PAPER
2016

CYBERCAOS: INCUBI E DESIDERI DELLA DIMENSIONE CIBERNETICA

PAOLA TAVOLA

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

CYBERCAOS: INCUBI E DESIDERI DELLA DIMENSIONE CIBERNETICA

Paola Tavola

UNIVERSITÀ DEGLI STUDI FIRENZE

Paper

2016

CYBERCAOS: INCUBI E DESIDERI DELLA DIMENSIONE CIBERNETICA

Introduzione - caos e reti

Il Caos viene generalmente definito come spazio infinito, privo di senso. Instabile, imprevedibile, irrazionale e incomprensibile. Condizione che viene superata attraverso la difficile e dolorosa separazione degli elementi grazie all'avvento di un principio ordinatore. Il *Nous* o intelletto di Anassagora che costituisce la fonte di ordine e armonia alla base della costruzione di un disegno razionale. Il Demiurgo di Platone che si pone come dio ordinatore.

All'interno di una rete, al contrario, il Demiurgo è assente. Le connessioni tra gli elementi permangono e anzi, si riproducono, si moltiplicano e si infittiscono aumentando la densità del sistema. Le reti, o network, sono caratterizzate da una struttura di connessioni che non necessariamente si organizza secondo gerarchie specifiche. Gli elementi, in questo caso i nodi della rete, sono collegati nonostante le ampie distanze e acquisiscono un nuovo ruolo attivo e talvolta decisivo per il funzionamento del sistema. Si generano così, le c.d. *distant proximities*[1]: dimensioni in cui ciò che sembra remoto è anche prossimo, a portata di mano, e in cui dinamiche di integrazione (globalizzazione) interagiscono con forze di frammentazione (localizzazione) dando nuovo valore alla dimensione locale delle reti.

Gli spazi divengono allo stesso tempo distanti e contigui e si delineano secondo geometrie variabili di *linkages* che creano un dinamismo di interconnessioni e interdipendenze, per cui l'interazione tra poche unità può generare conseguenze sull'intera struttura. "La rete agisce, per contagio, a un comportamento individuale dovuto a una situazione locale. È questa la potenza dei network"[2].

[1] Rosenau J. N., *Distant Proximities: Dynamics Beyond Globalization*, Princeton University Press, 2003.
[2] Menotti R., *Mondo Caos: Politica Internazionale e Nuovi Paradigmi Scientifici*, Laterza, 2010.

La caoticità, non solo si rivela quale caratteristica intrinseca delle reti, ma anche quale fattore funzionale, almeno in parte, alla loro evoluzione. E' necessario, infatti, che le reti non si estranino totalmente dalla componente caotica che le caratterizza: la loro evoluzione comporta la necessaria esposizione a fenomeni di perturbazione o turbolenza. Il rischio sarebbe quello di cadere in una stasi perpetua: una condanna alla fine del mutamento e del progresso e all'impossibilità delle reti di sopravvivere all'ambiente esterno in cui si inseriscono. "L'efficienza del sistema dipende dalla condizione che l'ordine non elimini completamente il caos"[3]. Caos, sviluppo e opportunità divengono insoliti partner comportando una rivalutazione della connotazione sostanzialmente negativa attribuita al termine in origine. Di fatto, sono proprio i feedback positivi[4], definiti come dinamiche auto-rinforzanti e fortemente destabilizzanti, che Robert Jervis individua essere il motore della crescita e del progresso dei sistemi[5]. Tuttavia, permane il fatto che alti livelli di complessità e dinamismo, come quelli tipici dei sistemi reticolari descritti, costituiscono i principali propulsori della crescita di incertezza, instabilità e imprevedibilità.

1. Cyberspazio: somma di incubi e desideri

Le considerazioni mosse in merito alla relazione esistente tra caos e reti risultano di utilità notevole se trasposte nell'analisi di ciò che è stato definito come la "rete delle reti": il cyberspazio o spazio cibernetico. Network di copertura globale. Nuova dimensione del progresso umano, caratterizzata da un'*unthinkable complexity* così come scritto da Gibson[6] nel 1984.

Il cyberspazio si è sviluppato all'interno di una realtà complessa e costituisce, esso stesso, un sistema in cui "we can never do merely one

[3] Jean C., Tremonti G., *Guerre Stellari: Società ed Economia nel Cyberspazio*, FrancoAngeli, Milano, 2000.
[4] In un contesto caotico, fenomeni e interazioni risultano essere complessi e non lineari. Le dinamiche prevalenti sono di norma ascrivibili a feedback (positivi o negativi), per cui a delle piccole azioni o variazioni conseguiranno azioni o variazioni di dimensioni e impatti più che proporzionali.
[5] Jervis R., *System Effects: Complexity in Political and Social Life*, Princeton University Press, 1997.
[6] Gibson W., in *Neuromancer* (1984), definisce il cyber spazio come "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts (…) A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding".

thing"[7] per cui, ogni azione o mutamento del sistema avrà conseguenze ed effetti molteplici, diretti o indiretti, prevedibili o imprevedibili. La costruzione, l'espansione e l'evoluzione del cyber spazio ne hanno fatto, in primis, un fondamentale fattore di crescita, moltiplicatore di ricchezza, informazioni, idee ed esperienze. Tuttavia, la rete delle reti è divenuta insieme "somma di tutti i desideri"[8] e in un certo senso, indirettamente e involontariamente rispetto alla sua concezione originaria, anche somma di tutti gli "incubi"[9].

Oltre alle 4 dimensioni (terra, mare, aria e spazio), in cui l'umanità ha tradizionalmente condotto le sue battaglie e che nel corso dei secoli sono state conquistate e regolamentate, il dominio cyber viene elevato al rango di quinta dimensione della conflittualità[10], acquistando un ruolo centrale per la conduzione della politica internazionale. Emblema di ciò, è l'avvenuta militarizzazione dello spazio cibernetico cui, ai pionieri americani[11] hanno fatto seguito altri attori della scena internazionale: Cina, Russia, Francia, Iran, India, Pakistan, Israele, Regno Unito, Germania[12] e le due Coree. Il cyberspazio diviene luogo di concretizzazione delle logiche della guerra e della pace e si rivela essere, insieme, moltiplicatore della potenza militare e fonte di nuove vulnerabilità. Considerato come "the most important global common"[13], il suo accesso risulta essenziale in termini di sicurezza nazionale, progresso militare, benessere economico e per il possesso delle informazioni, risorsa chiave per l'esercizio del potere. In termini generali dunque, si può affermare l'esistenza di una dipendenza generale del

[7] Jervis R., *System Effects: Complexity in Political and Social Life*, Princeton University Press, 1997.
[8] Menotti R., *Mondo Caos: Politica Internazionale e Nuovi Paradigmi Scientifici*, Laterza, 2010.
[9] *Ibidem.*
[10] Martino L., *La Quinta Dimensione della Conflittualità. La rilevanza strategica del Cyberspace e i Rischi di Guerra Cibernetica*, CSSII - Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università degli Studi di Firenze.
[11] "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". Emblematiche sono queste parole, pronunciate nel 1997 dA William Cohen, l'allora Segretario alla Difesa americano. Cit. Cohen W.S., Report of the Quadriennal Defense Review, U.S. Department of Defense, Washington DC, 1997, p. IV; ripresa da Martino L., *La Quinta Dimensione della Conflittualità. La rilevanza strategica del Cyberspace e i Rischi di Guerra Cibernetica*, CSSII - Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università degli Studi di Firenze.
[12] *Ibidem.*
[13] Pudas T. J., Mark D. Drapeau M. D., *Technology and the Changing Character of War*, in *Global Strategic Assessment 2009: America's Security Role in a Changing World*, Edited by Patrick M. Cronin, Institute for National Strategic Studies, National Defense University Press, 2009.

sistema globale (politico, economico, finanziario militare e sociale) da questa nuova dimensione.

Con ciò, risulta facile comprendere come l'essenza caotica del dominio cyber, determinata in gran parte dalla sua natura ibrida e volatile, dalla sua struttura reticolare e anarchica, dalle dinamiche di interdipendenza che vi si dispiegano e dai paradossi che vi si generano, così come dall'ampia dose di incertezza e ambiguità di cui questa dimensione si fa portatrice, lo trasforma in amplificatore della complessità e del caos che di base contraddistinguono l'arena internazionale attuale. Nuove vulnerabilità, asimmetrie e paradossi emergono all'interno dello scenario globale, complicando non poco la conduzione della politica internazionale da parte degli Stati. Ecco, dunque, che si delinea quella natura di incubo di cui sopra, portatrice di preoccupazione grave e continua; tormentosa ed assillante[14].

L'*information revolution* che ha interessato il sistema globale negli ultimi decenni, aumentando la pervasività del cyberspazio dalla natura tanto antropica quanto virtuale, ha segnato il passaggio del sistema internazionale da una struttura di potere sostanzialmente "verticale (piramidale)"[15] a una struttura di tipo "orizzontale (reticolare)"[16], comportando numerose delle implicazioni derivanti dalla natura caotica delle reti accennate poc'anzi. Il longevo sistema internazionale statocentrico si trova oggi a convivere con un sistema decisamente più dinamico, decentralizzato e multicentrico. Il primo, basato sulla centralità degli stati e fondamentalmente anarchico, anche se indebolito, di fatto, non è scomparso e si trova oggi a fare i conti con nuovi centri di potere diffusi che si sottraggono alla sovranità statale e ne minano le fondamenta. Norme, strutture e processi si scontrano e i paradigmi tradizionali vacillano. Le caratteristiche del cyberspazio danno nuova forma alle teorie, alle politiche e alla pratica nelle relazioni internazionali. Le interconnessioni virtuali sfidano i concetti tradizionali di geografia, confini, potere, influenza, rappresaglia e sicurezza. E con essi, la realtà che vi corrisponde. Le caratteristiche naturali dell'ambiente cibernetico e coloro che lo popolano sono i perni attorno

[14] Cfr. voce *incubo*, Vocabolario Treccani.
[15] Martino L., *La Quinta Dimensione della Conflittualità. La rilevanza strategica del Cyberspace e i Rischi di Guerra Cibernetica*, CSSII - Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università degli Studi di Firenze.
[16] *Ibidem.*

a cui nuove dinamiche e nuove strutture di potere si organizzano andando a determinarne il grado di ordine e disordine del sistema.

2. Geografia: accelerazione e imprevedibilità

Fu l'impero britannico, per primo, a comprendere il vantaggio strategico derivante dall'estensione della propria leadership nel settore delle comunicazioni cablate e a realizzare i primi cavi subacquei al fine di mettersi in collegamento in tempo reale con i suoi possedimenti[17]. Attualmente, i cavi sottomarini costituiscono l'infrastruttura basilare di internet e delle comunicazioni globali e il tramite attraverso cui passa il 93% dell'intero traffico globale[18]. A trovarsi in una posizione di supremazia, nel core della realizzazione e del controllo dei cavi sottomarini, oggi, sono gli Stati Uniti, i quali rivestono una posizione di quasi monopolio anche per quanto riguarda il controllo sui sistemi di *cloud computing*[19]. In generale, dunque, i *backbones* (spine dorsali) e gli *exchange points* (gangli) su cui si fonda l'arena digitale globale nascono e si sviluppano negli Stati Uniti, andando così a determinarne il ruolo di potenza leader nel settore. All'interno della nuova dimensione cibernetica di natura sostanzialmente intangibile, è chiara la permanenza di una componente fisica territoriale, e dunque tangibile, composta dagli elementi che compongono il c.d. *physical layer*[20] del cyberspazio cui si è fatto riferimento poc'anzi, così come dalle infrastrutture di *Information Communication Technology* (ICT). La rilevanza strategica della dimensione fisica del cyberspazio si è rivelata

[17] Il primo collegamento realizzato fu quello tra Dover e Calais, realizzato nel 1850, seguito nel 1858 dal primo cavo transatlantico in collegamento tra l'Irlanda e l'Isola di Terranova.

[18] Mayer M., Zacchetti E., *Arena Digitale e Politica Internazionale: una chiave interpretativa*, in Gori U., Lisi S. (a cura di), *Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013.

[19] Attraverso i sistemi di cloud computing i file degli utenti vengono salvati sui server di proprietà di aziende quali Facebook, Instagram, Dropbox, Google Drive, situati all'interno di data center. La maggioranza di questi data center risiede nel territorio degli Stati Uniti. Il numero di data centers negli USA, infatti ammonta a 1545, seguiti dai 232 del Regno Unito, 175 della Germania, 148 del Canada, 139 della Francia, India 106. Come emerge dai dati, il gap risulta di notevole ampiezza. Per riferimenti alla collocazione e al numero di data center si rimanda all'indirizzo http://www.datacentermap.com.

[20] Il cyberspazio può essere strutturato secondo quattro *layers* (strati) di cui il primo (*physical layer*), è costituito dalle fondamenta fisiche che danno vita al cyberspazio, quali PC, server, supercomputer, reti, sensori, trasduttori, canali e reti di comunicazione e data centers. Per una spiegazione dettagliata sui *layers* si rimanda a Choucri N., Clark D., *Cyberspace and International Relations: Toward an Integrated System*, ECIR review, August 2011. Si faccia riferimento, in particolare al cap. 3, pp. 8-13.

in passato, si rivela oggi e continuerà a rivelarsi di fondamentale importanza e ciò risulta evidente dall'atteggiamento mostrato dagli Stati Uniti, che mirano a conservare il loro status di potenza tecnologica mondiale, ponendosi al centro dei network e del loro controllo. É evidente, come il territorio rimanga un principio organizzativo fondamentale in grado di influenzare, almeno in parte, l'organizzazione del potere all'interno dello spazio cibernetico. Gli stati, compresa la rilevanza strategica del dominio cibernetico, di derivazione e controllo sostanzialmente statunitense, sono portati a dare credito alla "spinta imperialista ad ampliare la portata del controllo o l'impegno autarchico verso una sempre più grande auto-sufficienza"[21]. Di fatto, il monopolio americano, viene da più parti e sempre più spesso messo in discussione, tanto che in molti prospettano un futuro in cui il dominio cibernetico sarà organizzato in modo analogo al sistema internazionale westfaliano, portando alla realizzazione di una c.d. "cybervestfalia"[22].

Accanto a ciò, forte si fa sentire l'esigenza di adottare nuovi modelli di comportamento e nuovi schemi cognitivi al fine di adattarsi alla nuova geografia virtuale, nonostante la convinzione che questa non abbia comportato un superamento totale della geografia classica, e con essa della geopolitica, rimanga ampiamente diffusa[23] e persino comprovata, alla luce degli atteggiamenti imperialisti mostrati dagli Stati che ragionano, almeno in parte, ancora in termini di conquista territoriale. Se è vero, dunque, che la nuova complessità sistemica determinata dalla dimensione cyber non comporti uno stravolgimento totale delle classiche dinamiche che determinano i rapporti di forza tra gli attori all'interno dello scenario internazionale, tuttavia, come avanzato da Nye, permane il fatto che il cyberspazio "like the town markets in feudal

[21] Waltz K. N., *Theory of International Politics*, New York, Newbery Award Records, 1979; (trad. it. Narbone L., *Teoria della Politica Internazionale*, il Mulino, Bologna, 1987).

[22] Lozito N., *Cybervestfalia*, in A Che Servono i Servizi, Limes 7/2014. Il trend è facilmente riscontrabile nelle numerose iniziative intraprese per la realizzazione non solo di nuove linee di collegamento tramite cavi sottomarini, ma anche di reti alternative a quelle già esistenti, da parte di numerosi StatiUn esempio esplicativo, a riguardo è il progetto relativo alla costruzione di una via di collegamento tramite cavi sottomarini lanciato dai paesi BRICS.

[23] Cfr. Choucri N., *Cyberpolitics in International Relations*, The MIT Press, Massachussetts, 2012; Gori U., *Cyberspazio e Relazioni Internazionali: Implicazioni Geopolitiche e Geostrategiche* & Mayer M., Zacchetti E., *Arena Digitale e Politica Internazionale: una chiave interpretativa*, in Gori U., Lisi S. (a cura di), *Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013; Lamanna A., *Per una Geopolitica del Cyberspazio*, The Alpha Institute of Geopolitics and Intelligence, Marzo 2016; Martino L., *La Quinta Dimensione della Conflittualità. La rilevanza strategica del Cyberspace e i Rischi di Guerra Cibernetica*, CSSII - Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università degli Studi di Firenze; Vettore S., *Data Center, dominio del cyberspazio e declino dello Stato-nazione*, BloGlobal Osservatorio di Politica Internazionale (OPI), Research Paper n. 31, Febbraio2015

times, it will coexist with them [the geografical space and the state sovereignty] and greatly complicate what it means to be a sovereign state or a powerful country"[24].

Facendo riferimento all'emergere delle c.d. *distant proximities*, Rosenau individua la causa principale del loro avvento nella rivoluzione informatica a causa dello sconvolgimento, se non annullamento, delle dimensioni spazio temporali tradizionali che essa ha implicato. "I mezzi elettronici (...) trasformano il lineare in non lineare e il sequenziale in simultaneo"[25]. Virilio parla della fine dello spazio "di un piccolo pianeta sospeso nell'etere elettronico dei nostri odierni mezzi di comunicazione"[26].

La dimensione virtuale, dalla natura c.d. "dromologica"[27], comporta la compressione degli spazi, l'abbattimento delle barriere, la velocità e la simultaneità delle azioni e reazioni condotte al suo interno. Il mondo attuale perde le sue dimensioni che vengono riconfigurate da un'accelerazione tremenda che non riguarda più soltanto la storia, ma l'intera realtà, dando vita a un nuovo e unico spazio-tempo mondiale in cui istantaneità, simultaneità e ubiquità regnano sovrane. L'idea del filosofo francese è quella di un'accelerazione tale per cui il tempo riassorbe lo spazio attribuendo il potere a coloro che detengono "le tecniche di spostamento e comunicazione più efficienti e veloci"[28]. Di fatto, la nuova libertà creata dalla rivoluzione dell'informazione, come risultante di un annullamento degli spazi, non è tanto quella di potersi muovere nello spazio, ma piuttosto la libertà di non muoversi seppure ci si trovi continuamente a navigare all'interno di un network di estensione mondiale[29].

Lo spazio cibernetico è unico in quanto interamente costruito dall'uomo e soggetto a mutamenti molto più rapidi rispetto agli altri domini cui si è fatto riferimento precedentemente. Al suo interno, gli spostamenti non sono più soggetti agli "attriti" e alle tempistiche rallentate tipiche

[24] Nye J.S., *The Information Revolution and American Soft Power*, Asia-Pacific Review, Vol. 9, No. 1, 2002.
[25] Rosenau J. N., *Distant Proximities: Dynamics Beyond Globalization*, Princeton University Press, 2003.
[26] Virilio Paul, *La Bombe Informatique*, Éditions Galilée, 1998; (trad. it. Piana G., *La Bomba Informatica*, Raffaello Cortina Editore, Milano, 2000).
[27] *Ibidem*. Il termine dromologia "scienza della velocità, dal greco dromos, corsa (...) insegna che il territorio è lo spazio costituito dalle tecniche di spostamento e dalle tecniche di comunicazione, e ne deduce che il potere si concentra nelle mani di chi dispone delle tecniche di spostamento e comunicazione più efficienti e veloci" cit. pp. 139-140.
[28] *Ibidem.*
[29] *Ibidem.*

della dimensione fisica. Dunque, mentre in passato i processi e i fenomeni erano soggetti a dinamiche piuttosto lineari e a lunghi tempi di evoluzione, quelli che avvengono lungo strutture reticolari, come quella che caratterizza lo spazio cibernetico, risultano più rapidi, dinamici e non lineari, andando a compromettere notevolmente le capacità di previsione degli attori, nonostante proprio grazie alle reti essi possano vantare di una maggiore disponibilità di dati e informazioni. La nuova geografia virtuale, dunque, esercita un impatto notevole sulla metodologia attraverso cui le decisioni vengono formulate dai decisori politici, i quali sembrano rivelare una padronanza sempre più scarsa della realtà rispetto al passato. Simon-Belli, nella sua analisi riguardante il fattore temporale in relazione alla capacità di previsione e di analisi strategica, mostra come all'interno di sistemi altamente complessi, di ampie dimensioni e molto articolati, [quale il cyberspazio], il ruolo degli attori si riduce notevolmente, in quanto i comportamenti vengono costretti e fortemente predeterminati dal sistema. Gli attori, inoltre, si trovano a fare i conti con una realtà in cui i fattori di cui tener conto, non essendo più lineari e indipendenti, non possono essere semplicemente sommati l'uno all'altro[30]. Al contrario, è necessario valutare le numerose e sempre più fitte interdipendenze che si delineano tra i singoli fattori, nonché metterli a confronto con il sistema generale in cui si inseriscono, ovvero un unico network di dimensioni globali.

L'esigenza di previsione che permette agli attori di ottenere conforto dal raggiungimento di maggiore certezza, non può, oggi, risultare sempre assecondata a causa delle interazioni simultanee che fanno della classica divisione tra passato presente e futuro un'unico tempo globale e degli spazi lontani un'unico network. L'imprevedibilità degli eventi, così come di eventuali attacchi mossi all'interno del dominio cibernetico, entra dirompente nella realtà attuale, supportata dall'annullamento di distanze e successioni temporali, per cui gli effetti di un'azione si manifestano in modo simultaneo al suo scaturire e ad una distanza che può essere tanto prossima quanto lontana dal suo punto di origine. E' divenuto, con ciò, estremamente difficile effettuare delle previsioni che risultino più o meno affidabili al fine di pianificare strategie di lungo termine, così come realizzare modelli di difesa validi, i quali non possono più contare sui tempi di reazione prolungati del passato, ma

[30] Cfr. Simon-Belli C., *Teoria della Previsione e Analisi Strategica*, Le Lettere, Firenze, 1998. Si rimanda in particolare al cap. 2, pp. 48-54.

richiedono una risposta simultanea all'attacco. "Il contingente e il breve termine [prevalgono] sul generale e sulla visione di lungo periodo; la complessità sulla semplicità"[31]. All'interno di un tale contesto, gli attori sembrano condannati a far prevalere l'azione sul pensiero, la tattica sulla strategia e, la razionalità e la ragionevolezza che risiedono abitualmente alla base dei processi decisionali rischiano di essere sacrificate.

Di fatto, nuove forme di controllo decentrato e orizzontalmente strutturate divengono necessarie in sostituzione a quelle tipiche del passato, gerarchiche, rigide e verticali, al fine di garantire maggiore adattabilità ed elasticità all'imprevisto[32]. Risulta evidente come nella realtà attuale dominata dallo spazio cibernetico "entropia e complessità vanno considerate come le due facce di una stessa moneta: quella di un nuovo concetto di ordine, non riduttivo della complessità"[33]. Si vedrà, infatti, come la nascita del cyberspazio abbia effettivamente dettato la nascita di nuove strutture di potere e di controllo più dinamiche e flessibili, le quali, tuttavia, incidono notevolmente sulla complessità del sistema globale.

3. Potere: diffusione e networked governance

Il cyberspazio, in analogia con il sistema internazionale, si presenta come spazio privo di gerarchie formali, autorità sovrane e poteri giuridicamente vincolanti. Non esiste, al suo interno, alcuna autorità capace di influenzare in modo effettivo l'azione degli altri attori presenti sulla scena, o legittimata a detenere il monopolio dell'uso della forza. In analogia con la geometria delle strutture reticolari, non vi è nel cyberspazio un Demiurgo, detentore di un' autorità suprema, sia essa legittimata su base divina o democratica. A ciò inoltre, si somma la debolezza, se non quasi assenza, di un solido impianto di regole e

[31] Jean C., Tremonti G., *Guerre Stellari: Società ed Economia nel Cyberspazio*, FrancoAngeli, Milano, 2000.

[32] In termini di attacchi cibernetici, De Felice, analizzando il nuovo fattore tempo come fattore critico dei processi decisionali in merito alla gestione e al contrasto degli incidenti informatici, sottolinea la necessità di adottare nuovi meccanismi "non convenzionali", di natura fortemente decentrata, al fine di garantire tempi di reazione rapidi. De Felice N., Le Sfide della Cyber-War al Processo Decisionale in Materia di Politica Della Difesa, in Gori U., Lisi S. (a cura di), *Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013.

[33] Jean C., Tremonti G., *Guerre Stellari: Società ed Economia nel Cyberspazio*, FrancoAngeli, Milano, 2000.

norme condivise a livello internazionale. Al momento, si riconosce che la categoria delle norme internazionali concernenti il cyberspazio "opera nell'ombra"[34] delle altre categorie. A livello concettuale, per di più, si rileva la mancanza di una terminologia e di definizioni comuni: precondizione naturale necessaria a qualsiasi tipo di scambio e di interazione che possa risultare chiaro, anche e soprattutto su un piano giuridico e normativo[35].

In sostanza, il cyberspazio costituisce uno spazio anarchico. Manca, nell'arena digitale globale, una forma di regolamentazione del potere e un'autorità che sia in grado di applicarla. Piuttosto, siamo di fronte ad una dimensione in cui il potere si organizza tramite "regole tenui"[36], se non addirittura senza regole, sulla base dei rapporti di forza che si stabiliscono tra gli attori. Anarchia e forti dinamiche di interdipendenza convivono e, nonostante la permanenza di un generale stato di disordine, il potere si organizza.

In termini generali, l'americano Richard Haas considera lo scenario internazionale come un *nonpolar world*, una realtà "dominated by dozens of actors possessing and exercising various kinds of power"[37]. Sulla stessa linea, lo storico e politologo Ash scrive che attualmente "we have not so much a multi-polar as a no-polar world"[38], mentre Gori fa riferimento al concetto di politica post-internazionale, la quale "non si svolge più soltanto tra nazioni ma piuttosto con e fra sottoinsiemi di queste"[39]. In linea con queste considerazioni avanzate in termini generali, Nye fa riferimento a un processo c.d. di *power diffusion* attraverso cui si è realizzato un vero e proprio *empowerment* di quegli attori che tradizionalmente hanno ricoperto un ruolo marginale, se non addirittura assente, all'interno dell'arena internazionale. Il palcoscenico globale in cui primeggiavano gli stati nazionali nel ruolo di attori protagonisti, risulta più affollato e denso di vecchie comparse che, ora,

---

[34] Schmitt M. N., Vihul L., *The Nature of International Law Cyber Norms, Legal, Policy & Industry Perspectives*, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCDCOE Publications, Tallinn 2016.
[35] Basta pensare, a tale riguardo, alla divergenza che divide Stati Uniti e Russia per cui, mentre i primi utilizzano il termine *cyber domain*, i secondi ne rifiutano l'adozione e mantengono in uso il termine *information domain*.
[36] Mayer M., Zacchetti E., *Arena Digitale e Politica Internazionale: una chiave interpretativa*, in Gori U., Lisi S. (a cura di), *Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013.
[37] Haas R. N., *The Age of Nonpolarity*, Foreign Affairs, May-June 2008.
[38] Ash T. G., *As Threats Multiply and Power Fragments, the 2010s Cry Out for Realistic Idealism*, The Guardian, December 31 2009.
[39] Gori U., *Cyberspazio e Relazioni Internazionali: Implicazioni Geopolitiche e Geostrategiche*, in Gori U., Lisi S. (a cura di), *Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013.

appaiono in primo piano. Sebbene risulti necessario chiarire che questa diffusione del potere non comporta l'accesso a pari poteri da parte di tutti gli attori, per cui "larger states still have larger resources"[40], lo scenario cambia notevolmente.

Se infatti, tradizionalmente, la distribuzione del potere ha subito mutamenti e cambi di conformazione attraverso moti di transizione (*translatio imperii*), per cui si è assistito regolarmente al passaggio di potere da uno o più attori ad altri, oggi, si assiste a una vera e propria diffusione di potere su linee sia verticali che orizzontali. Lo spazio, quindi, si rimodella su strutture reticolari leggere in cui centri di potere diffusi si interconnettono l'uno all'altro portando ad un allontanamento dalle classiche strutture gerarchiche, siano esse multipolari, bipolari o unipolari. Lo stesso Nye fa riferimento a un ritorno ad una situazione simile a quella pre-westfaliana, ricordando di come i legami transnazionali fossero tipici del sistema feudale e di come gradualmente essi siano stati ristretti dall'avvento degli Stati nazionali. Se l'analogia tra il sistema attuale e quello feudale sembra reggere, tuttavia, bisogna tener conto di una notevole differenza: "three decades ago, transnational contacts (..) involved relatively small numbers of élites involved in multinational corporations, scientific groups, and academic institutions. Now the Internet, because of its low costs, is opening transnational communications to many millions of people"[41].

Una tale diffusione di potere, in primo luogo, è stata possibile grazie ai bassi costi e alle basse barriere di entrata del cyberspazio che, in termini puramente economici, se fossero stati elevati avrebbero reso il mercato soggetto a logiche monopolistiche o, nella migliore delle ipotesi, oligopolistiche. Il cyberspazio, al contrario, è un mercato fruibile ad una varietà sempre crescente di individui che divengono i soggetti del già citato *empowerment*, in termini di informazioni, risorse e mezzi. Nel 2007 un utente russo, all'interno di un post in cui venivano date precise istruzioni su come lanciare attacchi a specifici siti estoni, scriveva: "You do not agree with the policy of eSStonia??? (...) You may think you have no influence on the situation??? You CAN have it on the Internet!"[42]. L'*information revolution*, di fatto, "esalta l'individuo, spinge alla

[40] Nye J. S., *The Future of Power*, Public Affairs, New York, 2011.
[41] Nye J.S., *The Information Revolution and American Soft Power*, Asia-Pacific Review, Vol. 9, No. 1, 2002.
[42] Davis J., *Hackers Take Down the Most Wired Country in Europe*, Wired, August 21 2007. (http://www.wired.com/2007/08/ff-estonia/).

contestazione di ogni autorità, richiede società aperte e distrugge le società chiuse"[43].

Se il realista Raymond Aron considerava come parametro rilevante per la definizione di un sistema internazionale non solo la distribuzione di potenza, ma anche le diversità delle forme di governo, si noti, in questa sede, l'importanza di considerare la natura interna delle unità che compongono il sistema. I valori che esistono in seno agli attori determinano il sistema internazionale e influenzano la stabilità del sistema ed è per questo che Aron analizza tra i fattori determinanti "i modi di essere e di agire degli attori"[44]. Il carattere anarchico dello spazio cibernetico sembra infatti allontanarsi dal modello più puro di anarchia, in cui vige la contrapposizione tra unità di esatta uguaglianza[45]. L'anarchia, all'interno di questo dominio, non solo si organizza secondo una struttura di potere reticolare, non-polare e densa, ma presenta una natura alquanto polimorfa. I nuovi attori protagonisti e detentori di fette del potere all'interno del cyberspazio, tra cui settore privato, organizzazioni criminali, gruppi terroristici, hackers e attivisti si differenziano dalle entità statuali, sia in termini di razionalità, sia in termini di obiettivi, doveri, aspirazioni, risorse e interessi. Dunque, la diversità degli attori coinvolti nell'esercizio di potere determina una complessità maggiore dello scenario se paragonata a un sistema di potere diffuso, ma ostaggio esclusivo di attori di natura statale.

Questi nuovi attori, avvantaggiati dall'accesso allo spazio cibernetico, si strutturano e prendono posizione all'interno del nuovo network di potere globale, in cui "la rete agisce, per contagio, a un comportamento individuale dovuto a una situazione locale"[46], determinando la facoltà di ogni nodo (attore) di modificare e influenzare il sistema. I tradizionali rapporti di reciprocità tra territorio (cyberterritorio), politica e violenza vengono mesi in discussione, dal momento che un numero maggiore di attori di diversa natura riesce ad influenzare in modo determinante i

[43] Jean C., Tremonti G., *Guerre Stellari: Società ed Economia nel Cyberspazio*, FrancoAngeli, Milano, 2000.

[44] Cfr. Aron Raymond, *Paix et Guerre entre les Nations*, Calmann-Lévy, Parigi, 1968; (trad. it Airoldi Namer F., *Pace e Guerra tra le Nazioni*, Edizioni di Comunità, Milano 1983). L'autore, spiega come per comprendere una decisione non solo sia necessario fare riferimento alla congiuntura "costituita da rapporti delle forze, circoscritti in uno spazio storico", ma "bisogna mettere in risalto i fini ai quale [l'attore] mira, la maniera in cui pensa e il modo d'agire che adotta (...)".

[45] Waltz K. N., *Theory of International Politics*, New York, Newbery Award Records, 1979; (trad. it. Narbone L., *Teoria della Politica Internazionale*, il Mulino, Bologna 1987).

[46] Menotti R., *Mondo Caos: Politica Internazionale e Nuovi Paradigmi Scientifici*, Laterza, 2010.

processi di *decision making*, storicamente condotti all'interno di ristrette gerarchie burocratiche[47].

Si trova così ampio riscontro nello schema concettuale elaborato da Schmidt che concepisce il modello c.d. di *networked governance*[48] come *default modus operandi* della governance di Internet. Egli, prendendo in considerazione le azioni degli attori (autorità statali e grandi imprese) tradizionalmente coinvolti dell'esercizio del potere all'interno del cyberspazio, fa riferimento alla graduale affermazione di un modello ibrido di network e gerarchie che si dispiegano al suo interno. Tuttavia, in base alle considerazioni mosse poc'anzi e alla precocità delle gerarchie cui Schmidt fa riferimento, sembra piuttosto legittimo affermare la prevalenza della natura reticolare su quella gerarchica. Sulla base di ciò, vale la pena evidenziare alcune delle peculiarità strettamente legate al modello di *networked governance* che influenzano i livelli di complessità e instabilità all'interno dei processi di governance, aumentandone il carattere caotico.

Innanzitutto, l'accesso e l'appartenenza a una struttura di network, rispetto ad un'organizzazione di tipo gerarchico, risultano l'uno nettamente più facile e l'altra molto più mutabile. Come già accennato, le barriere all'entrata risultano minori e dunque sono maggiormente permeabili, andando ad aumentare il ventaglio di attori che possono accedere all'arena decisionale ed esercitarvi un certo grado di potere. Sulla base dell'argomentazione mossa dallo stesso Schmidt secondo cui "an obvious prerequisite to gain influence in networks is to be part of them at first"[49] risulta facile, ad esempio, trovare riscontro in un nuovo concetto di potere a larga partecipazione privata se si considera che l'architettura del cyberspazio è sostanzialmente l'erede di coloro che

[47] Cfr Nye J. S., *The Future of Power*, Public Affairs, New York, 2011. L'autore, secondo uno schema concettuale preciso, analizza le varie dinamiche che si svolgono all'interno del cyberspazio (intracyberspace) e al suo esterno (extracyberspace), attraverso l'utilizzo di *information instruments* e *physical instruments* da parte di diversi attori, sia in termini di soft power che in termini di hard power. In termini di soft power, nuovi attori risultano capaci di esercitare potere di persuasione e attrazione, organizzare campagne di sensibilizzazione o diplomazia pubblica al fine di smuovere l'opinione delle masse, così come influenzare la composizione e l'organizzazione delle agende politiche.

[48] Schmidt A., *Hierachies in Networks: Emerging Hybrids of Neyworks and Hierarchies for Producing Internet Security*, in Kremer J.-F. e Müller B., *Cyberspace and International Relations. Theory, Prospects and Challenges*, Springer Verlag Berlin Heidelberg 2014. L'autore definisce la *networked governance* come una "semi-permanent, voluntary negotiation system that allows interdependent actors to opt for collaboration or unilateral action in the absence of an overarching authority". Egli analizza le implicazioni del modello di networked governance con riferimento specifico all'azione degli attori (autorità statali e grandi imprese) tradizionalmente incaricati di fornire la sicurezza di Internet ed esercitare il potere, in termini generali, all'interno del dominio cibernetico.

[49] *Ibidem.*

hanno inizialmente dato forma e dimensione ai diversi *layers*[50] che lo compongono[51].

La struttura, dunque, in termini di esercizio del potere, risulta fortemente decentralizzata e piuttosto piatta, anche se non si realizza una condizione di assoluta parità di poteri tra i vari attori. I processi decisionali basandosi spesso sul consenso e l'accordo delle parti, rischiano di divenire lenti, macchinosi e complicati; ciò, nonostante la velocità e il carattere simultaneo dei processi che si verificano all'interno del cyberspazio richiedano l'elaborazione di risposte tempestive, se non istantanee. Le relazioni tra le unità della struttura e dunque tra gli attori presenti nel cyberspazio, si basano sulla fiducia, che tuttavia, risulta particolarmente difficile da costruire in un tale ambiente non solo tra stati, ma anche e soprattutto quando ad entrare in gioco sono attori di diversa natura e razionalità.

E' chiaro dunque, come il progressivo decadimento di una struttura internazionale di potere verticalmente e rigidamente organizzata abbia lasciato spazio a una struttura reticolare più fluida, dinamica, variabile, incerta e caotica. Questa, seppure rispecchi una maggiore adattabilità, necessaria e funzionale alla rapida evoluzione del progresso tecnologico e alle logiche della nuova geografia virtuale, tuttavia, costituisce anche la fonte di nuove asimmetrie, complessità e paradossi, richiamando così le logiche e le dinamiche che legano il caos alle reti.

4. Violenza: asimmetrie e paradossi

I nuovi attori che entrano a far parte dell'arena internazionale, non solo sono in grado di alterare i processi di *decision making*, ma riescono

[50] Il cyberspazio può essere strutturato secondo quattro layers (strati). Secondo la divisione elaborata da Choucri e Clark, oltre al *physical layer* (si veda nota n. 20), il cyberspazio si compone dei c.d. *logical layer*, *information layer* e il *layer* composto dagli utenti. Per una spiegazione dettagliata sui *layers* si rimanda a Choucri N., Clark D., *Cyberspace and International Relations: Toward an Integrated System*, ECIR review, August 2011. Si faccia riferimento, in particolare al cap. 3, pp. 8-13.

[51] "I servizi, le applicazioni, i motori di ricerca, le piattaforme, le caselle mail, i social network sono creati da aziende diventate enormi grazie al successo ottenuto. Le regole e gli standard, i capisaldi che rendono possibile l'interoperabilità tra i sistemi, invece, vengono dal mondo dei consorzi, enti e istituti, spesso attori pubblico-privati che si sono imposti agli albori e che il mondo ha accettato". Cit. Lozito N., *Cybervestfalia*, in A Che Servono i Servizi, Limes 7/2014. Si segnalano, in particolare, le americane Microsoft, Cisco, Comcast, AT&T, Google, l'IETF e ICANN. Si rimanda per una spiegazione dettagliata a Choucri N., Clark D., *Cyberspace and International Relations: Toward an Integrated System*, ECIR review, August 2011; con particolare riferimento al cap. 3, pp. 14-19.

anche a mettere in discussione il monopolio della violenza che, tradizionalmente, è rimasta una prerogativa esclusiva degli stati. Entriamo ora, in pieno, nella c.d. dimensione di incubo. "Tutto il nostro progresso tecnologico lodato - la nostra stessa civiltà - è come la scure in mano del criminale patologico"[52] scriveva Albert Einstein nel 1917. Queste parole, scritte dal premio Nobel per la fisica in una lettera indirizzata ad un amico, risultano oggi altamente esplicative delle conseguenze derivanti dal c.d. processo di *spin-in* dal civile al militare[53], concretizzatosi grazie all'avvento di tecnologie *dual-use*, per cui strumenti civili divengono strumenti di valore strategico-militare di facile accesso e notevole potenziale. La questione risulta piuttosto differente rispetto a ciò che si verificava durante il periodo della guerra fredda, in cui, al contrario, le tecnologie militari erano sviluppate specificatamente per applicazioni belliche e, solo in secondo luogo trovavano risvolti nell'ambito civile[54].

La natura di "incubo" risiede, qui, in un'effettiva propagazione delle minacce attraverso mezzi e strumenti messi a disposizione dalla moderna tecnologia sviluppatasi in ambito civile, che può facilmente acquisire il potenziale di arma e divenire la "scure" sopracitata, utilizzata da criminali, hackers o terroristi, così come da entità statuali come strumento per il perseguimento dei propri interessi strategici. La potenza industriale può e di fatto viene trasformata in potenza militare in modo molto rapido, comportando un abbassamento notevole della soglia di accesso alla violenza, per cui sia gli stati che gli attori di natura non-statale acquisiscono nuove capacità in termini di *hard power*, attraverso cui sono in grado di causare l'interruzione di intere società, così come creare danni in termini di distruzione fisica. Una stringa di dati malevoli, ad esempio, se introdotta in un sistema di gestione di *public utilities* o di un network di trasporto pubblico, potrebbe provocare danni a persone e cose, equiparabili a quelli conseguibili attraverso l'uso delle armi tradizionali[55].

---

[52] Cit. ripresa da Sven Sakkov, Direttore del Cooperative Cyber Defence Centre of Excellence della NATO, in Anna-Maria Osula and Henry Rõigas (Eds.), *The Nature of International Law Cyber Norms*, in *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications, Tallinn 2016.

[53] Jean C., Tremonti G., *Guerre Stellari: Società ed Economia nel Cyberspazio*, FrancoAngeli, Milano, 2000.

[54] *Ibidem.*

[55] Massolo G., *L'Italia di Fronte alle Sfide di Sicurezza dello Spazio Cibernetico*, in Gori U., Lisi S. (a cura di), *Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013.

Il cyberspazio riduce il differenziale di potenza non solo tra attori statali, ma anche tra attori statali e non, andando a delineare le geometrie perverse di un nuovo *playing field* senza precedenti nella storia, in primis, sulla base del fatto che nel mondo virtuale "a single virtual offense is almost cost free"[56]. In chiave Hobbesiana, allo stato Leviatano, unico detentore della funzione di protezione del popolo (e dell'uso legittimo della forza), si oppone, oggi, l'avvento di un Behemoth globale: portatore di uno stato di guerra di tutti contro tutti; *driver* di un ritorno ad una condizione che si avvicina allo "stato di natura" originario. Individui o gruppi organizzati spesso in forma di network sia pubblici che privati (hackers, attivisti o terroristi) sono in grado di realizzare attacchi DDoS[57], compromettere i sistemi SCADA[58] delle moderne infrastrutture attraverso l'utilizzo di malware, effettuare intrusioni e furti di dati e informazioni a danno di attori privati, governi e apparati militari, così come organizzare veri e propri network dediti al cyberspionaggio[59]. Un hacker, seduto davanti a uno schermo situato ovunque, può attaccare sistemi che si trovino ugualmente ovunque nel mondo; interrompere le loro funzioni; danneggiare le informazioni che si trovano al loro interno e gli algoritmi che ne governano il funzionamento; addirittura, egli può arrivare a distruggerli fisicamente attraverso il danneggiamento dei sistemi di comando.

Entra in gioco, così, uno dei paradossi di maggiore rilevanza che si dispiega in relazione al dominio cibernetico per cui, anche gli attori tradizionalmente più deboli (statali e non) possono ora influenzare, se non addirittura minacciare i più forti. Alla base di questo paradosso si colloca, in primis, l'elevata vulnerabilità dei paesi più tecnologicamente avanzati che deriva dalla pervasività dei mezzi di *Information Communication Technology* nelle società odierne e, in particolare, dalla

[56] Nye J. S., *The Future of Power*, Public Affairs, New York, 2011.
[57] I DDoS (Distributed Denial of Service) sono attacchi che si realizzano tramite la costruzione di reti di botnet, costituite da computer infettati detti anche zombie, i quali vengono guidati al fine di attaccare simultaneamente la rete internet di un target, andando a comprometterne il funzionamento. Esempi di attacchi di questo tipo risalgono a quelli subiti dall'Estonia nel 2007 e dalla Georgia nel 2008.
[58] I sistemi SCADA (Supervisory Control And Data Acquisition) sono sistemi informatici utilizzati per il monitoraggio elettronico di sistemi fisici. Essi vengono tipicamente utilizzati per il controllo e monitoraggio di infrastrutture e processi industriali. Proprio attraverso l'alterazione dei comandi trasmessi dal sistema SCADA, tramite l'inserimento di un virus informatico chiamato Stuxnet, fu realizzata la distruzione di gran parte delle centrifughe utilizzate per l'arricchimento dell'uranio all'interno del programma nucleare iraniano. Si veda Mugnato N., *L'Analisi Tecnologica delle Cyber Weapons per lo Sviluppo della Cyber Resilience*, in Gori U., Lisi S. (a cura di), *Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013.
[59] Nye J. S., *The Future of Power*, Public Affairs, New York, 2011.

complessa interdipendenza che si delinea tra questi, i sistemi militari, economici e le infrastrutture critiche dei paesi. Se tramite il cyberspazio, la possibilità di sganciare bombe non è reale, l'impatto derivante dall'utilizzo di armi cibernetiche potrebbe risultare altrettanto devastante. La valenza centrale di tale dominio, infatti, risiede nel suo essere l'infrastruttura critica per eccellenza da cui dipendono i sistemi di attacco e difesa degli Stati, nonché l'integrità degli interi Sistemi Paese. La natura critica delle minacce cibernetiche risiede, inoltre, nell'elevato potenziale di contagio derivante dalla struttura reticolare e interconnessa del cyberspazio.

Risulta chiaro, dunque, come venga a concretizzarsi un *trade-off* tra informatizzazione (sviluppo tecnologico e utilizzo delle reti) e sicurezza, per cui, secondo una logica alquanto paradossale, il potere diviene non solo fonte di forza (accesso alle informazioni e moltiplicatore della potenza convenzionale) ma anche fonte di debolezza. Se paesi come gli Stati Uniti, la Cina, la Russia, il Regno Unito e la Francia risultano essere detentori di maggiori capacità rispetto ad altri, tuttavia, all'interno del cyberspazio ha poco senso parlare di dominio in termini simili a quelli di potenza navale o aerea[60], per cui gli attori più tecnologicamente avanzati divengono anche i più vulnerabili. Nel campo delle relazioni internazionali si avverte, quindi, uno sconvolgimento totale delle logiche di potere e di influenza che va a vantaggio degli attori apparentemente e tradizionalmente più deboli.

Nella realtà attuale, ampiamente dominata dallo spazio cibernetico si rileva quindi la fondatezza del ragionamento di Jervis secondo cui, nel momento in cui un approccio o una via diretta fallisce al conseguimento di un obiettivo, una strada più indiretta potrebbe invece rivelarsi di successo[61]. Di fatto, dato che il cyberwarfare è divenuto a tutti gli effetti un modo di fare guerra, sfruttando la sua essenza profondamente asimmetrica, nazioni più deboli in termini di potenza convenzionale hanno la possibilità di investire in questo settore, al fine di colmare i gap che li distanziano da quelle tradizionalmente più forti. Il potere non è più un fattore tangibile e sembra ritorcersi contro coloro che lo detengono[62]. Lo scontro diretto tramite l'uso della forza fisica, teorizzato da Clausewitz, non corrisponde più necessariamente all'ideale di guerra

[60] Nye J. S., *The Future of Power*, Public Affairs, New York, 2011.
[61] Jervis R., *System Effects: Complexity in Political and Social Life*, Princeton University Press, 1997.
[62] Si veda, a tale riguardo, il cd. paradigma della guerra netcentrica illustrato da Pistoia D., *La Guerra Elettronica nella Quinta Dimensione*, in Gori U., Lisi S. (a cura di*), Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013.

attuale. Piuttosto, si apre oggi la possibilità di realizzare la sottomissione del nemico senza doverlo combattere, come scriveva Sun Tzu 2500 anni fa[63]. Addirittura, secondo Libicki, il quale si riferisce alla guerra cibernetica come *confidence game*, lo sviluppo di capacità cibernetiche offensive assume un valore altamente strategico anche in assenza della loro concreta manifestazione, ma semplicemente grazie all'impatto che questo esercita sulla triade formata da *fear*, *uncertainty* and *doubt* (FDU) in relazione all'affidabilità dei propri sistemi. "The persistent presence of a cyberwar capability, if irritating enough, serves to taunt institutions"[64].

Ci si chiede, alla luce di questo paradosso, se si possa parlare di una rivincita degli Stati che, tramite la costruzione di nuovi concetti e modalità di warfare, tentano di bypassare la supremazia dei più forti, in particolare degli Stati Uniti. Non è più dato per certo che il più debole debba necessariamente soccombere al più forte. E sulla base di ciò, fino a che punto si può allargare l'orizzonte della questione fino ad arrivare a parlare di una rivincita degli individui?

5. Strategie

5.1 Civilizzazione della guerra

Se dunque le armi privilegiate divengono quelle cibernetiche e gli obiettivi primari le infrastrutture critiche dei paesi, è chiaro che si assiste ad un altro stravolgimento: quello dei concetti di arma e campo di battaglia che comporta l'offuscamento della distinzione netta esistente tra civile e militare. Questa distinzione viene meno relativamente agli obiettivi, agli aggressori e alle responsabilità legate al mantenimento della sicurezza e della difesa. In termini di obiettivi il cyberspace diviene il nuovo "centro di gravità" Clausewitziano[65], il nuovo "centro vitale del nemico" di Douhet, la cui distruzione porta all'interruzione della società e alla compromissione dell'abilità di muovere guerra da parte del

[63] Geers, K., *Sun Tzu and Cyber War*, Cooperative Cyber Defence Centre of Excellence, February 9 2011.
[64] Libicki M. C., *Cyberwar as a Confidence Game*, Strategic Studies Quarterly, Spring 2011, Vol.5(1), pp. 132-146.
[65] Greathouse C. B., *Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?*, in Kremer J.-F. e Müller B., *Cyberspace and International Relations. Theory, Prospects and Challenges*, Springer-Verlag Berlin Heidelberg 2014.

nemico[66]. L'interdipendenza che si è generata nel campo dell'informazione rende quasi impossibile separare il governo dalle componenti civili. Basta pensare che negli Stati Uniti più del 98% delle informazioni governative scorrono attraverso mezzi di comunicazione civili[67]. Gli obiettivi sensibili della guerra cibernetica finiscono per essere tanto militari quanto civili, coinvolgendo interi Sistemi Paese: "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"[68].

L'interdipendenza tra i due mondi, inoltre, non è il solo fattore critico, laddove l'adozione di approcci focalizzati, che permettono di non imporre ripercussioni significative sulla popolazione civile, comporti spesso elevati livelli di difficoltà e di costi. Le risorse necessarie per la creazioni di virus e armi informatiche in grado di colpire esclusivamente target ben definiti e limitati, spesso, potrebbero andare ben oltre quelle a disposizione degli attori, mentre invece, la realizzazione di attacchi di impatto generale possono facilmente risultare più effettivi sia in termini di risultati che in termini di costi. Altro fattore di cui tenere conto in merito, risiede nella natura più o meno razionale degli aggressori. Se infatti, uno stato potrebbe rivelare la propensione a compiere attacchi mirati, sulla base di dettami etici e morali, ciò potrebbe non non essere vero per altri generi di attori che, anzi, potrebbero vertere di proposito verso la realizzazione di attacchi che coinvolgano anche la popolazione civile. Si assiste dunque, a una "civilizzazione della guerra nel senso peggiore del termine; una guerra civile perché civili sono gli obiettivi strategici che gravitano all'interno dell'ambiente cibernetico."[69] La pervasività dello spazio cibernetico e dei mezzi e strumenti messi a disposizione dalla tecnologia trasforma parte delle interazioni quotidiane della società civile globale in un campo di battaglia, in cui i

[66] *Ibidem*. L'autore spiega come Douhet, a differenza di Clausewitz che teorizzava azioni mirate contro obiettivi militari, considera i centri vitali del nemico l'industria e le strutture chiave che permettono ad uno stato di funzionare. Perciò, già in termini di potere aereo, la distruzione di questi centri vitali non permetteva di fare distinzione tra combattenti e non combattenti. Distinzione che viene a mancare anche all'interno dello spazio cibernetico.

[67] *Ibidem.*

[68] Cit. del Generale Keith B. Aleksander, Comandante dello U.S. Cyber Command, ripresa da Martino L., *La Quinta Dimensione della Conflittualità. La rilevanza strategica del Cyberspace e i Rischi di Guerra Cibernetica*, CSSII - Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università degli Studi di Firenze.

[69] Martino L., *La Quinta Dimensione della Conflittualità. La rilevanza strategica del Cyberspace e i Rischi di Guerra Cibernetica*, CSSII - Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università degli Studi di Firenze.

civili rischiano di divenire non solo i bersagli, ma anche i coautori degli attacchi, in modo del tutto involontario e inconsapevole[70].

Dunque, acquista sempre maggiore legittimità il concetto di sicurezza c.d. "condivisa" (tra settore pubblico e privato), sulla base del quale gli stati si trovano a dover cooperare con altri attori al fine di garantire la protezione all'interno del dominio cibernetico, così come nella realtà fisica, vista l'interazione tra i due mondi. E d'altronde, in termini di potere la questione risulta tutt'altro che irrilevante se si da ascolto al monito di Carl Schmitt secondo cui "colui che non ha il potere di proteggere l'altro, non ha nemmeno il diritto di esigerne l'obbedienza"[71]. Ritorna, in questo caso, l'utilità del concetto di *networked governance* di Schmidt[72], il quale afferma l'esistenza di una dipendenza della sicurezza di Internet da un *networked approach*, per cui nell'ambito della sicurezza e della difesa non si può più ragionare soltanto in termini strettamente militari, ma piuttosto urge la necessità di adottare nuovi approcci di tipo olistico che non escludano la componente civile come parte attiva nell'elaborazione e, allo stesso tempo, come destinataria delle nuove strategie.

5.2 Incertezza

Se Robert Jervis, riferendosi alla complessità del sistema internazionale, individua il limite della conoscenza umana come una delle maggiori vulnerabilità[73], lo stesso ragionamento si può riportare facilmente anche all'interno del dominio cibernetico. E, anzi, la sua valenza acquista un carattere ancora più determinante in questo ambiente dove la difficoltà di elaborazione degli scenari risulta già notevolmente complicata dalle sue caratteristiche geografiche.

---

[70] É possibile, ad esempio, che un utente sia completamente ignaro del fatto che il computer di cui fa uso sia parte di una rete botnet, una rete comandata a distanza ed utilizzata per scopi illegali come la distribuzione di spam, la realizzazione di attacchi DDoS, furto di dati o supporto di memorizzazione per contenuti illegali. Per una spiegazione più dettagliata sul funzionamento delle reti botnet si rimanda a http://www.antibot.it/it/content/cosa-sono-le-botnet

[71] Cit. ripresa da Joxe A., *L'Empire du Chaos*, Editions La Découverte & Syros, Paris 2002; (trad. it. Guareschi M., Grimaldi C., *L'Impero del Caos: Guerra e Pace nel Nuovo Disordine Mondiale*, a cura di Dal Lago A. e Palidda S., RCS Libri, Milano 2003).

[72] SchmidtA., *Hierarchies in Networks: Emerging Hybrids of Networks and Hierarchies for Producing Internet Security*, in Kremer J.-F. e Müller B., *Cyberspace and International Relations. Theory, Prospects and Challenges*, SpringerVerlag Berlin Heidelberg 2014.

[73] Jervis R., *System Effects: Complexity in Political and Social Life*, Princeton University Press, 1997.

All'interno del cyberspazio, si apre per gli attori la possibilità di agire ed dunque anche di muovere veri e propri attacchi in totale anonimato, data l'impossibilità di risalire in modo praticamente certo alla loro geolocalizzazione e dunque identità. I metodi e gli strumenti di indagine come il tracciamento a ritroso delle fonti degli attacchi risultano purtroppo inutili e vanificati nel momento in cui è possibile far rimbalzare gli attacchi attraverso un ampio numero di portali, realizzarli attraverso l'uso dei servizi di macchine innocenti, oppure saltando sulla connessione Wi-Fi di terzi. Basta pensare, a tale riguardo, agli attacchi di tipo DDoS la cui realizzazione avviene tramite il protocollo di trasporto UDP che "non necessita di instaurare una connessione tra l'attaccante e la vittima"[74], con la risultante che le uniche macchine che si rivelano responsabili dell'attacco sono quelle compromesse e non quella utilizzata originariamente da chi attacca. Non c'è da stupirsi, quindi, se la provenienza degli attacchi mossi all'Estonia nel 2007[75] sia fatta risalire a server di computer americani.

Nonostante l'analisi dei contesti strategici possa risultare di notevole aiuto per uscire, almeno in parte, dall'ombra dell'ignoto, all'interno del dominio cibernetico emerge un problema reale di attribuzione, data l'impossibilità di raggiungere uno stato di certezza che vada oltre ogni ragionevole dubbio, che permette agli autori degli attacchi di "trincerarsi dietro alla c.d. *plausible deniability*[76]" (negazione plausibile). "Dobbiamo dunque prepararci innanzitutto a non sapere dove e quando (e da chi...) saremo attaccati"[77], e dunque a gestire quella preoccupazione grave e continua, tormentosa ed assillante che l'incubo dell'ignoto porta con sé.

L'effettiva possibilità di agire in totale anonimato rende complicato per gli attori comprendere chi sono i propri nemici e di conseguenza i propri

[74] Muscas, G., *The Unbearable Lightness of DDoS*, in Gori U. Lisi S. (a cura di), *Information Warfare 2015. Manovre Cibernetiche: Impatto sulla Sicurezza Nazionale*, FrancoAngeli, Milano, 2016.

[75] Nel 2007 l'Estonia, è stata colpita da una forte ondata di attacchi informatici di tipo DDoS che hanno intasato il traffico IP di siti bancari, agenzie governative e media nazionali, causando una forte interruzione di alcuni servizi al pubblico e di fatto, riuscendo ad immobilizzare il paese. Per un'analisi dettagliata dell'attacco si rimanda a Davis J., *Hackers Take Down the Most Wired Country in Europe*, Wired, August 21 2007. (Disponibile a http://www.wired.com/2007/08/ff-estonia/).

[76] Martino L., *La Quinta Dimensione della Conflittualità. La rilevanza strategica del Cyberspace e i Rischi di Guerra Cibernetica*, CSSII - Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università degli Studi di Firenze. L'autore spiega che il termine sia stato coniato dalla Central Intelligence Agency (CIA) nel periodo dell'Amministrazione Kennedy, con lo scopo di permettere ai dirigenti politici di negare il loro coinvolgimento nelle operazioni realizzate contro individui ritenuti pericolosi per l'interesse nazionale.

[77] Massolo G., *L'Italia di Fronte alle Sfide di Sicurezza dello Spazio Cibernetico*, in Gori U., Lisi S. (a cura di), *Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013.

alleati. Per cui, anche la classica dicotomia alleato-nemico, che ha tradizionalmente regolato gli schieramenti e le alleanze all'interno delle relazioni internazionali, sembra venire meno, fungendo così da carburante per speculazioni, ambiguità e incertezze che incidono sulla probabilità di equivoci ed errori di calcolo tra gli Stati, i quali sembrano condannati a muoversi sulla base disospetti piuttosto che sull'effettiva sostanza della realtà.

Ragionando in termini di guerra cibernetica, risulta evidente come i concetti classici di rappresaglia e deterrenza vengano totalmente compromessi, essendo entrambi dipendenti dalla capacità di attribuire l'attacco ad un attore ben preciso. Nel corso del Summit di Newport (Galles) del 2014, la NATO ha approvato l'*Enhanced Cyber Defence Policy*, rendendo chiara la possibilità per gli stati membri dell'alleanza di invocare l'applicazione dell'Art. 5 del North Atlantic Treaty, relativo alla *collective self-defense*, anche nel caso di cyber attacchi che abbiano effetti paragonabili a quelli risultanti da attacchi di tipo convenzionale. La possibilità effettiva di rappresaglia, regolata anche in seno all'alleanza, tuttavia, incontra il limite pratico dell'attribuzione. Nel caso in cui, l'attacco subito dall'Estonia nel 2007 avesse comportato conseguenze atte a giustificare l'applicazione dell' Art. 5, contro chi l'eventuale rappresaglia avrebbe dovuto essere mossa vista l'impossibilità di identificare l'esatta provenienza degli attacchi e l'identità del nemico?[78]

Il classico modello di deterrenza grazie al quale è stato possibile evitare lo scontro totale durante l'era nucleare sembra cadere di fronte alle logiche proprie del dominio cibernetico. Ciò, anche in ragione del fatto che in tale contesto viene a mancare quella "difficoltà psicologica delle parti contrapposte (…) a superare il punto di non ritorno"[79]. Non è più possibile, oggi, fare affidamento su questa ancora di salvezza dallo scontro, dal momento che lo spazio cibernetico risulta popolato anche da attori totalmente irrazionali: "lo stesso ISIS dichiara l'intenzione di acquisire capacità cibernetiche distruttive"[80]. In relazione a ciò, dunque,

[78] Nonostante il Presidente Estone abbia formalmente accusato la Russia di aver favorito e dato appoggio logistico agli autori dell'attacco e nonostante la consapevolezza generale in seno all'alleanza di un coinvolgimento russo, le accuse non sono mai state accertate in toto, né formalmente sostenute.

[79] Gori U., *Manovre nel Cyberspazio: Prospettive*, in Gori U. Lisi S. (a cura di), *Information Warfare 2015. Manovre Cibernetiche: Impatto sulla Sicurezza Nazionale*, FrancoAngeli, Milano, 2016.

[80] *Ibidem.*

anche il modello c.d. di *deterrence by denial*[81], basato sull'utilizzo di sistemi di difesa attiva[82] col fine di rendere minimo il beneficio ottenibile da un attacco andando a scoraggiarne la realizzazione, cade di fronte all'irrazionalità totale di alcuni attori, i quali, secondo una logica che esula da quella tipica degli stati, sono disposti a trarre minimi guadagni e persino ad arrecare danni a se stessi. La deterrenza, all'interno del cyberspazio, dunque, non può più basarsi su semplici logiche di rappresaglia e, di fronte alla validità soltanto parziale di sistemi di difesa attiva, richiede di affiancare a questi delle strutture che siano altamente resilienti e flessibili.

Riferendosi all'identità ambigua dell'autore di un attacco, Libicki[83] parla, in termini generali, di *non-obvious warfare*, una categoria in cui annovera la stessa *cyberwarfare*, così come l'*electronic warfare* e i *proxy attacks*, rendendo chiara l'analogia tra questi ultimi e gli attacchi cibernetici, proprio per la presenza in entrambe le tipologie di una forma di anonimato dell'attaccante. Riferendosi ai proxy attacks egli chiarisce, infatti, come l'attribuzione divenga particolarmente difficile "because it generally requires the perpetrators be caught (…) but mostly because it requires tying the perpetrator to a major actor"[84]. A tal proposito, in una realtà in cui la guerra quale strumento della politica internazionale è divenuta moralmente inaccettabile e praticamente impossibile almeno tra le potenze maggiori, l'utilizzo della forza per procura diviene un mezzo che riveste un particolare *political appeal*[85] per gli Stati. Se a ciò, oltre ai costi minori in termini economici, si aggiunge la possibilità per gli Stati di una maggiore garanzia di poter nascondere la loro identità come garantito dagli strumenti del dominio cibernetico, allora è facile immaginare un futuro in cui guerre combattute da "proxy servers"[86] avranno la meglio su guerre combattute da "proxy forces"[87], andando a concretizzare realmente tutte le criticità cui si è fatto riferimento.

---

[81] Gori U., *Cyberspazio e Relazioni Internazionali: Implicazioni Geopolitiche e Geostrategiche*, in Gori U., Lisi S. (a cura di), *Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013.

[82] "If firewalls are strong, or the prospect of a self enforcing response seems possible ("an electric fence"), attack becomes less attractive". Nye J. S., *The Future of Power*, Public Affairs, New York, 2011.

[83] Libicki M. C., *The Specter of Non-obvious Warfare*, Strategic Studies Quarterly, Fall 2012, Vol.6(3), pp. 88- 101.

[84] Libicki M. C., *The Specter of Non-obvious Warfare*, Strategic Studies Quarterly, Fall 2012, Vol.6(3), pp. 88- 101.

[85] Mumford A., *Proxy Warfare and the Future of Conflict*, The RUSI Journal, 158:2, 40-46, 28 April 2013, DOI: 10.1080/03071847.2013.787733.

[86] *Ibidem.*

[87] *Ibidem.*

L'incertezza, dunque, come la già citata l'imprevedibilità, entra anch'essa dirompente nelle logiche che regolano i rapporti politico-strategici tra gli attori dello scenario internazionale ed evidenzia notevoli probabilità di espansione in futuro, andando a complicare il quadro generale e le capacità di comprensione e di azione degli attori all'interno del sistema. Lo scenario complessivo sembra dunque assomigliare a quello del campo di battaglia descritto da Clausewitz, in cui "ogni azione si compie in un certo senso in una luce crepuscolare che spesso come un chiarore di nebbia o di luna dà alle cose un contorno esagerato, un aspetto grottesco. Ciò che questa debole luce fa mancare alla visione completa deve essere suggerito dal talento o deve essere lasciato alla fortuna."[88] In ragione degli aspetti critici e dell'importanza che il cyberspazio riveste a livello strategico, risulta plausibile forse propendere verso il talento piuttosto che la fortuna. Un talento che merita di essere sviluppato attraverso forme di cooperazione e canali di *information sharing* tra stati, i quali permangono i più autorevoli nodi del network mondiale e con un ampio coinvolgimento del settore privato, attraverso la realizzazione di Public-Private Partnership, e dei gruppi di esperti[89]. Ciò, col fine principale di costruire una solida fiducia tra attori (statali e non), garantire la migliore resilienza ed elasticità dei sistemi possibile e ridurre la "nebbia" che quotidianamente incombe sul paesaggio cibernetico.

Conclusioni
- cybercaos –

Il cyberspazio può dunque essere concepito come cybercaos: spazio infinito, in cui i centri di potere si trovano ovunque, ma in confini da nessuna parte; privo di senso, o meglio, di regole solide e condivise che lo governino; instabile in quanto caratterizzato da grande dinamismo, mutamenti repentini e dinamiche di interdipendenza; imprevedibile,

[88] Cfr. Rusconi G. E. (a cura di), *Carl von Clausewitz: Della Guerra*, Einaudi, Torino, 2000. Si rimanda, in particolare, al Libro Secondo, *La Teoria della Guerra*, pp. 87.

[89] L'importanza di esperti risulta chiara dall'episodio raccontato da Ramo, in cui il programmatore DanKaminsky dopo aver scoperto una grave falla all'interno del sistema DNS (Domain Name Service), insieme a numerosi altri importanti informatici del web (ingegneri e hacker "white hat") fu in grado di riparare la falla in un tempo decisamente breve rispetto a ciò che i governi o le grosse società avrebbero potuto fare. Per una spiegazione dettagliata si rimanda a Ramo J. C., *The Age of Unthinkable. Why the New World Disorder Constantly Surprises Us and What We Can Do about It*, Little, Brown and Company, 2009; (trad. it Alba F., *Il Secolo Imprevedibile. Perché il Nuovo Disordine Mondiale Richiede una Rivoluzione del Pensiero*, Elliot Edizioni, Roma, 2009), pp. 245-250.

alla luce della sua natura "dromologica" e dell'istantaneità che domina al suo interno; irrazionale, in quanto dominato da logiche paradossali che rendono la guerra ampiamente civilizzata e ostaggio di nuovi attori non-razionali, che divengono i nuovi co-protagonisti del gioco mondiale; incomprensibile, vista la difficoltà di comprendere l'ambiente che si rileva in seno agli attori, in relazione tanto alla nuova "geografia virtuale", quanto al fattore dell'anonimato.

All'interno del cyberspazio, il potere si organizza secondo un modello che tende più verso una *networked governance* piuttosto che una struttura rigida di gerarchie verticali. Sebbene, dunque, esso sia portatore di un maggior grado di instabilità, dinamicità e caoticità all'interno di una realtà che è già caotica, l'imposizione di un ordine tramite la realizzazione di una "cybervestfalia"[90] andrebbe a comprometterne la natura libera, aperta e globale e con ciò, la sua essenza originaria di motore del progresso e della crescita dell'intero sistema mondiale.

Come ricorda Joxe nel suo libro, *L'impero del caos: guerra e pace nel nuovo disordine mondiale*, i periodi di disordine e caos hanno tradizionalmente scandito la storia in "cicli di decomposizione-ricomposizione del potere". Tuttavia, l'autore sottolinea un fattore di novità in relazione a questo andamento storico che si rispecchia perfettamente nello scenario descritto in merito allo spazio cibernetico. "Il problema principale del caos contemporaneo", egli scrive, "è che l'umanità, forse per la prima volta affronta un oceano di disordine senza un'implicita finalità ordinatrice. Ci troveremo quindi di fronte (...) a un sempre rinnovato disordine, in quanto l'ordine proposto dall'alto (...) è quello di obbedire al grande impero del caos". Ciò, si rivela particolarmente veritiero se si considerano tutte le conseguenze che la pervasività del dominio cibernetico comporta in termini di esercizio del potere, processi decisionali, accesso alla violenza e strategie di sicurezza e difesa.

Oggi, diventa necessario essere in grado di gestire il caos intrinseco allo spazio cibernetico, trasformando i rischi in opportunità, così come hanno saputo fare attori tradizionalmente e convenzionalmente più deboli, i quali hanno fatto dell'instabilità una nuova norma, cogliendo il caos come opportunità, arma e risorsa strategica. In una realtà in cui ad essere vincenti non sono tanto gli attori potenti in termini convenzionali, quanto quelli più elastici, malleabili e versatili, viene naturale trovare

[90] Lozito N., *Cybervestfalia*, in A Che Servono i Servizi, Limes 7/2014.

riscontro nell'esaltazione che Ramo fa della "capacità creativa e innovativa" di Hezbollah che, nel condurre lo scontro contro l'esercito Israeliano, di per sé altamente asimmetrico, ha fatto del caos il principio dinamico che gli ha permesso di progettare e realizzare l'impossibile[91].

All'interno di una realtà che si rivela strutturalmente instabile e al cui interno il potere diviene debolezza, l'imprevedibile diviene inevitabile e l'ignoto un vincolo paralizzante, l'accettazione dei nuovi paradigmi dettati dal caos intrinseco e allo stesso tempo funzionale ad essa e dunque, l'elaborazione di soluzioni innovative quali, la promozione della resilienza che prende il sopravvento sui concetti di difesa e resistenza, così come l'adozione di approcci olistici che permettano di abbracciare la complessità del sistema e lo sviluppo di una forma mentis che tenga conto di effetti indiretti e imprevedibili, si rivelano quale unica opzione disponibile al fine di esaltare i desideri e reprimere gli incubi.

[91] Ramo J. C.,*The Age of Unthinkable. Why the New World Disorder Constantly Surprises Us and What We Can Do about It*, Little, Brown and Company, 2009; (trad. it Alba F., *Il Secolo Imprevedibile. Perché il Nuovo Disordine Mondiale Richiede una Rivoluzione del Pensiero*, Elliot Edizioni, Roma, 2009). É necessario chiarire che l'autore, nel riferirsi ai modus operandi di Hezbollah, si distacca dall'ideologia e dai metodi utilizzati dallo stesso.

Bibliografia

Aron Raymond, *Paix et Guerre entre les Nations*, Calmann-Lévy, Parigi, 1968; (trad. it Airoldi Namer F., *Pace e Guerra tra le Nazioni*, Edizioni di Comunità, Milano 1983).

Ash T.G., *As Threats Multiply and Power Fragments, the 2010s Cry Out for Realistic Idealism*, The Guardian, December 31 2009.

Choucri N., *Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences*, Massachusetts Institute of Technology, October2013.

Choucri N., *Cyberpolitics in International Relations*, The MIT Press, Massachussetts, 2012.

Choucri N., Clark D., *Who controls cyberspace?*, Bullettin of the Atomic Scientists 2013, 69:5, 21-31.

Choucri N., Clark D., *Cyberspace and International Relations: Toward an Integrated System*, ECIR review, August 2011.

Davis J., *Hackers Take Down the Most Wired Country in Europe*, Wired, August 21 2007.

Geers, K., *Sun Tzu and Cyber War*, Cooperative Cyber Defence Centre of Excellence, February 9 2011.

Gori U. Lisi S. (a cura di), *Information Warfare 2015. Manovre Cibernetiche: Impatto sulla Sicurezza Nazionale*, FrancoAngeli, Milano, 2016.

Gori U., Lisi S. (a cura di), *Information Warfare 2012: Armi Cibernetiche e Processo Decisionale*, FrancoAngeli, Milano, 2013.

Greathouse C. B., *Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?*, in Kremer J.-F. e Müller B., *Cyberspace and International Relations. Theory, Prospects and Challenges*, Springer-Verlag Berlin Heidelberg 2014.

Haas R. N., *The Age of Nonpolarity*, Foreign Affairs, May-June 2008.

Jean C., Tremonti G., *Guerre Stellari: Società ed Economia nel Cyberspazio*, FrancoAngeli, Milano, 2000.

Jervis R., *System Effects: Complexity in Political and Social Life*, Princeton University Press, 1997.

Joxe A., *L'Empire du Chaos*, Editions La Découverte & Syros, Paris 2002; (trad. it. Guareschi M., Grimaldi C., *L'Impero del Caos: Guerra e Pace nel Nuovo Disordine Mondiale*, a cura di Dal Lago A. e Palidda S., RCS Libri, Milano 2003).

Lamanna A., *Per una Geopolitica del Cyberspazio*, The Alpha Institute of Geopolitics and Intelligence, Marzo 2016.

Libicki M. C., *The Specter of Non-obvious Warfare*, Strategic Studies Quarterly, Fall 2012, Vol.6(3), pp.88-101. 26

Libicki M. C., *Cyberwar as a Confidence Game*, Strategic Studies Quarterly, Spring 2011, Vol.5(1), pp.132-146.

Libicki M. C., *The Strategic Use of Ambiguity in Cyberspace*, Military and Strategic Affairs Vol.3, December 2011, pp.3-10.

Lozito N., *Cybervestfalia*, in A Che Servono i Servizi, Limes 7/2014.

Martino L., *La Quinta Dimensione della Conflittualità. La rilevanza strategica del Cyberspace e i Rischi di Guerra Cibernetica*, CSSII - Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali, Università degli Studi di Firenze.

Mearsheimer J., *Back to the Future: Instability in Europe After the Cold War*,International Security, Vol. 15, No. 1, Summer 1990.

Menotti R., *Mondo Caos: Politica Internazionale e Nuovi Paradigmi Scientifici*, Laterza, 2010.

Mumford A., *Proxy Warfare and the Future of Conflict*, The RUSI Journal, 158:2, 40-46, 28 April 2013, DOI: 10.1080/03071847.2013.787733.

Nye J. S., *The Future of Power*, Public Affairs, New York, 2011.

Nye J. S., *The Information Revolution and American Soft Power*, Asia-Pacific Review, Vol. 9, No. 1, 2002.

Pudas T. J., Mark D. Drapeau M. D., *Technology and the Changing Character of War*, in *Global Strategic Assessment 2009: America's Security Role in a Changing World*, Edited by Patrick M. Cronin, Institute for National Strategic Studies, National Defense University Press, 2009.

Ramo J. C.,*The Age of Unthinkable. Why the New World Disorder Constantly Surprises Us and What We Can Do about It*, Little, Brown and Company, 2009; (trad. it Alba F., *Il Secolo Imprevedibile. Perché il Nuovo Disordine*

Mondiale Richiede una Rivoluzione del Pensiero, Elliot Edizioni, Roma, 2009).

Rampini F., *L'Età del Caos: Viaggio nel Grande Disordine Mondiale*, Mondadori, Milano, 2015.

Rosenau J.N.,*Distant Proximities: Dynamics Beyond Globalization*, Princeton University Press, 2003.

Rusconi G. E. (a cura di), *Carl von Clausewitz: Della Guerra*, Einaudi, Torino, 2000.

Schmidt A., *Hierarchies in Networks: Emerging Hybrids of Networks and Hierarchies for Producing Internet Security*, in Kremer J.-F. e Müller B., *Cyberspace and International Relations. Theory, Prospects and Challenges*, Springer-Verlag Berlin Heidelberg 2014.

Schmitt M. N., Vihul L., *The Nature of International Law Cyber Norms,* in *International Cyber Norms: Legal, Policy & Industry Perspectives*, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016. 27

Simon-Belli C., *Teoria della Previsione e Analisi Strategica*, Le Lettere, Firenze, 1998.

Sterner E., *Retaliatory Deterrence in Cyberspace*, Strategic Studies Quarterly, Spring 2011.

Vettore S., *Data Center, dominio del cyberspazio e declino dello Stato-nazione*, BloGlobal Osservatorio di Politica Internazionale (OPI), Research Paper n. 31, Febbraio 2015.

Vettore S., *Sistema di Comunicazione globale e Relazioni Internazionali*, BloGlobal Osservatorio di Political Internazionale (OPI), Research Paper n. 6, Novembre 2013.

Virilio Paul, *La Bombe Informatique*, Éditions Galilée, 1998; (trad. it. Piana G., *La Bomba Informatica*, Raffaello Cortina Editore, Milano, 2000).

Waltz K. N., *Theory of International Politics*, New York, Newbery Award Records, 1979; (trad. it. Narbone L., *Teoria della Politica Internazionale*, il Mulino, Bologna, 1987).

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