GUERRE IBRIDE, OMICIDI MIRATI, DRONI: CONFLITTI SENZA FRONTIERE E SENZA DIRITTO

Mario G. Losano

"Drone warfare is a new form of state violence, hybridizing war and police action, that cannot easily be regulated by international laws of war or by the checks and balances of the U.S. Constitution. It is reminiscent of old colonial practices and yet is different from anything we have seen before" [1].

1. *Dalle guerre tradizionali alle guerre ibride*

Un'aspirazione millenaria domina le tecniche della guerra: allontanare il più possibile il combattente dal luogo dello scontro, in un'evoluzione che va dal corpo a corpo dapprima all'arco o balestra, poi alle rivoluzioni delle armi da fuoco e della guerra aerea, sino alle tecniche attuali dominate dall'informatica. La diffusione dell'informatica e del terrorismo hanno modificato i conflitti, che si presentano oggi come "guerre ibride": nell'evoluzione dalla guerra classica alla guerra ibrida (§§ 1-3) l'informatica assume una posizione di rilievo, tanto che si parla di *cyberwars* (§ 4). Ricompaiono anche i mercenari (§ 5). Oggi il drone realizza nel modo più compiuto l'aspirazione a separare i combattenti e caratterizza quindi le attuali guerre ibride (§ 6). In questo nuovo panorama bellico-informatico si sta trasformando radicalmente anche la protezione dei dati personali (§ 7).

---

[1] H. GUSTERSON, *Drone. Remote Control Warfare*, The MIT Press, Cambridge (Mass.), 2016, p. 8.

Come sempre nella storia della tecnologia, una parte del vecchio sopravvive anche nel mondo nuovo: l'orologio digitale non ha cancellato l'orologio meccanico, né la biro la penna stilografica. La parabola discendente del vecchio spesso incrocia quella ascendente del nuovo: la carica di Izbušenskij del Savoia Cavalleria avvenne nel 1942, durante la campagna di Russia, in piena era dei carri armati, che De Gaulle aveva teorizzato già negli anni '30 entrando anche in questo in collisione con il generale Pétain.

L'opera di Carl von Clausewitz, del 1832, fornisce una sintesi della guerra moderna ma tradizionale, che per lui è «null'altro che un'estensione del duello»[2]. A lui dobbiamo la constatazione tanto cinica quanto veritiera che le guerre scoppiano per colpa non di chi attacca, ma di chi si oppone all'attacco: oggi, a riprova di ciò, si ricorda l'*Anschluss* del 1938 dell'Austria alla Germania nazista, avvenuto senza spargimento di sangue.

Per comprendere meglio che cosa sono le guerre del XXI secolo può essere utile ricordare in sintesi che cosa è una guerra moderna ma tradizionale. Una grande enciclopedia tedesca dei primi anni del Novecento descrive la guerra così come si è svolta sino alla metà di quel secolo, cioè sino alla Seconda guerra mondiale[3]. Le parti contendenti intraprendono trattative diplomatiche. Il fallimento delle trattative è accompagnato dal ritiro degli ambasciatori e da un ultimatum. Se l'ultimatum non produce effetti, la dichiarazione di guerra segna con una precisa data ufficiale l'inizio delle ostilità. In questa visione classica della guerra il confine tra pace e guerra è chiaro nel tempo e nello spazio. Le parti contendenti, che sono Stati, affrontano le ostilità mediante gli eserciti ben individuati dalle rispettive uniformi. La "linea del fronte" stabilisce il confine tra il "teatro di guerra" e il restante territorio, dove vive la popolazione civile che non dovrebbe essere coinvolta nel conflitto. È chiara la delimitazione tra gli eserciti combattenti, segnalati dalle rispettive uniformi, e fra questi eserciti e la popolazione civile.

Nel Novecento queste di linee di demarcazione divengono sempre più incerte ed evanescenti. Infine, nel Nuovo Millennio, esse sembrano quasi del tutto scomparse e hanno comunque perso quasi ogni rilevanza: sono frontiere che le parti in lotta non si preoccupano più di rispettare, perché la loro guerra è ormai una "guerra ibrida", una guerra cioè in cui si mescolano elementi che, sino alla fine della Seconda guerra mondiale, andavano tenuti distinti.

Con la loro scomparsa, si trasformano anche alcune strutture organizzative sociali e militari. Un tempo, la polizia si occupava dell'ordine interno ai confini nazionali, mentre l'esercito operava al di fuori di essi. I servizi segreti interni

---

[2] C. VON CLAUSEWITZ, *Vom Kriege, Hinterlassenes Werk des Generals Carl von Clausewitz*, Ferdinand Dümmler, Berlin, 1832, pp. 3-4: «Der Krieg ist nichts als ein erweiterter Zweikampf»; e continua: «Jeder sucht der Andern durch phisische (sic) Gewalt zur Erfüllung seines Willens zu zwingen», cosicché «Der Krieg ist also ein Akt der Gewalt um den Gegner zur Erfüllung unseres Willens zu zwingen».

[3] AA.VV., *Mayers Konversations Lexikon* alla voce Krieg (guerra), 1904.

erano distinti da quelli esterni, ed entrambi operavano separatamente dalle polizie e dagli eserciti. Ma con le guerre ibride non è più chiaro né il fronte, né il combattente, né l'inizio o la fine del conflitto e perciò i compiti di quelle organizzazioni tendono a intrecciarsi, come vedremo in seguito.

La scomparsa del fronte, della separazione fra esercito e popolazione civile e, infine, dello stesso confine tra pace e guerra, è avvenuta lentamente. L'enciclopedia tedesca già ricordata registra l'inizio di questa evoluzione: la dichiarazione di guerra serve a per spiegare "al nemico e ai neutrali le ragioni della guerra" e determinare con precisione il momento dell'inizio delle ostilità. Ma già nel 1904 quella dichiarazione sembrava una pura (e inutile) formalità, «perché – scrive l'enciclopedia, – nei moderni rapporti di scambio e di stampa tutto il resto è già noto in anticipo a tutti. Un'espressa dichiarazione di guerra non è oggi [1904] a ragione considerata indispensabile, ma viene anzi sostituita dall'inizio delle ostilità». Il riferimento è all'attacco giapponese del 1904 a Port Arthur, nella guerra contro l'Impero Russo, avvenuto prima della dichiarazione di guerra: tecnica che i giapponesi ripeteranno a Pearl Harbor nel 1941 (un anno prima della già ricordata carica di cavalleria a Izbušenskij). La guerra diviene dunque sempre più informale, e l'informalità è la negazione del diritto. Per questo le nuove guerre ibride non si attengono più alle regole formulate al tempo delle guerre classiche.

Il diritto ha cercato di regolare la condotta della guerra sul piano tanto nazionale quanto internazionale. Ogni Stato emana delle norme giuridiche che regolano il comportamento dei propri militari: sono i codici militari di pace e di guerra. Nel diritto internazionale, soprattutto dopo la Seconda guerra mondiale, le regole riguardano non tanto il comportamento dei combattenti, quanto i più deboli (cioè chi non può più combattere perché ferito o prigioniero) e le popolazioni civili, sempre più spesso vittime della guerra. Il confine che separa la guerra dalla pace è divenuto infatti sempre più evanescente. Così, le Convenzioni di Ginevra dal 1906 al 1977 (che codificavano le consuetudini ottocentesche e che ancora oggi sono applicate dalla Corte Internazionale di Giustizia dell'Aja) regolano il diritto internazionale umanitario, quello cioè che cerca di tutelare i non combattenti, come i naufraghi, i feriti, i malati e la popolazione civile.

Intanto la guerra – nel senso classico (clausewitziano o, come si tende a dire oggi, "cinetico" [4]) del termine – si è trasformata e i trattati parlano ormai genericamente di "conflitto armato". Lo Statuto di Roma ha quindi per oggetto «i conflitti armati internazionali; i conflitti interni tra gruppi di persone organizzate, che si svolgano con le armi all'interno del territorio dello Stato, e raggiungano la soglia di una guerra civile o di insurrezione armata; i conflitti interni prolungati tra le Forze armate dello Stato e gruppi armati organizzati o tra tali

[4] L'aggettivo "cinetico" è uno degli eufemismi usati negli Stati Uniti per indicare le azioni letali che non si vogliono indicare come "guerre". L'espressione *cinetic warfare* è oggi comunemente usata in contrapposizione a *cyber warfare*, probabilmente perché l'attacco informatico avviene a tavolino, mentre l'attacco classico implica un movimento di truppe e di mezzi sul terreno.

gruppi». Sono invece escluse «le situazioni interne di disordine o di tensione, quali sommosse o atti di violenza isolati e sporadici e altri atti analoghi», di competenza del diritto penale interno dei singoli Stati. Le violazioni dello Statuto di Roma sono giudicate dalla Corte Penale Internazionale dell'Aja.

In Italia, il diritto interno si rifà alla vecchia nozione di guerra: la legge di guerra e neutralità è del 1938, i due codici penali militare di pace e di guerra sono del 1941. La Cassazione ha cercato più volte di tracciare un confine giuridico a proposito degli atti di terrorismo, ma la situazione si fa di anno in anno più confusa.

In generale, viene sempre di più alla luce la discrepanza fra gli attuali conflitti ibridi e le norme giuridiche nazionali e internazionali, ancora modellate su un'idea di guerra che non corrisponde più agli eventi reali. Con gli anni '50 del XX secolo si sono moltiplicate le guerre delegate (*proxy wars*), alle quali una grande potenza non partecipa direttamente, ma appoggia una della parti in lotta con mezzi economici e militari, con istruttori militari, con un certo numero di militari propri o di mercenari (*contractors*: attori su cui torneremo al § 5). Si susseguono così le guerra di Corea (1950), del Vietnam (1955-1975), l'invasione dell'Afghanistan e quella del Kuwait, che porterà alle Guerre del Golfo del 1991 e del 2003, dilagate poi nel Medio Oriente in conflitti che durano tuttora. L'essenza di queste guerre delegate è racchiusa in una frase che circolava ai temi della guerra in Vietnam: «In Vietnam, Urss e Usa si combattono fino all'ultimo vietnamita».

Le guerre delegate e le guerre ibride godono del favore delle lobby delle armi, di cui incrementano i loro affari, ma anche dei politici, perché incidono meno sul bilancio statale, perché è ridotto al minimo il traumatico rimpatrio delle salme dei soldati morti (così controproducente sul piano elettorale) e perché in questo modo si evitano molte critiche della stampa e degli oppositori, anch'esse con effetti così negativi sulle campagne elettorali. Dunque, i conflitti che hanno ormai perduto il carattere di guerra classica e hanno assunto quello di guerra ibrida. Su quest'ultimo concetto conviene ora soffermarsi.

2. *Le guerre ibride dal Novecento a oggi*

La nostra società è retta ormai dall'informatica, che è anche lo strumento principale della globalizzazione: di conseguenza, ogni società è oggi tanto vulnerabile quanto è vulnerabile l'informatica di cui fa uso; quindi più le società sono avanzate, più sono vulnerabili. La tendenza delle odierne città a trasformarsi in megalopoli informatizzate aumenta i rischi di interventi militari nelle reti e nei cloud collegati a servizi essenziali[5]. Per questo, fra gli strumenti della guerra ibrida, al primo posto si colloca la *cyberwar* (§ 4). Ritorneremo poi all'antico, ma

[5] F. RÖTZER, *Smart Cities in Cyberwar*, Westend, München, 2015; cfr. in particolare il capitolo *Smart Cities: Ziele des Cyberwar*.

solo apparentemente, esaminando il secondo elemento tipico della guerra ibrida, cioè i mercenari, oggi organizzati in moderne compagnie di ventura che sono *Private Military Companies*, cioè *corporations* locali o multinazionali (§ 5): un altro esempio della progressiva privatizzazione di funzioni che furono originariamente statali. Infine torneremo alla modernità, esaminando le inedite caratteristiche della guerra ibrida condotta con i droni (§ 6).

Nel XXI secolo i conflitti hanno sempre più perso il classico carattere di scontri armati fra eserciti nemici retti in certa misura dalle regole del diritto internazionale bellico, e sono andati acquisendo una struttura complessa, in cui gli avversari ricorrono in misura diversa alle forze armate tradizionali, a gruppi irregolari, alla guerriglia, al terrorismo (anche coinvolgendo i civili), al sabotaggio tecnologico (in particolare, la *cyberwar*), agli agenti sotto copertura o provocatori, all'assassinio politico (denominato in modo apparentemente meno crudo *targeted killing*), secondo una miscela che varia da caso a caso. Questa "guerra ibrida" è tipica dell'*asymmetric warfare*, cioè degli scontri in cui una delle due parti gode di una netta superiorità militare, come avviene nei conflitti oggi in corso contro lo Stato Islamico, nei quali non sono più gli eserciti tradizionali a controllare lo svolgimento della guerra.

In passato erano già guerre sempre più ibride i conflitti dell'Indocina, del Vietnam, dell'Afghanistan, del Libano nel 2006; oggi il caso dell'Ucraina è così esemplare che, per il futuro, gli Stati Baltici temono un'applicazione del modello ucraino a ciascuno di essi.

Non si tratta di timori vaghi: un documento prefigura il possibile corso di questi eventi futuri, simulando che negli Stati Baltici si ripeta la sequenza di eventi già vista in Ucraina. La conferma che questo è un pericolo non soltanto teorico viene anche dalla decisione della NATO, presa l'8-9 luglio 2016 nel summit di Varsavia, di rafforzare la propria presenza in quei territori. Pochi mesi dopo, insieme con altri Stati anche l'Italia era presente in Lettonia con 150 militari sotto l'egida della Nato. La Russia sente questa presenza come una minaccia e la sua risposta sta assumendo le forme iniziali di una guerra ibrida: nel febbraio 2017 una e-mail inviata alle autorità lettoni accusava falsamente i soldati tedeschi stazionati in Lettonia di aver violentato una minorenne: notizia d'autore ignoto subito rivelatasi falsa, ma che può caratterizzare i primi passi di una guerra, in cui la disinformazione può preparare il terreno a ulteriori interventi, come in Ucraina[6].

---

[6] *Spiegel On Line*, 16 febbraio 2017; cfr. anche C. WEISSFLOG, *Mit Fake News gegen Bundeswehr-Einsatz*, in *Neue Zürcher Zeitung*, 17 febbraio 2017: «Angesichts der Erfahrungen im Ukraine-Konflikt scheint indes eine russische Urheberschaft die einzig logische Vermutung zu sein». La Russia nega invece ogni coinvolgimento, secondo il Galateo della *cyberwar*. I tedeschi hanno subito ricordato il "Caso Lisa" del 2016, quando la televisione russa accusò senza fondamento gli immigrati di aver violentato a Berlino una tedesca d'origine russa: disinformazione che mirava a creare difficoltà interne alla politica tedesca sull'immigrazione. Cfr. C. WEISSFLOG, *Wie Putins Propaganda die Russlanddeutschen aufhetzt*, in *Neue Zürcher Zeitung*, 25 gennaio 2016.

In questa guerra informale, l'informatica è usata non solo per entrare illegalmente nei sistemi informativi altrui e carpirne informazioni, ma anche per compiere azioni che producono danni eguali o peggiori di un bombardamento: il sabotaggio delle reti informatiche di una struttura militare, delle ferrovie, della distribuzione elettrica o idrica di una grande città. Ed è chiaro che nella *cyberwar* non è possibile distinguere gli obiettivi militari da quelli civili: anzi, gli attacchi alle grandi reti informatiche colpiscono soprattutto i civili e assolvono le stesse funzioni dei bombardamenti a tappeto, come quello di Dresda: la loro finalità non è strettamente militare, ma mira a fiaccare la resistenza della popolazione civile.

3. Cyberwars*: l'informatica come arma*

L'informatica ha una funzione di primo piano nella guerra ibrida dell'ipotetico scenario baltico: in parallelo con le varie tecniche di disinformazione e di sovversione interna, «attacchi informatici paralizzano banche e reti governative: l'Estonia ha già subìto nel 2007 un attacco di questo tipo»[7]. Va sottolineato che la *cyberwar* è uno strumento ideale per la guerra ibrida: può arrecare danni ingenti all'avversario e, al tempo stesso, proteggere l'anonimato dell'aggressore che, per esempio, attacca la rete di una banca, di un ospedale o di un nodo ferroviario passando attraverso il centro di calcolo di un'università del sud-est asiatico.

Le Primavere Arabe (come apertura al mondo occidentale) e lo Stato Islamico (come rifiuto del mondo occidentale) hanno potuto ottenere importanti risultati con strumenti informatici semplici[8]. Ma ormai gli Stati hanno vere e proprie strutture militari dedicate alla *cyberwar*. Sembra che la Corea del Nord usi 6000 persone a questo fine e in effetti i risultati si sono visti quando, alla fine del 2014, il sistema informatico della Sony Corporation è stato sabotato da hackers per aver messo in circolazione il film *The Interview* sul dittatore Kim Jong Un. Però la stessa National Security Agency statunitense ha evitato di indicare esplicitamente il governo nord-coreano quale responsabile dell'attacco; l'ha fatto però Barack Obama, e la Corea del Nord ha risposto negando ogni addebito e anzi chiedendo un'inchiesta congiunta con gli USA, che naturalmente non si è fatta. Proprio la difficoltà di risalire con certezza all'autore di un attacco informatico trasforma questa tecnica nell'arma ideale per la guerra ibrida.

---

[7] D. BRÖSSLER, *War games*, in *Süddeutsche Zeitung*, 31 gennaio-1° febbraio 2015, p. 12. Al tema della guerra ibrida questo giornale dedica tre intere pagine (pp. 11-13).

[8] M. G. LOSANO, *La Rete e lo Stato Islamico. Internet e i diritti delle donne nel fondamentalismo islamico*, Mimesis, Milano 2017, in particolare il paragrafo *Hybrid war: scompare il confine tra guerra e pace*, pp. 68-74.

Per questo lo Shape (Supreme Headquarter Allied Powers in Europa) ha una "Sezione per la ciber-sicurezza", che tiene sotto controllo tutto quanto può essere rilevante per le reti della Nato e degli Stati membri. Però anche qui l'informatica si scontra con il diritto: poiché la Nato è un patto difensivo militare, non è previsto che essa possa bloccare il server da cui è partito l'attacco informatico. Bisogna quindi ripensare la formulazione del trattato in modo da includere i nuovi problemi introdotti dalla *cyberwar*. «La politica della Nato non ha finora fatto nulla in questa direzione. Finora non esiste una strategia precisa contro la *cyberwar* né contro la guerra ibrida. Nel vertice della Nato del 2014 i capi di Stato e di governo dei paesi della Nato hanno annunciato piani per poter prendere "misure efficacemente deterrenti contro le guerre ibride". È una formulazione vaga, ma in ultima analisi propone una concezione della difesa che cancella i confini tra militari e civili proprio come nell'attacco ibrido che si propone di respingere» [9].

In sintesi: nell'informatica operano strutture con algoritmi predatori, costruiti per superare ogni sicurezza logica, insita cioè nel *software*, ed entrare così nei sistemi di comunicazione che si vogliono sorvegliare. Questo accesso può essere illecito, ovvero autorizzato dall'autorità giudiziaria, ma è in ogni caso ignoto al proprietario dei dati. Poiché quest'ultimo è consapevole della possibilità di accessi fraudolenti, si premunisce con programmi che blocchino gli algoritmi predatori. Per informazioni su questi programmi sempre più sofisticati e perennemente in evoluzione bisogna ricorrere alla letteratura sull'argomento [10]. L'analisi delle comunicazioni interpersonali individua gli individui sospetti; l'analisi di altri strumenti elettronici (cellulari, navigatori, ecc.) individua i loro percorsi; a un certo punto, nella catena di comando, qualcuno decide di arrestare o addirittura di eliminare gli individui sospetti così individuati e pedinati: l'identificazione e l'eventuale uccisione oggi si fanno anche con i droni.

Questa procedura significa che non solo non esiste più la frontiera tra la pace e la guerra, e che tutti siamo potenzialmente obiettivi di un attacco, anche se per errore; ma significa anche che la guerra ibrida non conosce sosta, che è sempre in corso, perché nelle reti la ricerca di informazioni avviene con "rot", programmi che circolano ininterrottamente in rete; e – come vedremo – anche l'intervento dei droni è sempre possibile, 24 ore su 24.

Una peculiarità della guerra informatica è che essa non richiede necessariamente grandi strutture organizzative: tutto dipende dai fini che ci si propone. Lo Stato che vuole entrare nelle reti ministeriali o militari di un altro Stato de-

---

[9] D. BRÖSSLER, *War games*, in *Süddeutsche Zeitung*, cit., p. 12.

[10] Per un primo panorama: A. KIYUNA, L. B. KONYERS, *Cyberwarfare Sourcebook*, Lulu Press, Raleigh (NC) 2015, che illustra fra gli altri i «DDoS attacks, Bureau 121, camfecting, cyber attack threat trends, ECHELON, Fifth Dimension Operations, Intervasion of the UK, Military-digital complex, PLA Unit 61398, Stuxnet, and more».

ve disporre di un struttura vasta con specialisti che lavorano per lungo tempo prima di conseguire l'obiettivo (che può essere di puro spionaggio, o di sabotaggio vero e proprio). Invece lo sviluppo di programmi di intrusione in sistemi informatici altrui può essere realizzato con pochi specialisti ben preparati: il caso estremo è quello dell'hacker individuale che viola un sistema di sicurezza per fini ludici, o politici, o criminali [11]. Per illustrare questo "grado zero dell'intrusione" (anche se proprio "zero" non è) sono illuminanti due microstorie milanesi.

Prima microstoria milanese. Nell'estate del 2015, i giornali annunciavano: «Nella notte tra il 6 e il 7 luglio l'Hacking team viene hackerata» [12]. Apprendevo così che in via Moscova, quasi dirimpetto a casa mia, nell'appartamento d'una casa che il catasto definirebbe "di civile abitazione", operava legalmente una società produttrice del *software* di intrusione RCS (Remote Control System), usato per entrare nei computer altrui in modo non necessariamente illecito [13]. Infatti tra i suoi clienti Hacking Team annovera varie polizie italiane che, con l'autorizzazione di un giudice, usano quel programma per sorvegliare le comunicazioni informatiche sospette. Il problema sorse quando Hacking Team venne a sua volta hackerata: venne così alla luce che Hacking Team forniva quel *software* anche a regimi stranieri dittatoriali, come Sudan, Libia, Etiopia, che lo usavano per tenere sotto controllo gli oppositori politici.

Al tempo stesso, la diffusione del programma e dei suoi utenti metteva in pericolo la riservatezza di indagine giudiziarie e poliziesche in corso. I Carabinieri informavano che i documenti oggetto di indagini vengono gestiti dall'Arma, e non dalla società. Ma è stato sollevato il dubbio che attraverso una *back door* (un accesso ignoto all'utente) la società potesse controllare l'attività dei controllori. Su questo hackeraggio sono stati aperti procedimenti in Italia e all'estero.

Seconda microstoria milanese. Un'operazione del GICO ci porta a Vizzola Ticino (comune di circa 500 abitanti vicino a Varese), dove ha sede la società di servizi d'intercettazione "Area", posta sotto indagine e perquisita dalla procura delle Repubblica per aver fornito a Bashar al-Assad, in Siria, un *software* utilizzato dai servizi segreti di quello Stato per intercettare gli oppositori e i dissidenti. Sulla base di prove raccolte dalla Guardia di Finanza nella perquisizione, il

---

[11] Nella produzione di armi batteriologiche, basta un laboratorio in grado di produrre vaccini per produrre un'arma batteriologica.

[12] «Un'operazione che ha portato alla fuga di milioni di documenti custoditi nei server dell'azienda, oltre alla rivelazione di parte del codice sorgente di Galileo, il pacchetto che più di 40 governi usano per infiltrarsi nei computer e nei telefoni cellulari di jihadisti, trafficanti, criminalità organizzata» (ma anche di dissidenti) (*Vince ammette: «Contatti con Sudan, Libia, Etiopia»*, in *La Stampa*, 12 luglio 2015).

[13] La società ha una quindicina di dipendenti, sedi all'estero e un bilancio d'una quarantina di milioni di euro nel 2015. Altre notizie in R. MEGGIATO, *Cyberwar*, Hoepli, Milano, 2016, Appendice A, *Hacking Team*, pp. 179-194.

reato ipotizzato dalla Procura è la violazione dell'embargo comunitario per la vendita di questo tipo di tecnologie alla Siria.

Il fatto che basti poco per produrre strumenti di *cyberwar* impone di aggiornare anche le leggi sul commercio delle armi. Ma le cose si complicano perché i programmi incriminabili sono *dual use*, cioè possono avere un uso tanto civile, quanto militare. Una volta esportato un programma per uso civile, è di fatto impossibile determinare se poi è stato usato per altri fini. Inoltre, anche se le norme esistono, il problema è come applicarle a un bene – che è *anche* un'arma – immateriale come un *software*, che si può esportare in un pen-drive.

Si è detto che le guerre ibride esistevano sin dall'antichità. Ma con l'informatica le guerre ibride del XXI secolo si differenziano da tutte le guerre precedenti, perché ormai nelle reti non c'è mai pace, perché non ci sono più frontiere e perché tutti sorvegliano tutti in un cosmico gioco di guardie e ladri. Nei riguardi della *cyberwar* tre quesiti non hanno finora trovato risposta: la *cyberwar* evita la guerra tradizionale? oppure è un complemento della guerra tradizionale? oppure può essere la causa di una guerra tradizionale che, oggi, potrebbe essere anche una guerra atomica?

4. *Mercenari: la privatizzazione della guerra*

L'odierna compagnia di ventura si presenta come una "compagnia militare privata" ed è un'impresa che fornisce consulenze o servizi specialistici di natura militare, assimilabili a quelli delle compagnie di ventura e ai mercenari che funestarono il medioevo europeo.

Lo status giuridico del personale impiegato presso queste imprese, secondo le Convenzioni di Ginevra, è diverso da quello del personale militare che presta servizio in una forza armata regolare, perché i mercenari non hanno né gli obblighi né i diritti previsti per le milizie regolari. I *contractors* possono anche non agire secondo il diritto bellico ed il diritto internazionale umanitario e, se catturati, non vengono necessariamente riconosciuti come prigionieri di guerra. Il personale di queste *corporations* che utilizzi la forza offensiva in una zona di conflitto potrebbe essere considerato "combattente illegittimo", con riferimento alle convenzioni di Ginevra.

Basti un esempio. La compagnia militare privata Blackwater (oggi Academi, in precedenza Blackwater USA, Xe Services LLC e, fino al dicembre 2011, Blackwater Worldwide), è un'impresa privata statunitense fondata nel 1997 da Erik Prince, un ex-Navy SEAL erede di una ricca fortuna di famiglia. È considerata una delle più importanti compagnie militari private del mondo, con ruoli di primo piano come *security contractor* in Iraq per conto del governo degli Stati Uniti d'America.

Nel corso degli anni 2000 è divenuta famosa per esser stata coinvolta in di-

versi fatti di sangue durante le guerre in Iraq e in Afghanistan. Nel 2004 l'uccisione e lo scempio dei cadaveri di quattro "*contractors*" della Blackwater, in un'imboscata a Falluja, indusse le forze militari statunitensi ad avviare un'ampia operazione per riprendere il controllo militare sulla città. Nelle settimane successive all'evento, comunque, le famiglie dei mercenari uccisi denunciarono la Blackwater per le numerose anomalie nelle procedure operative cui avevano costretto i loro congiunti, sacrificando la sicurezza a interessi di "economizzazione" delle operazioni.

La Blackwater ha subìto inoltre pesanti critiche a causa alle politiche operative estremamente aggressive praticate dai propri agenti in Iraq: per garantire una forte cornice di sicurezza, i convogli della Blackwater usano abitualmente procedure preventive e dissuasive pericolose per la popolazione e per i passanti delle aree attraversate.

Il 16 settembre 2007, a Baghdad, queste procedure hanno portato a uno scontro a fuoco in cui diciassette iracheni (di cui almeno quattrodici civili innocenti) sono rimasti uccisi dal fuoco degli operatori della Blackwater. L'incidente, per il quale furono condannati quattro *contractors* della società, ha suscitato numerose polemiche, i cui risultati sono stati una revisione delle procedure operative imposte alla Blackwater dal Dipartimento di Stato, e un'inchiesta del Congresso degli Stati Uniti, nella quale sono state valutate anche altre denunce sull'operato della Blackwater in Iraq e Afghanistan. A causa di questi scandali, la compagnia decise nel 2007 di cambiare il proprio nome in "XE Services", in seguito modificato in "Academi".

I pochi esempi fin qui adotti illustrano in che cosa consiste la privatizzazione della guerra attraverso una compagnia di ventura, o compagnia militare privata: la compagnia citata non è ovviamente l'unica di cui gli Stati possono servirsi nel condurre guerre ibride, con l'obiettivo di non coinvolgere il proprio nome e le proprie truppe ufficiali e di aggirare le norme interne e internazionali sulla condotta di un conflitto armato.

5. *Droni: sicari occulti a pilotaggio remoto*

Alcune caratteristiche dei nuovi conflitti emergono chiari dagli esempi fin qui esaminati: il terrorismo (per esempio, nel caso dell'Isis) o la sovversione (per esempio, nel caso dell'Ucraina) non rispettano le frontiere nazionali, quindi sono ovunque; la *cyberwar* permette di individuare i sospetti accumulando e analizzando dati in una rete di computer che opera 24 ore su 24. Dunque, la guerra ibrida può essere in corso *sempre* e *ovunque*: però come intervenire *sempre* e *ovunque*? I droni, con tutto l'apparato che il loro impiego comporta, sono lo strumento per intervenire *sempre* e *ovunque*.

Il drone è un "aeromobile a pilotaggio remoto" caratterizzato dall'assenza

del pilota umano a bordo, ma controllato da un pilota e da un navigatore entrambi remoti, cioè a migliaia di chilometri di distanza. Un'altra denominazione corrente – "Unmanned aerial vehicle", UAV – è fuorviante, perché suscita l'immagine fantascientifica di una guerra condotta soltanto dalle macchine, di una guerra robotica. Sul drone stesso non vi è un pilota, ma il volo è controllato dal computer di bordo del velivolo, a sua volta sotto il controllo remoto del pilota presente sul terreno o in un altro aereo. Insomma, il drone non è un missile.

La storia dei droni inizia con i piccoli aerei telecomandati (via radio) dotati di piccoli motori a scoppio: la loro ridotta autonomia di volo ne limitava molto l'uso pratico. Il salto di qualità avviene quando su questi velivoli vengono montati motori elettrici, con pile sempre più potenti, che garantiscono una più lunga autonomia di volo. I modelli attualmente in uso (come i diffusi Predator e Reaper) hanno motori a vari combustibili e possono restare in volo fino a circa 40 ore. I dati tecnici riportati in questo scritto forniscono una prima idea delle caratteristiche di questi aeromobili, ma sono puramente indicativi perché destinati a mutare nei mesi successivi alla pubblicazione. Per un futuro non lontano si stanno sperimentando motori a energia solare, con un'autonomia di centinaia di ore. L'innovazione che i droni hanno introdotto nei conflitti e i problemi etici che solleva il loro uso come strumenti di omicidi mirati, di targeted killings, cioè di assassini politici, sta generando una vasta letteratura su di essi [14].

Il drone è il tipico mezzo *dual use*, perché – non mettendo a rischio la vita dei piloti o di un intero equipaggio – consente usi tanto civili quanto militari in contesti dall'accesso difficile o pericoloso, sintetizzati dalle "*three Ds*": "*dull, dirty, dangerous*": i droni, come tutti gli strumenti robotici, sono pensati per sostituire l'uomo nelle attività "ripetitive, sporche, pericolose". Nel caso del drone, il pilota remoto non corre alcun pericolo perché si trova a migliaia di chilometri dall'obiettivo, come si vedrà fra poco.

Gli usi in ambito civile possono qui essere soltanto accennati: la protezione civile può ispezionare in tempi stretti le zone rese inaccessibili da catastrofi (come nel terremoto del 2016 negli Abruzzi); i vigili del fuoco possono tenere sotto controllo dall'alto le singole persone (sia vittime, sia soccorritori) in un incendio o in un'inondazione; la polizia può ispezionare a distanza un luogo per verificare se vi si nascondono una o più persone, e se queste sono armate, e come; imprese e enti di ricerca li possono usare per tenere sotto osservazione vaste superfici agricole o marittime per controlli sull'inquinamento, e così via. Poiché

[14] Oltre agli altri volumi citati nel presente saggio, si vedano (in ordine di data di pubblicazione) I. G. R. SHAW, *Predator Empire. Drone Warfare and Full Spectrum Dominance*, University of Minnesota Press, Minneapolis 2016; A. COCKBURN, KILL CHAIN, *The Rise of the High-Tech Assassins*, Holt, New York, 2015; R. WHITTLE, *Predator: The Secret Origins of the Drone Revolution*, Holt, New York, 2014; B. GLYN WILLIAMS, *Predators. The CIA's drone War on al Quaeda*, Potomac Books, Washington (DC) 2013; B. J. STRAWSER (ed.*), Killing by Remote Control. The Ethics of an Unmanned Military*, Oxford University Press, Oxford, 2013.

l'uso civile dei droni si va diffondendo, i singoli Stati hanno emanato norme per evitare un eccessivo affollamento dei cieli e hanno istituito scuole che rilasciano una patente per il pilotaggio remoto dei droni civili.

In base a queste funzioni, l'industria produce droni di varie dimensioni: da quelli di poche decine di centimetri (che si possono comprare persino nei negozi di giocattoli) fino al Predator MQ1C Gray Eagle (sviluppato per l'esercito statunitense) che misura 8 metri di lunghezza e 17 metri di apertura alare.

Gli usi in ambito militare rendono il drone uno strumento essenziale nelle odierne guerre ibride. I droni utilizzati per scopi bellici possono essere attrezzati con sensori di ripresa che – come negli usi civili – permettono l'invio di informazioni in tempo reale, di notte e di giorno, alla stazione di controllo distanza (tanto a decine quanto a migliaia di chilometri). Essi sono però anche attrezzati con armamenti, che consentono la distruzione di obiettivi specificamente individuati: sono gli interventi "chirurgici", cui si richiamano i fautori dell'uso dei droni perché eviterebbero i "danni collaterali" ai civili, propri invece dei bombardamenti tradizionali.

Nella stessa operazione, le attività di ricognizione e distruzione possono essere disgiunte o congiunte. Un esempio di attività disgiunta è stato l'utilizzo dei droni per monitorare le attività di Osama bin Laden, fino all'intervento sul terreno delle unità speciali dell'esercito statunitense, che lo uccisero il 2 maggio 2011 [15]. Esempi di attività congiunta delle attività di ricognizione e distruzione dei droni sono i crescenti omicidi mirati di singole persone, i "targeted killings" su cui si tornerà tra poco.

Si interviene con il drone per centrare uno specifico obiettivo, cioè con l'aspirazione a limitare il teatro della guerra. Ma le caratteristiche del drone e dell'organizzazione che lo gestisce vanno in realtà in direzione contraria, col risultato di estendere il campo di battaglia nel tempo e nello spazio. La contraddizione insita nell'uso dei droni si manifesta in tre direzioni.

La dilatazione del campo di battaglia. I droni, come si è detto, sono studiati per colpire obiettivi circoscritti, evitando i danni collaterali tipici delle incursioni aeree tradizionali. Quindi il drone è lo strumento ideale per svolgere attacchi "chirurgici", delimitando così al massimo il campo di battaglia. In realtà, l'obiettivo dell'attacco viene segnalato da computer come punto finale di un'analisi che coinvolge molte banche di dati (militari, dei servizi segreti, di altra natura) e quindi esso può trovarsi ovunque: perciò il raggio d'azione del drone non ha limiti ed è caratterizzato da una *de-spazializzazione radicale dello stesso campo di*

[15] A. VEDASCHI, *Osama bin Laden: l'ultimo* targeted killing*. Gli Stati Uniti hanno dunque la licenza di uccidere?*, in *Diritto pubblico comparato ed europeo*, 2011, pp. 1196-1229. L'articolo esamina l'intero problema giuridico del *targeted killing*, e non solo l'"Operazione Geronimo" che eliminò Bin Laden, ma che – con quella denominazione rievocante le vicende del condottiero Apache – suscitò le proteste anche delle associazioni dei nativi statunitensi.

battaglia. Non esiste più un fronte tra due eserciti di due Stati: si fronteggiano Stati e non-Stati (al-Quaeda, Isis), i combattenti sono, almeno in parte, commisti alla popolazione civile; di conseguenza, il fronte non è determinabile a priori. In questo contesto il drone è potenzialmente in grado di intervenire sempre e dovunque: e di fatto interviene là dove lo manda il computer, individuando il *kill box* in cui intervenire anche in aree popolate.

Guerra ovunque – Everywhere war. I fautori dell'uso dei droni definiscono "chirurgico" o anche "chemioterapico" il loro intervento perché allontanerebbe dal corpo sano della società soltanto le cellule impazzite del terrorismo, senza "effetti collaterali"; in altre parole, il drone colpirebbe soltanto l'obiettivo predeterminato, ma non i civili delle vicinanze. Ciò è vero nel migliore dei casi. In generale, il drone produce l'effetto contrario, perché il suo intervento armato può avvenire sempre e dovunque.

Nelle aree colpite dai droni questa minaccia ubiqua e costante produce effetti diffusi nella popolazione locale. Per esempio, nelle aree tribali del Pakistan, il frequente uso dei droni ha generato un permanente stato di ansietà in intere popolazioni. Al di là dei problemi psicologici individuali che quest'ansietà permanente può provocare, l'intervento antitalebano dei droni statunitensi ha provocato un aumento dei sentimenti antiamericani, ha cioè risolto il problema puntuale dell'eliminazione di un leader islamista, ma è andato nella direzione contraria alla de-radicalizzazione dei mussulmani: de-radicalizzazione che dovrebbe essere il fine ultimo di quel conflitto. La tensione esistente in certe aree tribali pakistane è stata paragonata alla tensione che, in Sudamerica, hanno vissuto le popolazioni locali dei territori dove operavano gli squadroni della morte: ubiqui e imprevedibili come i droni. In queste aree il tentativo di pacificazione si traduce in un permanente stato di violenza.

Guerra sempre. Le caratteristiche del drone consentono anche di non porre limiti di tempo al suo intervento. I due elementi della tecnologia attuale dei droni che rendono possibile la "guerra ovunque" consentono anche di fare la "guerra sempre". Da un lato, il costo di un drone e del suo apparato umano operativo è minore di quello degli aerei tradizionali e, in particolare, la perdita del drone stesso, cioè dell'ultimo elemento dell'intero "sistema d'arma", rappresenta una spesa relativamente bassa [16]. Dall'altro, i piloti remoti operano in condizioni completamente diverse da quelle dei piloti di aerei tradizionali: sono seduti davanti a un video a migliaia di chilometri dall'obiettivo, quindi non corrono alcun rischio; seguono un "orario di lavoro" che ha un inizio e una fine sindacalmente regolati e, al termine del proprio turno, ritornano a casa loro in un contesto completamente pacifico.

[16] L'economicità dei droni, della loro produzione e della logistica che li circonda non implica una riduzione complessiva delle spese militari. Al contrario, nel bilancio di uno Stato le spese per la guerra ibrida si sommano alle spese per l'infrastruttura militare della guerra tradizionale.

Dal punto di vista operativo, il pilota remoto che ha terminato il suo turno è sostituito da un collega che inizia il turno successivo. Anche il drone che ha raggiunto il limite della sua capacità operativa viene sostituito da un nuovo drone, che ne continua l'attività senza interruzione. In questo modo la tecnica del drone elimina le limitazioni degli aerei tradizionali, come l'esaurimento del carburante e la stanchezza dei piloti. Questo avvicendarsi di droni e di piloti remoti premette una vigilanza di fatto ininterrotta sul luogo prescelto, che continua a essere sorvolato dai vari, successivi droni [17]. Questa continuità presenta due vantaggi operativi. In primo luogo, il pilota remoto può attendere il momento più opportuno per colpire: per esempio, può attendere che la persona da eliminare sia isolata, per evitare "danni collaterali" tra civili. In secondo luogo, l'osservazione è registrata per tutta la sua durata: se quindi, per esempio, in una strada da tempo sotto osservazione scoppia una bomba al passaggio di un blindato, si può ripercorrere a ritroso la registrazione ed eventualmente individuare chi, come e quando ha collocato l'ordigno.

La guerra ibrida contro il terrorismo ha finito per fare propri alcuni comportamenti dell'avversario. Le caratteristiche dei droni, fin qui sommariamente accennate, ne consentono un uso flessibile non sempre in armonia con le regole della guerra tradizionale. Questo sconfinamento etico e giuridico esige l'esame di alcuni problemi.

6. *Guerre ibride e la cancellazione della sovranità nazionale*

Nei droni, alla continua capacità di monitoraggio dell'obiettivo si contrappone l'immediatezza, la puntualità di un'unica azione: il drone più diffuso, il Predator, dispone di due o quattro missili "Hellfire", quindi la sua capacità offensiva si esaurisce in una sola incursione. Alle spalle dell'istantaneo intervento stanno però banche dati raccolti dalle più svariate fonti, informazioni dei servizi segreti delle varie armi e polizie, il lavoro di analisti sul campo e di agenti sotto copertura, la valutazione delle esigenze belliche e dell'entità dell'intervento da parte di vari livelli dei comandi militari: questo accumularsi di dati, analisi e valutazioni può durare mesi, se non anni. Quando il computer segnala che l'obiettivo è raggiungibile, il navigatore lancia il missile che distrugge l'obiettivo in pochi secondi. E qui si pone anche il problema degli eventuali "danni collaterali".

L'esplosione del missile "Hellfire" produce un cratere di circa dieci metri di diametro e proietta schegge anche letali per un centinaio di metri intorno. In

[17] La vigilanza continua è impossibile con il satellite, che sorvola l'obiettivo una sola volta nella sua orbita, ed è molto limitata con gli aerei tradizionali, che sono vincolati ai limiti umani e materiali sopra accennati.

più d'un caso l'obiettivo del "*targeted killing*" si trovava nella propria casa o in un contesto non isolato, quindi l'intervento del drone ha provocato alcune morti di civili: chi risponde per questi "danni collaterali"? In concreto è pressoché impossibile ricondurre a un'unica responsabilità il "danno collaterale", che è quindi destinato a restare impunito, anche se – secondo il diritto nato dalle guerre classiche – costituirebbe un crimine di guerra [18].

Un'altra conseguenza della puntualità dell'intervento è la mancanza di considerazione delle sovranità nazionali. L'uso del drone in una guerra classica – cioè in una guerra dichiarata tra Stati belligeranti – segue le regole, anche giuridiche, di ogni intervento aereo: in questo caso il drone non crea problemi inediti. Invece in una guerra ibrida il drone persegue un nemico non-statale, che non opera in un territorio giuridicamente delimitato e che giuridicamente non è un combattente ascrivibile a un esercito belligerante. In questa situazione, il drone opera a sua volta senza rispettare le sovranità nazionali. L'Afghanistan è lo Stato più colpito dalle incursioni dei droni, e gli attacchi ai Talebani afghani sono partiti dal Pakistan: però il Pakistan non è uno Stato belligerante ed è anzi un alleato degli Stati Uniti, che dal suo territorio lanciano gli attacchi alle aree tribali. Esiste un assenso non dichiarato del governo pakistano, ma formalmente le incursioni di droni ora ricordate violano la sovranità di questo Stato alleato.

Gli Stati Uniti non sembrano essersi preoccupati della sovranità di uno Stato alleato anche nel caso del rapimento di Abu Omar. Nel 2003, un gruppo di agenti della CIA, accompagnati da agenti dei servizi segreti italiani, rapì a Milano Abu Omar, mentre la procura di Milano stava indagando su di lui come sospetto islamista. Abu Omar venne trasferito in carceri segrete in Polonia ed Egitto, torturato e poi rilasciato. Non è possibile esaminare ora questa storia esemplarmente negativa dei rapporti fra due Stati alleati, né la sentenza – credo un unicum nel suo genere – con cui la magistratura italiana ha condannato gli agenti della CIA [19]. Resta

[18] Resta qui aperto il problema della responsabilità giuridica ed etica nell'individuazione dell'obiettivo del drone e nelle morti dei civili. Sono soprattutto i servizi d'informazione a indicare l'obiettivo. L'individuazione avviene attraverso l'analisi computerizzata di flussi informativi in rete, anche mediante i già ricordati algoritmi predatori. In questa attività ritengo che si possano riscontrare due analogie, che non è possibile sviluppare: (a) un'analogia con gli investimenti automatici via computer (non è più l'essere umano a decidere se vendere o comprare, ma il programma, cioè l'algoritmo); (b) un'analogia con la sorveglianza automatica degli e-mail e *social networks* (è il programma decide se una certa comunicazione è rilevante, i.e. pericolosa, o no, in base alla presenza di certe parole o di certi destinatari). Nel determinare l'obiettivo del drone, l'analista trasmette al pilota remoto il risultato fornito dal computer (persona, località). L'operatore del drone esegue come in un video gioco. Risulta pressoché impossibile ricostruire le responsabilità individuali, sia morali, sia giuridiche, tanto per la scelta del *targeted killing*, quanto per i danni collaterali.

[19] A. VEDASCHI, Extraordinary Renditions: *esiste una giustizia transnazionale?*, *Diritto pubblico comparato ed europeo*, 2013, pp. 1255-1292: oltre al caso Abu Omar, l'autrice analizza a fondo anche le *extraordinary renditions* in *enditions* di Khalid el-Masri, di Maher Arar e di Binyam Mohamed Habashi, nonché i loro riflessi giudiziari e internazionalistici.

il fatto che, se gli agenti statunitensi avessero avuto la finalità non di interrogare Abu Omar, bensì di eliminarlo, quest'ultimo avrebbe potuto essere oggetto di un *targeted killing* mediante un drone, e non di una *extraordinary rendition*.

Uno dei più emblematici *targeted killings*: è quello di Anwar al-Aulaqi, un predicatore mussulmano e cittadino statunitense residente in Virginia. Radicalizzatosi ed emigrato in Yemen, venne incluso in una *killing list* e ucciso da un drone. Questa uccisione di un cittadino americano senza processo sollevò una grande polemica negli Stati Uniti, che non è qui possibile ricostruire[20]. L'American Civil Liberties Union ha pubblicato il documento ufficiale che autorizza questa esecuzione extragiudiziaria[21].

Strumento ideale per la caccia all'uomo (senza responsabilità), l'uso del drone non distingue fra spazio politico interno e spazio politico esterno, come si è visto a proposito della sovranità nazionali dei singoli Stati. La cancellazione di questo confine ha avuto come conseguenza, nelle attuali guerre ibride, una progressiva erosione delle differenze operative tra forze armate e servizi segreti, all'estero, e – nella lotta al terrorismo – tra polizia e servizi segreti, all'interno.

Negli Stati Uniti, l'attentato dell'11 settembre 2001 ha indotto il Presidente Busch a dichiarare la *Global war on terror*, appoggiata dalle norme contenute nell'*Authorization for Use of Military Force Against Terrorist* e nel *Patriot Act*. Sulla base di queste norme, la CIA ha potenziato i suoi interventi all'estero, ritornando ai tempi della Guerra fredda con azioni sotto copertura sempre più simili a interventi militari. Parallelamente, il Pentagono ha rafforzato i servizi segreti dell'esercito (Intelligence Support Activity, ISA) ed ha istituito il Joint Special Operations Command (JSOC), che opera in coordinamento con l'ISA e che conduce operazioni sotto copertura analoghe a quella della CIA.

Il campo di battaglia non si è soltanto esteso, divenendo indeterminato, ma su di esso è anche calata la nebbia.

In conclusione, il computer (anche attraverso un drone da ricognizione) raccoglie in permanenza dati sui terroristi e sulle reti da loro usate. I dati alimentano l'analisi dei servizi per individuare i potenziali obiettivi. Gli obiettivi individuati vengono segnalati al drone d'attacco: non c'è più alcun rapporto tra il pilota remoto e l'obiettivo. In questo contesto di deresponsabilizzazione, come in un videogioco, il drone diviene lo strumento ideale per l'omicidio politico. L'indeterminatezza di tutti gli elementi in gioco non permette più al

---

[20] W. C. BANKS, *Regulating Drones: Are Targeted Killings by Drones Outside Traditional Battlefields Legal?*, in P. L. BERGEN, D. ROTHENBERG (eds.), *Drone Wars. Transforming Conflict, Law and Policy*, Cambridge University Press, New York 2015, pp. 129-159. Buona parte dell'articolo analizza il caso al-Aulaqi (trascritto al-Awlaki): pp. 133-151.

[21] OFFICE OF LEGAL COUNSEL MEMORANDUM, February 19, 2010, *Lethal Operation Against Shaykh Anwar Aulaqi*, in J. JAFFER (ed.), *The Drone Memos. Targeted Killing, Secrecy, and the Law*, The New Press, New York, London, 2016, pp. 61-72; le pp. 63-67 sono censurate per intero, mentre delle pp. 68 e 69 si salvano poche righe.

singolo partecipante un giudizio sul giusto o l'ingiusto – giudizio su cui si può fondare il rifiuto di eseguire l'ordine. Questa non è più una guerra tradizionale, quindi divengono inapplicabili le regole finora elaborate per la guerra tradizionale.

L'uso dei droni ha cambiato la natura del conflitto armato: il rapporto tra il pilota, remoto e intangibile, e l'obiettivo, sempre sotto tiro e spesso ignaro di esserlo, non è più il rapporto fra due combattenti, ma il rapporto fra cacciatore e preda. Si è così realizzata nel modo più radicale l'aspirazione millenaria di allontanare i combattenti l'uno dall'altro[22]. Al tempo stesso in noi osservatori della guerra ibrida sembra atrofizzarsi il senso del giusto e del bene, del diritto e della morale. Fin qui abbiamo parlato asetticamente di pratiche orrende: del sequestro di Abu Omar per ottenerne informazioni sotto tortura in prigioni segrete nel territorio dell'Unione Europea, o dell'assassinio politico di terroristi o presunti tali, per non parlare dei famigliari vicino a loro al momento dell'esplosione del missile; e non abbiamo potuto parlare dei *signature strikes* che sono omicidi mirati di persone non identificate, oppure dell'odiosa pratica del *double tap*, cioè del secondo missile su chi si accorre in aiuto delle vittime del primo[23]. Le parole dell'attivista dell'American Civil Liberties Union, che ha pubblicato i documenti statunitensi autorizzanti i *targeted killings*, devono indurci non solo a riflettere criticamente sugli indirizzi politici attuali, ma anche ad agire contro di essi. Quei documenti, scrive, «are a measure of the extent to which the perceived demands of counterterrorism are erasing rule-of-law strictures that were taken for granted only a generation ago»[24].

7. *Con l'informatica all'attacco e in difesa: e la* privacy*?*

Ritorniamo su uno dei temi affrontati alla fine delle considerazioni sulla *cyberwar*: piccole imprese – private – producono potenti *software* di sorveglianza (*spyware*) e li commerciano sul libero mercato, come si è visto nelle due microstorie milanesi del § 3. A loro si aggiungono le raccolte di dati personali delle

---

[22] Nell'ambiente militare statunitense ci si è chiesti se – per il conferimento delle onorificenze militari – il pilota remoto potesse essere definito come "combattente": infatti quelle onorificenze possono essere conferite soltanto ai combattenti.

[23] La tecnica del *double tap* (mutuata dai terroristi), consiste in un secondo attacco di droni contro chi è andato ad aiutare i colpiti dal primo attacco e si fonda sulla supposizione che, essendo sospetti terroristi i primi, lo siano anche i secondi: *guilt by association*. Questa sottospecie di *signature strike* è purtroppo così frequente, che un'associazione umanitaria ha adottato la regola di attendere sei ore prima di assistere le vittime di un attacco di droni. Questi "effetti collaterali" hanno coinvolto anche matrimoni e funerali, tanto che in certe aree tribali la popolazione ha smesso di assistere ai funerali. Cfr. H. GUSTERSON, *Drone. Remore Control Warfare*, cit., p. 96.

[24] J. JAFFER (ed.), *op. cit.*, p. 2.

grandi imprese come Google, Yahoo, ecc. a fini commerciali e pubblicitari. L'accumularsi di dati personali in memorie sempre più potenti con programmi sempre più sofisticati ha indotto il legislatore a proteggere questi dati personali con le leggi sulla *privacy* dalla fine degli anni '70.

Con l'avvento del terrorismo internazionale e delle guerre ibride la protezione dei dati personali è divenuta vitale non solo per l'ambito privato o commerciale, ma anche per quello della sicurezza nazionale. Dagli anni '90 è divenuto sempre più intenso il dibattito sulla prevalenza della sicurezza (bene pubblico) sulla riservatezza (bene privato), o viceversa. Da allora si constata una crescente erosione delle norme a tutela della *privacy* a vantaggio di quelle a tutela della sicurezza. Il problema poco trattato è questo: nella generale tendenza (nell'ambito del neoliberismo) a estendere progressivamente il potere esecutivo a scapito del potere legislativo, il pretesto della sicurezza viene usato per scardinare le tutele individuali a vantaggio di un crescente controllo dello Stato sui cittadini[25].

Se però diminuisce il controllo democratico sulla raccolta e gestione dei dati personali, cresce l'ambito di opacità sulle attività governative[26]. Anche qui, nulla di nuovo: questa opacità istituzionale è definita sin dall'antica Roma come *arcana imperii* e su di essa esiste la legislazione (e l'immensa letteratura) sulla trasparenza dell'amministrazione pubblica, sul segreto di Stato e sul diritto del cittadino ad essere informato. Negli Stati Uniti, questo diritto è stato rafforzato dal *Freedom of Information Act*, che ha permesso di rendere pubblici importanti documenti sui *targeted killings* nel volume *The Drone Memos* più volte citato.

Dall'opacità si sta passando all'oscurità, e il cuore di tenebra dello Stato si estende sempre più. Il cittadino non può rendersi conto se l'estensione dell'oscurità è dovuta alla difesa dello Stato oppure all'invadenza dello Stato nella sfera privata. Le gigantesche raccolte di dati personali possono servire, da un lato, a rendere sempre più individualizzate le prestazioni dello Stato sociale oppure a colpire gli individui che operano contro lo Stato. Ma questi ultimi possono essere terroristi, oppure dissenzienti politici. I programmi di Hacker Team e Area sono stati venduti anche a Stati non democratici che li usano per il controllo dei dissidenti, cioè dei fautori della democrazia rappresentativa.

Un riflesso legislativo delle guerre ibride è il crescente ridimensionamento della protezione dei dati personali, realizzata nei decenni anteriori attraverso le normative nazionali ed europee. Basti qui accennare a due casi, in cui la riserva-

---

[25] Il controllo dello Stato sui cittadini non è necessariamente un male: in uno Stato sociale ben organizzato, la conoscenza quanto più dettagliata dei dati di un cittadino può servire a distribuire meglio le prestazioni sociali. In un altro campo, si è progettato di sostituire il censimento quadriennale della popolazione con un "censimento permanente" fondato sui dati personali memorizzati e sempre attualizzati.

[26] Si rinvia, per l'approfondimento di questi temi, ai contributi di questo volume nella sezione intitolata *Sicurezza, lotta al terrorismo e segreto di Stato*.

tezza dei dati personali è limitata a favore della sicurezza collettiva, seguendo una tendenza che va affermandosi di pari passo con il diffondersi del terrorismo e delle guerre ibride.

La *Loi des renseignements* francese del 3 ottobre 2015 è stata portata davanti alla Corte di Giustizia dell'Unione Europea dalla *Association confraternelle de la presse judiciaire* nel giorno stesso della sua entrata in vigore. Questa legge permette una sorveglianza di massa non solo contro il terrorismo e la criminalità organizzata («qui portent gravement atteinte à la paix publique»), ma anche per proteggere «les interêts majeurs de la politique étrangère» o anche «les interêts économiques, industriels et scientifiques»[27]. È chiaro che questi sono i vasti obiettivi della guerra ibrida; però con norme di questo genere, in concreto, cade ogni protezione per le fonti del giornalismo investigativo. In quello stesso 3 ottobre venne rafforzata con un decreto Presidente della Repubblica la *Commission nationale de contrôle des techniques de renseignement* (che esisteva del 1991 dopo le intercettazioni all'Eliseo) per sorvegliare che la raccolta dei dati avvenga nel rispetto del *Code de la sécurité intérieure*.

Sempre sulla diffusione dei dati personali (e in particolare sulla loro cessione per ragioni di sicurezza) si è svolto il braccio di ferro tra Stati Uniti e i giganti della rete come Google o Yahoo dei dati personali. La Commissione Europea aveva concordato con gli Stati Uniti un accordo (impropriamente chiamato "trattato": *Safe-Harbor-Pact*) per il trasferimento negli USA dei dati personali dei cittadini europei. Questo accordo è stato annullato dalla Corte Europea di Giustizia il 6 ottobre 2015. La coincidenza fra le date della legge francese e della sentenza europea attesta quanto controverso sia il problema della tutela dei dati personali, e quanti rischi vi si nascondano. «La Corte europea di giustizia di Lussemburgo mette un freno all'invadenza degli Stati Uniti sui dati personali dei cittadini europei. Gli eurogiudici hanno bocciato l'attuale sistema di trasferimento dall'Ue agli Usa detto *Safe Harbor* (Approdo sicuro) – utilizzato dai giganti Usa di internet e da migliaia di imprese private – perché non garantisce il diritto fondamentale a un adeguato grado di protezione della *privacy*. Determinanti sono risultate le rivelazioni dell'ex agente della statunitense National Security Agency, Edward Snowden, sullo spionaggio di massa delle autorità Usa, che provocarono lo scandalo internazionale *Datagate*»[28].

Queste gigantesche raccolte di dati personali (*big data*) possono essere create

---

[27] F. JOHANNES, *Des journalistes attaquent la loi renseignements*, in *Le Monde*, 4-5 octobre 2015, p. 14. Dubbi su questa legge sono stati espressi dalla *Commission nationale consultative des droits de l'homme* e dalla *Commission Nationale Informatique et Libertés* (CNIL, cioè dal garante dei dati della Francia).

[28] I. CAIZZI, *Privacy non garantita negli Usa*, in *Corriere della Sera*, 7 ottobre 2015, p. 23: «L'altolà dell'Europa a Facebook. La Corte di giustizia boccia l'accordo sui trasferimenti dei dati personali. Effetto Snowden: Il caso partito dopo le rivelazioni dell'ex agente dell'agenzia per la sicurezza americana».

per fini democratici, ma un cambio di governo può gestirle nella direzione opposta.

Aldous Huxley nel romanzo *Brave New World* del 1932 descriveva un mondo in cui lo Stato giungeva al controllo totale dei cittadini attraverso l'eugenetica, una scienza allora nuova e promettente. Nell'immaginario collettivo, l'informatica del 2000 ha sostituito l'eugenetica del 1932, pervadendo ogni aspetto della vita sociale, comprese le guerre ibride di cui ci si è fin qui occupati.

Le guerre ibride presentano un *brave new world* per nulla tranquillizzante. In esso, tutti i nostri dati circolano fuori dal nostro controllo e possono essere usati contro di noi; non c'è più distinzione tra pace e guerra, tra fronte e retrovia, quindi tra civili e belligeranti; ognuno di noi è un potenziale obiettivo (*everywhere war*) e ognuno di noi è sempre sotto attacco. L'elenco potrebbe continuare, ma quanto detto fin qui può bastare per darci il benvenuto nel *brave new world* della globalizzazione bellico-informatica.