PAPER
APRILE 2018

LA QUINTA DIMENSIONE DELLA CONFLITTUALITÀ

-

L'ASCESA DEL CYBERSPAZIO E I SUOI EFFETTI SULLA POLITICA INTERNAZIONALE

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

-

L'ASCESA DEL CYBERSPAZIO E I SUOI EFFETTI SULLA POLITICA INTERNAZIONALE

Luigi Martino

UNIVERSITÀ DEGLI STUDI FIRENZE

Paper

Aprile 2018

RIGUARDO ALL'AUTORE

Luigi Martino 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

-

L'ASCESA DEL CYBERSPAZIO E I SUOI EFFETTI SULLA POLITICA INTERNAZIONALE

1. Introduzione

Il cyberspazio è diventato un elemento cruciale per le dinamiche politiche, sociali, finanziarie e umane del XXI secolo. Secondo i coniugi Alvin e Heidi Toffler l'attuale "era dell'informazione"[1] altro non è che il prodotto della "terza rivoluzione industriale"[2]. Infatti, la loro tesi futuristica poggia sulla concezione che la storia dell'umanità non è altro che il frutto di un'evoluzione a "ondate", di cui la "terza ondata" è il risultato del passaggio dalla rivoluzione industriale alla rivoluzione digitale. Tale rivoluzione, attraverso le moderne tecnologie interattive, è riuscita a plasmarsi velocemente a livello planetario, abbattendo così i limiti dello spazio e del tempo (Toffler e Toffler 1995)[3]. L'*Information Revolution* (teorizzata dai Toffler) ha dato vita a ciò che oggi conosciamo con il termine "spazio cibernetico", ambiente artificiale e frutto per eccellenza dell'attività umana. Proprio la natura antropica e artificiale dello spazio cibernetico ha contribuito a modellare le dinamiche delle interazioni umane e a surclassare concetti classici quali la partecipazione politica, il dibattito politico, il processo decisionale, la pace e la guerra. Proprio l'aspetto bellico (quindi politico) introduce una novità *sui generis*: l'avvenuta militarizzazione del cyberspazio ha portato all'affermazione della "quinta dimensione della conflittualità" dove tuttavia, il tipo di *armi-non militari* utilizzate per combattere, così come

[1] Per un'analisi dettagliata da un punto di vista filosofico sull'ampio concetto di *Information Age* si rinvia a Floridi 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*" (Floridi 2012, 11).

[2] Cfr. Toffler e Toffler, 1995.

[3] Per un approfondimento specifico da un punto di vista sociologico si rinvia anche a Dyson 1998.

gli obiettivi presi di mira, rende i sistemi informatici (soprattutto quelli civili) i nuovi centri di gravità da proteggere, contro un nemico che, il più delle volte, "agisce nelle ombre" in un ambiente sfumato e asimmetrico[4]. La pervasività e il rilevante impatto delle *Information and Communication Technologies* (ICTs), nonché la crescente interconnessione e interdipendenza globale raggiunta a vari livelli (politico-economico-sociale-finanziario-militare) ha fatto emergere anche un intrinseco *trade-off* tra informatizzazione e sicurezza nazionale e internazionale. Così come l'abbassamento della soglia di accesso alla violenza (dovuto in larga misura all'economicità degli strumenti informatici) e l'assenza di limiti geografici hanno causato un "affollamento" dell'arena internazionale e permesso l'ingresso ad attori (non-statali, terroristi, individui) un tempo relegati alla periferia della Comunità internazionale. La stessa caratteristica "geografica" dello spazio cibernetico ha portato alla consapevolezza che le attività sociali, le stesse relazioni intra e inter nazionali e le nuove minacce si diffondono tramite un *medium* di gran lunga più mutevole e pervasivo rispetto a tutti gli altri ambienti finora conosciuti.

2. La geografia dello spazio cibernetico tra dromologia, efemeralizzazione e geopolitica

Fin dalla metà degli anni '90 numerosi esperti hanno proposto svariate definizioni per spazio cibernetico, meglio noto con il termine anglosassone *cyberspace*[5]. Tra questi vi è Daniel T. Kuehl che descrive lo spazio cibernetico come:

[4] Cfr. Lynn 2010

[5] Secondo F. D. Kramer esistono 28 differenti definizioni del termine *cyberspace*. Cfr. Kramer, Starr, Wentz 2009. L'etimologia della parola "cyber" o "cibernetica" può essere ricollegata al termine greco κυβερνήτης e la prima attestazione si ha in Omero Iliade, XXIII, 316, in relazione al nocchiero che guida la nave battuta dai venti. Secondo Wikipedia "La radice *kyber* sta per "timone" e trova un parallelo nel latino *guber*, che ritroviamo nel gubernator, timoniere. *Kyber* e *guber* fanno evidente riferimento ad una comune progenitrice indoeuropea che significava timone. In ambedue le lingue il termine assume anche, per estensione, un significato metaforico che sta ad indicare colui che guida, o governa, una città o uno Stato: già nel greco di Platone è attestata, in questo significato più ampio di arte del governo, l'espressione *kybernetikè techne*". Tuttavia, volendo ricercare una radice etimologica della parola "cyberspace" possiamo riprendere la prima definizione storica coniata da William Gibson nel 1984 che descrive il *cyberspace* come "A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concept. A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the

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 (Kuehl 2009, 26- 28)[6].

La "peculiarità" del *cyberspace* è essenzialmente dovuta al fatto che alla sua formazione concorrono sia elementi naturali che virtuali, la cui natura "ibrida" riflette l'incertezza e l'incapacità di raggiungere una condivisione onnicomprensiva della descrizione cognitiva del termine *cyberspace*[7].

Secondo Martin C. Libicki, il *cyberspace* (a differenza degli altri domini naturali quali la terra, l'acqua, l'aria e lo spazio extra-atmosferico) è un *medium* virtuale e intangibile[8], la cui natura eterogenea – continua Libicki – è rappresentare questa realtà su tre livelli: fisico, sintattico e semantico[9].

Differentemente dalla percezione di Libicki, l'esercito statunitense pur raffigurando il cyberspace attraverso una simile triplice stratificazione, preferisce aggiungere un livello puramente "sociale" come descritto nella figura sottostante.

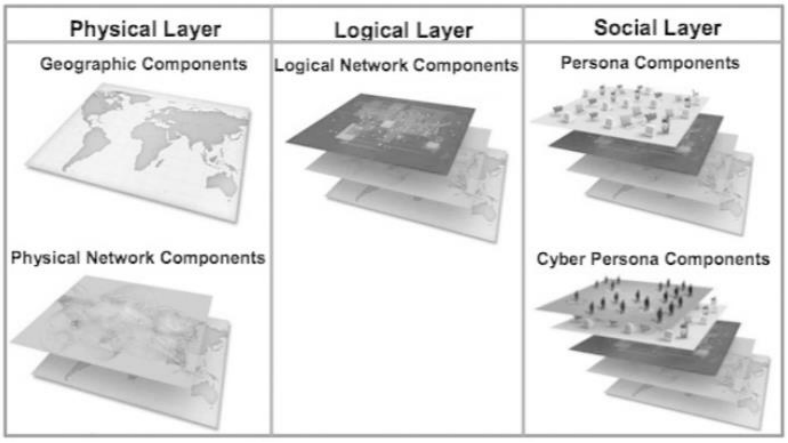

Fig. 1. Fonte: Department of the Army Headquarters, United States Army[10].

nonspace of the mind, clusters and constellations of data. Like city lights, receding", cfr. W. Gibson, *Neuromancer*, 1984

[6] Traduzione dell'autore.

[7] Cfr. Nye 2011. Tuttavia, persiste una diatriba più generale anche in merito a tutte le definizioni che includono il prefisso "cyber": *cyber terrorism, cyber war, cyber weapons, cyber operations*, ecc. Tale dibattito si inserisce anche nelle dinamiche politico-ideologiche tra chi come in "occidente" predilige il prefisso "cyber" e chi viceversa nella sfera "russofona" preferisce utilizzare il prefisso "information".

[8] Cfr. Libicki 2009. In riferimento a questo passaggio si legga: "Chapter Two: A Conceptual Framework" pp. 11-37.

[9] Cfr. Libicki 2009, 11-37.

[10] Cfr. Department of the Army Headquarters, United States Army Training and Doctrine Command 2010. Questa decisione scaturisce dalla consapevolezza che il cyberspazio, pur essendo una realtà

Secondo tale "triplice" rappresentazione, il primo strato (quello fisico) è composto dai cavi sottomarini o della rete ethernet, dai router e dispositivi di scambio dati e comunicazione. Sopra di questo vi è lo strato logico realizzato dai codici che permettono all'*hardware* di funzionare e comunicare. Il terzo strato è composto dal livello sociale che consiste nell'interazione tra gli utenti online (persone fisiche) e, sempre più spesso, tra *machine to machine*. Questi "tre livelli" vanno a costituire la prima cornice della mappatura dello spazio cibernetico. Tuttavia, l'elemento essenziale che distingue la geografia del dominio cibernetico (dalle altre realtà) è rappresentato dal suo carattere artificiale ed ibrido che, secondo quanto afferma Gregory J. Rattray: "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" (Rattray 2009). Tuttavia, cercare di descrivere un ambiente virtuale attraverso le dinamiche e i concetti degli spazi reali è un compito arduo[11]. Secondo la *National Military Strategy for Cyberspace Operations* (NMS-CO) del 2006, l'ambiente cibernetico può essere descritto attraverso l'acronimo *VUCA: Volatility, Uncertainity, Complexity, Ambiguity*[12]. Le caratteristiche peculiari del cyberspace sono essenzialmente due: la velocità di propagazione e l'abbattimento dei confini[13]. Queste sono saldamente legate alla natura "antropica" del cyberspazio, dove tutto si evolve in base alle scoperte tecnologiche e scientifiche. La staticità degli altri elementi naturali è dunque pressoché annullata da una "volubilità" continua che espande e muta la "geografia" del *cyberspace* istantaneamente, rivelando la natura *dromologica* (dinamica) dell'ambiente cibernetico[14], che insieme all'economicità dei mezzi, condiziona il rapporto di reciprocità tra territorio, interazioni sociali e dinamiche politiche. Invece, l'assenza di barriere (sia di accesso che di movimento) inclina in modo del tutto innovativo il senso spaziale delle attività umane, incluse quelle militari, ridisegnando le dinamiche del potere[15].

composta in larga misura da elementi tecnologici, rappresenta oggi un nuovo spazio delle interazioni sociali a tal punto che, in linea con questa evoluzione, si tende a paragonare l'elemento sociale come una concezione nuova del concetto storico di *agorà*.

[11] Cfr. Gray 2013.

[12] Cfr. Sherrer e Grund 2009.

[13] Cfr. Sherrer e Grund 2009.

[14] Questa definizione è stata suggerita da Paul Virilio in *La macchina che vede* (Virilio 1989), ed è stata ripresa dalla postfazione di C. Formenti a Virilio 2000.

[15] 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" Virilio 2000, 139.

La *deterritorializzazione*, l'*intangibilità*, l'*efemeralizzazione*[16] e la natura *dromologica* sono tutti elementi costitutivi dell'ambiente cibernetico che è soggetto a cambiamenti repentini ed immune da ostacoli di tipo naturale. Tuttavia, neanche il *cyberspace* si sottrae a tutte quelle dinamiche *geo* proprie dell'attività umana che modellano e influenzano il mondo reale. Così la dimensione geografica attribuita allo spazio cibernetico costringe a chiedersi se sia possibile far rientrare il *cyberspace* nella definizione di dominio naturale fino a definirlo un *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 "*placelessness*"[17]?

Le posizioni sulla classificazione dello spazio cibernetico quale *global common* sono varie[18]. A tal proposito, Colin S. Gray s'interroga sulla questione spinosa relativa alla "natura" da dover conferire a questo nuovo elemento delle odierne relazioni internazionali[19], sottolineando come ancora oggi sia in corso un lavoro "cognitivo" per la caratterizzazione di tale dominio e aggiungendo alla luce delle recenti evoluzioni in campo militare e tecnologico:

> 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 (Gray 2013, 15).

[16] R.B. Fuller conia tale principio filosofico. Sulla pagina di *Wikipedia* dedicata a Fuller è possibile leggere: "Fuller esplorò e propose il principio dell'«efemeralizzazione» – che in parole semplici significava «fare di più con meno». La ricchezza può essere aumentata riciclando le risorse in prodotti nuovi e di maggior valore, e i prodotti più sofisticati avrebbero richiesto minor materiale per la produzione. Nella realtà questo modello di sviluppo si è parzialmente avverato con la miniaturizzazione degli oggetti e degli strumenti".

[17] Termine ripreso da Gray 2013. Tuttavia, non esistendo 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".

[18] 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: Gray 1996a; Gray 1996b; Libicki 1996.

[19] Cfr. Gray 2013.

Secondo Gray, dunque, lo spazio cibernetico pur essendo un ambiente "*placelessness*", è costituito da elementi fisici e digitali che concorrono a renderlo allo stesso tempo reale e virtuale (Gray 2013). Non è un caso se la capacità politica (intesa qui come potere politico-militare) di influenzare l'accesso (o meno) al dominio cyber può avvenire soprattutto nello strato "geografico" *par excellence* ovvero, incidendo sul livello fisico-hardware. Infatti, come sottolinea David Clark, il livello fisico costituisce le fondamenta sulle quali poggiano gli altri strati del *cyberspace* e – soprattutto in termini geografici – presenta (rispetto agli altri) un *sense of location* che gli concede un grado di tangibilità prettamente "materiale". Non a caso, proprio la componente fisica è costituita da elementi e strutture tangibili come possono esserlo le c.d. *backbones* (dorsali di cavi ottici sottomarini), infrastrutture dalla quale transitano tra il 90 e il 95 per cento delle informazioni scambiate sul *web*[20].

Tali infrastrutture sono descritte (seppur artificiosamente) nella figura 2, dalla quale è possibile analizzare le "dinamiche del potere" in una delle componenti più importanti dello spazio cibernetico.

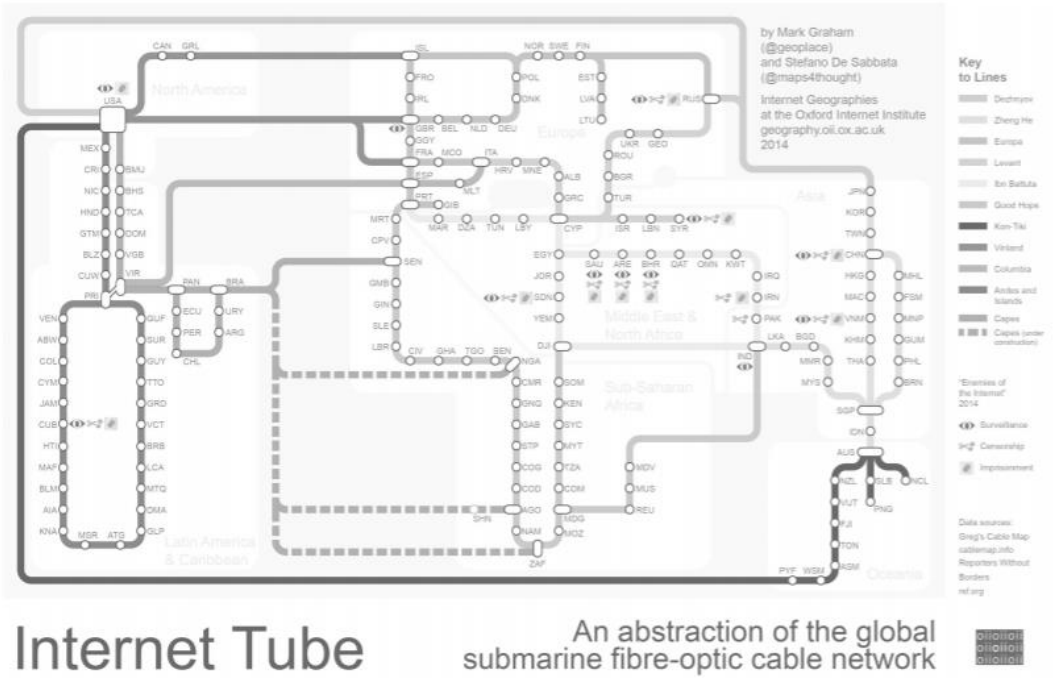

Fig. 2. Fonte: M. Graham, *Mapping the global submarine fibre-optic cable network*, Oxford Internet Institute

[20] Cfr. CableLab, *Cable Broadband Technology Gigabit Evolution*.

Dalla figura emerge soprattutto una "stratificazione" evidente di interdipendenza e interconnessione tra i Continenti suddivisi tra Paesi "minori" risultanti dai "nodi" della rete (nazioni collegate tra esse in modo reticolare) ed un unico *hub* centrale costituito dagli Stati Uniti che, in chiave politologica, rappresenta una posizione di egemonia rispetto agli altri attori. Infatti, come riportano gli stessi autori della mappa:

> The importance of being central in the submarine fibre-optic cable network is twofold. On the one hand, Internet users in central countries tend to have faster and cheaper connections to the Internet — there are no countries with low-cost Internet access that aren't also relatively well-connected. But we've also seen how certain central countries in the network have a history of engaging in surveillance of Internet traffic: as revealed by Edward Snowden [...] for both internal and foreign surveillance. [...] The United States is by far the most connected country in the world, with submarine cable landing points on both coasts that connect it to most other continents. [...] Europe dominates the immediately subsequent position in the rank. The two most central East-Asian country are China (17th), followed by India (29th), twelve positions below[21].

Tuttavia, l'attuale sistema internazionale (calato nella realtà dello spazio cibernetico) non può essere interpretato solo attraverso i classici capisaldi delle teorie delle Relazioni Internazionali, secondo le quali appunto, gli Stati rimangono gli attori egemoni della Comunità internazionale[22].

3. Gli effetti dell'era cibernetica sulla politica internazionale: le dinamiche del potere in un campo di battaglia senza "regole del gioco"

L'ascesa del dominio cibernetico a dimensione "propria" delle relazioni internazionali non è stata valutata da tutti gli osservatori con gli stessi standard in termini di rilevanza strategica. Secondo Thomas Rid, ad esempio, l'enfasi posta sul dominio cyber e la c.d. *cyber warfare* non sarebbe altro che una montatura pubblicitaria perché il rischio di una

[21] CableLab, *Cable Broadband Technology Gigabit Evolution*.

[22] La teoria delle Relazioni Internazionali che identifica nello Stato l'attore egemone della politica internazionale è rappresentata dal realismo. Secondo una disanima che ne dà U. Gori (Gori 2004, 15) 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".

guerra cibernetica, così come i disastri ipoteticamente paventati, non solo non si sarebbero mai palesati nel passato e nel presente, ma certamente – chiosa Rid – nel futuro: "*cyber war will not take place*" (Rid 2012)[23].

Tuttavia, secondo Joseph Nye, nell'era in cui viviamo si assiste per la prima volta non tanto alla *translatio imperii*, (trasformazione più che comune nei vari cicli storici)[24], ma a una vera e propria *diffusion of power* che mette in discussione il monopolio della violenza, prerogativa storica degli Stati-nazione[25]. Questo fenomeno favorisce la migrazione del potere dagli Stati verso attori non governativi[26] a tal punto che – continua Nye – "il problema di tutti i governi nell'era dell'informazione globale odierni è che sono in aumento le dinamiche che sfuggono anche agli Stati più potenti" (Nye 2011, 135).

In altre parole, interpretando l'analisi di Nye, si può dedurre come l'attuale era cibernetica non abbia solo incrementato esponenzialmente le informazioni disponibili per i singoli individui, i quali possono comunicare aggirando le censure burocratiche e le frontiere nazionali, ma abbia favorito anche un ruolo sempre più rilevante degli attori non statali[27].

Inoltre, dalla stessa analisi di Nye si evince come la rivoluzione tecnologica abbia favorito lo stravolgimento del concetto stesso di "potere" nelle dinamiche della politica internazionale trascinando il sistema verso un processo di s-politicizzazione della violenza. Infatti, l'aumento della diffusione delle tecnologie ICTs nel settore bellico, così come la relativa assenza di soglia di accesso a tali strumenti, hanno provocato un superamento del concetto classico di arma, dal momento che oggetti apparentemente pacifici, pensati e prodotti per l'ambito

[23] Cfr. anche Rid 2013.

[24] 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.

[25] Cfr. Nye 2011.

[26] Cfr Nye 2010. Invece per una disamina sul più ampio concetto della crisi della sovranità statale si rinvia a Krasner 2001.

[27] Cfr. Arquilla e Ronfeldt 2001. Sembrerebbe, dunque, che si venga a creare una certa affinità con la "società internazionale" teorizzata dalla c.d. Scuola Inglese e descritta in particolare da Hedley Bull il quale appunto, non limitandosi all'analisi stato-centrica, per descrivere l'anarchia che contraddistingue "la politica mondiale" prende in considerazione anche il ruolo svolto dagli attori non-statali. Per un approfondimento su questo tema si veda Bull 2017.

civile, si sono trasformati in mezzi offensivi di portata globale[28]. A tal proposito Alessandro Colombo sottolinea che:

> Se l'abbassamento della soglia d'accesso alle armi leggere aumentava la vulnerabilità delle società e degli stati deboli, la propensione delle tecnologie civili a essere trasformate in strumenti offensivi aumenta prima di tutto quella delle società complesse. [...] A mano a mano che crescono l'interconnessione e la concentrazione di ricchezza, capitale umano, conoscenza e comunicazione in un insieme di nodi strategici e simbolici – le 'città globali' come New York o, al suo interno, il World Trade Center – aumentano anche gli spazi (compreso quello virtuale) di un possibile attacco effettuato con mezzi 'non convenzionali' (non più nel senso di 'estremi', bensì di 'apparentemente pacifici'). (Colombo 2006, 285).

È evidente che nell'era dell'informazione è venuta meno la distinzione tra militare e civile non tanto sul piano della ripartizione dei ruoli, quanto piuttosto sullo stravolgimento del concetto moderno di campo di battaglia[29]. Non è certo 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[30].

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 – "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" (Virilio 2000, 134).

[28] Cfr. Liang e Xiangsui 2001.
[29] Cfr. Virilio 2000.
[30] Cfr. Virilio 2000.

4. Conclusioni

La militarizzazione del cyberspazio (ufficialmente decretata durante il Summit della NATO tenutosi a Varsavia nel 2016 ma, *de facto*, sancita nell'ultima decade da varie dottrine militari nazionali) ha sottoposto questa nuova dimensione alle dinamiche della conflittualità[31]. Il campo di battaglia è diventato (anche) virtuale e la capacità delle *cyber weapons* (strumenti virtuali) di arrecare danni reali è oggi un dato incontrovertibile[32]. Lo stesso scenario internazionale – sotto la spinta propulsiva della "rivoluzione informatica" – sta radicalmente evolvendosi da arena Stato-centrica a realtà *multistakeholders*; così come la struttura stessa del potere si sta trasformando da piramidale a reticolare[33]. Ne consegue che 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, multinazionali, individui) capaci di influenzare in maniera sempre più incisiva i processi decisionali[34]. Tuttavia, questi attori si confrontano e interagiscono all'interno di un *ungoverned space*[35] privo di un quadro normativo di riferimento, la cui natura dinamica e instabile sta dando forma a una nuova geografia del potere, capace di porre nuove opportunità e sfide alla politica internazionale[36].

[31] Riguardo alle implicazioni belliche nel cyberspazio cfr. Green 2015.
[32] Si pensi a tal proposito all'aumento esponenziale dell'utilizzo degli strumenti *cyber* per raggiungere finalità politiche. A titolo di esempio si riportano i casi di: Estonia (2007) Jackson 2013; Georgia (2008) Hollis 2011; Iran (2010) Zetter 2014; Ucraina (2015) Zetter 2016.
[33] Cfr. Ash 2009.
[34] Cfr. Eriksson e Giacomello 2006, 221-244.
[35] Cfr. Deibert e Rohozinski 2010, 255-272. Le iniziative internazionali attualmente in vigore con lo scopo specifico di creare un quadro di norme condivise per il dominio *cyber* sono portate avanti in sede ONU, OSCE e G7, tuttavia queste attività hanno il limite invalicabile di essere basate su impegni volontari e giuridicamente non vincolanti.
[36] Cfr. Gori e Martino 2015.

Riferimenti bibliografici

Arquilla, John and Ronfeldt, David
2001 *Networks and Netwar. The Future of Terror, Crime, and Militancy*, Santa Monica: RAND.

Ash, Timoty Garton
2009 "As Threats Multiply and Power Fragments, The 2010s Cry Out for Realistic Idealism", *The Guardian*, 31 dicembre 2009.

Bull, Hedley
2017 *La società anarchica. L'ordine nella politica mondiale*, Milano: ASERI.

Colombo, Alessandro
2006 *La guerra ineguale. Pace e violenza nel tramonto della società internazionale*, Bologna: Il Mulino.

Deibert Ronald J. and Rohozinski Rafal
2010 *Under Cover of the Net. The Hidden Governance Mechanism of Cyberspace, in Ungoverned Spaces. Alternatives to State Authority in an Era of Softened Sovereignty*, Redwood City: Stanford University Press.

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, http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf (consultato il 14 - 06 - 2017).

Dyson, Esther
1998 *Release 2.1: A Design for Living in the Digital Age*, New York: Broadway Books.

Eriksson Johan and Giacomello Giampiero
2006 "The Information Revolution, Security and International Relations: (IR)relevant Theory?", *International Political Science Review*, n. 27.

Floridi, Luciano
2012 *La rivoluzione dell'informazione*, Torino: Codice edizioni.

Gori, Umberto
2004 *Lezioni di Relazioni Internazionali*, Padova: CEDAM.

Gori, Umberto e Martino, Luigi (eds)
2015 *Intelligence e interesse nazionale*, Roma: Aracne editrice.

Gray, Colin S.
1996a "The Continued Primacy of Geography", *Orbis*, Vol. 40, No. 2, pp. 247-259.
1996b "A Rejoinder by Colin S. Gray", Orbis, Vol. 40, No. 2, pp. 274-276.
2013 *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*, Strategic Studies Institute, Carlisle PA.

Green, James A. (ed.)
2005 *Cyber Warfare: A Multidisciplinary Analysis*, London: Routledge.

Hollis, David
2011 "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf (consultato il 13.06.2017).

Jackson, Camille Marie
2013 "Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success", New Voices in Public Policy, Vol. VII, George Mason University, http://journals.gmu.edu/newvoices/article/view/69/95 (consultato il 13.06.2017).

Kramer, Franklin, Starr, Stuart and Wentz, Larry (eds)
2009 *Cyberpower and National Security*, Washington (D.C.): National Defense University Press.

Krasner, Stephen D.
2001 "Think Again: Sovereignty", *Foreign Policy*, http://www.foreignpolicy.com/articles/2001/01/01/think_again_sovereignty (consultato il 01.04.2017).

Kuehl, Daniel T.
2009 "From Cyberspace to Cyber-power: Defining the Problem", in Kramer, Starr, Wentz, *Cyberpower and National Security*, cit.

Liang, Quiao e Xiangsui, Wang
2001 *Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione*, Gorizia: Libreria Editrice Goriziana.

Libicki, Martin C.
1996 "The Emerging Primacy of Information", *Orbis*, Vol. 40, No. 2, pp. 261-274.
2009 *Cyberdeterrence and Cyberwarfare*, Santa Monica (CA): RAND.

Lynn, William J.
2010 "Defending a New Domain", *Foreign Affairs*, 1 Sept. 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynniii/defending-a-new-domain (consultato il 15.06.2017).

Nye, Joseph S.
2010 *Is America in Decline?*, http://www.chathamhouse.org/publications/papers/view/177645 (consultato il 1.04.2017).
2011 *The Future of Power*, New York: PublicAffairs.

Rattray, Gregory J.
2009 "An Environmental Approach to Understanding Cyberpower", in Kramer, Starr, Wentz, *Cyberpower and National Security*, cit.

Rid, Thomas
2012 "Think Again: Cyber War. Don't Fear the Digital Bogeyman. Virtual Conflict is Still More Hype Than Reality", *Foreign Policy*.
2013 *Cyber War Will Not Take Place*, London: C. Hurst & Co. Publishers Ltd.

Sherrer, Joseph H. and Grund, William C.
2009 "A Cyberspace Command and Control Model", in *Maxwell Paper*, Air War College No 47.

Toffler, Alvin and Toffler, Heidi
1995 *The Politics of the Third Wave*, Atlanta: Andrew and McMeel

Virilio, Paul
1989 *La macchina che vede*, Milano: SugarCo.
2000 *La bomba informatica*, Milano: Raffaello Cortina Editore.

Zetter, Kim
2014 "An unprecedented look at Stuxnet, the world's first digital weapon", *Wired*, https://www.wired.com/2014/11/countdown-to-zeroday-stuxnet/ (consultato il 13.06.2017).
2016 "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *Wired*, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (consultato il 13.06.2017)

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