o all'opposto, se si tratta di un politologo più predisposto allo studio della strategia militare[148]. Secondo Umberto Gori, una corretta definizione di *cyber warfare* deve scaturire dall'analisi strategico-situazionale del contesto in cui prende vita l'attacco cibernetico[149]. Infatti, come specifica Gori bisogna valutare il vero obiettivo finale dell'atto ostile (elemento razionale); inoltre, un atto *cyber* per essere definito "militare" deve avere una certa dose di complessità e di letalità (elemento violento), tali per cui possa provocare un'influenza sulle scelte del *target* (elemento coercitivo)[150]. Dello stesso avviso sono gli Autori di *On Cyber Warfare* quando a proposito dei modi di condurre la guerra cibernetica spiegano che: "Per riuscire a comprendere se un'azione ostile nello spazio cibernetico è o meno un atto di guerra, non è solo necessario osservare gli eventi ma è altrettanto indispensabile capire le intenzioni degli autori"[151]. In definitiva, un'azione diffusa tramite il dominio virtuale è classificabile come atto di guerra quando, parafrasando Clausewitz, lo strumento militare (anche virtuale) è utilizzato per costringere il nemico ad accettare la nostra volontà[152]. Secondo Gray (in aperta critica con la visione di John Arquilla e David Ronfeldt, autori del già citato saggio *Cyberwar Is Coming*!) l'atto *cyber*, per essere classificato un'azione di *warfare*, deve contenere un potenziale coercitivo tale da riuscire a piegare (anche solo in via di principio) la volontà del *target* prefissato; e questo potenziale (economico e organizzativo) lo possiedono solo gli Stati[153]. In ultima analisi, spiega Gray, anche qualora gli attacchi cibernetici avessero delle qualità autonome, dovrebbero essere considerati nel più ampio contesto politico-strategico del *warfare*[154]. Sorge spontaneo dunque chiedersi: se con la diffusione del potere viene sancito il declino dello Stato-nazione in termini di monopolio della violenza e delle informazioni, allora come è possibile che l'atto di *cyber warfare* possa essere classificato tale, solo ed esclusivamente, se l'attore che lo compie (o lo delega) è uno Stato? La risposta a questa domanda la ricaviamo dalle stesse parole di Nye il quale, a tal proposito scrive: "Il punto cruciale sollevato dalla diffusione del potere non è se lo Stato

[148] *Ibidem.*
[149] Cfr. U. Gori, *Cyberspazio e relazioni internazionali*...op. cit.
[150] *Ibidem.*
[151] Cfr. P. Cornish (et.al.) *On Cyber Warfare*...op. cit.
[152] Cfr. C. von Clausewitz, *Della Guerra*...op. cit
[153] *Ibidem.*
[154] Ivi, cit. 327.

continuerà ad esistere, bensì quale sarà il suo modo di funzionare"[155].

3.3 La militarizzazione del cyberspace

La consapevolezza del potenziale bellico del dominio cibernetico ha indotto molti *decisionmaker* a rivedere le proprie dottrine militari e difensive, adattandole all'era cibernetica. Come sempre gli Stati Uniti, data la loro superiorità effettiva in campo tecnologico e militare, sono stati i primi a ridefinire il loro approccio classico alla guerra in base alle novità introdotte dalla rivoluzione informatica[156]. Se si analizzano i documenti ufficiali della Casa Bianca, emerge un *continuum* strategico di lungo respiro che vede coinvolte nella militarizzazione e difesa del *cyberspace*, i presidenti Clinton, Bush jr. e Obama[157]. Tre presidenze del tutto differenti tra di loro sul piano delle agende politiche proposte, ma accumunate dalla volontà di rendere lo spazio cibernetico un vero e proprio dominio militare[158]. In effetti, già nel 1997 l'allora Segretario alla Difesa William Cohen, rendendosi conto della portata degli eventi, affermava che:

"La rivoluzione dell'informazione sta creando una Rivoluzione negli Affari Militari che cambierà profondamente il modo di combattere delle forze statunitensi. Dobbiamo sfruttare queste e altre tecnologie per dominare il campo di battaglia. Lo schema di riferimento in base al quale fare nostre queste nuove opportunità e garantirci così una posizione di supremazia è fissato dal documento *Joint Vision 2010*, il piano predisposto dal presidente del Comitato dei Capi di Stato Maggiore per le operazioni militari del futuro".[159]

---

[155] Cfr. J.S. Nye, *The Future of Power*...op. cit., cit. p.142

[156] Cfr. A. Joxe, *L'impero del caos. Guerra e pace nel nuovo disordine mondiale*, Sansoni Editore, Milano, 2003.

[157] Cfr. J.T. Richelson e M. Byrne, *When America Became a Cyberwarrior. A secret Document Shows the NSA has been Planning Attacks Since the Clinton Years*, in Foreign Policy, APRIL 26, 2013. URL:http://www.foreignpolicy.com/articles/2013/04/26/when_america_became_a_cyberwarrior_nsa_declassified?print=yes&hidecomments=yes&page=full [Consultato il 14-06-2013]

[158] *Ibidem.*

[159] Cfr. W.S. Cohen, *Report of the Quadriennal Defense Review*, U.S. Department of Defense, Washington DC, , 1997, p. IV. Citazione ripresa da F. P.B. Osinga, *Science, Strategy and War. The Strategic Theory of John Boyd*...op. cit.

È evidente, la predisposizione "futuristica" delle forze armate e dei decisori politici statunitensi verso una supremazia e un'effettiva militarizzazione dello spazio cibernetico che, entro il 2010 (*sic!*) sarebbe dovuta diventare realtà[160]. A tal proposito, nella *Joint Vision 2010* citata da Cohen, si legge:

"Entro il 2010 dovremmo essere in grado di modificare il modo in cui conduciamo le operazioni interforze di maggiore intensità. Invece di fare affidamento sulle concentrazioni delle forze e su una struttura sequenziale delle operazioni, punteremo a realizzare la concentrazione degli effetti con altri mezzi. La superiorità del dominio dell'informazione e gli sviluppi della tecnologia ci permetteranno di ottenere gli effetti desiderati attraverso l'applicazione mirata di una potenza di combattimento interforze. Armi di maggiore letalità ci permetteranno di sferrare attacchi che in passato richiedevano una concentrazione di mezzi esercitata in modo sequenziale. Con sistemi d'arma caratterizzati da una precisione superiore e una maggiore portata, i comandanti potranno conseguire il livello desiderato di distruzione o di soppressione delle forze nemiche utilizzandone un minor numero, riducendo quindi la necessità di ammassare uomini e mezzi, operazione che richiede tempo ed è di per sé rischiosa. Una migliore struttura di comando e controllo, basata su una 'intelligence' in grado di fornire un quadro di situazione aggiornato in tempo reale grazie alla fusione dei dati forniti da una molteplicità di fonti, renderà non più necessario ammassare le formazioni di manovra con giorni e ore di anticipo rispetto al momento stabilito per attaccare. Fornire informazioni 'targeting' o 'puntamento' in senso lato direttamente al più efficace tra i sistemi d'arma disponibili darà la possibilità di concentrare meno forze di quanto tradizionalmente necessario nel punto di applicazione dello sforzo principale. Tutto questo indica che saremo sempre più in grado di ottenere l'effetto della massa – l'indispensabile concentrazione di potenza di combattimento nel momento e nel punto decisivo – senza che sia più necessario ammassarvi direttamente le nostre forze" [161]

[160] Cfr. M. Nones e A. Marrone, *La trasformazione delle Forze Armate: il programma Forza NEC*, in Quaderni IAI, Roma, 2011.
[161] Cfr. Joint Chief of Staff, *Joint Vision 2010*, Washington DC, U.S. Department of Defense, 1997, p. 17.

Il successivo "balzo in avanti" nella militarizzazione del *cyberspace* ad opera degli Stati Uniti è stata la teoria bellica c.d. *Network Centric Warfare* (NCW), che esprime la summa delle linee guida iniziate nella seconda metà degli anni Novanta e le rielabora adattandole alle novità introdotte dalle *Information Technology*[162]. Tra i sostenitori di questo "nuovo paradigma militare" vi sono: David Gompert, Richard Kugler e il già citato Martin C. Libicki[163]. La rilevanza strategico-militare riconosciuta al dominio cibernetico dagli analisti americani ha comportato l'elevazione del *cyberspace* a nuova dimensione (la quinta) della conflittualità[164]. Nel febbraio 2003 l'amministrazione Bush emanava il primo documento ufficiale della Casa Bianca sulla militarizzazione del *cyberspace*: la *National Strategy to Secure Cyberspace*[165]. Questo documento avrebbe rappresentato la cornice entro la quale, si sarebbero mosse le varie scelte strategiche difensive degli Stati Uniti in relazione al dominio cibernetico[166]. La *U.S. National Defense Strategy* nel 2005, in linea con le direttive del 2003, per la prima volta riconobbe ufficialmente il "*cyberspace* come il nuovo teatro delle operazioni militari"[167]. Intanto, tra il 2003 e il 2005, gli Stati Uniti subirono un vero e proprio attacco da parte di *cracker* cinesi che riuscirono a penetrare migliaia di computer dell'amministrazione statunitense ai fini di sottrarre informazioni sensibili[168].

Nell'autunno del 2008 un *worm* denominato *agent.tbz* infiltrato nei *network* militari statunitensi mette in discussione l'intero sistema di sicurezza cibernetic[169]. L'operazione di *cyber-espionage* ha avuto origine in una base in Medio Oriente con l'introduzione di un *flash drive* infetto in un computer portatile in uso all'esercito americano[170]. La risposta operativa del Pentagono all'attacco fu l'operazione

[162] Cfr. Department of Defense, *DoD Report to Congress on NCW*, , CCRP Publications, Washington DC, luglio 2001.
[163] Cfr. D. Gombert, R. Kugler e M. C. Libicki, *Mind the Gap. Promoting a Transatlantic Revolution in Military Affairs*, National Defense University, Washington DC, 1997.
[164] Cfr. G.J. Rattray, *An Environmental Approach to Understanding Cyberpower*...op. cit.
[165] Cfr. The White House, *The National Strategy to Secure Cyberspace*...op. cit.
[166] *Ibidem.*
[167] Cfr. Department of Defense, *The National Defense Strategy of the United States*...op. cit.
[168] L'operazione passò alla storia con il nome di *Titan Rain*. Cfr. B. Graham, *Hackers Attack Via Chinese Web Sites*, Washington Post,August 25, 2005 URL: http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html [consultato il 13-06-2013].
[169] Cfr. Wired, *Danger Room, The Return of the Worm That Ate the Pentagon*, URL: http://www.wired.com/dangerroom/tag/operation-buckshot-yankee/. [consultato il 14-03-2013]
[170] *Ibidem.*

difensiva o meglio di "pulizia" nota come "*Buckshot Yankee*"[171]. Mentre tra il 2009 e il 2010 venne istituito *l'US Cyber Command* (USCYBERCOM)[172]. L'*USCYBERCOM* centralizza il controllo delle operazioni nello spazio cibernetico, organizza le risorse informatiche esistenti e sincronizza la difesa delle reti militari statunitensi[173]. Proprio la creazione dell' *US Cyber Command* ha influito sulle scelte degli altri Paesi nel propendere verso un allineamento con le scelte americane. Ad esempio nel dicembre 2009, la Corea del Sud ha annunciato la creazione di un *Cyber Warfare Command*, soprattutto in risposta alla creazione della Corea del Nord di una unità speciale dedita alla guerra cibernetica[174]. Nel 2010, anche la Cina ha istituito il suo primo reparto dedicato alle azioni condotte tramite lo spazio cibernetico[175], è nota ad esempio, *l'Unità 61398* dell'Esercito cinese specializzata soprattutto nelle attività di *cyber* spionaggio e *cyber defense*[176]. Al seguito si potrebbero citare i maggiori Paesi: Russia, Francia, Cina, Iran, India, Pakistan, Israele, Regno Unito, Germania[177]. La "quadratura del cerchio" della militarizzazione del *cyberspace* arriva nel luglio 2011, quando il Dipartimento della Difesa (DoD) pubblica la *Strategy for Operating in Cyberspace*[178]. D'altronde, il dinamismo americano volto alla difesa del *cyberspace*, da un lato manifesta le necessarie contromisure utili per contrastare l'esponenziale crescita delle minacce provenienti dal dominio cibernetico[179], dall'altro riprende la visione strategica della c.d. *full spectrum dominance* che mira a un'integrazione di tutti i cinque domini del *warfare* terra, mare, aria, spazio extra-atmosferico e spazio cibernetico, in un'ottica della conduzione del potere nella politica internazionale, che coincide appunto con le direttive

[171] *Ibidem.*
[172] *Ibidem.*
[173] U.S. Department of Defense, *Cyber Command Fact Sheet*, 21 May 2010, URL: http://www.stratcom.mil/factsheets/Cyber_Command [consultato il 15-03-2013]
[174] Cfr. Koreatimes.co.kr, *Cyber Warfare to Be Launched in January* 10-07-2010
[175] T. Branigan, *Chinese Army to Target Cyber War Threat*, The Guardian, London, 25 July 2010.
[176] Cfr. Mandiant Report, *Exposing One of China's Cyber Espionage*, URL: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [consultato il 25-05-2013]
[177] Per una visione di insieme di questi Paesi si rinvia a S. Even e D. Simen-Tov, *Cyber Warfare: Concepts and Strategic Trends*, in Institute for National Security Studies, Tel Aviv, Memorandum No. 117, May 2012
[178] Cfr. Quadrennial Defense Review Report…op. cit
[179] Cfr. E. Nakashima *Pentagon creating teams to launch cyberattacks as threat grows*, The Washington Post, March 12, 2013. URL: http://articles.washingtonpost.com/2013-03-12/world/37645469_1_new-teams-national-security-threat-attacks [consultato il 13-06-2013]

emanate dalla *Joint Vision 2010*[180]. Il progetto GIG è il classico esempio di interdipendenza strategica dei sistemi militari statunitensi dal dominio cibernetico. Esso è gestito da un paradigma operativo basato sulle c.d. *Networked Operations* (NetOps)[181]. Le NetOps si basano su un quadro operativo "net-centrico" che prevede un'effettiva superiorità informativa, c.d. *Information Superiority* ottenibile solo attraverso il mantenimento della connessione in rete e mediante la conoscenza condivisa della situazione (*Shared Situational Awareness*).

3.6 Modi, mezzi e fini degli attacchi cibernetici

Le varie fasi che hanno accompagnato la militarizzazione del *cyberspace*, (comprese le prime avvisaglie delle vulnerabilità, nonché la consapevolezza dei vantaggi strategici offerti dall'ambiente operativo cibernetico), hanno portato negli ultimi anni a una vera e propria fase di "proliferazione" di armi cibernetiche[182]. La relativa economicità, il facile reperimento sul mercato civile degli strumenti informatici "malevoli", e le tecnologie *dual-use capability* hanno indotto numerosi esperti a formulare, soprattutto dopo l'ufficializzazione della militarizzazione dello spazio cibernetico da parte degli Stati Uniti, una serie di iperboli del tipo "Cyber-Pearl-Harbour"[183] o "Apocalisse Cibernetica"[184]. Niente di tutto questo è accaduto e forse mai accadrà, ma certamente come avverte Colin S. Gray, questi allarmismi non fanno altro che favorire lo spreco delle risorse verso settori che mal si prestano alla costruzione di una efficace strategia della difesa. Il Generale Keith B. Alexander Comandante dell'*U.S. Cyber Command*, nella sua testimonianza

[180] Cfr. Joint Chief of Staff, *Joint Vision 2010*...op. cit.; M. Nones e A. Marrone, *La trasformazione delle Forze Armate*...op. cit

[181] Il Pentagono ha definito 5 linee guida per mantenere la sicurezza della GIG: (1) access control; (2) system integrity; (3) cryptography; (4) audit and monitoring; and (5) configuration management and assurance. Cfr. U.S. General Accounting Office, *Information Security: Technologies to Secure Federal Systems*, GAO-04-467 (Washington, D.C. March 9, 2004).

[182] Cfr. N. De Felice, *Le sfide della cyber-war al processo decisionale in materia di politica della Difesa*, in *Information Warfare 2012*...op. cit., pp. 39-46.

[183] J. Arquilla, *Panetta's Wrong About a Cyber 'Pearl Harbor'*, in Foreign Policy, NOVEMBER 19, 2012, URL: http://www.foreignpolicy.com/articles/2012/11/19/panettas_wrong_about_a_cyber_pearl_harbor [consultato il 14-06-2013]

[184] *Ibidem.*

davanti al Congresso ha elencato gli obiettivi sensibili a un attacco cibernetico: "Sistemi di difesa aerea, armi militari e sistemi di comando e controllo, infrastrutture civili quali la rete elettrica, acquedotti, dighe, centrali nucleari, sistema finanziario e il sistema dei trasporti e delle comunicazioni"[185]. In altre parole, il rischio di un attacco cibernetico coinvolge l'intero Sistema Paese. Secondo Alexander, la pericolosità e l'asimmetria delle minacce di una guerra cibernetica risiedono proprio in questa combinazione tra obiettivi civili e militari, che rendono inadeguate tutte le misure di deterrenza militare studiate per gli altri domini del *warfare*[186]. Secondo Lynn ci possono essere tre tipi di possibili minacce cibernetiche: lo sfruttamento della rete a fini di spionaggio e sottrazione dati (*cyber crime*); l'intrusione nella rete (ad esempio per negare le corrette funzionalità del servizio) e infine, il sabotaggio a fini di distruzione di infrastrutture fisiche[187]. A tal proposito scrive Lynn: "È possibile immaginare attacchi alle reti militari e alle reti civili, che causano seri danni economici, distruzione fisica o addirittura la perdita di vite umane"[188]. Quindi, specifica Lynn, è in corso una vera e propria *escalation* delle minacce cibernetiche che rispecchia il passaggio dalla semplice interruzione dei servizi telematici alla vera e propria distruzione di infrastrutture fisiche[189]. Secondo Umberto Gori, per giungere a una definizione di arma cibernetica bisogna che lo strumento utilizzato debba essere letale (distruttivo di cose o persone); che debba causare danni a un obiettivo a tal punto che, la percezione del *target* preso di mira sia indirizzata verso la minaccia imminente[190]. In sostanza – scrive Gori – "L'unico elemento oggettivo [per classificare un'arma cibernetica come arma da guerra N.d.A.] è la valenza letale (distruttiva) dello strumento"[191]. Tenendo conto di questi *advices*, proviamo a suddividere gli strumenti che concorrono a formare "l'arsenale militare" cibernetico. Secondo Thomas Rid e Peter McBurney per armi cibernetiche si deve intendere: "Un codice informatico utilizzato, o progettato per essere utilizzato, con lo scopo di minacciare o provocare danno fisico, funzionale, o mentale a un

[185] Cfr. S. Even e D. Simen-Tov, *Cyber Warfare: Concepts and Strategic Trends*, in Institute for National Security Studies, Tel Aviv, Memorandum No. 117, May 2012.
[186] Cfr. S. Even e D. Simen-Tov, *Cyber Warfare: Concepts and Strategic Trends*, in Institute for National Security Studies, Tel Aviv, Memorandum No. 117, May 2012.
[187] *Ibidem.*
[188] *Ibidem.*
[189] *Ibidem.*
[190] Cfr. U. Gori, *Cyberspazio e relazioni internazionali*...op. cit.
[191] *Ibidem.*

sistema informatico, a infrastrutture o a gli esseri viventi"[192]. Questa definizione presenta una limitazione poiché riduce lo spettro delle azioni possibili tramite il *cyberspace* alle sole operazioni di tipo informatico e attraverso l'utilizzo di codici *malware*, mentre non tiene conto dei possibili attacchi cinetici, che agendo direttamente sulle infrastrutture *hardware* possono provocare danni rilevanti. Per quanto riguarda, invece, il punto di analisi delle altre possibili forme di tecnologie offensive operanti nel cyberspazio, che concorrono ad aumentare il "raggio d'azione" delle minacce cibernetiche, è possibile segnalare ad esempio le *backdoor* e la c.d. tecnica *jamming*. L'altro elemento non preso in considerazione dalla definizione di Rid e McBurney è lo spettro elettromagnetico (EMS); costituente naturale che contribuisce alla formazione dell'ambiente cibernetico[193]. Si pensi ad esempio al supporto dato dalle Unità di forze speciali dell'esercito americano che "montanti a cavallo" in una *covert mission* contro postazioni talebane in Afghanistan, alla fine del 2001 sono riuscite, attraverso l'utilizzo dello spettro elettromagnetico e con dispositivi elettronici e sensori guida GPS, a indirizzare verso i *target* prescelti i missili lanciati dai B-52[194]. Non è un caso se anche i nuovi aerei da combattimento degli Stati Uniti come gli F-22, trasportando sistemi e sensori che sfruttano lo spettro elettromagnetico, riescano a condividere i dati in tempo reale con le altre piattaforme site sul teatro bellico[195]. Attraverso lo spettro elettromagnetico dunque, la guerra cibernetica si presta ad azioni a più ampio raggio; è il caso delle forme di guerra elettronica quando si attua una vera e propria "manipolazione dell'EMS". Tutte queste operazioni anche appartenenti a una categoria diversa rispetto alla guerra cibernetica, se pensate nel contesto di un conflitto militare convenzionale rientrano nella fattispecie di azioni belliche di *cyber warfare* come dimostra *l'Operazione Orchard*. Il 6 settembre 2007, l'esercito israeliano, prima di procedere al bombardamento di un impianto nucleare in Siria, ha utilizzato un aereo senza pilota Suter armato di uno strumento informatico con tecnologia *jamming* che ha permesso di "disturbare, emettere falsi segnali e inserire false

[192] Cfr. T. Rid e P. Mc Burney, *Cyber Weapons*...op. cit., cit. p.7
[193] Cfr. D. Pistoia, *La Guerra Elettronica nella quinta dimensione,* in *Information Warfare* 2012...op. cit., pp. 65-72.; J.W. Greenert, *Imminent Domain*, in Proceedings Magazine – December 2012 Vol. 138/12/1,318 URL: http://www.usni.org/magazines/proceedings/2012-12 [consultato il14-06-2013]
[194] Cfr. Max Boot, *Special forces and Horses*, in Armed Forces Journal (November 2006)
[195] *Ibidem.*

informazioni nella rete di difesa aerea siriana e ha portato gli operatori del comando e controllo, a credere che non ci fossero penetrazioni di piattaforme nemiche nello spazio aereo controllato". In realtà i caccia israeliani pur non godendo di tecnologia *stealth* (per passare inosservati ai radar siriani) sono riusciti a eludere i sistemi di tracciabilità e portare a compimento la missione radendo al suolo l'intero impianto nucleare siriano, il tutto senza che vi fosse la prova evidente del coinvolgimento israeliano nell'esplosione del sito nucleare[196]. Pur non rientrando nel novero specifico della guerra cibernetica, l'esempio appena citato rende l'idea della potenziale vulnerabilità alla cui sono soggetti gli *assets* militari una volta inglobati in un sistema netcentrico e soprattutto, richiamano l'attenzione sulla poliedricità delle minacce provenienti dallo spazio cibernetico[197]. I pericoli non si devono limitare solo alla difesa informatica, ma devono prevedere anche dottrine di difesa elettronica intesa come:

"Capacità di manipolare lo spettro elettromagnetico e di inibire le capacità offensive del nemico, che non può essere applicata unicamente al mondo radar, ma troverà perfetta applicazione nella Guerra Cibernetica, dove la manipolazione dello spettro determina l'alterazione dei dati, causando gravi danni alla catena di comando e controllo" [198].

È evidente a questo punto che anche la guerra elettronica (*EW*), una volta inglobata nella quinta dimensione della conflittualità, rientra a tutti gli effetti nell'alveo della guerra cibernetica. Contrariamente alle tecniche che utilizzano lo spettro elettromagnetico come *medium* per costruire azioni militari di difesa e di attacco, i *cyber attacks* propagati attraverso azioni di *overload* hanno una connotazione ibrida. La tecnica di *Distribuited Denial of Service* (*DDoS*) si appoggia a delle *botnets* (costituite a volte da milioni di computer) che attaccano la rete Internet di un *target* (pubblico o privato) impedendole di funzionare, come per esempio è accaduto in Estonia nel 2007 e in Georgia nel 2008 (poco prima degli scontri con le truppe russe)[199]. Questa tipologia di attacchi cibernetici laddove si è verificata, non è

[196] Cfr. D. Pistoia, *La Guerra Elettronica nella quinta dimensione*...op. cit.
[197] Cfr. U. Gori, *Dai DDoS allo Stuxnet*...op. cit., in particolare p. 35
[198] Cfr. D. Pistoia, *La Guerra Elettronica nella quinta dimensione*....op.cit.
[199] Cfr. J.S. Nye, *The Future of Power*...op.cit

stata valutata dalla Comunità Internazionale come una forma di "guerra" nel senso tradizionale del termine[200]. A tal proposito, basti pensare al tipico esempio dell'attacco *DDoS* subito dall'Estonia nel 2007 che oramai costituisce un "caposaldo" negli studi di settore[201]. L'attacco *DDoS* si è rivolto contro i siti istituzionali e finanziari estoni, e ha determinato la relativa paralisi dell'intero sistema informatico del paese Baltico. Come ha giustamente affermato James Hendler, della *Defense Advanced Research Projects Agency* del Pentagono (DARPA): "Questi tipi di attacchi sono paragonabili più a una sommossa che a un attacco militare"[202]. Un altro fattore di non poco rilievo che ha spinto la Comunità Internazionale (NATO e Unione Europea in particolare) a ridimensionare le vicende estoni, è dato dalla relativa impossibilità di stabilire con esattezza l'origine degli attacchi, proprio perché i *cracker* sono riusciti a "instradare" le intrusioni attraverso *server* non solo russi ma anche americani[203]. L'esempio appena citato ci permette di comparare gli effetti prodotti da un attacco cibernetico tramite modalità "*soft*" e temporanee, che ben poco si prestano alla catalogazione di atti di guerra, con un altro esempio ritenuto dalla "dottrina" il primo vero caso di *cyber war*: il *worm Stuxnet*. Come sottolinea Umberto Gori, se l'esempio estone rappresenta il primo vero evento di *Infowar*, viceversa il primo vero caso di *cyber war* è avvenuto con l'attacco cibernetico sferrato con il super *virus Stuxnet* nei confronti degli impianti nucleari iraniani[204]. Secondo Gori, questa valutazione prende vita dall'analisi del contesto strategico situazionale, e parte dall'individuazione di alcuni fattori principali scaturiti dall'attacco subito dagli iraniani: Il *target* scelto per l'attacco (centrale nucleare) è classificato dagli iraniani come un obiettivo militare; l'azione ha prodotto effetti e danni reali a cose (distruzione materiale delle centrifughe); la complessità per la pianificazione e l'esecuzione dell'azione permette di stabilire un enorme dispendio di risorse economiche e di *intelligence* e quindi si ravvisa la partecipazione di una entità statale capace di sopperire ai costi. La motivazione politica è evidente[205]. A questo punto dunque, appare evidente il valore fondamentale dell'analisi situazionale del

[200] Cfr. R.A. Clarke e R. K. Knake, *Cyber War. The Next Threat*...op. cit.
[201] *Ibidem.*
[202] Cfr. United Press International: *Analysis: Who Cyber Smacked Estonia?* Cit. ripresa da J.S. Nye, *The Future of Power*...op. cit.
[203] Cfr. J.S. Nye, *The Future of Power*...op. cit.
[204] Cfr. U. Gori, *Dai DDoS allo Stuxnet*...op. cit
[205] Cfr. U. Gori, *Cyberspazio e relazioni internazionali*...op. cit.

contesto strategico nel quale matura l'attacco cibernetico. La valutazione oggettiva del contesto serve a classificare un atto cibernetico nella sua condotta reale, per esempio: se l'intento principale di un attacco informatico è ricercare il guadagno finanziario con mezzi criminali (come possono essere gli strumenti di *phishing* o azioni di furto di identità e dati informatici), il fine ultimo è talmente evidente che permette di classificare tale condotta come un atto di *cyber crime* e/o *cyber espionage*[206]. Se l'intento dell'attacco è esclusivamente la volontà di arrecare un danno significativo a uno Stato o ad alcuni suoi cittadini, l'intrusione informatica subita da infrastrutture civili e/o militari ricadrebbe con ogni probabilità nell'alveo di un classico "atto di guerra" disciplinato dallo *jus ad bellum*[207].

3.7 Give me a plausible deniability: attacchi cibernetici e diritto internazionale

La militarizzazione del *cyberspace* ha costretto gli attori della politica internazionale a una vera e propria corsa all'equipaggiamento di armi cibernetiche o *cyber weapons*[208]. Questo processo frenetico però, non è stato regolamentato da una legislazione internazionale atta a disciplinare e sanzionare l'utilizzo delle armi cibernetiche equiparandole a strumenti militari *tout court*. Questa *vacatio legis* crea delle dissonanze oggettive, soprattutto riguardo al crimine internazionale di aggressione[209]. Come avverte Cassese, le esemplificazione dell'elemento oggettivo del crimine di aggressione si riferiscono esclusivamente alle sue forme "tradizionali" mentre, non vi è alcuna disciplina sulle forme di aggressione quali ad esempio, quelle perpetrate da uno Stato attraverso metodi e mezzi di guerra di "nuova generazione" o appunto, perpetrati attraverso mezzi virtuali come gli attacchi cibernetici[210]. Dello stesso avviso è Francesco Lombardi, secondo cui, la mancanza di regole nell'ambito

[206] Cfr. P. Cornish (et.al.) *On Cyber Warfare*...op. cit

[207] Cfr. M. Moscini, *World Wide Warfare –Jus ad bellum and the Use of Cyber Force*, in A. Bogdany and R. Wolfrum (eds.), Max Planck Yearbook of United Nations Law, vol. 14, 2010, p. 96.

[208] Cfr. S. Mele, *Cyberweapons. Aspetti giuridici e strategici*, versione 2.0, Istituto Italiano di Studi Strategici Niccolò Machiavelli, Roma, giugno 2013.

[209] Cfr. A. Cassese, *Lineamenti di diritto internazionale penale. I. Diritto sostanziale*, il Mulino, Bologna, 2005

[210] *Ibidem.*

della *cyber warfare* riflette una riluttanza dei legislatori internazionali a porre sotto l'alveo dei principi del diritto internazionale una guerra che in larga misura è stata classificata erroneamente, diversa dalle altre prendendo come punto di paragone gli strumenti utilizzati[211]. Secondo Lombardi, così facendo verrebbero sacrificati i principi unanimi dello *jus ad bellum*[212], validi per tutte le forme della conflittualità[213]. L'ambiguità delle definizioni – avverte Lombardi – influenza anche la dottrina giuridica che a stento sembra adeguarsi ai nuovi mezzi di conduzione delle ostilità, rimanendo invece ancorata alla vecchia concezione dei conflitti armati intesi come un confronto con mezzi "reali" tra attori contrapposti[214]. Ne consegue che, la mancata disciplina giuridica delle azioni di *cyber warfare* e la relativa capacità di condurre azioni in completo anonimato incoraggerebbero gli attori, statali e non, a privilegiare lo strumento cibernetico per conseguire degli obiettivi che, se perseguiti con mezzi convenzionali, si presterebbero alla stigmatizzazione dalla Comunità Internazionale[215]. È in questo frangente dunque, che è possibile ravvisare un'analogia tra le azioni di *cyber warfare* e le c.d. *proxy warfare*, laddove gli autori degli attacchi, grazie all'alto grado di anonimato concesso dall'ambiente cibernetico, possono trincerarsi dietro la c.d. *plausible deniability*. La negazione plausibile è un termine coniato durante l'Amministrazione Kennedy dalla *Central Intelligence Agency* (CIA) attraverso la c.d. *doctrine of plausible deniability*, per permettere ai dirigenti politici di negare qualsiasi coinvolgimento nelle operazioni covert dell'Agenzia contro soggetti ritenuti pericolosi per gli interessi nazionali statunitensi[216]. Il concetto della *plausible deniability* è ritornato in auge in un eminente lavoro di Peter W. Singer dedicato all'ascesa delle *Private Military Firm*

[211] Cfr. F. Lombardi, *Cyber Warfare, qualiregole…?,* in Informazioni della Difesa, 5/2010, p.74.
[212] Ibidem. Lo jus ad bellum è il corpo giuridico che disciplina il ricorso alla forza da parte degli Stati nelle relazioni internazionali. Oggi, la più importante fonte dello *jus ad bellum* è la Carta delle Nazioni Unite. Alcuni aspetti di questa legge, come ad esempio le modalità precise che disciplinano l'uso della forza in un caso di legittima difesa, per esempio, non sono regolati dalla Carta delle Nazioni Unite e devono essere derivati dal diritto consuetudinario che si riflette nella pratica dello Stato e *opinio juris* e identificato nella giurisprudenza internazionale. Cfr. R. Kolb, *Origins of the Twin Terms jus ad bellum/jus in bello*, International Review of the Red Cross, Vol. 320, 1997, p. 553.
[213] Cfr. F. Lombardi, *Cyber Warfare, qualiregole*…?…op. cit.
[214] *Ibidem.*
[215] *Ibidem.*
[216] Cfr.Wikipedia.org, Plausible Deniability, URL: http://en.wikipedia.org/wiki/Plausible_deniability [consultato il 13-06-2013]

(PMF)[217]. Secondo Singer, il privilegio di utilizzare compagnie militari private (mercenarie) è dato in larga misura dalla possibilità: "Per un governo di razionalizzare le spese militari in termini economici e umani; negare il proprio coinvolgimento o scaricare su altri la responsabilità"[218]; soprattutto – sottolinea Singer – l'utilizzo di società private: "colloca le decisioni importanti lontano dall'influenza e dal controllo del popolo"[219]. La conseguenza della privatizzazione della guerra, secondo Singer, provoca un ripensamento totale della sicurezza internazionale[220]. Scrive l'Autore: "La nascita delle PMF mette in dubbio uno delle premesse fondamentali dello studio della sicurezza internazionale, ovvero che gli Stati possiedano il monopolio dell'uso della forza"[221]. Dello stesso avviso è Andrew Mumford autore di un articolo sul *RUSI Journal* dal titolo "*Proxy warfare and the Future of Conflict*", dove sottolinea la stretta assonanza tra la *cyber warfare* e le guerre per procura[222]. Secondo Munford, la guerra cibernetica e le caratteristiche strategico-operative della *proxy warfare* presentano delle analogie; dunque, è naturale credere che la nuova forma di "guerra per procura" del XXI secolo sarà la *cyber warfare*[223].

3.8 Dalla deterrenza nucleare alla resilienza cibernetica

Durante la guerra fredda i paradigmi della deterrenza nucleare si basavano essenzialmente sul concetto di un "equilibrio del terrore", dove vigevano chiare le distinzioni tra amico e nemico. Gli obiettivi militari erano ben scissi da quelli civili e la pace e la guerra avevano una loro forma ben precisa e governata[224]. Queste "certezze" erano la base ordinante del sistema internazionale bipolare, dove la deterrenza e la dissuasione erano ben governate e garantite dai concetti militari: *Mutual Assured Destruction* (MAD) e *Second Strike*

[217] Cfr. P. W. Singer, *Corporate Warriors. The Rise of the Privatized Military Industry and Its Ramification for International Security*, in *International Security*, Vol. 26, No. 3 (Winter 2001/02), pp. 186–220.
[218] *Ibidem.*
[219] *Ibidem.*
[220] *Ibidem.*
[221] *Ibidem.*
[222] Cfr. Andrew Mumford, *Proxy Warfare and the Future of Conflict*, in *The RUSI Journal*, 158:2, pp. 40-46. URL: http://dx.doi.org/10.1080/03071847.2013.787733 [consultato il 12-06-2013]
[223] *Ibidem*, in particolare si rinvia alle pp. 43L44.
[224] Cfr. A. Colombo, *La disunità del mondo. Dopo il secolo globale*, Feltrinelli, Milano, 2010.

Capability[225]. In sostanza, nell'era nucleare la deterrenza poggiava su un equilibrio bipolare simmetrico tra Stati "in termini di potenziale distruttivo". Entrambi gli attori egemoni avevano come obiettivo condiviso il mantenimento dello *status quo* atto a scongiurare una "mutua distruzione". Classico esempio di tale "visione strategica" sono le varie crisi che hanno interessato quel periodo storico, affrontate con il *modus operandi* durante la crisi missilistica di Cuba, con un'elevata dose di *Realpolitik* attraverso l'istituzione di canali di comunicazione diretti[226]. Un'altra peculiarità del sistema internazionale bipolare consisteva nell'elevata soglia di accesso alla violenza, dettata dal numero limitato di attori capaci di sviluppare armamenti nucleari e cosa ancora più importante, vi era la possibilità di rintracciare facilmente l'autore di un atto ostile e provvedere alla rappresaglia nonché la possibilità di individuare la posizione geografica esatta degli arsenali e dei missili balistici. In sintesi dunque, per riprendere un paradigma tanto caro al realismo: durante la guerra fredda, pur perdurando l'anarchia del sistema internazionale, i rapporti di forza governavano le relazioni internazionali esulandole dall'avvento di un'entropia destabilizzante[227]. L'abbassamento della soglia di accesso alla violenza e il conseguente affollamento dell'arena internazionale, rendono vani i modelli strategici della deterrenza, soprattutto a causa delle evidenti difficoltà di identificare la fonte di un attacco. Ciò comporta una relativa incapacità di pianificare la rappresaglia che snatura le strategie di *counterforce* dirette a distruggere le forze avversarie[228]. La questione si infittisce ancora di più se l'autore dell'attacco non è uno Stato, ma un attore non-statale che agisce dentro i confini di uno Stato sfruttando le sue infrastrutture informatiche per l'azione ostile[229]. È evidente che rispetto alle regole rigide che hanno governato l'epoca bipolare e soprattutto le relazioni internazionali infra statali, nell'era cibernetica bisogna rintracciare nuove "linee guida" capaci di adattarsi alla natura della minaccia (intangibile e anonima) e dell'ambiente operativo (globale e dinamico). Per fare fronte a tali minacce si può adottare una politica

[225] Cfr. E. Di Nolfo, *Storia delle relazioni internazionali. Dal 1918 ai giorni nostri*, Editori Laterza, Roma-Bari, 2008; Id. *Il disordine internazionale. Lotte per la supremazia dopo la Guerra fredda*, Bruno Mondadori, Milano-Torino, 2012.
[226] Cfr. H.A. Kissinger, *L'arte della diplomazia*, Sperling & Kupfer Editori, 2004.
[227] Cfr. K.N. Waltz, *Teoria della politica internazionale*...op. cit.
[228] *Ibidem.*
[229] Cfr. U. Gori, *Cyberspazio e relazioni internazionali*...op. cit.

di deterrenza basata sul diniego (*detereence by denial*) che poggia essenzialmente su veri e propri sistemi di difesa attiva (*firewall*) capaci di reagire in modo istantaneo, rendendo inefficaci e controproducenti gli attacchi cibernetici in termini di calcolo tra costi e benefici[230]. È giusto notare come tale approccio tende a "sfaldarsi" di fronte alle azioni condotte da attori non razionali come possono esserlo i gruppi terroristici o gli individui che agiscono per ricavi personali. Dunque, insieme alla ricerca di nuove dottrine di impiego di difesa attiva, diventa imprescindibile trovare delle misure capaci di rendere le infrastrutture informatizzate, (mezzo e bersaglio degli attacchi cibernetici) "elastiche" di fronte alle crescenti minacce. Due concetti sono centrali per la costruzione di una difesa efficace contro attacchi cibernetici: resilienza e flessibilità. La resilienza, infatti, applicata alla dimensione cibernetica, esprime la capacità di un dato sistema di adattarsi alle condizioni d'uso, e di resistere agli eventi in modo tale da garantire la funzionalità e la continuità dei servizi erogati, nonché la capacità di recupero e una rapida ricostruzione di fronte agli attacchi cibernetici. A tal proposito, Gregory Rattray suggerisce di applicare alle minacce cibernetiche gli stessi piani operativi messi in piedi dalla sanità pubblica per fronteggiare la diffusione delle epidemie[231]. L'idea di Rattray scaturisce dalle analogie e dai parallelismi che intercorrono tra i metodi di trasmissione e diffusione delle patologie virali e di quelle virtuali[232]. Lo studio condotto da Rattray poggia fondamentalmente sull'evidente interdipendenza a livello globale dei Paesi informatizzati dalle infrastrutture che concorrono alla creazione del *cyberspace* (il c.d. livello fisico-*hardware*), dove in caso di "infezione" si ha un alto rischio di trasmissione virale[233]. Infatti, Rattray in occasione dell'intervento americano in Iraq del 2003, ricorda che il Pentagono aveva pianificato il *blackout* dei servizi informatici iracheni, ma all'ultimo istante il presidente Bush decise di rinunciare all'operazione per l'elevato rischio di effetti collaterali in Europa (in Francia soprattutto) dovuti all'interdipendenza tra i sistemi *hardware* delle infrastrutture informatiche delle due aree regionali[234]. Secondo

[230] Cfr. J.S. Nye, *The Future of Power*...op. cit.
[231] G. Rattray, C. Evans e J. Healey, *American Security in the Cyber Commons*...op. cit.
[232] *Ibidem.*
[233] *Ibidem*. Un noto caso di trasmissione virale di virus cibernetici è stata la diffusione di Stuxnet. Cfr. S. Mele, *Cyber-weapons: aspetti giuridici e strategici*. Versione 2.0, Istituto Italiano di Studi Strategici "Niccolò Machiavelli", Roma, 2013.
[234] G. Rattray, C. Evans e J. Healey, *American Security in the Cyber Commons*...op.cit.

Rattray, così come i rischi patogeni vengono affrontati dalla stretta collaborazione tra la sanità pubblica locale e l'Organizzazione Mondiale della Sanità, allo stesso modo per far fronte ai pericoli del *cyberspace*, sarebbe opportuno creare degli enti preposti al coordinamento, all'allerta e all'isolamento della diffusione delle minacce. Solo così –avverte Rattray – si potrebbe localizzare e isolare il focolaio virale, impedendo dunque che un'infezione epidemica si trasformi in una vera e propria pandemia[235]. Secondo Rattray, solo ponendo il dovuto accento sul rischio epidemico mondiale, ne può scaturire un reale approccio cooperativo tra i vari attori della politica internazionale odierna (Stati, ONG, aziende private, comuni cittadini), accomunati tutti dal rischio di contagio[236]. Su una scia diversa si pone il Progetto *Clean-state Design of Resilent, Adaptative, Secure Hosts* (CRASH) della *Defense Research Projects Agency* (DARPA) che mira ad adattare le strategie del sistema immunitario biologico nel sistema informatico dotandolo di un meccanismo diffuso di monitoraggio e di allerta delle minacce, ed inoltre, capace di fornire autonomamente una risposta elastica e resiliente agli attacchi; ed infine in grado di auto-ristrutturarsi in caso di danni subiti[237]. In questo "approccio difensivo" è implicita la necessità di creare una *cyber security* improntata alla cooperazione tra settore pubblico e privato, capace di fronteggiare in modo "olistico" le minacce, senza concentrarsi eccessivamente sul fronte degli *assets* militari. In definitiva, la resilienza e l'elasticità fanno emergere un dato di fatto incontrovertibile in termini di difesa e di sicurezza: nell'era cibernetica non è più valido il precetto secondo il quale il debole soccombe al forte. Viceversa, in questo nuovo paradigma dell'umanità dove la conflittualità si dipana in un ambiente asimmetrico e vulnerabile, sembrano essere destinati a sopravvivere solo gli attori più versatili[238].

---

[235] *Ibidem*. L'Autore prende in analisi le procedure seguite durante l'avvento della SARS (Sindrome Acuta Respiratoria Severa) che ha portato a una stretta cooperazione internazionale per limitare il contagio e la diffusione del virus anche tra vari paesi notoriamente contrapposti come ad esempio la Corea del Nord e gli USA.

[236] *Ibidem.*

[237] R.Boyle, *DARPA Looking to Reinvent Network Security, With Inspiration from Adaptive Biological Systems* , Popular Science, URL: http://www.popsci.com/science/article/2010-06/darpa-wants-secure-networks-inspired-human-biology [consultato il 16-06- 2013]

[238] E. Sterner, *Retaliatory Deterrence in Cyberspace*, in Strategic Studies Quarterly, Spring 2011, pp. 62-80.

4. GLI EFFETTI DELL'ERA CIBERNETICA SULLA POLITICA INTERNAZIONALE

4.1 Il declino dello Stato e la s-politicizzazione della guerra

La guerra, come amava definirla Carl von Clausewitz, è un'attività sociale che non può essere ridotta né ad arte né a scienza[239]. Essa ha quindi, un'anima *in fieri* che si adatta ai tempi e ai modi che la propagano. Proprio per questo Clausewitz scrive: "la guerra [...] rassomiglia al camaleonte perché cambia di natura in ogni caso concreto"[240]. Subordinando la guerra alla politica, si è cercato sin dall'epoca Moderna di porre dei limiti giuridici e militari alla violenza. È con la pace di Westfalia del 1648 che vengono sancite queste regole di comportamento per imporre dei confini alla violenza tra gli Stati. Il sistema internazionale basato sullo *jus publicum europaeum*, che poneva gli Stati su una posizione di *ceteris paribus*, ha garantito il superamento delle sanguinose guerre di religione combattute in nome del principio discriminatorio di "guerra giusta"[241]. Proprio a tal proposito Carl Schmitt, l'Epimeteo cristiano[242], spettatore di due conflitti mondiali e dell'equilibrio del terrore nucleare, nella sua opera sul *Nomos della terra*, mentre esalta i valori "ordinanti" dello *jus publicum europaeum* nel diritto internazionale, avverte che:

"Questa consapevolezza del fatto che il diritto e la pace poggiano originariamente su *delimitazioni in senso spaziale*, [...] ci aiuterà a comprendere che il problema centrale di ogni ordinamento giuridico

[239] Cfr. C. von Clausewitz, *Della guerra*...op. cit. In particolare Clausewitz scrive che "La guerra non appartiene né al dominio dell'arte né a quello della scienza, ma al dominio della vita sociale. È un conflitto di grandi interessi, che ha una soluzione sanguinosa, e solamente in questo differisce dagli altri. Si potrebbe piuttosto paragonarla al commercio che a qualsiasi altra arte, poiché il commercio è anch'esso un conflitto di interessi e attività: e alla guerra si accosta ancor più la politica, che può anch'essa, a sua volta, considerarsi come un commercio in grande scala." cit. p. 130. Per un'analisi sul pensiero clausewitziano si rinvia all'introduzione dell'opera di Clausewitz da parte di G. E. Rusconi, Enaudi editore, Torino, 2000.

[240] Ivi, cit. p. 40

[241] Cfr. C. Schmitt, *Il Nomos della Terra nel diritto internazionale dello <jus publicum europaeum>*, Adelphi Edizioni, Milano, 1991.

[242] Così amava definirsi Schmitt. Cfr. C. Resta, *Stato mondiale o Nomos della terra. Carl Schmitt tra universo e pluriverso*. Edizioni Diabasis, Reggio Emilia, 2009.

non è tanto quello dell'abolizione della guerra, ma piuttosto quello della sua delimitazione o regolamentazione"[243].

L'attuale struttura del sistema internazionale evidenzia, però, quanto sia lontana oggi la concezione clausewitziana e schmittiana della guerra e della politica, della pace e della violenza. Lo sfaldamento dell'ordine mondiale Stato-centrico si rivela essere il fattore principale dello stravolgimento delle divisioni classiche tra guerra e pace[244]. Tale dinamica ha subito un'accelerazione fulminea che, dalla fine dell'era storica definita da Eric J. Hobsbawm "secolo breve"[245], ha portato lo Stato-nazione tradizionale attore egemone della politica internazionale, a svolgere un ruolo sempre più sfumato nel mondo globalizzato[246]. Oggi giorno dunque, la forma politica dello Stato-nazione viene erosa da più parti: da un lato, il declino del sistema internazionale a composizione pressoché unipolare con un ruolo egemone da parte degli Stati Uniti, inizia a spalancare nuovi scenari sul piano della politica post-internazionale[247] e sugella la crisi della sovranità degli Stati nazionali[248]. Dall'altro lato, le entità non statali che nel passato avevano un ruolo ben definito e soprattutto più delimitato, oggi riescono a modificare (talune volte anche a creare) i processi di *decision making* mettendo in discussione soprattutto il monopolio della violenza, prerogativa assoluta degli Stati

[243] Cfr. C. Schmitt, *Il Nomos della Terra*… op.cit., cit. p. 65. Alla luce dei fatti appena descritti si evince dunque che l'appello di Schmitt sia rimasto nient'altro che una *vox clamantis in deserto*

[244] Cfr. A. Colombo, *La guerra ineguale. Pace e violenza nel tramonto della società internazionale*, Il Mulino, Bologna, 2006

[245] Cfr. E. J. Hobsbawm, *Il secolo breve. 1914-1991*, Rizzoli, Milano,2006.

[246] La teoria delle Relazioni Internazionali che identifica nello Stato l'attore egemone della politica internazionale è rappresentata dal realismo. Secondo una disanima che ne da U. Gori, *Lezioni di Relazioni Internazionali*, CEDAM, Padova, 2004, nel capitolo relativo a *Le teorie generali (o paradigmi interpretativi) delle Relazioni Internazionali* , (sub-voce) *Il realismo*, è possibile leggere: "Il realismo nasce come reazione all'idealismo, che aveva una concezione ottimistica della natura dell'uomo e delle relazioni internazionali e che era alla base della nascita delle grandi Organizzazioni internazionali e dello sviluppo del diritto internazionale della nostra epoca. L'idealismo teorizzava che fosse sufficiente modificare le strutture del sistema internazionale per migliorarlo (vedi i 14 punti Wilsoniani); il carattere utopistico di questa 'visione' delle relazioni internazionali fu evidenziato dal fallimento della Società delle Nazioni. I fatti storici hanno dunque messo in crisi questa scuola di pensiero" cit. p. 51.

[247] Cfr. A. Colombo, *La guerra ineguale*…op. cit.; P. Williams, *From The New Middle Ages To a New Dark Age: The Decline of The State and U.S. Strategy*, Strategic Studies Institute, June 2008. URL: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=867[consultatoil15-05-2013]

[248] Cfr. S. D. Krasner, *Think Again: Sovereignty, in Foreign Policy*, January 1, 2001, URL: http://www.foreignpolicy.com/articles/2001/01/01/think_again_sovereignty [consultato il 26-02-13]

nazionali[249]. Ne consegue che in questa congiuntura sociale prima ancora che politica, si debba intravedere lo sfaldarsi oltre che delle strutture politiche nazionali, anche delle forze militari e delle classiche dinamiche che governano la guerra. D'altronde, "le nuove guerre"[250] vengono sostenute dai moderni mezzi militari messi a disposizione dall'evoluzione tecnologica che consente la "virtualizzazione" dei conflitti[251]. A tal proposito, Luciano Bozzo osserva:

"Ovunque in Occidente, e per qualche buona ragione storica massimamente in Europa, nella seconda metà del secolo scorso la guerra è divenuta impopolare. Non così le missioni, pur armate, per il mantenimento, la costruzione e magari l'imposizione della pace, gli interventi umanitari e quelli diretti al consolidamento dei regimi democratici e alla tutela dei diritti dell'essere umano: tutti legittimati dal riferimento ai principi universalistici oramai prevalenti". [252]

Dello stesso avviso è Alain Joxe, secondo il quale, la fine del confronto bipolare ha di fatto reso il concetto odierno di guerra allo stesso tempo fluido e sfuocato[253]. In particolar modo – secondo Joxe – dopo la dialettica Est-Ovest, sulla quale poggiavano le relazioni internazionali post-belliche, è diventato impossibile scandire il tempo e lo spazio della conflittualità del XXI secolo. Difatti, se vi è stata una "rivoluzione militare" questa è stata inaugurata dagli Stati

[249] Cfr. Instituto Españolos de Estudios Estratégicos, Los Actores no Estatales y la Seguridad Internacional: su Papel en la Resolución de Conflictos y Crisis, Centro National de Inteligencia, Cuaderno de Estrategia n. 147, Agosto 2010.
URL: http://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_147_Actores_No_Estatales.pdf [consultatoil26-02-2013]

[250] Cfr. M. Kaldor, *Le nuove guerre. La violenza organizzata nell'età globale*, Carocci Editore, Roma, 1999.

[251] Cfr. U. Gori, *Evoluzione della conflittualità: dalle guerre tradizionali alla information warfare. Verso una geopolitica virtuale?,* prolusione tenuta in occasione dell'inaugurazione dell'Anno Accademico della scuola dell'Aeronautica Militare a Pozzuoli nel 2011. In particolare l'Autore scrive: "La storia della guerra ci conferma la validità di questa intuizione o, se vogliamo, di questa legge naturale. La guerra, da azione reciproca di forza materiale che produce distruzioni fisiche e spargimento di sangue, è diventata *virtuale*".
URL: http://www.aeronautica.difesa.it/News/Documents/pdf/Pozzuoli%20inizia%20l'Anno%20Accademico_2011/Prolusione%20Prof%20Gori.pdf [consultato il 27-02-2013]

[252] Cfr. L. Bozzo, *Terroristi, insorti o partigiani? Le aporie linguistiche della "guerra al terrorismo",* in AA.VV. Quaderni di Relazioni Internazionali, ISPI, n. 14, Maggio 2011.

[253] Cfr. A. Joxe, *L'impero del caos*...op. cit.

Uniti durante la guerra del Golfo nel 1991[254]. L'esibizione *maxima* di questo nuovo modo di condurre la guerra iper-tecnologico e a-cronologico[255]. Secondo questa concezione "caotica" del panorama internazionale siamo dunque di fronte a uno stravolgimento epocale dell'approccio alla guerra. Sulla stessa scia di Joxe si pone Mary Kaldor la quale ha coniato il termine "nuove guerre" per descrivere i mutamenti avvenuti sulla scena internazionale a partire già dall'ultimo ventennio del Novecento[256]. La tesi centrale della Kaldor poggia sulla considerazione che le dinamiche belliche contemporanee si pongono lungo il *fil rouge* che collega il declino dello Stato moderno con la fine della violenza organizzata.

4.2 La diffusione del potere e la violenza illimitata

Secondo i coniugi Alvin e Heidi Toffler, l'attuale "era dell'informazione"[257] altro non è che il prodotto della "terza rivoluzione industriale"[258]. La loro tesi poggia sulla concezione che la storia dell'umanità è frutto di un'evoluzione a "ondate"; infatti, passando dalla rivoluzione agricola alla rivoluzione industriale, si è

[254] La guerra del Golfo del 1991 passata alla storia come *Operation Desert Storm* è stata molto discussa e anche molto analizzata. Volendo assottigliare al massimo la ricerca si rinvia al saggio di J. S. Nye, *Why the Gulf War Served the National Interest*, in The Atlantic Monthly, July 1991, Volume 268, No 1, pp. 56-64. L'Autore molto realisticamente scrive: *"Why did a majority of the people living in the central part of North America think it in their interest to send half a million soldiers 6,ooo miles away to the Persian Gulf? The simplest answer is one word: oil. To quote one of the bettere placards at a peace march, "if Kuwait exported broccoli, we wouldn't be there now"*. cit. p. 56. URL: http://m.theatlantic.com/past/docs/issues/91jul/nye.htm. [consultato il 14-02-2013]

[255] Per quanto riguarda invece un'analisi da una prospettiva diversa, puramente strategico-militare, si rinvia al saggio di W. J. Perry, *Desert Storm and Deterrence, Fall 1991*, in Foreign Affairs. Risulta molto interessante ai fini della ricerca riportare tale passaggio dell'Autore: *"In Operation Desert Storm the United States employed for first time a new class of military systems that gave American froces a revolutionary advance in military capability. […] This new conventional military capability adds a powerful dimension to the ability of the United States to deter war. While it is certainly nota s powerful as nuclear weapons, it is more a credible deterrent,particulary in regional conflicts vital to U.S. national interests."* URL: http://m.foreignaffairs.com/articles/47141/william-j-perry/desert-storm-and-deterrence [consultato il13-02-2013]

[256] Cfr. M. Kaldor, *Le nuove guerre*…op.cit.

[257] Per un'analisi dettagliata da un punto di vista filosofico sull'ampio concetto di *Information Age* si rinvia a L. Floridi, *La rivoluzione dell'informazione*, Codice edizioni, Torino, 2012. In questo saggio l'Autore per primo esprime l'ambiente nel quale si diffonde l'interazione tra individui e l'informazione ovvero scrive che "sotto molti profili non siamo entità isolate quanto piuttosto organismi informazionali interconnessi, o *inforg*, che condividono con agenti biologici e artefatti ingegnerizzati un ambiente globale costituito in ultima analisi dalle informazioni, *l'infosfera*" cit. p. 11.

[258] Cfr. A. Toffler e H. Toffler, *The Politics of the Third Wave*, Andrew and McMeel, Atlanta, 1995.

giunti ai nostri giorni alla "terza ondata". Le nuove scoperte tecnologiche hanno concesso ai paesi ad alta industrializzazione l'opportunità di trasmettere le informazioni in tempo reale. Le gerarchie burocratiche, investite da questa "tempesta di fuoco di mutamenti", rischiano di essere sostituite da organizzazioni *networked* non statali perdendo così, gran parte delle loro funzioni governative[259]. Si verrà a creare in questo modo, continuano i fautori della visione rivoluzionaria, un nuovo modello di *governance* mondiale che sostituirà le vecchie gerarchie nazionali e permetterà la nascita di comunità trasversali sul modello di convivenza neo-feudale, segnando così il superamento dello Stato-nazione[260]. L'elemento centrale che caratterizza più di tutti l'attuale sistema internazionale è l'intangibilità delle azioni protratte attraverso il dominio cibernetico[261]. In questo ambiente, allo stesso tempo sfumato e virtuale, possono accedere sia gli Stati che gli attori non statali i quali, attraverso lo spazio cibernetico riescono a scavalcare i limiti (fisici o normativi) imposti dalla gerarchia statale per accedere ad un numero indefinito di informazioni e di funzioni in passato relegate all'*establishment*[262]. Tale potenziale pervasivo e anarchico non si limita solo ad alcuni settori specifici interconnessi con il dominio cibernetico, quali potrebbero essere lo spostamento di denaro o di altri beni come la proprietà intellettuale, ma rientrano nel novero di queste attività anche e soprattutto questioni puramente militari[263]. Secondo Nye, nell'era in cui viviamo per la prima volta si assiste non tanto alla c.d. *translatio imperii*, (trasformazione più che comune nei vari cicli storici)[264], ma a una vera e propria "*diffusion of power*" che mette in discussione il monopolio della violenza, prerogativa storica degli Stati-nazione. Questo fenomeno favorisce la migrazione del potere dagli Stati verso attori privati non governativi[265]. L'odierno panorama internazionale,

[259] Cfr. A. Toffler, *Lo choc del futuro*, Rizzoli Editore, Milano, 1971.
[260] Cfr. A. Thoffler e H. Toffler, *The Politics of the Third Wave…op. cit.; Id., War and Anti-War: Survival at the Dawn of the 21st Century*, Little Brown and Company,Boston,1993.
[261] *Ibidem.*
[262] Cfr. A. Thoffler e H. Toffler, *Foreword: The New Intangibles*, in J. Arquilla and D. Ronfeldt (eds.), In *Athena's Camp: Preparing for Conflict in the Information Age*, ed. by RAND, Santa Monica, 1997, pp. xiii-xxiv.
[263] *Ibidem.*
[264] Su questo tema si rinvia a due lavori eminenti: P. Kennedy, *Ascesa e declino delle grandi potenze*, a cura di A. Cellino, Garzanti Editore, Milano, 1993; E. N. Luttwak, *La grande strategia dell'impero romano*, a cura di P. Diadori, Rizzoli Editori, Milano, 1981.
[265] Cfr. J. S. Nye, *Is America in Decline?, Transcript by Chatham House*, May 2010. URL: http://www.chathamhouse.org/publications/papers/view/177645; [consultato il 01-01-2013]. Invece per una disamina sul più ampio concetto della crisi della sovranità statale si rinvia a: S. D.

da qualcuno definito non tanto multipolare o unipolare quanto piuttosto "apolare"[266], poggia su un ripensamento rivoluzionario della concezione originaria dell'amministrazione del potere. In altre parole, attraverso la diffusione del potere e il superamento dei tratti caratteristici dello Stato-nazione, si concretizza la negazione del senso di giustizia e del fine ultimo di un'azione violenta che, con i moderni mezzi di propagazione delle minacce messi a disposizione dalla tecnologia, acquista una dimensione intangibile, globale e indiscriminata, non più espressione di fini politici condivisi[267]. In altre parole, come avvertono John Arquilla e David Ronfeldt, la rivoluzione dell'informazione ha favorito e rafforzato le *networked organizations*, dando loro un vantaggio operativo rispetto alle classiche forme piramidali e statiche come lo sono gli Stati nazionali[268]. Si viene a creare non solo un incremento esponenziale delle informazioni

---

Krasner, *Think Again: Sovereignty,* in *Foreign Policy*, January 1, 2001, URL: http://www.foreignpolicy.com/articles/2001/01/01/think_again_sovereignty; [consultato il 13/03/13]

[266] Cfr. T.G. Ash, *As Threats Multiply and Power Fragments, The 2010s Cry Out for Realistic Idealism*, in "The Guardian", 31 dicembre 2009.

[267] Sant'Agostino riprende il celebre dialogo tra *Alessandro e il pirata* per porre il senso di giustizia quale discrimine tra un'azione commessa per il bene comune piuttosto che a fini personali; il brigante si differenzia dal capo politico perché persegue l'arricchimento personale attraverso ilbottino. "Se si toglie la giustizia, cosa sono gli Stati se non grandi bande di ladri? D'altra parte, cosa sono le bande di ladri se non piccoli Stati? Anch'essi sono un gruppo di uomini governati dall'autorità di un capo, impegnati in un patto sociale, d'accordo su una legge per dividersi il bottino".

[268] Anche questo aspetto è stato molto discusso dalla dottrina militare e dagli studiosi delle Relazioni Internazionali in generale, per una visione di insieme si rinvia al lavoro condotto Instituto Españolos de Estudios Estratégicos *Los Actores no Estatales y la Seguridad Internacional*...op. cit. In uno studio diffuso dal Pentagono, già nel 1994, si rilevava il ruolo sempre più crescente che stava acquisendo in quegli anni tale fenomeno, in particolare questo documento, reperibile in rete, cita le forze diverse dagli Statinazione come "futuri nemici" e si aggiunge che "le minacce alla sicurezza poste da entità che non sono Stati nazione utilizzando tecnologie moderne che danno loro capacità simili a quelle degli Stati nazione stanno diventando sempre più visibili, sfidando il tradizionale contesto degli Stati nazione. A seconda dello scopo, si possono individuare tre categorie:

1) Subnazionali. Le minacce subnazionali comprendono i conflitti politici, razziali, religiosi, culturali ed etnici, e tali conflitti mettono in discussione dall'interno le caratteristiche precipue e l'autorità degli Stati nazione.

2) Anazionali. Le minacce anazionali non sono associate ai paesi cui appartengono. Tali entità non fanno parte di uno Stato nazione né desiderano acquisire tale status. Criminalità organizzata regionale, pirateria e attività terroristiche sono esempi di questo tipo di minacce.

3) Metanazionali. Le minacce metanazionali trascendono i confini degli Stati nazione ed operano su scala interregionale o persino mondiale. Tra queste vi sono movimenti religiosi, organizzazioni criminali e organizzazioni economiche informali che agevolano la proliferazione delle armi".
Cfr. TRADOC Pamphlet 525-5 FORCE XXI OPERATIONS, *A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century*, 1 August 1994, URL: http://webapp.dlib.indiana.edu/cgi-bin/virtcdlib/index.cgi/4240520/FID2/ACDOCS/VISION/B004.PDF [consultato13/03/13].

disponibili per i singoli individui, i quali possono comunicare aggirando le gerarchie burocratiche e le frontiere nazionali, ma soprattutto emerge un ruolo sempre più rilevante degli attori non statali. Questi favoriti dall'ambiente cibernetico, si strutturano in *network* e dispongono di un'ampia flessibilità di adattamento. In tal modo, "ogni nodo [della rete] può comunicare con l'altro", modificando e influenzando il processo di *decision-making*, attraverso azioni di pressione sui decisori politici[269]. Le minacce prodotte dall'intangibilità di attori non statali *networked* verso sistemi statici, si possono facilmente ravvisare sui campi di battaglia afghano e pachistano dove, non solo al Qaeda, ma anche i suoi alleati Talebani, agiscono contro gli eserciti regolari secondo questo *modus operandi* reticolare. A tal proposito, il generale statunitense Stanley McCrystal (prima di ritirarsi a vita privata) ha lasciato un commentato lapidario:

"Proprio come i loro alleati di al Qaeda, i Talebani sono più collegati a rete rispetto al nostro esercito, più come una comunità di interessi che come una struttura societaria [...] è diventato ormai chiaro per me e per molti altri che per sconfiggere un nemico strutturato in rete dobbiamo diventare anche noi stessi una rete"[270].

Se da un lato dunque, la rivoluzione tecnologica ha consentito un processo di "democratizzazione dell'informazione senza precedenti"[271], dall'altro si assiste alla s-politicizzazione della violenza e allo stravolgimento del tradizionale concetto di arma. D'altronde, già i colonnelli cinesi Qiao Liang e Wang Xiangsui nel loro celebre libro "*Guerra senza limiti*", avevano posto l'accento su come si sarebbe evoluto il concetto di guerra e di violenza all'alba del nuovo mondo post-bipolare, egemonizzato dalla supremazia militare statunitense[272]. In particolare, gli autori evidenziano come gli Stati Uniti, a dimostrazione della loro vittoria sull'avversario sovietico e per imporre il nuovo *design*, non avessero tardato a "mostrare i

[269] Cfr. J. Arquilla and D. Ronfeldt, *Networks and Netwar. The Future of Terror, Crime, and Militancy*, Published by RAND, Santa Monica, 2001.
[270] Cfr. S. A. McCrystal, *It Takes a Network*, Foreign Policy n. 185, 2011, pp. 66-70, citazione ripresa da H. H. Dinnis, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, cit. p. 17
[271] Cfr. L. Floridi, *La rivoluzione dell'informazione*... op. cit., cit. p. 7.
[272] Cfr. Q. Liang e W. Xiangsui, *Guerra senza limiti*...op. cit.

propri muscoli" in occasione dell'eccezionale dispiegamento di forza militare durante la guerra del Golfo del 1991, rivelando la superiorità americana in campo tecnologico prima ancora che militare, e segnando un punto di cesura netto dal tradizionale concetto di guerra e di armenti[273]. La conseguente risposta al "monopolio tecnologico e militare" statunitense non può che perpetrarsi attraverso dinamiche asimmetriche; questa asimmetria non interviene esclusivamente sul piano tattico o operativo militare, ma nel suo più ampio concetto strategico[274]. In questo senso si può parlare di "guerra senza limiti", laddove gli estremi sfuggenti non sono tanto quelli della morale o dell'etica, ma piuttosto quelli della pervasività degli strumenti messi a disposizione dalla moderna tecnologia[275]. È evidente che si è venuta a creare nell'era dell'informazione una netta cesura della distinzione tra militare e civile, non tanto sul piano della ripartizione dei ruoli, quanto piuttosto sullo stravolgimento del concetto del moderno campo di battaglia[276]. Non è certo un eufemismo né tanto meno un allarmismo spicciolo raggiungere la consapevolezza che i moderni mezzi messi a disposizione dalle odierne scoperte tecnologiche combinati all'ormai definitivo raggiungimento della globalizzazione "dei servizi e delle genti", riescano a rendere la quotidianità un vero e proprio teatro bellico, all'interno del quale, ognuno di noi può essere ritenuto non solo un bersaglio, ma anche un potenziale autore indiretto di un atto ostile[277]. In altre parole, così come scrive Paul Virilio, oramai il monitor del computer altro non è che una finestra dalla quale poter attuare degli scambi tanto pacifici quanto bellici e aggiunge che: "Grazie alla paziente attuazione di un'interattività estesa all'insieme del nostro pianeta, la *information warfare* prepara la prima guerra mondiale del tempo o, più esattamente, la *prima guerra del tempo mondiale*, di questo "tempo reale" degli scambi tra le reti"[278].

---

[273] *Ibidem.*

[274] Per una definizione specifica del concetto di asimmetria nelle sue ampie varianti, politiche, strategiche, tattiche o operative, cfr. S. Metz and D. V. Johnson II, *Asymetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*, in Strategic Studies Institute, January 2001.
URL:http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA387381&Location=U2&doc=GetTRDoc.pdf [consultato il 14-02-2013]

[275] *Ibidem.*

[276] Cfr. P. Virilio, *La bomba informatica*, Raffaello Cortina Editore, Milano, 2000.

[277] *Ibidem.*

[278] Ivi, cit. 134

4.3 Dall'era post-eroica alla guerra post-umana

Come insegna Tucidide "la guerra è maestra di violenze"[279]. Secondo lo *strategos* ateniese, tre sono i motivi per i quali un uomo decide di abbracciare le armi: l'onore, l'interesse e la paura[280]. I tre motivi tucididei risuonano "arcaici", così come i disastri della guerra dipinti da Francisco Goya appaiono, oggi, così lontani nei nostri ricordi che le pozze di sangue frutto di scontri campali tra eserciti contrapposti rimangono un brutto episodio della crudeltà umana[281]. La società occidentale, per effetto del progresso e della prosperità, si è calata dentro un'amnesia storica collettiva e ha deciso che non potendo eliminare la guerra, questa debba diventare *hidden*, invisibile[282], in modo tale da riuscire a garantire una *geriatric peace*[283]. Amnesia storica, calo demografico, perdita del senso dell'onore, sono termini che ben rappresentano l'era contemporanea; il problema non è più se sia utile o meno combattere una guerra, quanto piuttosto se sia possibile combatterla[284]. Il "possibile" è dato dalla cifra derivante dal calcolo tra costi/benefici dettato dalla riluttanza sociale ad accettare la perdita di vite umane, e nella reticenza ad abbandonare il proprio stile di vita dell'opulenza[285]. Anche la guerra, azione sociale, si adatta ai tempi; se l'operazione americana in Iraq nel 1991 è stata l'occasione per sfoggiare la superpotenza militare e civile degli Stati Uniti, l'improvviso abbandono della Somalia da parte delle truppe statunitensi dopo la perdita di diciotto militari nell'ottobre 1993 non solo segna la *débâcle* dell'Operazione *Black Hawk Down*, ma rappresenta la nemesi naturale di questo nuovo corso storico che, con un'espressione eloquente Edward N. Luttwak ha definito "era post-eroica"[286]. La guerra del Kossovo del 1999 e la definitiva ritirata del soldato europeo dal suo stesso campo di battaglia, inaugura l'avvento della dottrina militare occidentale basata sull'*opzione morti zero*[287]. Le società occidentali sono talmente allergiche alle perdite

[279] Cfr. Tucidide, *La guerra del Peloponneso*, Rizzoli, Milano, 1986.
[280] *Ibidem.*
[281] F. Goya, *I disastri della guerra*,Abscondita, 2011, Milano
[282] Cfr. G. Friedman, *America's Secret War: Inside The Hidden Worldwide Struggle Between The United States and Its Enemies*, Broadway Books, New York, 2004.
[283] Cfr. M. L. Haas, *A Geriatric Peace? The Future of U.S. Power in a World of Aging Populations*, in International SecurityVol.32, No 1 (Summer 2007), pp. 112-147.
[284] Cfr. E.N. Luttwak, *Strategia. La logica della guerra e della pace*...op. cit.
[285] *Ibidem.*
[286] *Ibidem.*
[287] *Ibidem.*

(umane ed economiche) da essere in effetti "de-bellicizzate"; il risvolto della medaglia è la baldanza dei terroristi islamici[288]. Dello stesso avviso è René Girard, che a proposito della contrapposizione tra Occidente e terroristi, scrive:

"In Occidente gli individui sono uniti solo dal consumismo, dalla ricchezza, dai beni materiali. E i musulmani pensano: "avranno anche a disposizione armi pericolosissime, ma sono così deboli dal punto di vista umano che non sarà poi così difficile distruggere interamente la loro civiltà". È così che la pensano e hanno in parte ragione"[289].

Non a caso la baldanza della *full spectrum dominance* si è basata sulla creazione di tecniche militari risk-free con dispositivi di arma capaci di garantire un combattimento a distanza di sicurezza, in modo tale da eliminare tutti gli effetti collaterali di un conflitto armato tradizionale[290]. Non è un caso se, stando a quanto scrive David E. Sanger nel suo libro *"Confront and Conceal"*[291], al momento del cambio di consegne tra il Presidente George W. Bush e Barack Obama, il Presidente uscente ha voluto far dono di due consigli al nuovo inquilino della Casa Bianca: "non abbandonare i bombardamenti mirati con i droni e continua con il progetto della cyber warfare"[292]. Che Obama abbia seguito e ampliato la dottrina della "guerra invisibile" lo si legge nelle pagine ufficiali della *Strategic Defense Guidance* del 2012 la quale prevede: l'incremento crescente delle missioni degli aeromobili senza pilota (UAV); il progresso della capacità di resilienza e attacco dell'apparato cibernetico americano[293]. Questi esempi, insieme all'incremento delle operazioni condotte dalle forze speciali, dimostrano l'avvenuta assimilazione di un modo di fare la guerra *leading from behind* (dal sedile posteriore)[294]. La guerra combattuta con strumenti *risk-free* ha

[288] *Ibidem.*
[289] Ivi, cit. p. 22.
[290] *Ibidem.*
[291] Cfr. D.E. Sanger, *Confront and Conceal. Obama's Secret Wars and Suprising Use of American Power*, Crown Publishers, New York, 2012.
[292] *Ibidem.*
[293] Cfr. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21 Century Defense*, Washington, The White House, January 2012, URL: http://www.defense.gov/news/Defense_Strategic_Guidance.pdf [consultato il 18-06-2013]
[294] Cfr. C. Krauthammer, The Obama doctrine: Leading from behind, in The Washington Post, April 29, 2011, URL:http://www.washingtonpost.com/opinions/the-obama-doctrine-leading-from-behind/2011/04/28/AFBCy18E_story.html [consultato il 18-06-2013]

il pregio di essere una guerra "pulita" scevra da qualsiasi rischio di essere ripresa dai *network* internazionali; in altri termini è una guerra facile[295]. Il rischio implicito è l'azzardo morale nell'uso indiscriminato di questi strumenti che, in caso di fallimento, non generano conseguenze gravi per chi combatte dietro uno schermo o con in mano un *joystick*[296]. *Deterritorializzazione, intangibilità, ubiquità, velocità, economicità*, sono lemmi che rappresentano il nuovo ambiente entro il quale si accinge a muoversi il camaleonte clausewitziano[297]. Secondo Martin van Creveld questa "ennesima rivoluzione negli affari militari" ha "snaturato" la guerra, con il conseguente superamento della concezione trinitaria tanto cara a Clausewitz (governo, popolo, esercito). Spiega van Creveld che la guerra contemporanea avendo una natura intra-statale non può essere più sottomessa alle limitazioni della politica. Non permette più una distinzione tra combattenti e non-combattenti. Non distingue più il campo di battaglia né tantomeno rispetta i limiti territoriali dello Stato e soprattutto, la vittoria in termini militari non è né decisiva né tantomeno il fine ultimo della guerra[298]. In sintesi, secondo van Creveld, il paradigma clausewitziano della guerra come "continuazione della politica con altri mezzi" non trova più corrispondenza in una società altamente tecnologizzata e soprattutto dove "buona parte dell'attuale potenza militare è semplicemente irrilevante quale strumento per estendere o difendere interessi politici su gran parte del globo"[299]. Infatti, come dimostra il caso americano in Afghanistan e in Iraq, nonostante la schiacciante superiorità tecnologica degli Stati Uniti, di fronte a conflitti asimmetrici (non convenzionali o ad alta intensità) nelle operazioni di controguerriglia, che si dipanano prevalentemente nell'ambiente urbano, il numero delle truppe sul terreno (*boots on the ground*) diventa decisivo a dispetto dei vantaggi tecnologici[300]. Accanto al consolidamento dell'*Information Technology* si assiste allo sviluppo delle c.d. tecnologie emergenti conosciute con l'acronimo NBIC (*Nanotechnology, Biotechnology, Information Technology, Cognitive Science*): nanotecnologie, biotecnologie, tecnologie

[295] Cfr. M. Ferraresi, *L'azzardo morale dei droni*, in Il Foglio, Anno XVIII N. 26, 31 gennaio 2013, p. 1.
[296] *Ibidem.*
[297] Cfr. F. Volpi, *Il potere degli elementi*, in C. Schmitt, *Terra e Mare. Una riflessione sulla storia del mondo*, Adelphi, Milano, 2002.
[298] Cfr. M. van Creveld, *The Transformation of War*, The Free Press, New York, 1991
[299] Ivi, cit. p. 27.
[300] Cfr. M. Nones e A. Marrone, *La trasformazione delle Forze Armate*...op. cit.

dell'informazione, scienze cognitive, che adattate alla conflittualità, hanno come scopo finale di giungere alla guerra post-umana attraverso la robotica antropomorfa[301]. Esiste una coincidenza quantomeno singolare che lega l'avvento dell'era cibernetica con alla divulgazione del termine "post-umano". Entrambi si diffondono negli anni Ottanta del Ventesimo secolo in concomitanza con i primi racconti di William Gibson ritenuto l'ideatore del termine *cyberspace*[302]. Il termine post-umano viene utilizzato da scienziati visionari o "futurologi" come Eric Drexler che nel 1986 pubblicava il suo documento *Engines of creation*[303], basandosi sull'idea che le nuove frontiere della ricerca consentiranno presto agli individui di controllare e modificare la propria morfologica[304]. Un altro documento importante di questo filone di pensiero è il testo di Hans Moravec dal titolo *Mind Children* pubblicato nel 1988[305]; Moravec teorizza la possibilità di trasferire l'intera personalità di un essere umano su di un supporto diverso dal suo corpo naturale attraverso il processo di *personality download*[306]. Esiste dunque un *continuum* tra gli esperimenti condotti dai ricercatori del *post-human* e l'ipotesi dei fautori "cibernetici": ricercare attraverso dei *software* e con l'aiuto dei computer di giungere a simulare attività umane[307]. Come giustamente avverte Chris Hables Gray: "Con l'era cibernetica si inaugura l'avvento di un nuovo tipo di cittadino, di un nuovo senso dell'umano"[308]; in sintesi, si assiste alla creazione del c.d. *cyborg citizen* che segna il passaggio dall'*interazione* all'*integrazione* uomo-macchina[309]. È il caso ad esempio del progetto finanziato dal Pentagono a un team di ricercatori dell'Università della California con una concessione di 4 milioni di dollari per studiare le basi della c.d. *computer-mediated telepathy* (telepatia sintetica)[310]. Il progetto denominato *Silent Talk* ha l'obiettivo di consentire la comunicazione

[301] Cfr. M.C. Roco e W.S. Bainbridge, *Converging Technologies for Improving Human Perfomance*, Springer, 2004.
[302] Cfr. A. Caronia, *Corpi e informazioni. Il post-human da Wiener a Gibson, in Post-umano. Relazione tra uomo e tecnologia nella società delle reti*, a cura di M. Pireddu e A. Tursi, Guerini e Associati, Milano, 2006, pp. 43-56.
[303] Cfr. E. Drexler, *Engines of creation. The coming era of nanotechnology*, Anchor, New York, 1986
[304] *Ibidem.*
[305] Cfr. H. Moravec, *Mind Children. The Future of Robot and Human Intelligence*, Harvard University Press, Cambridge (USA), 1988.
[306] *Ibidem.*
[307] *Ibidem.*
[308] Cfr. C.H. Gray, *Cyborg Citizen. Politics in the Posthuman Age*, Routledge, London, 2002.
[309] *Ibidem.*
[310] Cfr. N. Shachtman, *Army Funds 'Synthetic Telepathy' Research*, in WIRED, 08.18.08URL: http://www.wired.com/dangerroom/2008/08/army-funds-synt/ [consultato il18-06-2013]

tra utenti su un campo di battaglia senza l'uso della voce, ma attraverso l'analisi dei segnali neurali[311]. Anche l'agenzia privata *Northrop Grumman* finanziata da fondi pubblici americani sta lavorando su un progetto innovativo: un binocolo in grado di interfacciarsi con la mente inconscia del soldato[312]. Il programma poggia sulla tecnologica cognitiva c.d. *Threat Warning System*, questo prototipo combina ottiche avanzate con gli elettrodi dell'elettroencefalogramma, e agendo sul subconscio può essere utilizzato per avvisare il soldato sulla minaccia prima ancora che la mente cosciente abbia elaborato le informazioni[313]. Pur assistendo ad una vera e propria "robotizzazione" della guerra, l'equivoco sostanziale che bisogna sfatare è quello di credere che una guerra pulita, a rischio zero, invisibile, distante, possa decretare la fine della conflittualità dall'esperienza umana. Una guerra pur essendo s-naturata è pur sempre "maestra di violenza"; non a caso, come avverte Clausewitz: "la violenza si arma con le invenzioni delle arti e delle scienze per far fronte alla violenza"[314]. Esiste dunque, un errore di fondo nel considerare queste "nuove tecniche militari" foriere di un'era senza guerra. In realtà come spiega Virilio, il centro urbano diventa il vero teatro bellico dell'era informatica guidata da una logica bellica che prevede una grammatica globale; laddove – così scrive Virilio – se l'*interattività* sta all'informazione come la *radioattività* sta all'energia, allora siamo di fronte al rischio di un "incidente" non più *locale* e precisamente situato, ma *globale* e generalizzato; in altri termini di fronte a un fenomeno in grado d'intervenire simultaneamente ovunque[315].

[311] *Ibidem.*
[312] Cfr. S. Weinberger, *Pentagon to Merge Next-Gen Binoculars With Soldiers' Brains*, in WIRED, 05.01.07, URL: http://www.wired.com/gadgets/miscellaneous/news/2007/05/binoculars [consultato il 18-06-2013]
[313] *Ibidem.*
[314] Cfr. C. von Clausewitz, *Della guerra*...op. cit.
[315] Cfr. P. Virilio, *La bomba informatica*...op. cit

CONCLUSIONI

Sin dalle prime pagine di questa ricerca si è cercato di porre l'accento sul radicale mutamento di paradigma subito dalle relazioni internazionali con il consolidamento della Rivoluzione Informatica, espressione massima dell'era cibernetica. L'*Information Revolution* ha provocato uno sconvolgimento totale sulle istituzioni sociali e politiche dell'era industriale, e ha imposto il passaggio definitivo dalla politica internazionale basata su una distribuzione del potere *verticale* (piramidale) verso una struttura *orizzontale* (reticolare). L'avvento della "democratizzazione dell'informazione" e la conseguente *diffusion of power*, insieme alla multipolarità dei centri di potere, rischiano di generare, nelle relazioni internazionali odierne, un'entropia tale da rendere vani qualsiasi modello di dissuasione e deterrenza valido per la *Realpolitik* kissingeriana. La razionalità sfugge di fronte alla possibilità di condurre una guerra con strumenti non militari che garantiscono l'anonimato e l'istantaneità e assicurano l'immunità da azioni di rappresaglia punitiva. La *dual-use capability* conferita dall'*Information Technology* ha reso la guerra allo stesso tempo *on the cheap*. Si assiste inoltre, alla "civilizzazione della guerra" nel senso peggiore del termine; una guerra "civile" perché civili sono gli obiettivi strategici che gravitano all'interno dell'ambiente cibernetico. Si preannuncia dunque, un ulteriore mutamento di paradigma questa volta nel settore della conflittualità, dove i nuovi "centri di gravità" non sono più militari, ma civili. Si pensi ad esempio a quanto è avvenuto con *Stuxnet*: il *modus operandi sui generis* di questo *malware* può essere adattato a *penetrare* qualsiasi sistema SCADA, al di là se sia connesso a Internet o meno. La consapevolezza che la maggior parte (se non tutte) le Infrastrutture Critiche (dighe, centrali elettriche, centrali atomiche, gasdotti, acquedotti, sistemi aerei, radar, ecc.) poggiano su questo tipo di sistema di comando e controllo informatico, rende l'idea della rilevanza strategica e dei rischi provenienti dal *cyberspace*. È lungo queste certezze del pericolo e della vulnerabilità degli interi sistemi informatizzati, che deve emergere la consapevolezza che il rischio si possa tramutare in un "incidente del futuro", avvenimento distruttivo capace di paralizzare un intero Paese. La struttura reticolare è espressione dell'interdipendenza raggiunta a livello globale dalle società interconnesse ai sistemi informatici. L'interdipendenza a sua volta, se da un lato garantisce un miglioramento dei servizi e l'abbattimento delle

barriere del tempo e dello spazio, dall'altro segna un *trade-off* tra livello di informatizzazione e vulnerabilità agli attacchi cibernetici. Un singolo evento prodotto su un nodo della rete tende a propagarsi e a diffondersi "a cascata" all'intero sistema come un effetto domino. Verrebbe da chiedersi se l'interdipendenza non decreti l'avvento di una sana cooperazione internazionale fra tutti gli attori a rischio di guerra cibernetica; il perdurare del "sacro egoismo nazionale", l'affollamento e il caos dell'arena internazionale, nonché la scarsa sensibilità degli attori privati verso i rischi alla sicurezza, fanno cadere qualsiasi utopica trasformazione del sistema internazionale in un condominio di *gentlemen*. L'era cibernetica, dal canto suo, obbliga ad accettare un nuovo *Zeitgeist* politico, militare e culturale di riferimento. Diventa impensabile nell'era post-industriale e post-internazionale, pretendere di governare le dinamiche internazionali con gli stessi modelli di pensiero atrofizzati su gerarchie piramidali, incapaci di gestire delle minacce e degli eventi che si muovono alla velocità della luce. Questo *Zeitgeist* si impone anche sulla strategia la quale, come avverte Colin Gray, converte i risultati ottenuti a livello tattico in effetti di livello strategico strumentali ai fini della politica. Non avere una strategia valida per elaborare una pianificazione di difesa o per condurre una guerra, sarebbe come giocare a scacchi senza re sulla scacchiera[316]. Non è un caso se emerge, anche negli Studi Strategici, la necessità di rivoluzionare le stesse dottrine difensive basate sulla massa e sulla forza, a favore di modelli più malleabili, più elastici, più resilienti, con la perfetta cooperazione tra settore pubblico e privato. Come già notava John Boyd, agli albori di quella che sarebbe diventata la *Rivolution on Military Affairs*, in questo nuovo corso storico: "sopravvive solo chi è in grado di cambiare più in fretta"[317]. È questo il vero sovvertimento del paradigma internazionale introdotto dalla rivoluzione dell'informazione laddove, la politica internazionale non più retta dai rapporti di forza tra il forte e il forte, ma tra il "forte e il folle", necessita di una *omeostasi*[318] in grado di reagire alle minacce divenute istantanee, ibride e globali. In questa breve ricerca, si è cercato di porre l'accento sulla *rilevanza strategica del cyberspace e i rischi di guerra cibernetica*, nella consapevolezza che il rischio peggiore, nelle previsioni strategiche, è dato dal diniego di riconoscere l'esistenza del *cigno nero*, salvo poi

[316] Cfr. C.S. Gray, *Modern Strategy*, Oxford University Press, Oxford, 1999.
[317] Cfr. F.P.B. Osinga, *L'arte della guerra di Boyd*...op. cit
[318] Auto-regolazione che consente agli organismi viventi di mantenersi in uno stato di equilibrio dinamico.

esserne sorpresi e catalogarlo come *evento inatteso*. A tal proposito, appaiono quanto mai validi i precetti di Machiavelli che invita il Principe virtuoso a prevedere nei tempi "quieti" le avversità della fortuna: "la quale dimostra la sua potenza dove non è ordinata virtù a resisterle: e quivi volta e' suoi impeti, dove la sa che non sono fatti gli argini né e' ripari a tenerla"[319]

[319] Cfr. N. Machiavelli, *Il Principe*, Einaudi, Torino, 1995.

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies