

## IL DOMINIO DEGLI SPAZI: IL COSMO, LA CYBERWAR E L'URGENZA DI UNA DOTTRINA OPERATIVA PER LA GUERRA FUTURA

GERMANA TAPPERO MERLO

1. *Il dominio degli spazi.*- Se ne parla ormai da circa un ventennio, dalla pubblicazione del saggio di due analisti statunitensi, John Arquilla e David Ronfeldt, dal titolo profetico *Cyberwar is coming!*<sup>1</sup> e dal libro, apparso qualche anno dopo, *Guerra senza limiti*, dei generali cinesi Qiao Liang e Wang Xiangsui<sup>2</sup>, in cui non solo venivano anticipati i caratteri salienti di quelli che sarebbero poi stati gli attacchi terroristici del 2001, ma veniva anche evidenziato l'aspetto più rivoluzionario delle guerre future, ossia quelle combattute nello "spazio non naturale", virtuale, fittizio, proprio delle nuove tecnologie, vale a dire lo spazio cibernetico, che comprende le reti di informazione e di comunicazione<sup>3</sup>, e tutti i dispositivi fissi e mobili connessi ad internet. Se i due ricercatori statunitensi si concentravano più sulle caratteristiche rivoluzionarie ed accattivanti degli attacchi cibernetici intesi come guerra per il controllo dell'informazione, la *infowar* o *noopolitik*<sup>4</sup>, i generali cinesi delineavano, fra analisi geostrategiche e suggestioni filosofiche, i probabili aspetti di conflitti non così tanto avveniristici. Gli attacchi con il *malware*<sup>5</sup> Stuxnet alla centrale atomica iraniana di

---

<sup>1</sup> Si veda ARQUILLA, RONFELDT, *Cyberwar is Coming!*, in *Comparative Strategy*, Vol. 12, No. 2, Spring 1993, 141-165.

<sup>2</sup> Si veda LIANG, XIANGSUI, *Unrestricted Warfare*, Beijing, 1999.

<sup>3</sup> Sull'utilizzo di telefoni cellulari e internet nei conflitti più recenti, si veda FITSANAKIS, ALLEN, *Cells Wars: The Changing Landscape of Communications Intelligence*, RIEAS Research Paper, n. 131, May 2009.

<sup>4</sup> La scelta di questa definizione da parte degli autori è stata dettata dalla volontà di dare alla *infowar* o guerra delle informazioni nel cyberspazio una connotazione meno tecnologica e più ideale, che appartiene appunto alla noosfera, o sfera del pensiero umano, secondo i suoi ideatori Vladimir Vernadsky e Theilard de Chardin.

<sup>5</sup> Il *malware* è un *software* deleterio (della cui famiglia fanno parte i *worm*, le *logic bombs*, gli *sniffer*, i *trojan horses*, tutti genericamente definiti virus, ma con obiettivi illeciti diversi) creato per danneggiare computer collegati ad una rete, sfruttando la vulnerabilità delle "falle di sistema" e inducendoli così ad azioni diverse da quelle a cui sono dedicati.

Bushehr nel settembre 2010 o quelli DoS<sup>6</sup> a siti governativi dell'Estonia nel 2007 o durante la guerra in Georgia nel 2008, sono solo gli esempi più conosciuti di questo nuovo modo di fare la guerra, nella sua manifestazione più rivoluzionaria e che riporta nuovamente alla Cina e all'antico saggio dello stratega Sun Tzu sull'*Arte della guerra*, dove la vittoria si doveva ottenere senza aver indotto il nemico a combattere.

Nel gennaio 2001, inoltre, con un lieve ritardo rispetto agli interventi dei generali cinesi, la commissione congiunta statunitense, presieduta dal deputato Ronald Rumsfeld, nominata per definire la gestione e l'organizzazione della sicurezza dello spazio per gli Stati Uniti, prospettava il rischio di una "Pearl Harbour spaziale", volta a distruggere le reti satellitari statunitensi e, di conseguenza, a compromettere la sicurezza delle operazioni militari terrestri ad esse collegate<sup>7</sup>. Il nuovo secolo si apriva, quindi, con l'ipotesi di un attacco dallo spazio al territorio americano e alle sue strutture politiche ed economiche, così come, parallelamente, si prospettavano scenari da guerre stellari con possibili attacchi nel cosmo contro impianti satellitari statunitensi, vitali per le attività commerciali e per la mappatura terrestre, strategica per l'*intelligence* e, di conseguenza, per le autorità militari. Il rapporto suggeriva, quindi, di impegnarsi in una politica atta a difendere gli interessi della nazione e a dissuadere i nemici dall'intraprendere azioni offensive, attraverso maggiori investimenti nelle nuove tecnologie e incentivi all'industria aerospaziale nazionale. In pratica, per la loro sicurezza, gli Stati Uniti dovevano impedire ad altre nazioni di insediarsi nello spazio attraverso una sua massiccia militarizzazione, dotandolo e difendendolo con armi sempre più sofisticate e con basi orbitanti, che solo la ricchezza finanziaria e la supremazia tecnologica statunitensi erano in grado di garantire e mantenere.

---

<sup>6</sup> L'attacco DoS (*Denial of Service*, o nella sua forma più vasta *distributed denial-of-service*, DDoS) si concretizza attraverso un flusso eccezionale di richieste simultanee ad un sistema informatico che fornisce un servizio (come ad esempio un sito web), portandolo al

limite delle sue prestazioni, e a renderlo incapace di funzionare. Obiettivi di attacchi DoS sono solitamente siti istituzionali, soprattutto di istituti finanziari, banche e gestori di carte di credito, e gli autori sono stati individuati, almeno sino ad ora, in cyber criminali alle dipendenze di organizzazioni malavitose.

<sup>7</sup> Si veda *Report of Commission to Assess United States National Security Space Management and Organization*, Washington DC, January 11, 2001, VIII. Lo stesso concetto è stato ampiamente ripreso in BURKE, *Space Threat Warning: Foundation for Space Superiority. Avoiding a Space Pearl Harbor*, Maxwell AFB (AL), 2006, e ricordato nel recente testo di CLARKE, KNAKE, *Cyber War. The Next Threat to National Security and What To Do About It*, New York, 2010.

La Pearl Harbor degli Stati Uniti del XXI secolo sarebbe arrivata, tuttavia, l'11 settembre di quello stesso anno, ma su ben altri obiettivi: si sarebbe trattato solo di un rinvio di un'emergenza che è tornata attuale con l'amministrazione Obama, sebbene presentata come manovra economica per rilanciare, attraverso la ricerca e l'innovazione tecnologica, l'industria privata dello spazio e garantire fondi per 6 miliardi di dollari, in cinque anni, e 2500 nuovi posti di lavoro<sup>8</sup>.

Nel gennaio 2007, il rischio di un'aggressione dallo spazio era già apparso alle autorità militari statunitensi più realistico rispetto al passato, dopo un attacco, da parte della Cina, a un satellite meteorologico obsoleto, con un impatto così potente da allarmare i vertici del Pentagono. La risposta americana, nel febbraio del 2008, con la distruzione di propri satelliti orbitanti sull'oceano Pacifico, di fatto stracciava i vecchi accordi Asat degli anni '80, che vietavano esperimenti balistici antisatelliti, e faceva emergere la vulnerabilità dell'ancora più antico Trattato sullo spazio, approvato dalle Nazioni Unite nel 1967<sup>9</sup>. Sembrava, quindi, aprirsi una nuova era che, accantonata per un momento la guerra al terrorismo, imponeva alle potenze mondiali nuovi parametri strategici, in cui giocava un ruolo forte il dibattito sulle installazioni antimissilistiche e antisatellitari ubicate nella vecchia Europa e puntate contro la Russia, proprie della presidenza di G. W. Bush e retaggio di una tanto obsoleta quanto logorante logica di guerra fredda.

Le stesse autorità statunitensi, tuttavia, dovevano ben presto confrontarsi con un'altra minaccia, in cui confluivano soggetti esclusi dalla competizione spaziale: dalla rete internet, già ampiamente utilizzata dai terroristi come veicolo di propaganda e rivendicazioni di attentati, provenivano sempre più numerose minacce di attacchi – nell'ultimo anno si calcola siano andati a segno oltre cento incursioni soltanto negli Stati Uniti – talmente complessi da rischiare di compromettere seriamente l'attività economica e la sicurezza nazionale. Nell'autunno del 2008, inoltre, un'infiltrazione del *worm agent.tbz* nei *network* militari statunitensi – attraverso una chiavetta “infestata” inserita in un portatile in dotazione ad un ufficiale presso una base in Medio Oriente – rese manifesta ai vertici del Pentagono la vulnerabilità del loro intero sistema di sicurezza, obbligandoli ad una lunga e laboriosa

---

<sup>8</sup> Si veda MOLINARI, *Il contrordine di Obama: “Torneremo nello spazio”*, in *La Stampa*, 15 aprile 2010.

<sup>9</sup> Si veda *Treaty on Principles Governing the Activities of States in the Exploitation and Use of Outer Space, Including the Moon and Other Celestial Bodies*, in <http://www.unoosa.org/oosa/SpaceLaw/outerspt.html>.

operazione di “pulizia” (*Operation Buckshot Yankee*)<sup>10</sup>. Si trattava solo di uno dei numerosi attacchi registrati in quell’anno contro diversi siti istituzionali e le loro relative reti intranet, fra i quali il Dipartimento della Difesa, quello per la Sicurezza interna, alcune delle agenzie di *intelligence* e persino la Casa Bianca.

In differenti occasioni i vertici politici e militari avevano manifestato la consapevolezza di non essere preparati alle nuove sfide del cyberspazio: di fronte ad un innalzamento così rapido del rischio per la sicurezza nazionale, l’amministrazione Obama decise di istituire un *Cyber Command* militare. In pratica, la *cyberwar* diventava una priorità per le forze armate degli Stati Uniti e la difesa stessa di quel territorio<sup>11</sup>. Il documento, del novembre 2009, *National Cyber Security Incident Response Plan*, dello stesso presidente dava vita, nel settembre dell’anno successivo, alla terza simulazione internazionale, la *Cyber Storm III*<sup>12</sup>, al fine di testare la vulnerabilità dei sistemi di rete di fronte a una vera e propria “tempesta telematica”, in grado di paralizzarli e compromettere il normale funzionamento quotidiano di un Paese. Infatti, se le strutture militari sono già dotate di sistemi che ne garantiscano una certa qual sicurezza, le infrastrutture civili – ed è una condizione comune a Stati Uniti e a molti Paesi europei, tranne qualche rara eccezione – ne sono praticamente sguarnite o, comunque, indotte a dotarsi di costosi sistemi di difesa in continua evoluzione.

La vulnerabilità dei nuovi sistemi Ict<sup>13</sup> (ossia le tecnologie di informazione e di comunicazione), capisaldi per il futuro del capitalismo mondiale qualunque sia il suo modello di sviluppo, e l’inevitabile relazione che esiste fra spazio cibernetico e cosmo, ossia il luogo in cui stazionano e operano i satelliti sia per uso civile che militare – entrambi, infatti, sono da tempo utilizzati come moltiplicatori di potenza per le forze di superficie<sup>14</sup> – impone di considerare il futuro dei rapporti fra le grandi potenze attraverso quello che definisco “il dominio degli spazi”. In pratica, in un futuro alquanto prossimo, il pos-

---

<sup>10</sup> <http://www.wired.com/dangerroom/tag/operation-buckshot-yankee/>.

<sup>11</sup> Si veda *Quadrennial Defense Review Report*, Washington DC, Feb. 2010, 37-39; LYNN, *Protecting the Domain: Cybersecurity as a Defense Priority*, [http://www.csis.org/-media/csis/events/090615\\_sf\\_lynn.pdf](http://www.csis.org/-media/csis/events/090615_sf_lynn.pdf).

<sup>12</sup> [http://www.dhs.gov/files/training/gc\\_1204738275985.shtm](http://www.dhs.gov/files/training/gc_1204738275985.shtm); <http://www.dhs.gov/-xlibrary/assets/cyber-storm-3-media-fact-sheet.pdf>.

<sup>13</sup> I primi a parlare del *military potential* dei sistemi Ict furono i membri della Federazione Russa nel corso della 54ª Sessione dell’Assemblea Generale delle Nazioni Unite del 1999; si veda <http://www.unidir.org/pdf/articles/pdf-art2642.pdf>.

<sup>14</sup> Si veda FITSANAKIS, ALLEN, *op. cit.*, 7.

nesso e il controllo degli strumenti e delle reti, terrestri e spaziali, di raccolta e di trasmissione dei dati apparterranno solo a quelle nazioni in grado di fronteggiare e superare attacchi nemici atti a paralizzare la vita politica, economica e finanziaria del Paese. Ma non solo: significherà soprattutto essere in grado di partecipare finanziariamente alla ricerca nell'alta tecnologia specifica di questi settori e di detenere quelle risorse strategiche rappresentate dai metalli rari sempre più indispensabili per la fabbricazione degli strumenti propri delle guerre future. Sta emergendo, infatti, una diffusa preoccupazione legata al problema dell'“accesso alle terre rare”, così definiti in chimica quei metalli strategici necessari per la costruzione di navi militari, missili e fibre ottiche<sup>15</sup>, che già sta deteriorando i rapporti commerciali fra Cina e Giappone e sta allertando il resto del mondo più industrializzato: si tratta dell'ennesima prova della stretta relazione fra ricchezza economica, investimento nella ricerca e geostrategia che caratterizza le moderne relazioni militari fra le nazioni e definisce l'esclusivo ruolo di potenza solo per un ristretto numero di soggetti.

Dominare questi spazi, il cosmo e quello cibernetico, significherà anche essere in grado di impedire qualsiasi azione offensiva contro obiettivi e interessi dell'intera Comunità internazionale, dato che è impossibile limitarne il rischio ad un solo Paese, vista la natura globale di questi due elementi. Il concetto di dominio è già per sua natura totalizzante: lo è ancor più quando si tratta di conquistare e controllare il cosmo e questo spazio innaturale, specifico della rete. Inoltre, nella logica del dominio degli spazi, il compito più gravoso è rappresentato proprio dal suo mantenimento perché esso comporterà, inevitabilmente, il rischio di confronto continuo con potenziali concorrenti. A quel punto, e per garantire strategicamente quel dominio, saranno indispensabili alleanze politiche in cui la condivisione di modelli economici e finanziari, fondamentali per l'incessante ricerca tecnologica, sarà risolutiva per la sua realizzazione. Ancora una volta, l'elemento chiave per la definizione dei protagonisti delle relazioni internazionali è dato dal modello economico e finanziario vincente, ossia quello in grado di superare le crisi e sostenere livelli nazionali di crescita e di

---

<sup>15</sup> Si veda FUBINI, *Missili, computer e auto. Pechino blinda il controllo sui 17 minerali dell'hi-tech*, in *Corriere della Sera*, 18 agosto 2010. Negli ultimi anni la domanda di questi metalli è triplicata, da 40 a 120 mila tonnellate l'anno, e si ipotizza di raggiungere le 200 mila per l'impulso dato dalla costruzione di motori verdi. La Cina esportava il 75% della sua produzione (il 97% di quella mondiale); proprio in seguito al cambiamento di strategie produttive ma soprattutto diplomatiche, le sue esportazioni sono scese al 25%.

ricchezza proprie di una superpotenza. A questo proposito, vista la grave crisi economica che sta investendo gli Stati Uniti e l'Occidente, contrapposta ai livelli di crescita di Cina, India, Brasile e Russia<sup>16</sup>, impensabili per il resto del mondo più industrializzato, sembrano profilarsi già chiaramente fin da ora i soggetti di quel confronto futuro per la conquista e il mantenimento del dominio degli spazi.

Tuttavia, se vi è un'ampia bibliografia relativa ai rischi e alle contromisure proprie di una guerra fra potenze che le vede confrontarsi con minacce terra-aria, missili balistici intercontinentali, guerre e scudi spaziali<sup>17</sup>, al contrario, vi è ancora una certa riluttanza da parte degli analisti a considerare l'eventualità e la pericolosità degli attacchi provenienti dalla rete.

È convinzione di chi scrive, infatti, che l'aspetto più subdolo e pernicioso del confronto futuro fra potenze passi attraverso il cyberspazio, la cui caratteristica principale è data dalla totale assenza di delimitazioni o confini fisici e geografici, propri degli altri ambienti bellici, come la terra, l'acqua e l'aria, e che lo avvicina alla natura infida e codarda degli attacchi terroristici. Tuttavia, la *cyberwar* è ancora poco percepita come minaccia e viene soltanto associata al semplice crimine informatico, e il suo contrasto è limitato a un controllo poliziesco della rete, illudendosi che la minaccia possa provenire da incauti o presuntuosi cibernauti, banalmente ed erroneamente definiti *hackers*<sup>18</sup>. Il dubbio che vi siano strutture ben più complesse e motivate a raggiungere obiettivi politici decisamente più ambiziosi del semplice desiderio, specifico degli *hackers* appunto, di dimostrare le proprie capacità di intrusione in reti di computer, è stato superato dalla certezza che questi attacchi siano troppo articolati e possano provenire solo da organizzazioni statali nemiche. Si tratta, infatti, più di azioni proprie dei *crackers*, ossia di abili programmatori impegnati ad eludere o ad eliminare blocchi imposti a *software* e il cui fine è riuscire a trarre profitto dalle loro azioni. Se costoro vengono ingag-

---

<sup>16</sup> Si veda, tra gli altri, SARTORI, *L'ascesa dei Bric e gli assetti militari globali*, <http://www.affarinternazionali.it/>.

<sup>17</sup> Per un'analisi esauriente al riguardo si veda GARIBALDI, *I Signori dello Spazio*, Casalecchio (BO), 2007.

<sup>18</sup> L'*hacker*, infatti, viola un sistema o una rete solo per modificare il codice sorgente di programmi per migliorarne le prestazioni, inducendo i gestori del sistema violato a prendere coscienza di un problema di sicurezza, o per aggiungere nuove funzionalità. L'*hacker* non agisce per interesse economico e spartisce con la comunità cibernetica il principio per cui la condivisione della conoscenza è un punto di forza. Non a caso movimenti come l'*open source* e il *copyleft* sono nati e si sono sviluppati attraverso comunità di *hacker*.

giati da organismi complessi di carattere criminale vero e proprio, ossia dalla malavita organizzata, il fine è il guadagno economico; ma se costoro vengono assoldati da Stati, gli scopi sono spionistici o, come nel caso appunto di Stuxnet, pericolosamente destabilizzanti<sup>19</sup>.

Questo avviene perché lo spazio cibernetico ammassa non solo le informazioni e i dati più sensibili della vita politica, economica e sociale di un Paese, ma da esso dipende lo stesso funzionamento di settori nevralgici per la produzione nazionale, per la sicurezza e l'incolumità dei suoi cittadini, sempre più esposti alle intrusioni banditesche nella rete internet o addirittura, come nel caso iraniano, per mezzo di semplici chiavette usb. Il più grave errore compiuto nell'era della globalizzazione, in questo campo, è stato proprio quello di affidare ad una rete non certo immune da falle di sistema, tutto l'insieme di informazioni proprie della vita politica, economica, finanziaria ma soprattutto militare degli Stati, rendendo più vulnerabile la loro difesa anche da parte degli organismi istituzionali preposti.

Questo estendersi dello spazio cibernetico dalla pacifica vita quotidiana a scenari più conflittuali fra potenze è anche testimoniato da un altro aspetto caratteristico della globalizzazione, ossia quello più comunemente noto come *infowar*, in cui la gestione e il dominio dell'informazione *on line* vengono definiti attraverso confronti fra alta ricerca tecnologica, riconoscimento di brevetti e massima vigilanza dei motori di ricerca, in cui giocano un ruolo strategico il possesso e il controllo del *cloud computing* (informatica a nuvole), ossia quella parte di spazio cibernetico composto da batterie di *server* di proprietà dei grandi operatori, in cui vanno a confluire tutte le informazioni e i dati più sensibili immessi in rete dagli utenti, dagli indirizzi di posta elettronica, ai dati bancari o a tutte le informazioni personali di cui abbondano i *social network*. Lo "stoccaggio" di questi dati da parte dei grandi *provider* di servizio, le leggi che ne regolano il flusso e la loro relativa sicurezza, costituiscono ancora una dura sfida sia per i privati che per i governi: sono in gioco, infatti, la protezione della *privacy* e delle libertà civili.

---

<sup>19</sup> Le conseguenze dell'"infezione" da parte di questo virus sembrano essere state ben più disastrose di quanto ipotizzato alla sua prima apparizione; non si è trattato, infatti, di un'intrusione al solo fine di dimostrare la vulnerabilità del sistema o di rubare dati, quanto dell'assunzione del controllo dell'impianto nucleare e del sistema industriale ad esso collegato. Si è trattato di un attacco allo Scada (*Supervisory control and data acquisition*), ossia di quei sistemi di supervisione e acquisizione dati che fanno funzionare centrali elettriche, telefoniche e nucleari, reti ferroviarie e aeree, acquedotti, impianti petroliferi e anche installazioni militari. V. <http://www.fabioghioni.net/>.

La *infowar* rappresenta, però, un altro capitolo del dominio degli spazi, dagli aspetti allarmanti per gli obiettivi colpiti – i dati personali e la libertà d’informazione – ma gestibili; si tratta più di un confronto, di una competizione fra culture, che può anche limitarsi ai soli scontri fra *tycoon* delle informazioni, in cui il contrasto fra Google e la Cina<sup>20</sup>, o le rivelazioni di *wikileaks* sulla guerra in Afghanistan, o la campagna contro il regime iraniano condotta su *Twitter* e il suo conseguente blocco da parte di un sedicente *Iranian Cyber Army*<sup>21</sup>, rappresentano solo alcuni fra gli esempi più noti e recenti e palesano solo parte delle problematiche. Si tratta di fenomeni che caratterizzano quel concetto di “armi di comunicazione di massa”, attraverso cui – secondo i suoi più ferventi sostenitori, fra i quali il Segretario di Stato, Hillary Clinton – si gioca “la difesa dei diritti umani e il futuro dei rapporti commerciali internazionali”<sup>22</sup>, ma che, di fatto, contrappone modelli politici, economici e finanziari fortemente antitetici e in cui è in gioco il controllo dei flussi d’informazione e, nel suo aspetto più delicato ma urgente, la formazione delle nuove generazioni che più utilizzano internet. Si tratta, tuttavia, di un altro capitolo della guerra futura nella rete che merita un’analisi a parte più approfondita.

Quel che ci preme sottolineare, invece, in questo saggio sono i caratteri salienti di questa *cyberwar*, che già sta allarmando i vertici militari di molte nazioni, per lo meno quelle più digitalizzate. È necessario, infatti, prendere sempre più coscienza che lo spazio cibernetico è diventato così totalizzante da trasformarsi addirittura in uno strumento di politica nazionale: la sua violazione, da parte di soggetti stranieri, lo conduce irreparabilmente nella sfera della politica di sicurezza nazionale, della diplomazia e dei rapporti di forza fra Stati, come ha chiaramente dimostrato l’affaire iraniano Stuxnet. Inevitabile, quindi, associare ai nuovi rischi provenienti dallo spazio e dalla rete internet, minacce e contromisure proprie di scenari bellici e tentare di definire i

---

<sup>20</sup> Si veda THOMAS, *Google Confronts China's "Three Warfares"*, in *Parameters*, Summer 2010, 101-113.

<sup>21</sup> Si tratta di una frangia riconosciuta delle Guardie Rivoluzionarie Iraniane e il cui scopo è “prevenire la distruzione del sistema sociale e culturale iraniano”, e al cui interno è stato istituito un “Centro per l’Investigazione del Crimine Organizzato” al fine di “supervedere il terrorismo, lo spionaggio, i crimini economici e sociali nello spazio virtuale”. Nata dal reclutamento governativo di organizzazioni di *hackers* molto abili, ma soprattutto rei di aver violato siti governativi, è stata responsabile di numerosi attacchi sul web, soprattutto di siti di dissidenti all’estero, di agenzie stampa, di radio e di *social network*, come *Twitter*. <http://en.irangreenvoice.com/article/2010/feb/19/1236>.

<sup>22</sup> Si veda BORGIA, *Riflessioni sull’accesso ad internet come diritto umano*, in questa *Rivista*, 2010, 395-414.

caratteri fondamentali di questo tipo di guerra futura e la sua dottrina d'impiego.

2. *Probabili aspetti di una guerra futura.* - Se per il controllo delle aree ricche di “terre rare” è possibile ipotizzare per il futuro – come ha dimostrato il blocco della loro esportazione verso il Giappone, deciso dalla Cina in seguito all’incidente di Senkaku del settembre 2010<sup>23</sup> – anche conflitti fra nazioni guerreggiate davvero sul terreno, come lo sono stati per il petrolio, i gasdotti e le acque, il confronto fra potenze attraverso la *cyberwar* avrà, forse, toni più nascosti e segreti, ma il suo obiettivo finale risulterà pari a quello delle azioni terroristiche, puntando più alla destabilizzazione della forza nemica che alla sua eliminazione. Da quel che si profila, dati gli esempi conosciuti sino ad ora, si tratterà, infatti, di una guerra senza lo schieramento fisico di forze militari e senza scontri armati, con un concetto di vittoria sul nemico che non sarà in termini di sua soppressione ma di sua incapacità a svolgere qualsiasi attività e a gestire le proprie sorti politiche ed economiche. Il nemico non sarà conquistato fisicamente ma debellato, proprio nel suo senso più ampio e totalizzante. E tutto ciò avverrà in un arco di tempo molto limitato.

È difficile credere a questa evoluzione degli scenari bellici quando sono ancora aperti fronti di lunghe guerre guerreggiate, come nella regione Afpak o in Medio Oriente e in Africa, passando attraverso la guerriglia delle Farc colombiane o gli attentati terroristici di matrice islamica. Tuttavia, se per costoro valgono strategie e tattiche ormai datate e ancora dipendenti dall’evoluzione di una tecnologia militare sempre più dispendiosa, ingombrante, la cui dotazione per gli Stati risulta sempre meno gradita all’opinione pubblica, gli strumenti ad alta tecnologia propri del cyberspazio non sono meno costosi, ma possono essere ben occultati se ben gestiti, e soddisfare quell’impostazione dottrinale che vuole le nuove guerre sempre più veloci e con il minor coinvolgimento di soldati sul campo per ridurre il rischio di perdite. Tuttavia, a tutt’oggi, a questo generico approccio strategico e ai frequenti conflitti nello spazio cibernetico non corrisponde un’adeguata

---

<sup>23</sup> Si veda BRADSHER, *Amid Tensions, China Blocks Vital Exports for Japan*, in *The New York Times*, 23 Sept. 2010. Già prima di questo incidente erano apparsi negli Stati Uniti rapporti ufficiali che evidenziavano i rischi di dipendenza dai metalli rari provenienti dalla Cina per la costruzione di numerosi sistemi d’arma in dotazione alle forze armate statunitensi; si veda, *Rare Earth Materials in the Defense Supply Chain*, 14 Apr. 2010, <http://www.gao.gov/new.items/d10617r.pdf>.

dottrina di impiego delle contromisure in grado di definire chiaramente i protagonisti, le loro responsabilità e gli obiettivi leciti di una guerra che si sta diffondendo soprattutto fra grandi potenze economiche. Non è un caso che nei suoi aspetti strategici e legali la *cyberwar*, a tutt'oggi, posseda un'ampia zona grigia.

Questo limite è dovuto, forse, al fatto che si tende ancora a ridurre gli attacchi in rete ad azioni proprie del crimine informatico: l'elemento che fa la differenza fra una guerra cibernetica e un *cybercrime*, sta nei soggetti che operano queste azioni di disturbo e negli obiettivi colpiti. Il crimine nello spazio cibernetico ha, solitamente, come scopo immediato il vantaggio economico, che sia personale o collettivo – dal furto d'identità, ai dati bancari, transazioni finanziarie illecite e così via – e può sconfinare nello spionaggio industriale o militare, in quanto l'obiettivo finale è sottrarre informazioni. La *cyberwar*, colpendo in particolare infrastrutture come telecomunicazioni, centrali elettriche, sistemi di trasporto, reti finanziarie, mira alla paralisi di settori strategici di una nazione, danneggiandola economicamente, ma soprattutto rendendo estremamente vulnerabile il normale svolgimento della sua vita civile. Se poi la stessa nazione è esposta su scenari bellici, l'obiettivo di un'intrusione propria di una *cyberwar* può essere il sistema di comando, controllo e comunicazioni delle operazioni militari, che da tempo ha incorporato, oltre alla tradizionale *intelligence*, anche l'informatica (C4I)<sup>24</sup>.

La violazione dello spazio cibernetico diventa, quindi, in questo caso, un atto militare e la sua gravità dipende solo dall'obiettivo colpito e dal vantaggio che ne è derivato: un semplice portatile infettato, anche se di un alto ufficiale, non crea un *casus belli*, ma se questo virus – come nel caso delle forze armate statunitensi e dell'*agent.btz* visto in precedenza – si diffonde, copia dati, apre *backdoors*<sup>25</sup> e attraverso queste invia a *server* remoti informazioni al punto da compromettere piani operativi e imporre una riorganizzazione delle difese e del sistema di informazione di un Paese impegnato su un fronte, non vi è dubbio che si tratti di un'azione ostile a cui opporre contromisure su piano operativo, ma soprattutto politico e diplomatico.

---

<sup>24</sup> Si veda Committee to Review DoD C4I Plans and Programs, *Realizing the Potential of C4I: Fundamental Challenges*, Washington DC, 1999.

<sup>25</sup> Le *backdoors* o *porte di servizio* sono strumenti, attivabili attraverso *malware*, che consentono di superare in parte o del tutto le procedure di sicurezza di un sistema informatico e permettere ad un *cracker* di prenderne il controllo. Sono pericolose per le informazioni presenti nel sistema, ma anche perché utilizzate per avviare attacchi DDoS.

Possiamo, tuttavia, aggiungere un ulteriore elemento inquietante ma non improbabile, come ha dimostrato il caso Stuxnet: se ad essere colpito, o “infettato” da un *malware*, è una centrale nucleare, o un sistema di distribuzione delle acque o di controllo della rete ferroviaria di una nazione, tale da compromettere l’incolumità della sua popolazione – probabilità peraltro non remota, dato che con quel virus sono stati infettati oltre 30mila computer<sup>26</sup> – possiamo azzardare a definire un attacco cibernetico come “un’arma di distruzione di massa”<sup>27</sup>. Da tutto ciò si deduce la chiara distinzione fra semplice *cybercrime* e vera e propria *cyberwar*. Sono, quindi, gli obiettivi finali che fanno la differenza e non concordiamo con chi afferma che si tratti solo di questioni di denaro<sup>28</sup>, come hanno dimostrato, per esempio, le azioni di *crackers* russi di intrusione e sabotaggio dei sistemi georgiani, azioni dettate da motivazioni colme di un forte sentimento nazionalistico e di un’agguerrita avversione morale contro l’Occidente. Sono questi fanatismi che li rendono pericolosamente ingaggiabili da potenze ostili e gli attacchi informatici, investiti da motivazioni ideologiche, perdono la loro valenza “criminale” e assumono una matrice politica, che può avere fini eversivi o rivoluzionari, comunque pericolosi per la sicurezza della nazione colpita.

Proprio per via della confusione che ancora domina al riguardo, le capacità di un attacco informatico non fanno ancora parte ufficialmente degli arsenali a disposizione degli Stati; tuttavia, visto il numero crescente di incursioni, si sta diffondendo la consapevolezza, presso un numero sempre maggiore di Stati, che esse siano parte integrante del potenziale militare nemico. Ecco che la salvaguardia della sicurezza nazionale, così come delle operazioni militari in un contesto conflittuale, impone la definizione di una dottrina operativa.

Per fare questo è necessario comprendere la natura di questo tipo di guerra, che ben si configura nel concetto di guerra asimmetrica<sup>29</sup> globale, propria dei conflitti dopo l’11 settembre e di cui la guerra al

---

<sup>26</sup> Sulle origini del virus e la sua diffusione si veda BAHÉLI, *Iran sotto attacco, le nuove frontiere della cyber war*, <http://temi.repubblica.it/>.

<sup>27</sup> <http://www.cis.fordham.edu/news/ICCS.html>. Vi è anche chi ha intravisto similitudini con le armi nucleari; si veda al riguardo anche l’intervento di SHACKELFORD, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, in [http://works.bepress.com/scott\\_shackelford/5](http://works.bepress.com/scott_shackelford/5); CABANA, *Cyber Attack Response: The Military in a Support Role*, in *Air&Space Power Journal*, 4 Apr. 2000.

<sup>28</sup> *Report McAfee 2009 sulla criminologia virtuale. L’era della guerra informatica è alle porte*, disponibile su [www.McAfee.com](http://www.McAfee.com).

<sup>29</sup> Si veda GHIONI, PREATONI, *Ombre asimmetriche. La guerra cibernetica e i suoi protagonisti*, Roma, 2005.

terrorismo<sup>30</sup> è stata l'espressione più potente e totalizzante. Se nella lotta contro le cellule di *al Qaida*, la natura asimmetrica è stata evidente, perché era chiara la forte disparità fra grandi potenze militari e gruppi armati di terroristi, non altrettanto palesi sono i termini di confronto fra nemici nella *cyberwar*, in cui i protagonisti degli attacchi sono ancora più occulti dei terroristi e la loro individuazione risulta estremamente complessa, sebbene ogni attacco lasci tracce in rete che è possibile ripercorrere a ritroso per individuarne l'origine<sup>31</sup>. Per fare questo, tuttavia, occorre avere strumenti e esperienza pari o almeno simili; fatto estremamente difficile da realizzare, data la disparità di conoscenze e di informatizzazione dei sistemi nazionali. Tuttavia, è plausibile che il confronto fra Stati con forte armamento tradizionale e quelli meno sviluppati avvenga nell'unico spazio in cui non sono necessarie grandi disponibilità finanziarie, ossia internet. È in questo modo che si realizza l'asimmetria della *cyberwar*.

Inoltre, a differenza dell'asimmetria della lotta al terrorismo, gli Stati più vulnerabili in un conflitto cibernetico risultano quelli più informatizzati, come nel caso dell'Estonia, appunto, più volte oggetto di attacchi – pare per opera di *crackers* russi – proprio perché si tratta di una nazione con il più alto grado di digitalizzazione di dati e di servizi in Europa. Gli attacchi di tipo DoS condotti nel 2007 portarono, infatti, alla completa paralisi del Paese, impedendo ai cittadini estoni tutte le transazioni economiche e finanziarie *on line*. Se si tratta, poi, di ricorrere a una strategia offensiva, ancora una volta ad essere favoriti nel confronto sembrano essere quelle potenze emergenti meno dotate finanziariamente ma tecnologicamente all'avanguardia, in quanto risulta poco costoso lanciare attacchi<sup>32</sup>, ma estremamente oneroso

---

<sup>30</sup> Anche le azioni terroristiche si configurano da sempre come asimmetriche perché l'obiettivo dei terroristi, ossia la parte economicamente e tecnologicamente più debole, è colpire il nemico, lo Stato, la parte più forte, in maniera improvvisa e provocare un forte shock psicologico nell'opinione pubblica. L'asimmetria, nel caso dell'azione terroristica, è data dalla disparità fra le forze offensive e gli obiettivi colpiti, e da un fattore fondamentale per questo tipo di conflitto, ossia la sorpresa dell'attacco.

<sup>31</sup> Il "problema di attribuzione" è oggetto di ricerca degli esperti del settore informatico che stanno sviluppando tecniche per il rilevamento geografico dei *crackers*, così come stanno elaborando meccanismi di autenticazione, proprio al fine di ridurre l'anonimato sulla rete e risolvere l'urgente problema dell'attribuzione delle responsabilità.

<sup>32</sup> Nel 2009, il colosso finanziario Citibank registrava perdite per decine di milioni di dollari dopo un attacco da parte di *crackers* con il *malware Black Energy* acquistabile su internet a soli 40 dollari. Il *Zeus Trojan*, responsabile d'aver infettato 74mila computer in 196 paesi, ha un costo di circa 700 dollari. Pare che a gestire una larga fetta di questo commercio in rete sia il *Russian Business Network* (RBN), un'organizzazione cybercriminale che opera in rete attraverso falsi nomi ed è attiva soprattutto nel furto di identità, nella diffusione di

difendersi da essi. Non a caso, gli Stati Uniti e Israele sono all'avanguardia nella difesa dei loro *assets* spaziali e cibernetici.

Ecco perché l'asimmetria è il carattere saliente della *cyberwar* e la sua globalità dipende solo dal fatto che lo spazio cibernetico, in cui è connessa ormai ogni singola nazione è – per sua stessa natura – senza limiti territoriali: è un conflitto che non può essere circoscritto in confini fisici perché la rete, come il cosmo, non ne possiede. Inoltre, l'evoluzione della tecnologia permette la sua espansione e la sua diffusione a sempre più numerosi e nuovi soggetti. Questo fatto ricorda il dibattito dottrinale quando, sui campi di battaglia della prima guerra mondiale, apparve l'arma aerea: l'accresciuta precarietà delle difese terrestri e, di conseguenza, dei confini nazionali rimetteva in gioco le dottrine operative in cui dominava la guerra di contrapposizione, statica, logorante, e rilanciava tattiche dinamiche, in cui la minore difendibilità dei propri confini diventava un elemento operativo fondamentale, e la distinzione fra obiettivi civili e militari poneva interrogativi nuovi e di difficile soluzione nell'immediatezza dell'emergenza bellica.

Dalla mancanza di limiti territoriali dipende, almeno stando all'attuale stato della conoscenza tecnica, anche un altro fattore strategico, ossia la difficoltà di definire la fonte degli attacchi informatici, come nel caso di Stuxnet e l'Iran. Fin dall'inizio, proprio per la complessità dell'intera operazione, che ha compromesso anche alcuni sistemi telematici occidentali, la totalità dei più esperti addetti ai lavori escludeva l'ipotesi che si trattasse di un'azione isolata di singoli *crackers*<sup>33</sup>, propendendo, infatti, per responsabilità statali; avendo individuato l'origine del virus in Bielorussia, per alcuni si profilava addirittura l'ipotesi che l'operazione fosse gestita dal Mossad israeliano per far incrinare i rapporti fra Iran e Russia<sup>34</sup>. Allo stato attuale della conoscenza tecnica, qualora si riuscisse a definire la provenienza di un atto ostile, nell'immediatezza dell'attacco – come nel caso di Stuxnet o, comunque, di “infezioni” importanti di siti istituzionali – si rimarrebbe, comunque, nell'ambito delle ipotesi che riconducono agli attriti propri delle relazioni internazionali. Ciò è dovuto all'asimmetria

---

materiale pedopornografico e vendita in rete di *malware* a prezzi decisamente accessibili. Si veda KREBS, *Mapping the Russian Business Network*, in *The Washington Post*, [http://voices.washingtonpost.com/securityfix/2007/10/mapping\\_the\\_russian\\_business\\_n.html](http://voices.washingtonpost.com/securityfix/2007/10/mapping_the_russian_business_n.html).

<sup>33</sup> Si veda al riguardo KEIZER, MORATI, *Stuxnet, un malware senza precedenti*, in <http://www.cwi.it/>.

<sup>34</sup> <http://punto-informatico.it/2998692/PI/News/stuxnet-worm-all-assalto-del-nucleare-iraniano.aspx>.

delle conoscenze tecniche dei differenti Stati, la rapidità dei flussi informativi e infettivi e, soprattutto, la globalità dello spazio cibernetico. Nella *cyberwar* scompare, quindi, il concetto di territorio fisico, fondamentale nei rapporti diplomatici e militari, rimettendo anche in discussione sia la geostrategia che la geopolitica ad essi collegati. Venendo a mancare due fattori strategici, come la territorialità e l'individuazione sicura dei responsabili, risulta compromesso, a nostro avviso irrimediabilmente, anche il concetto di "guerra preventiva": non è facile, infatti, identificare fisicamente nel cyberspazio il nemico, le sue intenzioni bellicose e l'"arsenale" a sua disposizione, e colpirlo con mossa preventiva, come è accaduto nell'ultimo decennio per conflitti quale quello in Iraq e come è stato teorizzato dai suoi più ferventi ideatori<sup>35</sup>.

A differenza delle azioni terroristiche, condotte da persone fisiche di cui si può definire la provenienza ed eventualmente anche le responsabilità dello Stato "mandante", il sabotaggio o il vero e proprio attacco cibernetico proviene appunto da quello "spazio virtuale" indefinito che rende difficoltosa l'identificazione dei responsabili e, di conseguenza, la loro ubicazione geografica, così come le regole del loro ingaggio, con inevitabile confusione per coloro che debbono arginare il fenomeno e opporre adeguate contromisure, soprattutto diplomatiche e, nel caso estremo ma non improbabile ormai, anche militari.

Un esempio a tale riguardo è dato dalla guerra in Georgia dell'agosto 2008, con l'intrusione di *crackers* nazionalisti russi<sup>36</sup>: in pratica, mentre le forze russe invadevano il territorio dell'Ossezia del Sud, un pesante attacco informatico di tipo DDoS paralizzava la rete telematica governativa georgiana<sup>37</sup>, bloccando qualsiasi azione del governo e dei mezzi di informazione. Le autorità centrali decidevano,

---

<sup>35</sup> Si veda al riguardo, *Guerra preventiva*, in CIPRIANI (A.), CIPRIANI (G.), *La nuova guerra mondiale. Terrorismo e intelligence nei conflitti globali*, Milano, 2005, 27-36.

<sup>36</sup> Vi furono oltre 10mila attacchi ai principali *database* nazionali, 66 DDoS e centinaia di *web defacement*, ossia di modifica di *homepage*, e soprattutto l'uso di *botnet*, ovvero decine di migliaia di computer e *server* violati e utilizzati per attacchi mirati. Le autorità russe hanno negato il loro diretto coinvolgimento, anche se la simultaneità degli attacchi, quello militare e quello cibernetico, fa propendere almeno in un concorso di azioni, in quanto i *crackers* sarebbero stati informati dell'avvio delle operazioni belliche. Inoltre, nonostante la loro vulnerabilità, non sono state colpite infrastrutture critiche, a dimostrazione di un possibile coordinamento fra autorità russe e *crackers*, al fine di evitare danni fisici irreparabili, soprattutto alla popolazione civile. <http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf>.

<sup>37</sup> Chiunque avesse voluto partecipare a quell'attacco – avendone avuto informazione in tempo, ovviamente, e senza nemmeno possedere particolari capacità tecniche – poteva accedere a siti web filorussi, scaricare il *software* e partecipare all'azione DDoS.

quindi, di ricollocare l'intero *asset* telematico ufficiale negli Stati Uniti (pare senza l'iniziale autorizzazione di Washington), in Estonia e in Polonia<sup>38</sup>. In pratica, le infrastrutture telematiche americane – così come quelle estoni e polacche – per lo più private, fornivano asilo ed assistenza alla Georgia, coinvolta in un conflitto sia militare che cibernetico, senza la preventiva approvazione del governo statunitense. Da questo fatto è scaturito un interessante dibattito circa il concetto di neutralità di una nazione, in questo caso gli Stati Uniti, e le sue responsabilità reali, di fronte a casi come quello georgiano<sup>39</sup>. Una nazione fortemente digitalizzata, coinvolta e contrapposta suo malgrado a un'altra potenza impegnata in un confronto bellico, con il rischio di ripercussioni, sia diplomatiche ma, *in primis*, soprattutto telematiche, costituisce uno scenario inquietante e di difficile soluzione, stando allo stato attuale della giurisprudenza al riguardo.

A ciò si aggiunge un'altra caratteristica delle nuove guerre asimmetriche e che, in realtà, è già diventata consuetudine anche nella *cyberwar*, ossia la totale assenza di una dichiarazione di guerra vera e propria, così come al nemico non si attribuisce più alcuna parità formale o sostanziale per cui è, di volta in volta, un "nemico dell'umanità", una canaglia o un dittatore oppure, nel caso della guerra cibernetica, semplicemente ed erroneamente, un *hacker*. Questo fatto, di per sé, annulla ogni valenza strategica anche alla rappresaglia come risposta tattica ad un attacco. Ne deriva che lo stesso traguardo della vittoria finale presenta aspetti vaghi, discutibili e ambigui.

La neutralità, il coinvolgimento reale e non supposto di una nazione, la sua entrata in una cyberguerra e la sua conclusione, rappresentano, quindi, gli elementi più controversi e dibattuti della nuova forma di guerra elettronica e necessitano urgentemente di una regolamentazione internazionale, proprio per evitare che le autorità di un Paese si debbano ritrovare coinvolte loro malgrado in un conflitto iniziato senza alcuna dichiarazione di intenti o per semplice interesse economico privato.

La guerra nel cyberspazio, inoltre, proprio per le caratteristiche tecniche dell'ambiente in cui si trova a operare, induce a ridiscutere il

---

<sup>38</sup> Si veda SVENSSON, *Georgian President's Web Site Moves to Atlanta*, in *AP News*, 11 Aug. 2008; SHACHTMAN, *Estonia, Google Help 'Cyberlocked' Georgia*, in *Wired*, 11 Aug. 2008; MARKOFF, *Georgia Takes a Beating in the Cyberwar with Russia*, in *The New York Times*, 11 Aug. 2008; <http://georgiamfa.blogspot.com/2008/08/statement-of-ministry-of-foreign.html>; <http://www.tulsys.com/news>; <http://www.president.pl/x.node?id=20043119>.

<sup>39</sup> Si veda KORN, KASTENBERG, *Georgia's Cyber Left Hook*, in *Parameters*, Winter 2008-09, 60-76.

ruolo di altri due concetti considerati tradizionali nelle relazioni internazionali, come l'unilateralismo, che scompare, e il rischio di proliferazione, che invece aumenta la sua valenza dottrinale. Nel cyberspazio il dominio unilaterale da parte di una singola nazione – per intenderci quello ipotizzato da Rumsfeld per lo spazio, ma che di fatto ha caratterizzato la storia militare statunitense dopo la guerra fredda e, in particolare, gli anni dell'amministrazione G. W. Bush – è impossibile, dato l'aumento incontrollato delle capacità di avviare una guerra cibernetica da parte di un numero crescente di nazioni: ciò dipende dalla condivisione delle informazioni e degli strumenti tecnici, caratteristica basilare dello spazio globale cibernetico.

Da tutto ciò deriva il ritorno sulla scena di un concetto che è proprio della deterrenza nucleare, ossia quello della proliferazione degli strumenti offensivi (*cyberattacks proliferation*) che, viste le caratteristiche di diffusione dei mezzi tecnici propri del cyberspazio – ossia la banda larga sempre più estesa per favorire l'*e-commerce* – registra un aumento esponenziale. Non è un caso che, come forma di difesa, alcuni esponenti militari statunitensi<sup>40</sup> abbiano già rispolverato una terminologia propria della guerra fredda come “cyber deterrenza”, o “cyber dissuasione” in cui la “*strategic triad*” (riferita ai mezzi nucleari terrestri, marittimi e aerei), è diventata “*cyber triad*”, ossia l'urgenza di dotare l'esercito, la marina e l'aviazione con mezzi atti a fronteggiare un *cyber attack*<sup>41</sup>. Tuttavia, è nostra opinione che, viste le caratteristiche di anonimato degli attacchi, la natura nascosta e globale dei suoi protagonisti, l'estrema interconnessione dei sistemi di informazione, affidarsi ad un approccio unilaterale, con una impostazione strategica e una terminologia proprie della deterrenza nucleare<sup>42</sup>, possa risultare pericolosamente fuorviante per le autorità militari incaricate di fronteggiare attacchi di *cyberwar*.

Il ripetersi di intrusioni, le loro implicazioni politiche e diplomatiche, le contromisure sino ad ora prese unilateralmente, inducono a un confronto urgente, ampio, globale, aperto a tutti i soggetti che operano nel campo della sicurezza su come disciplinare le reazioni a possibili attacchi di *cyberwar*. Se, da quanto visto sino ad ora, l'unilateralismo non ha più ragione d'esistere, significa che è urgente trovare accordi

---

<sup>40</sup> Si veda MCCONNELL, *To Win the Cyberwar, Look to the Cold War*, in *The Washington Post*, 28 Feb. 2010.

<sup>41</sup> Si veda *Stuxnet; a Cyber “Cold Start”?*, in <http://www.thenews.com.pk/30-09-2010/opinion/7472.htm>.

<sup>42</sup> Si veda LIBICKI, *Cyberdeterrence and Cyberwar*, Santa Monica (CA), 2009.

collegiali fra Stati e organismi sovranazionali per disciplinare questa materia, preferendo non contrapporsi fra blocchi, non solo per evitare una guerra fredda nel cyberspazio, ma soprattutto per scoraggiare l'utilizzo criminale della rete, e trovare soluzioni comuni ed univoche per contrastare queste aggressioni deleterie. Se, tuttavia, queste considerazioni possono essere cariche di idealismo e, quindi, risultare di difficile attuazione, è comunque necessario comprendere che solo agendo globalmente, di comune accordo fra nazioni, è possibile limitare gli attacchi in rete al rischio del solo crimine informatico e impedire che raggiungano i loro obiettivi ben più pericolosi perché bellicosi.

3. *L'urgenza di una dottrina operativa.*- La scarsa letteratura al riguardo, per lo più presente – nemmeno tanto paradossalmente – su siti di *hackers*, ossia di coloro coinvolti loro malgrado negli attacchi a rischio di *cyberwar*, insiste sull'urgenza di definire al più presto le linee guida giuridiche per opporre le giuste contromisure; questo compito spetta alle autorità statali in comune accordo con i privati, ossia i gestori delle infrastrutture proprie della rete internet. Il rischio maggiore, al di là di quelli visti in precedenza di vera e propria guerra fra nazioni, è quello di permettere che da semplice crimine informatico – o anche solo di spionaggio industriale in rete – l'intrusione si riveli più catastrofica per l'incolumità delle persone fisiche, quando ad essere oggetti di attacchi siano sistemi di trasporto, dighe, acquedotti, centrali per l'energia, ossia tutto ciò che oramai possiede un indirizzo *ip* comandabile. Sebbene vi siano misure di sicurezza informatica appositamente studiate e installate, tuttavia, l'estrema velocità con cui nascono e si propagano forme di *malware* e la loro intrinseca insidiosità, impongono continui aggiornamenti non sempre realizzabili dai privati e i cui caratteri principali sconfinano in ambiti propri delle autorità pubbliche.

Al problema dell'individuazione dei responsabili degli attacchi in rete si affianca, infatti, quello delle responsabilità dei gestori delle infrastrutture, che appaiono differenti da Paese a Paese, perché diversa è la normativa che regola la gestione delle informazioni in rete, la sicurezza informatica, il concetto di violazione della *privacy*<sup>43</sup> e così

---

<sup>43</sup> Un esempio significativo al riguardo è dato dall'accordo di mutua collaborazione fra Google e National Security Agency (Nsa), ossia fra il più importante motore di ricerca e la principale agenzia di *intelligence* statunitense, che ha allertato gli internauti su quale potrebbe essere, in futuro e in base a questo accordo, il livello di intrusione dell'Agenzia nella *privacy* di chi utilizza la rete. Su quanto dibattuto presso gli ambienti politici e istituzionali statuniten-

via. Eppure, nel caso di attacco per l'avvio di una *cyberwar*, sono coinvolti per primi i privati per il solo fatto che da loro dipende il mezzo con cui si propaga l'aggressione. Ciò non avviene, per esempio, in Cina dove l'intera rete è di proprietà e sotto diretto controllo delle autorità centrali: certamente questo fatto costituisce un grosso limite per quanto riguarda la libertà d'informazione<sup>44</sup> e tutto quanto attiene il libero mercato, dal commercio alle transazioni finanziarie. A vigilare sulla sicurezza della propria infrastruttura informatica, infatti, è personale direttamente dipendente dal governo centrale (tanto da essere etichettato dal Dipartimento della Difesa statunitense come *cybermilitia*)<sup>45</sup>: non si tratta solo di censura, come normalmente e opportunisticamente viene divulgato dalla maggioranza dei mass media occidentali. La pirateria informatica e le attività di *crackers* sono diventate, infatti, un problema sociale complesso anche in Cina che, annualmente, registra un danno di oltre un miliardo di dollari, con attività che vanno dalle minacce all'estorsione. Solo nell'ultimo anno, il 98% delle imprese cinesi ha subito frodi, facendo posizionare la Cina al primo posto nella classifica dei Paesi più colpiti da cybercriminali, a cui seguono Colombia (94%) e Brasile (90%)<sup>46</sup>. Infatti, l'arretratezza dei *software* a disposizione degli utenti cinesi rende fallace il sistema di sicurezza informatica, anche quella utilizzata dalla rete governativa. Inevitabile che le autorità centrali si attivino in prima persona per arginare il rischio, così grave per la pacifica e diffusa realizzazione del socialismo di mercato<sup>47</sup>, troppo vulnerabile alle possibili infiltrazioni da parte di cybercriminali nazionali, ma anche di potenze occidentali nella rete militare per scopi spionistici e in quella globale nazionale al fine di alimentare il dissenso interno. Tuttavia,

---

si, proprio in relazione alla *privacy* e alla carenza di una cornice legale in cui andrà ad operare il *Cyber Command*, si veda [http://www.nsa.gov/public\\_info/\\_files/speeches\\_testimonies/100603\\_alexander\\_transcript.pdf](http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf).

<sup>44</sup> Su questo aspetto si è scatenato lo scontro fra Google e Cina e ha dato l'opportunità agli Stati Uniti, per voce del suo Segretario di Stato, Hillary Clinton, di sottolineare il valore universale della libertà di e su internet, tanto da ipotizzare persino un mini cyber-asse del male, composto per l'appunto da Cina, Tunisia, Uzbekistan, Vietnam, Egitto e Arabia Saudita, protagonisti della censura della rete. Si veda al riguardo, DESIDERIO, *Usa-Google vs Cina: la guerra dei bit/1*, in <http://temi.repubblica.it/limes/usa-google-vs-cina-la-guerra-dei-bit/10616>.

<sup>45</sup> Si veda SHANE, *China's Cyber-Militia*, in *The National Journal*, 31 May 2008.

<sup>46</sup> Si veda al riguardo ECONOMIST INTELLIGENCE UNIT, *Global Fraud Report*, [www.kroll.com](http://www.kroll.com), 22-23.

<sup>47</sup> Si veda TAI, *The Internet in China. Cyberspace and Civil Society*, New York, 2006, cap. 3; ZHANG, WOESLER, *China's Digital Dream: The Impact of Internet on Chinese Society*, London, 2004.

non è nemmeno segreta la strategia delle autorità cinesi di fronte all'eventualità di una *cyberwar*<sup>48</sup>, in cui gli obiettivi economici e commerciali delineano l'ipotesi di una guerra cibernetica fra Pechino e potenze più industrializzate.

Dall'altro lato, gli stessi attacchi informatici all'Occidente di cui si è avuta chiara l'origine cinese<sup>49</sup>, riconducono inevitabilmente a responsabilità di *crackers* al servizio delle autorità centrali, dando una valenza diversa all'intrusione, non più solo criminale. Come reagire in questi casi? Come si può distinguere un'offensiva tipica di spionaggio industriale o commerciale da un vero e proprio attacco di natura più ampia, in cui è in gioco la sicurezza di una o – viste le caratteristiche globali della rete – più nazioni?

Il punto di partenza dovrebbe essere la definizione univoca, veramente globale, da parte degli organismi sovranazionali preposti alla sicurezza, della chiara distinzione fra *cybercrime* e *cyberwar*, superando quelle barriere politiche ma soprattutto culturali, che impediscono di definire, per esempio, i termini giuridici che prevedano, qualora siano colpevoli di azioni criminali o spionaggio industriale, l'estradizione di soggetti, oppure, nel caso di guerra, la definizione degli ambiti in cui attuare azioni legali transnazionali, come l'embargo o le sanzioni economiche. Se nel caso del crimine informatico si registra, a livello mondiale, una sensibilità maggiore e un'intensa attività di collaborazione fra autorità statali e imprese, soprattutto quelle private più attente alla sicurezza in rete, non altrettanto vale per il rischio di guerra informatica fra Stati. Sino ad ora sono stati raggiunti accordi bilaterali o al massimo regionali; ma è la natura del terreno di confronto, ossia la globalità della rete, che suggerisce quanto questi sforzi possano essere lodevoli ma pericolosamente insufficienti.

Una volta compreso che la *cyberwar* non è poi così improbabile e che un crimine informatico può trasformarsi da un momento all'altro in un'emergenza internazionale, compito urgente e che spetta in primo luogo ai giuristi internazionalisti è proprio quello di definire i contorni legali in cui inquadrare nozioni che definiscano sia lo *jus ad bellum*,

---

<sup>48</sup> Si veda al riguardo WEI, ZHEN, *Recent Development in the Study of the Thought of People's War under Informatized Conditions*, in *China Military Science*, vol. II, 2009; O'BRIEN, *Rising Airpower: The People's Liberation Army Air Force in the Early 21<sup>st</sup> Century*, in *Air&Space Power Journal*, 24 Apr. 2003.

<sup>49</sup> [http://thecable.foreignpolicy.com/posts/2010/01/22/the\\_top\\_10\\_chinese\\_cyber\\_attacks\\_that\\_we\\_know\\_of](http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of); US-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, *Capability of the People's Republic of China to Conduct CyberWarfare and Computer Network Exploitation*, McLean (VA), 2009, 67-74.

ossia i principi legali che regolano l'entrata in guerra di una nazione, sia lo *jus in bello*, quelli che definiscono i comportamenti delle parti in caso di un attacco informatico tanto devastante da portare al conflitto. Da ciò dipende la coesistenza pacifica nel cyberspazio, ma soprattutto e in primo luogo la salvaguardia dell'incolumità della popolazione civile.

Vi è, inoltre, un altro rischio con maggiori probabilità di realizzarsi, ossia l'uso della *cyberwar* da parte di organizzazioni terroristiche<sup>50</sup>, posizionate in cima alla lista delle cyber potenze, dopo Stati Uniti, Cina, Russia, Iran, Francia e prima di Israele. La rete di per sé è uno degli strumenti preferiti dai gruppi terroristici e non solo per rivendicare le proprie azioni, ma anche per propaganda, ingaggio di nuovi militanti, raccolta di fondi e così via. Rifacendosi a quanto scritto più sopra, relativamente al limitato costo di programmi malevoli da lanciare in rete e infettare obiettivi sensibili, si può facilmente dedurre che il cyberspazio possa essere un terreno d'azione futuro per i terroristi. Senza voler creare facili allarmismi, tuttavia, è necessario prendere coscienza che è più probabile per il singolo cittadino cadere vittima di un attacco terroristico in rete che di un atto condotto con strumenti tradizionali, come dirottamenti aerei, autobombe, etc. Si tratta di un ampliamento del concetto di *cyberwar*, sebbene si sia più propensi a considerare il *cyberterrorism* – ma il dibattito è molto ampio e presenta numerose sfaccettature che variano per via di impostazioni culturali differenti – più come un'azione criminale: anche in questo caso, la distinzione fra un atto criminale e quello terroristico dipende dagli obiettivi colpiti e degli scopi che si vogliono raggiungere. Ed è chiara, ormai globalmente, la natura destabilizzante, caotica e fortemente limitativa della quotidianità propria delle azioni terroristiche rispetto alle azioni criminali, volte per lo più a ottenere vantaggi economici e finanziari. Gli effetti negativi della *cyberwar* – e quindi del *cyberterrorism* – come visto sino ad ora, possono limitarsi a semplici danni economici o finanziari fortemente penalizzanti, ma anche allargarsi a settori nevralgici, come il traffico aereo e ferroviario, gli acquedotti e così via e mettere a repentaglio la vita stessa dei cittadini. Qualora non si profili l'eventualità di una guerra, di certo per questi motivi vengono soddisfatte tutte quelle evenienze atte a definire alcuni

---

<sup>50</sup> È stato attribuito a Osama bin Laden anche il primato di aver lanciato il primo manifesto sul cyberterrorismo, nel 2000, dal titolo *Al-jihad al-electronic*. Si veda GHIONI, *Hacker Republic*, Milano, 2009, 61; ALSHECH, *Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad*, in <http://www.jpost.com/Home/Article.aspx?id=53004>.

tipi di attacchi informatici, che provengano da Stati o da gruppi terroristici, come “crimini contro l’umanità”.

La definizione dei termini giuridici comporta, quindi, un lungo percorso di rielaborazione di concetti, estremamente laborioso e difficoltoso, data anche la tendenza – almeno sino ad ora – a circondare di segretezza gli innumerevoli attacchi informatici a cui sono sottoposti quotidianamente siti istituzionali, politici, economici, finanziari, industriali ma anche militari. Il rischio e le emergenze proprie della *cyberwar* dovrebbero essere, invece, oggetto di dibattito pubblico e di confronto internazionale<sup>51</sup> che chiariscano i termini sui tempi e le modalità delle armi informatiche e definiscano i contorni giuridici in cui poter delineare una dottrina operativa di difesa o di risposta. Ciò è possibile solo attraverso la condivisione delle informazioni fra imprese e strutture private – più vulnerabili agli attacchi – e le agenzie governative preposte alla sicurezza non solo della rete, ma della nazione vera e propria. La condivisione di informazioni e di esperienze è strategica per dare una risposta a interrogativi, come quello di stabilire fino a che punto possano spingersi i governi per proteggere la sicurezza dei loro cittadini<sup>52</sup>, così come dell’evenienza di istituire un trattato internazionale, possibilmente sotto l’egida delle Nazioni Unite, sull’uso delle armi informatiche<sup>53</sup>, tenendo conto che il bando di questi “nuovi sistemi d’arma” non ha ragione di esistere, dato che l’evoluzione tecnica è così veloce che un’eventuale lista di armi cibernetiche vietate dovrebbe essere aggiornata a ritmo frenetico.

È auspicabile, infatti, che si proceda dapprima a questo tipo di cooperazione, da regionale a internazionale, per l’elaborazione dei termini giuridici ed, in seguito, per quelli operativi militari veri e propri, in modo da affrontare la *cyberwar* attraverso un insieme di tecnologia difensiva e di approcci analitici che utilizzino al meglio quanto appreso con l’*information warfare*, l’azione diplomatica e la condivisione delle esperienze: e dato l’alto numero di attacchi, che ben contribuiscono a comporre una casistica chiara dei caratteri di questa guerra è opportuno che gli enti sovranazionali preposti agi-

---

<sup>51</sup> Si veda CHE, *Securing a Network Society. Cyber-Terrorism, International Cooperation and Transnational Surveillance*, RIEAS Research Paper, n. 113, Sept. 2007.

<sup>52</sup> Si veda RATTRAY, *Strategic Warfare in Cyberspace*, Boston, 2001; l’autore nei riguardi del cyberspazio sottolinea l’importanza che ha avuto il dibattito pubblico per la definizione del concetto di *counterforce* contrapposto a quello di rappresaglia nella definizione della strategia nucleare degli Stati Uniti negli anni ’50 e ’60.

<sup>53</sup> Si veda SCHJØLBERG, *Wanted: A United Nations Cyberspace Treaty*, in NAGORSKI, (ed.), *Global Cyber Deterrence*, New York, 2010.

scano al più presto. Anche solo un protocollo di intesa a livello internazionale, che escluda gli obiettivi “civili” dai *cyberattacks* nel corso di una guerra informatica fra Stati e che ne preveda le contromisure in caso di violazione, potrebbe costituire un primo passo per fare uscire la *cyberwar* dalla sua zona grigia legale e strategica. La definizione, invece, della dottrina operativa in caso di attacco potrebbe anche solo essere limitata a organismi regionali per la sicurezza come l’OSCE o di mutua difesa come la NATO: quanto può valere in una guerra cibernetica l’articolo 5 del Trattato NATO che prevede il principio di difesa comune per cui un attacco contro un suo membro rappresenta un attacco al resto delle nazioni che vi fanno parte? A questo e ad altri interrogativi cerca di dare una risposta il gruppo di lavoro guidato dall’ex Segretario di Stato, Madeleine Albright, e creato all’interno della NATO in vista della ridefinizione di ruoli e compiti dell’organismo proprio per affrontare con un nuovo *strategic concept* le sfide nel cyberspazio. Ma il punto di partenza deve essere, obbligatoriamente, la presa di coscienza del rischio che il dominio degli spazi sia il vero oggetto del contendere globale fra nazioni anche quelle, come l’Italia, fra gli ultimi posti nella classifica dei Paesi digitalizzati e non certo in grado, da sola, di competere per la conquista dello spazio, ma nemmeno di evitare i contraccolpi di una *cyberwar* lanciata da *crackers* con fini destabilizzanti o terroristici.

4. *Conclusioni*- Le nuove sfide fra potenze militari riconducono, quindi, al dominio degli spazi: il cosmo è da tempo obiettivo di conquista e di rinata competizione, mentre quello cibernetico è diventato terreno di scontro anche fra nazioni meno dotate militarmente ma tecnologicamente più avanzate solo in questo primo decennio del XXI secolo, da quando nuovi soggetti politici ed economici si sono affacciati nell’arena della politica internazionale. La condivisione delle innovazioni tecnologiche proprie dei sistemi Ict ha permesso la nascita di nuovi sistemi d’arma, complessi ma accessibili ad un numero sempre più ampio di soggetti e non necessariamente solo Stati-nazione, che ha finito per influenzare globalmente i sistemi di sicurezza nazionali. Nessun sistema d’arma, fino ad ora, aveva compresso in maniera così drastica gli inevitabili dislivelli di potenza militare, propri della competizione tradizionale fra Stati, potendo contare su *know how* e mezzi propri, come dimostra il caso di Israele, ad esempio, all’avanguardia in questo campo e senza la dipendenza da tecnologie o assi-

stenze straniere<sup>54</sup>. Compreso, quindi, che la *cyberwar* è diventata una realtà diffusa, sebbene secretata, ed estremamente pericolosa, perché si adatta ad essere ampiamente utilizzata in scenari sensibili, come ad esempio quello mediorientale, e da soggetti fortemente destabilizzanti, come i gruppi terroristici, è ora urgente affrontarla nella convinzione che i nuovi equilibri di forza geopolitica hanno ragione di esistere in questa competizione senza più confini territoriali per un unico obiettivo, ossia la creazione di una *cyber diplomacy* in grado di regolamentare i rapporti fra i suoi protagonisti.

Le pressioni più insistenti al riguardo provengono proprio dalla nazione che maggiormente viene indicata come “mandante” o addirittura individuata come “fonte” degli attacchi informatici, ovvero la Russia<sup>55</sup>, a dimostrazione che quanto avviene nello spazio cibernetico può essere frutto di manipolazioni esterne e diventare un'emergenza nazionale in grado di compromettere le relazioni diplomatiche. Gli sforzi per fronteggiare le minacce e limitare i danni a semplici strutture, senza conseguenze devastanti per la popolazione civile, sono stati per lo più bilaterali o regionali<sup>56</sup>, e hanno registrato anche l'impegno di nazioni, come la Cina, sovente coinvolta in azioni di crackeraggio, sia per scopi militari che civili<sup>57</sup>.

Se la diplomazia rallenta o, peggio, fallisce e ad emergere sono gli interessi nazionali o regionali che fanno capo ad una superpotenza del cyberspazio, il rischio di una sua “militarizzazione”, così come si sta prospettando per il cosmo, delinea scenari molto inquietanti. Nel maggio del 2009, il presidente Obama evidenziava la sua preoccupazione circa l'inadeguatezza statunitense nell'investire nella sicurezza delle infrastrutture digitali<sup>58</sup>, ma ancor prima, già nel 2000, il presidente Putin lamentava per la Russia carenze di questo tipo e nello

---

<sup>54</sup> Si vedano, al riguardo, le dichiarazioni del capo dell'*intelligence* israeliana, Amos Yadlin, riportate in WILLIAMS, *Spymaster Sees Israel as World Cyberwar Leader*, <http://www.reuters.com/article/idUSTRE5BE30920091215>.

<sup>55</sup> Su tale argomento si veda <http://www.unidir.org/pdf/articles/pdf-art2645.pdf>; <http://www.unidir.org/pdf/articles/pdf-art2642.pdf>.

<sup>56</sup> Si veda GADY, AUSTIN, *Russia, The United States, and Cyber Diplomacy. Opening the Doors*, New York, 2010, [http://search.mod.gov.cn/search/gfbsearch/sitesearch\\_eng.jsp#](http://search.mod.gov.cn/search/gfbsearch/sitesearch_eng.jsp#); [http://eng.mod.gov.cn/TopNews/2010-10/08/content\\_4198942.htm](http://eng.mod.gov.cn/TopNews/2010-10/08/content_4198942.htm).

<sup>57</sup> Si veda al riguardo [http://search.mod.gov.cn/search/gfbsearch/sitesearch\\_eng.jsp#](http://search.mod.gov.cn/search/gfbsearch/sitesearch_eng.jsp#); [http://eng.mod.gov.cn/TopNews/2010-10/08/content\\_4198942.htm](http://eng.mod.gov.cn/TopNews/2010-10/08/content_4198942.htm).

<sup>58</sup> *President Obama's Remarks on Securing U.S. Cyber Infrastructure*, 29 May 2009, <http://www.america.gov/st/texttransenglish/2009/May/20090529161700eaifas0.1335871.htm>; CYBERSPACE POLICY REVIEW, *Assuring a Trusted and Resilient Information and Communications Infrastructure*, Washington DC, 2010, [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf).

sviluppo di tecnologie spaziali tali da compromettere la stessa sicurezza nazionale<sup>59</sup>: in entrambi i casi, si auspicava un maggior sforzo economico da parte delle rispettive nazioni per affrontare una mutazione così radicale dei propri sistemi di sicurezza dovuta all'incessante evoluzione tecnologica e alle nuove minacce provenienti dall'esterno. E come visto sino ad ora, l'approntare misure difensive nella *cyberwar* risulta essere estremamente laborioso in termini di politica nazionale e internazionale, ma soprattutto induce a investimenti decisamente onerosi per la ricerca e per l'innovazione tecnologica.

Lo scenario assume caratteristiche allarmanti quando, già nel 2004, in un altro testo dei due già citati generali cinesi, Qiao Liang e Wang Xiangsui, si affermava, senza tanti preamboli, che terminata l'era delle guerre per l'espansione territoriale e per il controllo delle risorse naturali, il vero obiettivo dei conflitti futuri sarebbe stato il controllo dei flussi dei capitali finanziari<sup>60</sup>. Date queste linee strategiche ipotizzate da due autorevoli esponenti dell'ambiente militare cinese e le caratteristiche oramai estremamente informatizzate di dati economici e bancari, operazioni finanziarie e di Borsa, il rischio è che veramente possa avverarsi il confronto fra potenze attraverso sofisticate *cyberwars* in grado di annientare la struttura economica, produttiva e finanziaria di una o più nazioni. Allo stato attuale della difesa e della sicurezza dei flussi di dati, circolanti nel cyberspazio, anche secondo i massimi esperti statunitensi, il rischio di un 11 settembre informatico o un *cybergeddon* è realmente plausibile.

Tuttavia, senza arrivare a scenari così catastrofici, sebbene probabili, sono segnali chiari e credibili e, a nostro avviso anche premonitori di scontri più cruenti, quelli provenienti dalle dispute sul cyberspazio che parlano di controllo delle informazioni e di rispetto dei diritti umani e che vedono contrapporsi chiaramente l'Occidente e tutto quanto si ricollega alla globalizzazione di stampo americano, e quanto ad essa si sta velocemente opponendo, in termini di modelli economici e culturali, come la Cina, appunto<sup>61</sup>. Che lo scontro fra grandi potenze militari si combatta ormai su piano economico e finanziario è chiaro da tempo; ad aggravare questo aspetto interviene il

---

<sup>59</sup> *Information Security Doctrine of the Russian Federation*, Sept. 2000. <http://www.mid.ru/nsosndoc.nsf/le5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b?OpenDocument>.

<sup>60</sup> Si veda LIANG, XIANGSUI, *Fully Calculating the Costs and Profits of War*, in WEIGUANG (ed.), *On the Chinese Revolution in Military Affairs*, Beijing, 2004.

<sup>61</sup> Si veda TAPPERO MERLO, *L'Aquila e il Toro. Globalizzazione post-americana e conflitti*, Trento, 2009.

confronto, non armato ma non per questo meno pericoloso, fra livelli di crescita produttiva, in cui l'Occidente sta perdendo terreno in seguito alla depressione innescata dai crolli di Borsa del 2008 e dalla crisi ancora più profonda di tipo strutturale, a favore di nazioni come Cina, India, Russia e Brasile. Se a ciò si aggiunge che le sorti dell'alta tecnologia su cui punta la leadership mondiale statunitense e il confronto a colpi di bit e terabyte con i suoi principali antagonisti, dipende da quel 97% di produzione cinese di metalli rari, c'è di che preoccuparsi, in particolare per le sorti dello sviluppo industriale e finanziario trainato dall'altalenante destino dell'economia della nazione americana. Anche da questo elemento, che possiamo definire di *cybereconomy*, come quello della lotta per il controllo delle informazioni o *infowar*<sup>62</sup> – in cui ben si adatta ed opera l'inganno, arma preferita dallo stratega Sun Tzu – dipende il futuro di ciò che abbiamo definito “il dominio degli spazi”, l'identificazione dei suoi protagonisti e delle forme di lotta per la sua conquista e il suo controllo. La *cyberwar* rappresenta il suo aspetto più pernicioso e dalle conseguenze più deleterie per la popolazione civile: è necessario intervenire urgentemente per evitare di venirci sopraffatti, nella consapevolezza che, in futuro, la coesistenza pacifica fra Stati non sarà messa in pericolo dai conflitti guerreggiati sui campi di battaglia ma, paradossalmente, dal confronto fra modelli economici e finanziari vincenti, in grado quindi di permettere lo sviluppo e l'evoluzione di un'alta tecnologia atta a difendere la globalità delle nazioni da assalti destabilizzanti nel cyberspazio, qualunque sia la loro origine.

---

<sup>62</sup> Si veda in particolare MAINOLDI, *Echelon e la società del futuro*, in <http://temi.repubblica.it/limes/echelon-e-la-societa-del-futuro/9569>.

