Eunomia. Rivista semestrale di Storia e Politica Internazionali
Eunomia VIII n.s. (2019), n. 2, 67-88
e-ISSN 2280-8949
DOI 10.1285/i22808949a8n2p67
http://siba-ese.unisalento.it, © 2019 Università del Salento

VALERIO GRECO

Cyberspazio. La nuova arena del potere

Abstract: *The cyberspace, place of action and object of contention between old and new actors of the international relations, in the XXI century became crucial for the power and for the international policy issues. After land, sea, air and outer space, the cyberspace represents the fifth dimension of conflicts and the new arena of the power. Indeed, the international scenario driven by the IT revolution and the globalizing trends, is moving from unipolar to multipolar, causing a deterioration of the statocentric structure. For this reason, the interest in the cyber domain is motivated by the new way of policy making inside it. In this new strategic environment is necessary to refresh the classic deterrence theory to obtain an effective defense, by means of a cyber security. It should be based on a strong global collaboration, whose aim is reducing the risk of a «data war», fought with bits.*

Keywords: Cyberspace; Information and Communications Technology (ICT); Cyberpolitics; Cyberpower; Hi-tech war; Digital Militarization; Cybersecurity.

I progressi nel settore scientifico e tecnologico hanno favorito lo sviluppo economico e reso più affidabile, sotto alcuni aspetti, la *national security*; in effetti, l'analisi dei fatti storici dimostra che i grandi mutamenti nella politica mondiale sono sempre stati la conseguenza di guerre e rivoluzioni tecnologiche ed economiche (si pensi alla rivoluzione industriale): tutto è stato condizionato dalla costante ricerca di risorse, materiali ed immateriali; e quando c'è uno spostamento continuo di esse il sistema internazionale muta in maniera incisiva, con una modifica delle alleanze e la nascita di nuovi avversari come effetti più diretti.

Allo stesso modo ed in maniera ancora più marcata, le *Tecnologie dell'Informazione e della Comunicazione* (TIC)[1] stanno modificando radicalmente le dinamiche delle RI attraverso un rimodellamento della struttura del sistema internazionale, un rinnovamento dei suoi processi tradizionali,[2] così come la raccolta

[1] Infrastrutture "geneticamente" legate al dominio cibernetico.

[2] Si pensi alla "diplomazia digitale" come causa di una trasformazione radicale nei processi di comunicazione. Dopo gli ultimi dieci anni si può parlare di una vera e propria rivoluzione in ambito diplomatico; in particolare, l'adozione di piattaforme di *social media* da parte dei ministeri degli esteri ha notevolmente cambiato il modo in cui la *Public Diplomacy* gestisce le informazioni, le crisi internazionali

di dati sensibili per l'*intelligence* e la creazione di nuovi problemi per la politica mondiale.

La tecnologia, perciò, avvicina il mondo ed allo stesso tempo lo divide, in quanto strumenti come Internet e i satelliti sono ampiamente utilizzati anche e soprattutto in ambito militare da entità subnazionali e da singoli individui che sottraggono il tradizionale monopolio del controllo e della forza agli stati. Ulteriori sviluppi nei settori della nanotecnologia, della robotica e dell'intelligenza artificiale, infatti, potranno modificare ulteriormente i rapporti di forza fra le nazioni, introducendo nuovi strumenti nella conduzione dei conflitti futuri: si tratta di un progresso esponenziale che porta ad un aumento di potenza e a una diminuzione contestuale dei costi, con conseguenze facilmente immaginabili. La sfida per il controllo delle informazioni, la difesa da intrusioni e l'incessante raccolta di esse, perciò, rappresentano il nuovo campo di battaglia nel quale il fragile confine tra civile e militare viene meno.

Lo sviluppo tecnologico, ed in particolare delle TIC, dunque, non favorisce tutti nella stessa misura; i paesi che hanno la capacità di innovarsi maggiormente e prima degli altri, infatti, godono di vantaggi strategici importanti. Si prevede uno scenario in cui si assisterà all'avvio di una serie di competizioni commerciali e politiche nel settore degli *Internet services*; ed è facile comprendere che il confronto per il controllo della rete avrà delle ripercussioni sull'intero sistema internazionale. In effetti, emerge a chiare lettere una vera e propria geopolitica del *cyberspace*, dimensione che, come tutti gli altri *habitat* dell'attività umana, si conferma essere sottomessa alle azioni della politica.

La tecnologia, insomma, come sempre è accaduto nella storia, resta la più importante variabile interpretativa per comprendere le relazioni internazionali e i mutamenti negli assetti di potere: nell'era cibernetica chi sarà tecnologicamente più all'avanguardia dominerà il mondo.

ed i negoziati, in un quadro globale nel quale i nuovi soggetti non governativi hanno assunto un crescente ruolo di influenza.

1. *Il* cyberspace *e la guerra cibernetica: verso l'e-conflitto*

Come insegna Tucidide, «la guerra è maestra di violenze»;[3] e secondo lo stratega ateniese tre sono i motivi per i quali un uomo decide di abbracciare le armi: l'onore, l'interesse e la paura. Questi ultimi, però, risultano "arcaici" nell'ambito della società occidentale odierna che, per effetto del progresso e della prosperità, ha deciso di rendere "invisibile" la guerra non potendo eliminarla definitivamente. Il problema, perciò, non riguarda più il fatto se sia utile o meno combatterla, quanto piuttosto se sia possibile affrontarla; ed il "possibile" è dato dalla cifra derivante dal calcolo tra costi e benefici dettato dalla contrarietà della società ad accettare la perdita di vite umane e dalla riluttanza ad abbandonare il proprio stile di vita basato sul benessere.

Anche i conflitti, pertanto, si adattano ai tempi; negli ultimi anni, in particolare, si è assistito all'avvento della dottrina militare occidentale basata sull'opzione "morti zero": le società moderne sono talmente allergiche alle perdite (umane ed economiche) da essersi de-bellicizzate, creando tecniche militari *risk-free* ("prive" di rischio) con dispositivi di arma capaci di garantire un combattimento a distanza di sicurezza, in modo tale da eliminare tutti gli effetti collaterali di un conflitto armato tradizionale. In altri termini, è una guerra facile che, nel caso di fallimento, non genera conseguenze gravi per chi combatte dietro uno schermo o con in mano un *joystick*. Pur assistendo ad una vera e propria robotizzazione della guerra, comunque, l'equivoco sostanziale che bisogna sfatare è proprio quello di credere che una *clean war*, a rischio zero, invisibile, distante, possa decretare la fine della conflittualità dall'esperienza umana; una guerra, infatti, per quanto "snaturata" è pur sempre "maestra di violenza"; esiste un errore di fondo, perciò, nel considerare queste nuove tecniche militari annunciatrici di un'era priva di conflitti.

Dopo aver analizzato l'impatto dell'era cibernetica sulle odierne relazioni internazionali e aver posto l'accento sulle varie peculiarità della natura geopolitica e geografica del *cyberspace*, dunque, è opportuno approfondire le conseguenze del *medium* cibernetico dal punto di vista più strettamente militare, sulla base delle

[3] TUCIDIDE, *La Guerra del Peloponneso*, a cura di E. SAVINO, Milano, Garzanti, 2007.

seguenti premesse:

- nel *cyberspace* i confini tra il fisico ed il virtuale, così come quelli tra il militare ed il civile, tendono a confondersi;
- la guerra cibernetica può consentire agli attori coinvolti di raggiungere i loro obiettivi politici e strategici senza la necessità di un conflitto armato;
- nel breve periodo, le azioni condotte attraverso i sistemi informatici (per mezzo di *server* stranieri, identità fittizie, etc.) favoriscono l'anonimato e una relativa impunità;
- sul piano giuridico, le operazioni di *cyber war* ricadono generalmente nella cosiddetta "negazione plausibile";[4]
- il *cyberpower*, che concede un potere sproporzionato anche ad attori minori e relativamente deboli, può essere esercitato da stati[5] o da soggetti non statali in tempo di guerra così come in tempo di pace.

Ai fini di questo saggio è opportuno, inoltre, porsi le seguenti domande che serviranno come linee guida per individuare le caratteristiche fondamentali della guerra cibernetica:

- Che cosa si intende per *cyber warfare*?[6]
- Quando è possibile classificare un'azione virtuale come un atto di guerra?
- Chi sono gli attori principali?
- Come agiscono?
- Perché agiscono?

[4] Tale termine, coniato dall'*intelligence* americana durante l'amministrazione Kennedy, definisce quei casi in cui sia possibile dichiararsi formalmente estranei a qualsiasi fattispecie condannabile commessa da terzi dei quali si abbia responsabilità o comando diretto. Normalmente la negazione plausibile è una misura di salvaguardia verso chi ricopre incarichi pubblici al fine di preservare la sua buona fede nel momento in cui dovesse trovarsi costretto a dichiarare di essere ignaro dei fatti oggetto di inchiesta. In ambito di *cybersecurity*, nello specifico, si parla di "crittografia negabile" con riferimento all'uso di sistemi crittografici che consentono ad un utente, qualora gli venga estorta la *password* di un archivio cifrato, di negare l'esistenza dell'archivio stesso.

[5] È opportuno evidenziare che, nonostante la diffusione del potere abbia sancito il declino dello stato-nazione in termini di monopolio della forza e delle informazioni, il punto non è se lo stato continuerà ad esistere, bensì quale sarà il suo modo di funzionare.

[6] In lingua inglese, il termine "guerra" si traduce in due modi: *war*, che indica una situazione di conflitto tra stati; *warfare*, che si riferisce ai modi di combattere una guerra (per esempio, guerra convenzionale, biologica, chimica, nucleare e così via).

- Dove colpiscono?
- Quali sono i principali strumenti operativi?

2. *La guerra del futuro: alla ricerca di una definizione*

Studi su una possibile guerra che sfrutti interamente le potenzialità del cyberspazio sono iniziati negli Stati Uniti quando è andata diffondendosi la paura per il cosiddetto *Millennium Bug.*[7] Da allora sono state approfondite le ricerche al riguardo, ma l'accrescere dell'interesse verso un fenomeno, inevitabilmente, porta con sé anche molto rumore, confusione e generalizzazione; così anche le attività informatiche di adolescenti irresponsabili possono trasformarsi in *cyber* crimini[8] e le azioni di classico spionaggio andate male possono diventare attacchi bellici. Alla luce di ciò, risulta chiaro che, con il termine cyberspazio, non si fa riferimento soltanto ad un *social network* o ad una piazza virtuale, ma anche ad un potenziale campo di battaglia con cecchini appostati e pronti a mietere vittime a colpi di *bit*.

Non esiste, tuttavia, una definizione univoca e condivisa su che cosa debba intendersi per "guerra cibernetica" data l'immaturità di questo campo di ricerca rispetto alle dinamiche della conflittualità tradizionale consolidatesi nel tempo. Scott Borg, dunque, evidenzia l'importanza di esplicare tale concetto per superare gli errori di valutazione dovuti soprattutto alle definizioni fuorvianti di politici inesperti e giornalisti accondiscendenti che hanno diffuso l'idea errata che la guerra non avesse più a che fare con un gran numero di vittime e con gravi danni materiali ed economici.[9] La guerra, invece, si diffonde *anche* attraverso il *medium* cibernetico ma con l'obiettivo reale di causare danni alle infrastrutture fisiche e ai sistemi militari.

---

[7] Dall'inglese "*millennium*" (millennio) e "*bug*" (insetto) – termine usato nel gergo informatico per indicare gli errori contenuti in un programma – questa espressione si è diffusa con l'avvicinarsi dell'anno 2000. I computer più obsoleti, infatti, indicavano la data del sistema con due sole cifre (l'anno 1998, ad esempio, era segnato come "98"); il "cambiamento di millennio", quindi, poteva portare a problemi inaspettati, quando le banche dati informatiche avrebbero datato i nuovi documenti del 2000 con la cifra "00", creando confusione con la data 1900.

[8] Nel 1999, Jonathan James, un ragazzino di appena quindici anni, attraverso l'installazione di una *backdoor* sui server della NASA e del Dipartimento di stato americano, è riuscito ad insinuarsi all'interno dei loro computer, spiando migliaia di *e-mail* contenenti molti documenti riservati, tra cui anche *password* di dispositivi militari.

[9] Cfr. S. BORG, *Logica della Guerra Cibernetica*, in «Limes», 26 aprile 2012.

Dello stesso avviso è Colin S. Gray, secondo il quale la mancanza di una definizione univoca è dovuta ad una serie di errori di valutazione che non contribuiscono a rendere giustizia all'affare *cyber*;[10] valutazioni distorte che prendono piede a seconda della specializzazione del loro promotore, il quale può essere un politologo maggiormente predisposto allo studio della strategia militare o, all'opposto, un esperto di informatica.

Secondo Martin Libicki, uno dei più autorevoli studiosi in tale settore, la *cyber war* consiste nell'utilizzo di ogni forma di tecnologia informatica per attaccare e distruggere attività di stati e organizzazioni, attraverso azioni politicamente motivate; essa, quindi, corrisponde a una forma di conflitto ben diversa da quelle classiche, che punta a sottomettere l'avversario alla propria volontà, senza agire fisicamente per conquistare il suo territorio; per questo, la guerra cibernetica può anche essere considerata come una forma di supporto ad azioni convenzionali.[11]

La *cyber war*, quindi, per essere definita "guerra" necessita di determinati elementi distruttivi e/o coercitivi, includendo oltre a tutte le forme di attacco anche quelle di difesa nell'ambito del *cyberspace*. Secondo Richard Clarke e Robert Knake, infatti, per *cyber warfare* si deve intendere «un'azione da parte di uno Stato atta a penetrare i sistemi informatici o le reti di un altro Stato con la finalità di causare danni o distruzione».[12]

Umberto Gori, infine, afferma che una corretta definizione di *cyber war* deve derivare dall'analisi del contesto in cui prende vita l'attacco cibernetico. Dal punto di vista dello studioso, infatti, è necessario valutare l'obiettivo finale dell'atto ostile; e perché un atto *cyber* possa essere definito "militare" deve avere una certa dose di letalità, tale da influenzare le scelte politiche.[13]

Un'azione diffusa digitalmente, in definitiva, è classificabile come atto di guerra

[10] Cfr. C.S. GRAY, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*, Carlisle, PA, SSI, 2013.
[11] Cfr. M.C. LIBICKI, *Cyberdeterrence and Cyberwar*, Santa Monica, CA, Rand, 2009.
[12] R.A. CLARKE - R.K. KNAKE, *Cyber War: The Next Threat to National Security and What to do About It*, New York, HarperCollins Publishers, 2010, p. 6.
[13] Cfr. U. GORI, a cura di, *Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche*, Milano, FrancoAngeli, 2019.

quando, interpretando Clausewitz,[14] lo strumento militare (anche virtuale) è utilizzato per costringere il nemico ad accettare la volontà di chi sferra l'attacco.

3. *L'erosione della sovranità nazionale e la "spoliticizzazione" della guerra*

La guerra, secondo Carl von Clausewitz, è un'attività sociale che non può essere ridotta né ad arte né a scienza; essa, dunque, si evolve continuamente e si adatta ai tempi e ai modi attraverso cui si sviluppa. Proprio per questo Clausewitz scrive che «la guerra […] rassomiglia al camaleonte perché cambia di natura in ogni caso concreto».[15]

Con la nascita dello stato moderno, la guerra è stata subordinata alla politica per cercare di porre dei limiti giuridici e militari alla coercizione. Nello specifico, è stata la pace di Westfalia[16] a sancire le regole di comportamento per imporre dei confini alla violenza tra le nazioni; e ciò ha garantito il superamento delle sanguinose guerre di religione combattute in nome del principio discriminatorio di "guerra giusta".[17] Proprio a tal proposito, Carl Schmitt, spettatore di due conflitti mondiali e dell'equilibrio del terrore nucleare, ha evidenziato che sono le delimitazioni spaziali assegnate alla pace e alla guerra a far comprendere che il problema centrale di ogni ordinamento giuridico non è tanto quello dell'abolizione della lotta armata, ma quello della sua delimitazione o regolamentazione.

L'attuale struttura del sistema internazionale, tuttavia, evidenzia quanto siano lontane le concezioni clausewitziana e schmittiana della guerra e della politica, della pace e della violenza. Lo sfaldamento dell'ordine mondiale stato-centrico, infatti, si è

[14] Carl Philipp Gottlieb von Clausewitz è stato un generale, scrittore e teorico militare prussiano. Maggior generale nell'esercito prussiano, combattente durante le guerre napoleoniche, è famoso per aver scritto il trattato di strategia militare *Della Guerra*, pubblicato per la prima volta nel 1832, ma mai completato a causa della morte precoce dell'autore.

[15] C. VON CLAUSEWITZ, *Della Guerra*, a cura di G. CARDONA, Milano, BUR Rizzoli, 2009, p. 130. Per l'autore, la guerra appartiene al dominio della vita sociale e rappresenta un conflitto di grandi interessi che ha una soluzione sanguinosa, e soltanto in questo differisce dagli altri. Egli la paragona all'arte del commercio (anch'esso, infatti, è un conflitto di interessi) e la accosta alla politica che può essere considerata, a sua volta, come un commercio su larga scala.

[16] La pace di Westfalia del 1648 mise fine alla cosiddetta guerra dei Trent'anni e alla guerra degli Ottant'anni.

[17] Cfr. C. SCHMITT, *Il Nomos della Terra nel Diritto Internazionale dello «jus publicum europaeum»*, a cura di E. CASTRUCCI, Milano, Adelphi, 1991.

rivelato il fattore principale dello stravolgimento della divisione classica tra guerra e pace;[18] lo stato-nazione come tradizionale attore egemone della politica internazionale, dunque, si è ritrovato a svolgere un ruolo sempre più sfumato nella società odierna (altamente tecnologizzata e globalizzata) in quanto la sua forma politica classica è stata erosa da più parti:

- da un lato, il declino del sistema internazionale a composizione unipolare (con gli USA come potenza egemone) ha iniziato a spalancare nuovi scenari sul piano della politica internazionale, dando il colpo di grazia alla sovranità degli stati;
- dall'altro, le entità non statali, che in passato avevano un ruolo ben definito e soprattutto più delimitato, ormai si sono "statalizzate" grazie alla loro capacità di modificare i processi decisionali, mettendo in discussione specialmente il monopolio della violenza, finora di "proprietà" degli stati nazionali.

Alla luce di questo, ci si deve aspettare lo sgretolamento, oltre che delle strutture politiche nazionali, anche delle forze militari e delle classiche dinamiche conflittuali. De-territorializzazione, intangibilità, ubiquità, velocità ed economicità rappresentano i pilastri su cui poggiano le "nuove guerre",[19] le quali vengono combattute attraverso i mezzi militari moderni messi a disposizione dall'evoluzione tecnologica che ha consentito la "virtualizzazione" delle operazioni belliche. Ciò ha portato al conseguente superamento della concezione trinitaria tanto sostenuta da Clausewitz (governo, popolo, esercito); la guerra contemporanea, così, non può essere più sottomessa alle limitazioni della politica, né tantomeno rispetta i limiti territoriali dello stato e, soprattutto, la vittoria militare non è né decisiva né il fine ultimo dello scontro.[20]

Secondo Alain Joxe, la fine del confronto bipolare ha reso sfocato il concetto odierno di guerra: con il venir meno della contrapposizione Est-Ovest, sulla quale

[18] Cfr. A. COLOMBO, *La Guerra ineguale. Pace e violenza nel tramonto della Società Internazionale*, Bologna, Il Mulino, 2006.
[19] Cfr. M. KALDOR, *Le nuove guerre. La violenza organizzata nell'età globale*, Roma, Carocci, 1999.
[20] Cfr. M. VAN CREVELD, *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*, New York, The Free Press, 1991.

poggiavano le relazioni internazionali post-belliche, è diventato impossibile scandire il tempo e lo spazio della conflittualità del XXI secolo; e se si è affermata una "rivoluzione militare", essa è stata inaugurata dagli Stati Uniti durante la guerra del Golfo nel 1990-91, i quali hanno esibito questo nuovo modo iper-tecnologico di "domare il camaleonte clausewitziano".[21]

Con l'affermarsi di questa concezione "caotica" del panorama internazionale, quindi, ormai si è di fronte a quella che può essere definita una "spoliticizzazione" della guerra e ad uno stravolgimento epocale del tradizionale concetto di arma.[22]

4. *Dall'unipolarismo e/o multipolarismo all'apolarismo*

Il saggista statunitense Alvin Toffler ha affermato che l'attuale "era dell'informazione" altro non è che il prodotto della "terza rivoluzione industriale".[23] La sua tesi poggia sulla concezione che la storia dell'umanità è frutto di un'evoluzione "a ondate": passando dalla rivoluzione agricola a quella industriale, infatti, si è giunti alla "terza ondata" dei nostri giorni. Le gerarchie del potere, dunque, investite da questi mutamenti, rischiano di essere gradualmente sostituite da

[21] I colonnelli cinesi Qiao Liang e Wang Xiangsui, nel loro celebre libro *Guerra senza limiti*, avevano già posto l'accento su come si sarebbe evoluto il concetto di guerra e di violenza all'alba del nuovo mondo post-bipolare. In particolare, gli autori evidenziano come gli USA, in seguito alla loro vittoria sull'avversario sovietico, non avessero tardato nel mostrare di avere il monopolio tecnologico e militare in occasione dell'eccezionale dispiegamento di forze durante la guerra del Golfo, rivelando la superiorità americana in campo tecnologico prima ancora che militare, e rompendo con i tradizionali concetti di guerra e di armamento. Cfr. Q. LIANG - W. XIANGSUI, *Guerra senza limiti. L'arte della guerra asimmetrica fra terrorismo e globalizzazione*, Gorizia, LEG, 2007.

[22] Una *cyber arma* (o *cyber weapon*) può essere definita come un'apparecchiatura, un dispositivo, ovvero qualsiasi insieme di istruzioni informatiche dirette a danneggiare illecitamente un sistema informatico o telematico avente carattere di infrastruttura critica, le sue informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Le *cyber weapons* offensive possono essere di tre tipi: semplici, moderatamente complesse e complesse, e ciò in funzione della conoscenza ottenuta sui sistemi di controllo dell'obiettivo. Nel primo caso, si sfrutta direttamente la mancanza di autenticazione; nel secondo, si procede preliminarmente ad individuare il processo di controllo e, nel terzo, il processo stesso viene alterato di nascosto con la conseguenza che il bersaglio non si rende conto del pericolo. Dato che molte strutture sono isolate da Internet, inoltre, vengono studiate altre soluzioni (oltre alle chiavette USB), come l'uso di segnali radio per inserire *malware* in remoto. L'uso di armi cibernetiche, comunque, presenta anche dei problemi e, per questo, può essere limitato in zone critiche al fine di evitare danni collaterali a strutture civili (ospedali, etc.); anche perché un codice distruttivo, tramite tecniche di *reverse engineering*, può essere rimbalzato contro il mittente.

[23] Cfr. A. TOFFLER - H. TOFFLER, *The Politics of the Third Wave*, Atlanta, Andrews and McMeel, 1995.

cyber organizzazioni non statali e di perdere gran parte delle loro funzioni governative; in questo modo, potrebbe crearsi un nuovo modello di *governance* mondiale con il conseguente superamento dello stato-nazione.

L'elemento centrale che caratterizza l'attuale panorama internazionale, come già accennato, è l'intangibilità delle azioni poste in essere attraverso il dominio cibernetico; in questo ambiente "evanescente", perciò, possono accedere sia gli stati che gli attori non statali, i quali riescono a scavalcare i limiti (fisici e/o normativi) imposti da ogni nazione per accedere a un numero indefinito di informazioni e di funzioni. Ed è importante evidenziare che tale potenziale non si limita a settori specifici interconnessi con il dominio cibernetico, come lo spostamento di denaro o di altri beni, ma rientrano nell'ambito di queste attività anche e soprattutto questioni esclusivamente militari.

Secondo Nye, si sta assistendo per la prima volta ad una vera e propria "diffusione del potere" capace di mettere in discussione il monopolio della violenza, prerogativa storica degli stati: si tratta di una migrazione della sovranità nazionale verso attori privati non governativi.[24] Per i fautori della visione rivoluzionaria, perciò, è in corso una revisione radicale della concezione originaria dell'amministrazione del potere; grazie ai moderni mezzi di propagazione delle minacce messi a disposizione dalla tecnologia, in altre parole, le azioni violente stanno diventando sempre più intangibili e globali, non più espressioni di fini politici condivisi.[25]

Già nel 1994, in uno studio condotto dal Pentagono si è parlato di "futuri nemici" con riferimento a quelle forze diverse dagli stati-nazione che, attraverso l'utilizzo delle tecnologie moderne, acquisiscono capacità simili a quelle statali. A seconda dello scopo di ognuna di esse, si possono individuare tre categorie:

[24] Cfr. J. NYE, *Is America in Decline?*, Londra, Chatham House, 2010.
[25] «Se si toglie la giustizia, cosa sono gli Stati se non grandi bande di ladri? D'altra parte cosa sono le bande di ladri se non piccoli Stati? Anch'essi sono un gruppo di uomini governati dall'autorità di un capo, impegnati in un patto sociale, d'accordo su una legge per dividersi il bottino». SANT'AGOSTINO, *La Città di Dio*, a cura di D. MARAFIOTI, Milano, Mondadori, 2015, p. 167.

1. forze subnazionali: da esse derivano minacce subnazionali che comprendono i conflitti politici, razziali, religiosi, culturali ed etnici. Sono questi ultimi che mettono in discussione dall'interno l'autorità delle nazioni;

2. forze anazionali: da esse derivano minacce che non sono associabili ai paesi cui appartengono; tali entità, infatti, non fanno parte di uno stato-nazione né desiderano acquisire tale *status*. Per fare qualche esempio, si pensi alla criminalità organizzata regionale ed alle attività terroristiche;

3. forze metanazionali: da esse derivano minacce che oltrepassano i confini degli stati ed agiscono su scala interregionale o mondiale. Tra queste vi sono movimenti religiosi, organizzazioni economiche informali, etc.

La rivoluzione tecnologica, quindi, da un lato ha consentito un processo di democratizzazione dell'informazione senza precedenti e, dall'altro, ha favorito e rafforzato le cosiddette *networked organizations* che hanno acquisito un vantaggio operativo rispetto alle classiche forme piramidali e statiche che caratterizzano la struttura statale. Ciò permette una comunicazione diretta tra i vari "nodi" che compongono la rete; essi, aggirando le gerarchie burocratiche e le frontiere nazionali, influenzano e modificano il processo di *decision making* attraverso azioni di pressione sui decisori politici.

Le minacce prodotte dall'intangibilità degli attori non statali verso sistemi statici, così, si possono identificare facilmente sui campi di battaglia come quello afghano e pakistano dove, non solo al Qaeda, ma anche i suoi alleati talebani, sono "strutturati in rete" ed agiscono contro gli eserciti regolari secondo questo *modus operandi* reticolare.

Per cui si può parlare di una "guerra senza limiti", con la consapevolezza che i mezzi moderni messi a disposizione dalle attuali scoperte tecnologiche,[26] combinati

[26] Accanto al consolidamento delle tecnologie dell'informazione si è assistito allo sviluppo delle cosiddette "tecnologie emergenti" conosciute con l'acronimo NBIC: nanotecnologie, biotecnologie, tecnologie dell'informazione e scienze cognitive che, adattate alla conflittualità, hanno lo scopo finale di simulare attività umane (robotica antropomorfa). Con l'era cibernetica, pertanto, è stato inaugurato l'avvento di un nuovo tipo di cittadino, di un nuovo senso dell'umano; si è assistito, in pratica, alla creazione del cosiddetto *cyborg citizen*, che ha segnato il passaggio dall'interazione all'integrazione uomo-macchina. È il caso, ad esempio, del progetto finanziato dal Pentagono (sono stati concessi circa quattro milioni di dollari) ad un *team* di ricercatori dell'Università della California per studiare le basi

con le tante opportunità offerte dal processo di globalizzazione, rendono la quotidianità un vero e proprio teatro bellico ed il monitor di un computer la finestra principale dalla quale ogni individuo può attuare degli scambi tanto pacifici quanto bellicosi.[27]

5. *Il nuovo volto della guerra: la* digital militarization

La consapevolezza del potenziale bellico del dominio cibernetico ha spinto molti capi di governo a rivedere le proprie dottrine militari e difensive, adattandole alla nuova era. Ad oggi la maggior parte degli stati, escludendo le grandi *cyber* potenze come USA, Russia e Cina, non dispongono di mezzi efficaci di attacco e di difesa nel *cyberspace*, ed è per questo che molte nazioni hanno da poco attivato dei programmi governativi per lo sviluppo delle proprie capacità in tale settore. In questo modo, è ragionevole pensare che nel momento in cui buona parte dei paesi metterà a punto un piano cibernetico efficace, cominceranno a verificarsi *cyber* azioni militari più rilevanti. Al momento, comunque, non si può parlare di "prima *cyber* guerra"; nonostante la messa a punto di una serie di *cyber* attacchi spionistici,[28] infatti, gli stati e i nuovi attori hanno ancora bisogno di conoscersi meglio da questo punto di vista per

della cosiddetta *computer-mediated telepathy* (telepatia sintetica); il progetto, denominato *Silent Talk*, ha l'obiettivo di consentire la comunicazione tra utenti su un campo di battaglia senza l'uso della voce, attraverso l'analisi dei segnali neurali. Anche la società privata americana Northrop Grumman, finanziata da fondi pubblici, sta lavorando su un progetto innovativo: un binocolo in grado di interfacciarsi con la mente inconscia del soldato; sulla base della tecnologia cognitiva *Threat Warning System*, tale prototipo agisce sul subconscio di chi lo indossa, avvisandolo della minaccia prima ancora che la mente cosciente abbia elaborato le informazioni.

[27] Cfr. P. VIRILIO, *La bomba informatica*, Milano, Raffaello Cortina Editore, 2000.

[28] Uno degli attacchi *hacker* più vecchi, e il primo a suscitare clamore, è stato il *Morris worm* che ha preso il nome del suo creatore Robert Tapas Morris, uno studente della Cornell University. Il ragazzo aveva sviluppato il *worm* per misurare la vastità del cyberspazio e non per scatenare una violazione informatica maligna; ma quando il virus è stato immesso in rete, il codice di Morris, dopo aver "incontrato" un errore, si è trasformato in un *malware* capace di infettare più di seimila computer e provocare danni che, secondo alcune stime, hanno raggiunto i cento milioni di dollari. Nel 1982, invece, la *Central Intelligence Agency* (CIA) è riuscita a penetrare i sistemi informatici di un gasdotto siberiano, installando un codice malevolo all'interno di essi; così, quando è stato attivato, il programma ha mandato in panne il sistema che controllava le pompe del gas causando un aumento di pressione e la conseguente esplosione dell'intera struttura energetica. Degno di nota anche un caso più recente: secondo i servizi segreti statunitensi le elezioni americane del 2016 sarebbero state condizionate da un attacco informatico ai danni del comitato elettorale di Hillary Clinton, ordinato direttamente dal presidente russo Putin per favorire il candidato del Partito repubblicano Donald Trump.

poter stabilire la propria posizione di partenza nella *cyber* arena.

Gli USA, grazie a una superiorità effettiva in campo tecnologico e militare, sono stati i primi a ridefinire il loro approccio classico alla guerra in base alle novità introdotte dalla rivoluzione informatica.[29] Dall'analisi dei documenti ufficiali della Casa Bianca, infatti, emerge un prosieguo strategico che ha visto coinvolti nella militarizzazione e nella difesa del *cyberspace* i presidenti Clinton, Bush, Obama e lo stesso Trump; quattro presidenze del tutto differenti tra loro sul piano delle agende politiche proposte, ma accomunate dalla volontà di rendere lo spazio cibernetico un vero e proprio dominio militare.[30]

Già nel 1997, in effetti, l'allora segretario alla difesa William Cohen affermava che «la rivoluzione dell'informazione sta creando una rivoluzione negli affari militari che cambierà profondamente il modo di combattere delle forze statunitensi. Dobbiamo sfruttare queste e altre tecnologie per dominare il campo di battaglia. Lo schema di riferimento in base al quale fare nostre queste nuove opportunità e garantirci così una posizione di supremazia è fissato dal documento *Joint Vision 2010*, il piano predisposto dal presidente del Comitato dei capi di stato maggiore per le operazioni militari del futuro».[31]

Dalla lettura delle righe precedenti si evince la predisposizione "futuristica" delle forze armate e dei politici statunitensi verso una supremazia e un'effettiva

[29] Cfr. A. JOXE, *L'impero del caos. Guerra e pace nel nuovo disordine mondiale*, Milano, Sansoni, 2003.
[30] Al momento del cambio di consegne tra il presidente uscente George W. Bush e Barack Obama, il primo ha voluto far dono di due consigli al nuovo inquilino della Casa Bianca: non abbandonare i bombardamenti mirati con i droni e continuare con il progetto della *cyber warfare*. Che Obama abbia poi seguito e ampliato la dottrina della "guerra invisibile" lo si legge nelle pagine ufficiali della *Strategic Defense Guidance* del 2012, la quale ha previsto: l'incremento crescente delle missioni degli aeromobili senza pilota ed il progresso per quel che riguarda la capacità di resilienza e attacco dell'apparato cibernetico americano. L'ex presidente Barack Obama, durante un suo discorso nel 2014, ha auspicato, inoltre, che la "neutralità della rete" (o *net neutrality*) venga protetta con un regolamento quanto più vincolante possibile. In base al suo punto di vista, il regolamento dovrebbe contenere alcuni principi affinché i *provider* trattino tutti gli utenti di Internet nella stessa maniera. Si pensi al *No Blocking*: se un utente chiede l'accesso ad un sito ed il contenuto è legale, non deve essere permesso al *provider* di bloccarlo; in questo modo si otterrebbe, secondo Obama, un mercato totalmente libero e competitivo e non si avvantaggerebbero le società vicine agli *Internet Service Provider* (ISP). Si può ricordare anche il *No Throttling*: il divieto per gli ISP di velocizzare o di rallentare intenzionalmente alcuni contenuti in base al tipo di servizio o agli interessi degli ISP stessi.
[31] W.S. COHEN, *Report of the Quadriennal Defense Review*, Washington DC, U.S. Department of Defense, 1997, p. IV.

militarizzazione del cyberspazio che, entro il 2010, sarebbero dovute diventare realtà; nel documento citato da Cohen, effettivamente, si legge che «entro il 2010 dovremmo essere in grado di modificare il modo in cui conduciamo le operazioni interforze di maggiore intensità […]. La superiorità del dominio dell'informazione e gli sviluppi della tecnologia ci permetteranno di ottenere gli effetti desiderati attraverso l'applicazione mirata di una potenza di combattimento interforze. Armi di maggiore letalità ci permetteranno di sferrare attacchi che in passato richiedevano una concentrazione di mezzi esercitata in modo sequenziale. Con sistemi d'arma caratterizzati da una precisione superiore e una maggiore portata, i comandanti potranno conseguire il livello desiderato di distruzione o di soppressione delle forze nemiche utilizzandone un minor numero, riducendo quindi la necessità di ammassare uomini e mezzi, operazione che richiede tempo ed è di per sé rischiosa. Una migliore struttura di comando e controllo, basata su una "*intelligence*" in grado di fornire un quadro di situazione aggiornato in tempo reale grazie alla fusione dei dati forniti da una molteplicità di fonti, renderà non più necessario ammassare le formazioni di manovra con giorni e ore di anticipo rispetto al momento stabilito per attaccare».[32]

Il successivo passo in avanti nella militarizzazione del *cyberspace* da parte degli Stati Uniti è stato fatto con l'affermazione della nuova teoria bellica *Network Centric Warfare* (NCW) che rielabora le linee guida definite nella seconda metà degli anni novanta adattandole alle novità introdotte in seguito all'evoluzione tecnologica. La NCW si sviluppa su tre livelli:

- quello strategico,[33] con il controllo di tutte le dimensioni del terreno di scontro;
- quello tattico, con la capacità di superare in velocità l'avversario;[34]
- quello "strutturale", con i sensori che consentono lo scambio dei dati in

[32] JOINT CHIEF OF STAFF, *Joint Vision 2010*, Washington, DC, U.S. Department of Defense, 1997, p. 17.
[33] Considerando il binomio tecnologia-strategia si può affermare che è la prima a dettare la seconda, pur essendoci un rapporto di reciprocità ed interazione tra le due componenti.
[34] Sono il livello tecnologico (velocità di trasmissione dell'informazione, etc.) e la conoscenza dell'avversario che consentono di superare le asimmetrie nei fattori di potenza e che compensano anche l'inferiorità numerica e delle forze convenzionali.

tempo quasi reale;

Il nuovo paradigma militare e la rilevanza strategica riconosciuta al dominio cibernetico dagli analisti americani, dunque, hanno comportato l'innalzamento del *cyberspace* a nuova dimensione (la quinta) della conflittualità.

Nel 2003, l'amministrazione Bush ha emanato anche la *National Strategy to Secure Cyberspace*, il primo documento ufficiale della White House sulla militarizzazione del cyberspazio, che rappresenta la cornice entro la quale sono state fatte le successive scelte strategiche difensive in relazione al dominio *cyber*; e la *U.S. National Defense Strategy* del 2005 in linea con le direttive del 2003, ha riconosciuto per la prima volta lo spazio cibernetico come il nuovo teatro delle operazioni militari.

Tre anni dopo, però, un virus denominato *agent.tbz*, infiltrato nei *network* militari statunitensi – l'operazione di *cyber* spionaggio è partita da una base in Medio Oriente con l'introduzione di una penna USB infetta in un computer portatile in uso all'esercito americano – ha messo in discussione l'intero sistema di sicurezza cibernetico americano.[35] Il Pentagono, in tutta risposta, ha avviato l'operazione difensiva nota come *Buckshot Yankee* e, tra il 2009 ed il 2010, è stato istituito lo *U.S. Cyber Command*, che centralizza il controllo delle operazioni nello spazio cibernetico, organizza le risorse informatiche esistenti e sincronizza la difesa delle reti militari statunitensi.

La quadratura del cerchio della militarizzazione del *cyberspace* è arrivata nel 2011 quando il dipartimento della Difesa americano ha pubblicato la *Strategy for Operating in Cyberspace*. D'altronde, il dinamismo statunitense orientato alla difesa del cyberspazio, da un lato manifesta le contromisure necessarie per contrastare la crescita esponenziale delle minacce provenienti dalla *cyber* arena, dall'altro riprende la visione strategica della cosiddetta *Full-spectrum dominance*,[36] che mira ad un'integrazione di

[35] Va specificato che già tra il 2003 ed il 2005, con l'operazione *Titan Rain*, gli USA hanno subito un vero e proprio attacco da parte di pirati informatici cinesi, che sono riusciti a penetrare migliaia di computer dell'amministrazione statunitense con il fine di sottrarre informazioni sensibili.

[36] Traducibile in italiano come "dominio sull'intero spettro", tale concetto militare statunitense è alla base di una teoria secondo cui la vera superiorità militare può essere raggiunta solo se l'intero strumento militare ottiene il controllo generale e simultaneo di tutto lo spettro del campo di battaglia: oltre al controllo dei quattro livelli classici (terra, mare, cielo e spazio extra-atmosferico) ci deve essere anche quello del cyberspazio attraverso la gestione dei canali di flusso dell'informazione.

tutti e cinque i domini della *warfare*, la quale coincide, appunto, con le direttive emanate dal *Joint Division 2010* e dal più attuale *Joint Division 2020*.

La creazione dello *U.S. Cyber Command* ha influito in maniera incisiva anche sulle scelte degli altri paesi che si sono allineati all'approccio degli Stati Uniti. Nel 2009, ad esempio, la Corea del Sud ha annunciato la creazione di un *Cyber Warfare Command* soprattutto in risposta alla creazione da parte della Corea del Nord di un'unità speciale da impegnare nella guerra cibernetica. L'anno successivo la Cina ha istituito il suo primo reparto dedicato alle azioni condotte tramite lo spazio cibernetico.[37] In Europa, invece, gli stati hanno reagito alla NCW in ordine sparso: si pensi alla *Network Enabled Capability* (NEC) britannica, alla *Network Based Defense* svedese, alle *operazioni net-centriche francesi*, etc. Anche in Italia la NCW ha assunto la forma, meno dispendiosa, della NEC che consente di rendere progressivamente *net*-centriche piattaforme e mezzi già esistenti.[38] Insomma, anziché concepire la NCW come una filosofia per ottenere la superiorità militare come fanno gli USA, gli stati europei guardano alla NEC come ad un modo per accrescere l'efficacia degli strumenti bellici ed ottenere i risultati ricercati, combinando l'utilizzo di strumenti diplomatici e di strumenti militari (*Effect Based Approach*).

La NEC, comunque, nonostante i suoi risvolti positivi, presenta alcune vulnerabilità fra le quali un'eccessiva dipendenza dall'informazione, maggiori rischi in caso di attacchi cibernetici e la mancanza di interoperabilità con alleati non attrezzati con gli strumenti della guerra in rete; e a ciò si aggiungano le resistenze culturali delle forze armate, i costi e la maggiore complessità nell'acquisizione dei materiali necessari. L'armonizzazione fra i paesi e la soluzione dei problemi sono così divenuti due obiettivi fondamentali della NATO che ha elaborato il concetto di *NATO Network*

[37] È nota, ad esempio, l'*Unità 61398*, divisione informatica dell'esercito cinese, specializzata soprattutto nelle attività di *cyberdefense* e *cyber* spionaggio.

[38] Il progetto di "Forza NEC" dell'esercito italiano è concepito per essere funzionale a tutti i tipi di conflitto, da quelli ad alta intensità alle forme di contrasto al terrorismo transnazionale. La filosofia di questo progetto si riassume, in sintesi, nella possibilità di collegare, in maniera diretta ed immediata, ogni singolo soldato con il centro decisionale. Il militare al fronte potrà così accedere a banche dati come se fosse di fronte al proprio PC, potrà comunicare inviando messaggi facilmente componibili, sarà in grado di vedere di notte come di giorno e di inviare immagini a tutte le unità collegate in rete.

Enabled Capability (NNEC), più vicino alle concezioni europee che a quelle americane.

È innegabile, in ogni caso, che per gli stati europei la guerra in rete ha costi molto alti, è complessa ed è soggetta al rischio di perdere efficacia in caso di neutralizzazione anche di una sola funzionalità. In effetti, ciò è stato dimostrato durante le operazioni in Afghanistan e in Iraq per le quali il fattore umano fa ancora la differenza ed il numero delle truppe sul terreno diventa decisivo a dispetto dei vantaggi tecnologici. Nel caso di conflitti asimmetrici (non convenzionali), infatti, la tecnologia perde di valore, se non altro perché non è difficile fornire false informazioni a chi sull'informazione basa la propria superiorità.

6. *Civilizzazione della guerra: forme, strumenti e scopi degli attacchi cibernetici*

Le varie fasi della militarizzazione del cyberspazio hanno portato a una "proliferazione" di armi cibernetiche: la relativa economicità degli strumenti informatici "malevoli", il facile reperimento di essi sul mercato civile e le tecnologie *dual-use* hanno spinto molti esperti a parlare di "Cyber Pearl Harbour" o di "Apocalisse cibernetica", soprattutto dopo l'ufficializzazione della militarizzazione dello spazio *cyber* da parte degli Stati Uniti. Ma come descritto nei paragrafi precedenti, fino ad ora non è accaduto niente di tutto questo e forse mai accadrà; questi allarmismi, inoltre, non fanno altro che favorire lo spreco di energie e risorse verso ambiti poco incisivi nella costruzione di un'efficace strategia della difesa. Allo stesso tempo, comunque, non si può negare una concreta evoluzione del settore che potrebbe portare a questa tipologia di scontro.

Il generale Keith B. Alexander, Comandante dell'*U.S. Cyber Command*, ha elencato gli obiettivi sensibili ad un attacco cibernetico, tra i quali i sistemi di difesa aerea, le armi militari, i sistemi di comando e/o controllo e le infrastrutture civili come la rete elettrica, gli acquedotti, le dighe, le centrali nucleari, il sistema finanziario ed il sistema dei trasporti e delle comunicazioni; in altre parole, il rischio di un *cyber* attacco coinvolge interi Sistemi Paese e, secondo l'ufficiale, la pericolosità e l'asimmetria di una *cyber war* risiedono proprio in questa combinazione tra obiettivi civili e militari, che rendono inadeguate le misure di deterrenza bellica studiate per gli

altri domini della conflittualità.[39]

Se le armi privilegiate divengono quelle cibernetiche e gli obiettivi primari le infrastrutture critiche degli stati, perciò, ne deriva uno stravolgimento dei concetti di armamento e di campo di battaglia, con un conseguente offuscamento della netta distinzione esistente tra "civile" e "militare"; e tale diversificazione viene meno anche relativamente agli obiettivi, agli aggressori e alle responsabilità legate al mantenimento della sicurezza e della difesa (si pensi che negli USA più del novantotto percento delle informazioni governative scorre attraverso canali di comunicazione civili). Il cyberspazio, pertanto, rappresenta il nuovo centro di gravità, e una guerra totale combattuta al suo interno porterebbe allo "stallo" dell'intera società.[40] L'interdipendenza tra i due mondi, quindi, rende quasi impossibile separare la politica dalle componenti civili; senza contare il fatto che le risorse necessarie per la creazione di virus e armi informatiche in grado di colpire esclusivamente *target* ben definiti e limitati, spesso, potrebbero andare ben oltre quelle a disposizione degli attori, mentre, invece, la realizzazione di attacchi di impatto generale possono facilmente risultare più concreti sia in termini di risultati che in termini di costi.

Altro fattore di cui tenere conto risiede nella natura più o meno razionale degli aggressori: se uno stato ha la propensione a compiere attacchi mirati guidato da principi etici e morali, ciò può non valere per altri attori che, di proposito, potrebbero realizzare attacchi che coinvolgono l'intera società. Si sta assistendo, pertanto, ad una "civilizzazione della guerra", una guerra civile perché civili sono gli obiettivi strategici che gravitano all'interno dell'ambiente *cyber*. L'affermarsi dello spazio cibernetico e il diffondersi degli strumenti tecnologici, pertanto, stanno via via trasformando parte delle interazioni quotidiane della società globale in dei veri e propri scontri, con il popolo che non solo rischia di essere un bersaglio, ma anche il coautore degli attacchi

[39] Cfr. S. EVEN - D. SIMAN-TOV, *Cyber Warfare: Concepts and Strategic Trends*, Memorandum 117, Tel Aviv, INSS, May 2012.

[40] Il teorico della guerra aerea Giulio Douhet, a differenza di Clausewitz che teorizza azioni mirate contro obiettivi militari, considera i centri vitali del nemico l'industria e le strutture chiave che permettono ad uno stato di funzionare. Perciò, già in termini di potere aereo, la distruzione di questi centri non permette di distinguere i combattenti dai non combattenti; distinzione che viene a mancare anche all'interno del *cyberspace*. Cfr. G. DOUHET, *The Command of the Air*, Norwalk, Easton Press, 1994.

seppur in modo del tutto involontario ed inconsapevole.[41] Vista l'interazione tra i due mondi, perciò, acquista sempre maggiore legittimità il concetto di "sicurezza condivisa" tra settore pubblico e settore privato, sulla base del quale gli stati si trovano a dover cooperare con altri attori al fine di garantire la protezione all'interno del dominio cibernetico, così come nella realtà fisica; nell'ambito della sicurezza e della difesa, quindi, non si può ragionare soltanto in termini strettamente militari ed occorre adottare nuovi approcci che non escludano la componente civile come parte attiva nell'elaborazione e, allo stesso tempo, come destinataria delle nuove strategie. Secondo Lynn[42] si può parlare di tre tipologie di minacce cibernetiche:

- lo sfruttamento della rete con l'obiettivo di "spiare" e sottrarre dati (*cyber crime* e/o *cyber* spionaggio);
- l'intrusione nella rete (per far venire meno, ad esempio, la corretta funzionalità del servizio);
- il sabotaggio con l'obiettivo di distruggere le infrastrutture fisiche.

Nello specifico, tra le possibili forme di tecnologie offensive operanti nel cyberspazio e che concorrono ad aumentare il raggio d'azione delle minacce cibernetiche, si possono segnalare alcune armi elettroniche come la *backdoor* (dall'inglese "porta di servizio", che rappresenta un metodo per aggirare la normale autenticazione in un sistema informatico) e la cosiddetta tecnica *jamming* (l'atto di disturbare volutamente le comunicazioni radio).[43] Degno di nota anche lo *spettro elettromagnetico* (EMS), componente naturale che contribuisce alla formazione

[41] È possibile, ad esempio, che un utente sia completamente ignaro del fatto che il suo computer sia parte di una rete comandata a distanza ed utilizzata per scopi illegali come la distribuzione di *spam*, il furto di dati o la realizzazione di attacchi informatici.

[42] Cfr. W.J. LYNN III*, Defending a New Domain: The Pentagon's Cyber Strategy*, in «Foreign Affairs», LXXXIX, September-October 2010, pp. 97-108.

[43] Al proposito si può ricordare l'*Operazione Orchard*: il 6 settembre 2007, l'esercito israeliano, prima di procedere al bombardamento di un impianto nucleare in Siria, ha utilizzato un aereo senza pilota armato di uno strumento informatico con tecnologia *jamming* che ha permesso di disturbare, emettere falsi segnali e inserire false informazioni nella rete di difesa aerea siriana, facendo credere agli addetti al controllo che non ci fossere penetrazioni nemiche nello spazio aereo controllato. I caccia israeliani, così, sono riusciti a eludere i sistemi di tracciabilità e portare a compimento la missione, radendo al suolo l'intero impianto; il tutto senza che vi fosse la prova evidente del coinvolgimento di Israele.

dell'ambiente cibernetico[44] e grazie al quale la *cyber war* si presta ad azioni a più ampio raggio.

È evidente, quindi, che anche la *electronic war* (EW) e le armi appena descritte, una volta inglobate nella quinta dimensione della conflittualità, rientrano a tutti gli effetti nell'ambito della guerra cibernetica. Ma occorre precisare che, contrariamente alle tecniche che utilizzano lo spettro elettromagnetico come mezzo per costruire azioni militari di attacco e di difesa, i *cyber attacks* hanno una connotazione ibrida; questi ultimi, infatti, nel momento in cui si sono verificati non sono stati valutati dalla comunità internazionale come una forma di guerra nel senso tradizionale del termine, anche a causa della impossibilità di stabilire con esattezza l'origine degli attacchi. Basti pensare all'attacco in Georgia nel 2008 (di cui si è già parlato nel primo capitolo) oppure all'attacco subito dall'Estonia[45] nel 2007 che, ormai, costituiscono un punto

[44] Si pensi al supporto dato dalle forze speciali dell'esercito americano che, durante una missione segreta contro postazioni talebane in Afghanistan nel 2001, sono riuscite, attraverso l'utilizzo dello spettro elettromagnetico e con dispositivi elettronici e sensori guida GPS, a indirizzare verso gli obiettivi prescelti i missili lanciati dai bombardieri.

[45] Quest'ultimo è stato rivolto contro i siti istituzionali e finanziari estoni ed ha determinato la paralisi dell'intero sistema informatico del paese baltico. In quegli stessi anni, alla luce di quanto accaduto, l'ex presidente estone Toomas Hendrik Ilves ha confrontato il mondo di Internet con lo "stato di natura" delineato dal filosofo inglese Thomas Hobbes, ovvero uno stato di belligeranza di tutti contro tutti; ed il passaggio dallo "stato di natura" a quello "civile" si avrebbe con la stipula di un contratto per mezzo del quale gli uomini, rinunciando autonomamente ai loro diritti naturali, si sottomettono alla volontà di un potere superiore (persona fisica o persona giuridica) e si obbligano, pertanto, a non opporgli resistenza. Ilves, così, conscio che dai tempi di Hobbes il concetto di democrazia e l'inquadramento dei rapporti tra cittadino e autorità statale hanno subìto dei mutamenti significativi, ha auspicato un nuovo contratto tra cittadini e governi sulla falsariga di quanto immaginato dal filosofo John Locke (egli, partendo da presupposti simili a quelli di Hobbes, ritiene necessario un potere superiore che, però, non vada ad annullare i diritti che l'uomo ha nello "stato di natura"; tranne, naturalmente, il diritto di farsi giustizia da solo). L'aspetto più interessante del discorso dell'ex presidente è il passaggio dal quale si deduce il suo timore della possibilità di una "westfalizzazione della rete". Questo termine è stato utilizzato per descrivere il fatto che l'ordine sociale, economico e politico del tradizionale sistema dei confini nazionali, derivante dalla pace di Westfalia, non fosse applicabile al mondo di Internet a causa della propria essenza virtuale. Ilves, invece, nel suo discorso ha voluto lanciare un monito sul rischio che la rete possa essere "westfalizzata", che vengano, cioè, tracciati dei confini all'interno di essa. Egli ha legato tale rischio all'iniziativa di alcuni paesi, da lui definiti autoritari, i quali vorrebbero sostituire l'attuale modello di governo di Internet, fondato sul sistema "compartecipativo", con un sistema "intergovernativo". Gli stati che sostengono il ricorso ad una *governance* della rete sul modello "intergovernativo" poggiano le loro motivazioni principalmente sul fatto che non vi sia una regolamentazione del *web* condivisa internazionalmente e sulla necessità di prevenire e reprimere i *cyber* reati, attività quest'ultima di competenza esclusiva dei governi. Ilves ha affermato che tali motivazioni, seppur pienamente condivisibili, nascondono in realtà la volontà di controllare e regolare il cyberspazio in modo da limitare anche la libera circolazione delle informazioni e delle idee; ed ha aggiunto che, qualora si adottasse il

fermo negli studi di settore. Tali vicende permettono di comparare gli effetti prodotti da un attacco cibernetico tramite modalità "*soft*" e temporanee, che ben poco si prestano alla catalogazione di atti di guerra, con un altro esempio, ossia il virus *Stuxnet*: mentre le prime sono considerate da molti studiosi i primi veri eventi di *information war*, il secondo viene valutato come il primo vero caso di *cyber warfare*; una valutazione che prende vita dall'analisi del contesto strategico e dall'individuazione di alcuni fattori principali scaturiti dall'attacco subito dagli iraniani:

- il *target* scelto per l'attacco (centrale nucleare) è classificato dal governo di Teheran come un obiettivo militare;
- l'azione ha prodotto danni reali a cose (distruzione materiale delle centrifughe);
- la complessità per la pianificazione e l'esecuzione dell'azione permette di stabilire un enorme dispendio di risorse economiche e ciò fa percepire la partecipazione di un'entità statale capace di affrontare i costi elevati.

Appare evidente, pertanto, l'importanza della valutazione oggettiva del contesto strategico nel quale si sviluppa l'attacco *cyber*: se l'intento principale di quest'ultimo è quello di ottenere un profitto, tale condotta potrà essere classificata come un atto di *cyber crime* e/o *cyber* spionaggio; se il fine dell'attacco corrisponde, invece, alla volontà di arrecare un danno ad uno stato e/o ai suoi cittadini, esso potrà essere classificato come vero e proprio atto di guerra disciplinato dallo *jus ad bellum* (o

---

sistema "intergovernativo", ci sarebbe il rischio di arrivare ad applicare ad Internet il principio giuridico del " *cuius regio, eius rete*", versione contemporanea del "*cuius regio, eius religio*", stabilito con il trattato di Augusta del 1555. Secondo l'ex presidente estone, questa contrapposizione potrebbe dar luogo ad uno scontro fra civiltà ed a scontrarsi sarebbero, da una parte, quelle nazioni che vogliono sottoporre a censura e a restrizione Internet e, dall'altra, le nazioni democratiche che reclamano una normativa universale che garantisca la libertà d'espressione e di circolazione delle idee. Per mostrare il rischio di ingerenze governative nella rete, qualora Internet venisse regolato secondo il principio "*cuius regio, eius rete*", Ilves ha citato le iniziative poste in essere in Egitto per fronteggiare le dimostrazioni di massa del gennaio 2011, sfociate nella destituzione di Mubarak. In tale occasione le autorità egiziane di allora sono arrivate ad impedire alla popolazione, per ben cinque giorni, l'uso della rete e della messaggistica sui cellulari. Cfr. http://www.freedomonline.ee/node/131.

diritto di guerra).[46]

Quella che si sta vivendo, quindi, è probabilmente una pagina di storia ancora tutta da scrivere: come reagiranno gli stati ad una così grave ingerenza nei propri affari interni? E se una risposta arriverà con il tempo, di che tipo sarà, e quando giungerà? Non è pensabile che venga ignorata ancora per molto l'*escalation* che si sta verificando nel dominio *cyber*; ed in questo mondo in cui i conflitti tendono a marginalizzare sempre più le forze, le strategie e le tecniche "convenzionali" a favore di quelle "ibride" ed innovative, il *cyberspace* sembra rappresentare la nuova "terra di conquista". Una dimensione grigia, quasi senza regole, che, se occupata e sfruttata adeguatamente, permette di influenzare anche le altre dimensioni per i propri scopi strategici, senza rischiare (quasi) niente. È uno scenario troppo appetibile per chi ha ambizioni di portata globale per non essere sfruttato appieno; e chi lo ha capito per tempo sta già affinando le tattiche, arruolando i propri *cyber* soldati, mettendo a punto le proprie armi, puntandole dritte verso i bersagli individuati. Tutto è pronto: chi sarà il prossimo a fare "fuoco"?

[46] Lo *jus ad bellum* è il corpo giuridico che disciplina il ricorso alla forza da parte degli stati nelle relazioni internazionali; ed esso si basa su criteri che devono essere consultati prima di scatenare uno scontro armato in modo da determinare se sia possibile l'entrata in guerra e se sia una guerra giusta. Ad oggi, la più importante fonte dello *jus ad bellum* è la Carta delle Nazioni Unite. Cfr. M. ROSCINI, *World Wide Warfare – Jus ad Bellum and the Use of Cyber Force*, Leida, Brill, 2010.