



Cattedra

RELATORE

CANDIDATO

Anno Accademico

INDICE

Introduzione.....	2
Capitolo 1 - La trasformazione della guerra nel dibattito teorico.....	4
1.1 Il concetto di guerra nella tradizione classica	5
1.2 Il superamento della guerra esclusivamente convenzionale	6
1.3 Le nuove dinamiche dei conflitti nel contesto contemporaneo.....	9
Capitolo 2 - La guerra ibrida: nascita e definizione del concetto	13
2.1 Origine del termine e sviluppo nella letteratura.....	14
2.2 Definizioni di guerra ibrida e principali interpretazioni teoriche	18
2.3 Elementi costitutivi della guerra ibrida.....	22
Capitolo 3 - L'evoluzione della guerra ibrida nei conflitti moderni.....	29
3.1 Continuità e discontinuità rispetto alle forme di guerra tradizionali	30
3.2 Guerra ibrida e mutamento degli attori del conflitto.....	36
3.3 La guerra ibrida come modello di conflitto del XXI secolo	39
Conclusioni.....	42
Bibliografia.....	45

INTRODUZIONE

I mutamenti bellici del nuovo millennio sfidano le categorie teoriche e il diritto internazionale classico, che per lungo tempo hanno costituito la base per comprendere la conflittualità tra i diversi soggetti politici. Se la modernità era stata caratterizzata dalla distinzione netta tra lo stato di pace e lo stato di guerra, la contemporaneità ci consegna uno scenario in cui tale confine appare sempre più sfumato, sottile e difficile da definire. È in questo solco che si inserisce il concetto di *Guerra ibrida*, un termine che ha guadagnato centralità nel dibattito strategico e accademico per descrivere la complessità delle nuove minacce.

Il presente elaborato di tesi si propone di analizzare la genesi, la definizione e l'evoluzione del concetto di guerra ibrida, cercando di comprendere come la combinazione di mezzi convenzionali, tattiche irregolari, pressioni economiche e offensive nello spazio cibernetico stia ridefinendo il volto della conflittualità globale. La scelta di questo tema nasce dalla necessità di comprendere la vulnerabilità delle moderne democrazie occidentali di fronte a minacce che agiscono spesso al di sotto della soglia del conflitto armato palese. La guerra ibrida non ha necessariamente come obiettivo la distruzione fisica dell'avversario sul campo di battaglia, ma punta piuttosto a destabilizzarne il tessuto sociale, a influenzarne i processi decisionali e a minarne la fiducia nelle istituzioni.

L'obiettivo centrale della ricerca è duplice, da un lato, fornire una solida base teorica tale da permettere la distinzione tra la guerra ibrida e le forme di guerra del passato; dall'altro, esaminare come questo paradigma si sia evoluto nel tempo per diventare lo strumento privilegiato sia da Stati che da entità non statali, infrangendo così i modelli interpretativi classici della dottrina.

Per dare risposta a tali interrogativi, il lavoro è stato articolato in tre capitoli principali, il primo Capitolo tratta la trasformazione del concetto di guerra nel dibattito teorico. Partendo dal paradigma classico della guerra come scontro tra eserciti regolari, si analizzeranno gli elementi che hanno portato al superamento del modello puramente convenzionale, evidenziando le nuove dinamiche dei conflitti contemporanei.

Il secondo capitolo entra nel vivo della definizione di guerra ibrida, attraverso l'analisi della letteratura accademica del settore, con particolare attenzione ai lavori di Frank Hoffman, verranno isolati gli elementi costitutivi di questa strategia: dall'uso della disinformazione ai cyber-attacchi, fino all'impiego di attori per procura, i cosiddetti "*proxy*".

Il terzo capitolo, infine, esamina l'evoluzione della guerra ibrida nei conflitti moderni. Si analizzeranno i punti di continuità e discontinuità con il passato ed il modo in cui il mutamento degli attori coinvolti abbia reso la dimensione ibrida il modello di riferimento per comprendere le tensioni geopolitiche del XXI Secolo.

In conclusione, l'elaborato si propone l'obiettivo di individuare le sfide future per la sicurezza internazionale, mettendo così in evidenza come la natura stessa del potere e della conflittualità sia oggi subordinata alla capacità di esercitare un controllo dominante sullo spazio dell'informazione e sulle tecnologie emergenti. In questo nuovo scenario la dimensione conoscitiva e il dominio cibernetico non sono più semplici conseguenze dell'azione militare ma ne diventano il baricentro strategico. Ne deriva che la sovranità degli attori internazionali si gioca sempre più sulla resilienza delle proprie infrastrutture digitali e sulla capacità di gestire flussi di informazioni in grado di influenzare sia l'opinione pubblica che i processi decisionali prima ancora dell'impiego della forza cinetica.

CAPITOLO PRIMO

LA TRASFORMAZIONE DELLA GUERRA NEL DIBATTITO TEORICO

Il primo capitolo di questo lavoro si propone di tracciare un percorso analitico volto a comprendere la metamorfosi dell'atto bellico, partendo dalle fondamenta della dottrina strategica tradizionale fino alle complessità dei conflitti odierni. Comprendere la “guerra ibrida” richiede, infatti, una riflessione preliminare sulla natura stessa della guerra e sulla sua evoluzione storica e teorica. Non si può definire l'*ibridismo* senza prima aver delineato il “convenzionale”, ovvero quel modello di conflitto simmetrico che ha dominato il panorama internazionale dalla Pace di Vestfalia fino alla fine della Guerra Fredda.

La ricerca partirà dall'esame dei modelli classici, con particolare attenzione al pensiero di Carl von Clausewitz, il cui trattato “Della Guerra” (*Vom Kriege*) rimane ancora oggi il punto di riferimento per la comprensione del conflitto come atto politico. Si osserverà come il modello della “guerra assoluta” e la distinzione netta tra combattenti e civili abbiano costituito per secoli la norma internazionale.

Tuttavia, il mutamento degli equilibri geopolitici e l'avanzamento tecnologico hanno progressivamente indebolito questa solidità. Nella seconda parte del Capitolo, l'attenzione si sposterà sul superamento della guerra esclusivamente convenzionale, indagando come la comparsa di minacce asimmetriche e irregolari abbia costretto gli analisti a rivedere le categorie classiche. Infine, verranno esplorate le nuove dinamiche dei conflitti contemporanei segnate dalla globalizzazione e dalla rivoluzione digitale che hanno trasformato il campo di battaglia da uno spazio puramente fisico ad un ecosistema multidimensionale.

Questa ricognizione teorica è fondamentale per evidenziare come la guerra non sia un fenomeno statico, ma un “camaleonte”, per citare ancora Clausewitz, capace di adattare la propria forma ai mutamenti della società e della tecnologia, preparando così il terreno per la definizione di guerra ibrida che verrà trattata nel capitolo successivo.

1.1 IL CONCETTO DI GUERRA NELLA TRADIZIONE CLASSICA

Per cogliere il potenziale dirompente della conflittualità ibrida, occorre preliminarmente esaminare il paradigma che essa mira a sovvertire, ovvero la concezione convenzionale della guerra. Questo modello non rappresenta soltanto una modalità di scontro fisico, ma un'istituzione politica e giuridica complessa, consolidatasi in Europa a partire dalla Pace di Vestfalia del 1648¹. Tale evento segnò la nascita dello Stato moderno come unico detentore del monopolio della forza legittima, trasformando la guerra da una violenza privata e disordinata a un affare di Stato regolamentato².

Nella tradizione classica, la guerra è definita come uno scontro armato tra unità politiche sovrane, ovvero gli Stati, che si riconoscono reciprocamente come *justus hostis* (nemico legittimo)³. Questo riconoscimento è fondamentale, in quanto, il nemico non è un criminale da annientare, ma un avversario con cui si può negoziare e, infine, concludere una pace⁴. La distinzione tra stato di pace e stato di guerra è netta e binaria; il passaggio dall'uno all'altro è sancito da protocolli formali, come la dichiarazione di guerra, che delimita chiaramente il tempo e lo spazio del conflitto.

Il pilastro teorico di questa visione è l'opera del generale prussiano Carl von Clausewitz⁵, *Vom Kriege* (Della Guerra)⁶. Clausewitz fu il primo a *sistematizzare* l'idea che la guerra sia un atto di forza destinato a costringere l'avversario a sottomettersi alla nostra volontà, ma sempre subordinato a un fine superiore, ovvero la politica. Il suo celebre assioma che definiva la guerra come «la continuazione della politica con altri mezzi» implica che il conflitto armato non sia

¹ La Pace di Vestfalia (o Westfalia) fu un insieme di trattati firmati nel 1648 a Münster e Osnabrück che posero fine alla Guerra dei Trent'anni e alla Guerra degli Ottant'anni, stabilendo un nuovo equilibrio di potere in Europa, affermò il diritto di ogni stato a governarsi autonomamente senza interferenze esterne, creando le basi per lo stato moderno non confessionale ed è considerata una delle pietre miliari della storia europea, definendo il moderno sistema di stati nazionali sovrani e gettando le basi per le relazioni internazionali per i secoli a venire.

² H. Bull, *La società anarchica. Uno studio sull'ordine nella politica mondiale*, Vita e Pensiero, Milano 2005, pp. 30-45.

³ *Iustus hostis* (nemico giusto) è un concetto del diritto internazionale classico e della teoria della guerra, che identifica il nemico come un avversario con cui uno Stato può ingaggiare un conflitto armato legittimo, un pari in guerra, riconoscendo la sua condizione di belligerante ma non necessariamente la giustizia della sua causa, mentre il diritto moderno si concentra sull'aggressione illegittima e i *jus in bello* (diritti nella guerra). Questo concetto permetteva di limitare la violenza bellica, trattando il nemico come un soggetto di diritto internazionale, non un criminale, a differenza della visione moderna che criminalizza l'aggressore.

⁴ C. Schmitt, *Il nomos della terra nel diritto internazionale dello jus publicum europaeum*, Adelphi, Milano 1991, p. 162.

⁵ Carl von Clausewitz (1780 - 1831) è stato un generale prussiano e uno dei teorici militari più influenti della storia, noto principalmente per il suo fondamentale lavoro "*Vom Krieg*" (Della guerra).

⁶ *Della guerra* (in tedesco: *Vom Kriege*) è un'opera di Carl von Clausewitz, composta di otto libri. Pubblicato nel 1832, è ancor oggi considerato uno dei più grandi trattati di strategia militare mai scritti, ed è tuttora adottato come libro di testo da numerose accademie militari.

un'anomalia o un'esplosione di violenza irrazionale, ma un linguaggio razionale attraverso il quale lo Stato persegue i propri interessi nazionali⁷.

Un concetto di fondamentale importanza per l'analisi della trasformazione bellica è la *trinità clausewitziana*. Clausewitz identifica tre forze motrici che governano ogni guerra: l'impulso cieco, ovvero l'odio e l'inimicizia che risiedono nel popolo; il gioco delle probabilità e del caso, che riguarda le forze armate, il genio del comandante ed infine la natura subordinata di strumento politico ovvero la ragione, che compete al governo. In questo schema, la stabilità del conflitto è data dal perfetto bilanciamento tra questi tre fattori. La guerra classica è considerata tale perché queste tre sfere sono ben distinte e comunicanti tra di loro: il popolo sostiene, i soldati combattono, il governo decide.

Sotto un punto di vista operativo e giuridico, il modello classico si fonda sulla distinzione tra combattenti e civili. Tale separazione, regolamentata nel tempo fino alle Convenzioni di Ginevra⁸, impone che la violenza sia rivolta esclusivamente contro gli apparati militari avversari. La guerra si svolge su campi di battaglia geograficamente definiti ed attraverso tattiche lineari. Si tratta della cosiddetta *guerra simmetrica*, dove gli sfidanti utilizzano mezzi simili e condividono le stesse regole d'ingaggio⁹.

In sintesi, la tradizione classica ha cercato di regolamentare, per così dire, il conflitto, confinandolo all'interno di margini gestibili e prevedibili. La guerra ibrida, come vedremo nei capitoli successivi, agirà esattamente per frantumare queste categorie: colpirà la popolazione civile per bypassare l'esercito, utilizzerà mezzi non militari per ottenere scopi politici e, soprattutto, annullerà la distinzione tra pace e guerra, operando in una *zona grigia* dove il riconoscimento dell'avversario e la responsabilità dell'attacco diventano impossibili.

1.2 IL SUPERAMENTO DELLA GUERRA ESCLUSIVAMENTE CONVENZIONALE

Il processo di disgregazione del modello convenzionale rappresenta uno dei mutamenti sociopolitici più profondi dell'ultimo secolo. Per secoli, la guerra era stata intesa come un'attività regolata da norme giuridiche e consuetudini cavalleresche, fondata sulla simmetria

⁷ C. von Clausewitz, *Della guerra*, a cura di E. Arbrile, Mondadori, Milano 1970, p. 38.

⁸ Le Convenzioni di Ginevra sono una serie di trattati internazionali fondamentali del diritto umanitario, originati nel 1864 e aggiornati principalmente nel 1949, che stabiliscono le regole per la protezione delle vittime dei conflitti armati, come feriti, prigionieri di guerra, civili e personale medico, definendo standard di trattamento umano e sancendo il divieto di atrocità come tortura, omicidi e rappresaglie. Il termine si riferisce comunemente al corpus del diritto di guerra.

⁹ M. Kaldor, *Le nuove guerre. Violenza organizzata nell'età globale*, Carocci, Roma 1999, pp. 20-35.

dei mezzi e degli obiettivi. Tuttavia, il XX Secolo ha agito da acceleratore per il superamento di questa visione, trasformando il conflitto da uno scontro tra apparati militari ad una condizione pervasiva che coinvolge l'intera struttura della società¹⁰.

- La crisi del modello industriale e la “Guerra Totale”

Il primo segnale di discontinuità con il passato si manifesta con le due Guerre Mondiali. In questi contesti la distinzione tra fronte militare e fronte interno crolla definitivamente. La mobilitazione totale delle risorse industriali, scientifiche e umane ha trasformato ogni cittadino in un potenziale ingranaggio della macchina bellica e di conseguenza in un bersaglio legittimo. La cosiddetta *guerra totale*¹¹ ha introdotto l'idea che la vittoria si ottenga non solo sconfiggendo l'esercito avversario, ma distruggendo la capacità produttiva e la resistenza psicologica della popolazione civile. Questo cambiamento ha incrinato il pilastro clausewitziano della distinzione tra popolo e governo portando la violenza ben oltre il campo di battaglia tradizionale¹².

- L'era nucleare e la *congelazione* della simmetria

Un secondo momento di svolta fondamentale è rappresentato dall'avvento dell'arma atomica. Come teorizzato da Raymond Aron¹³, l'introduzione della bomba nucleare ha creato un paradosso strategico: le grandi potenze, pur possedendo mezzi di distruzione immensi, non possono più utilizzarli in uno scontro diretto senza rischiare l'autoannientamento. Questo stato di “pace armata” ha costretto i conflitti a defluire verso forme non convenzionali¹⁴. La guerra non è sparita, ma è diventata limitata o indiretta. Lo Stato ha iniziato a delegare la violenza a gruppi ribelli, milizie locali o movimenti di liberazione nazionale, dando vita alle guerre per procura (*proxy wars*)¹⁵. In questi scenari, la sovranità statale viene aggirata e la responsabilità

¹⁰ E. Jünger, *La mobilitazione totale*, in Foglie e fiori, Adelphi, Milano 2003, pp. 95-120.

¹¹ La locuzione *guerra totale* è nata nel XX secolo per descrivere una guerra in cui gli Stati usano tutte le risorse a loro disposizione allo scopo di distruggere l'abilità di un altro Paese o Nazione di impegnarsi in guerra. Divenne così fondamentale il ruolo della popolazione. La pratica della guerra totale è stata in uso sotto diverse forme per secoli, ma le peculiarità di un modo di combattere che coinvolge l'intera popolazione civile sono state pienamente riconosciute come un modo specificamente sui generis di guerra solo nella seconda metà del ventesimo secolo.

¹² R. Aron, *Il secolo della guerra totale*, Rizzoli, Milano 1954.

¹³ Raymond Claude Ferdinand Aron (1905 - 1983) è stato un filosofo, sociologo, storico e politologo francese. Fu promotore di un liberalismo moderno, controcorrente rispetto al prevalente milieu intellettuale di sinistra e ispirato al pacifismo.

¹⁴ R. Aron, *Pace e guerra tra le nazioni*, Edizioni di Comunità, Milano 1970, pp. 412-430.

¹⁵ Una guerra per procura (o *proxy war*) è un conflitto armato in cui potenze maggiori combattono indirettamente, sostenendo forze locali o fazioni avversarie con denaro, armi, addestramento e supporto logistico, invece di affrontarsi direttamente per evitare i costi e i rischi di una guerra totale, specialmente nell'era nucleare. Questo

degli atti bellici diventa sfumata, prefigurando quella ricerca di ambiguità che sarà centrale nella guerra ibrida¹⁶.

- La Guerra tra la gente e l'ascesa dell'insorgenza

A partire dalla decolonizzazione e dai conflitti della seconda metà del Novecento (Vietnam, Afghanistan, Algeria), si è assistito al successo della guerra asimmetrica¹⁷. Il generale britannico Rupert Smith¹⁸ ha coniato il termine “guerra tra la gente” per descrivere questo nuovo paradigma. In questa forma di conflitto, gli obiettivi non sono più territoriali, ovvero conquistare una collina o una capitale per fare un esempio, ma riguardano la volontà della popolazione¹⁹. L'insorgenza e la guerriglia hanno dimostrato che un attore tecnologicamente inferiore può neutralizzare una superpotenza se riesce a operare in modo invisibile all'interno del tessuto sociale. La forza bruta convenzionale perde efficacia contro un nemico che non difende confini, non indossa uniformi e utilizza la propaganda come arma principale. La vittoria, dunque, si sposta dal piano *cinetico* (quanti soldati uccido) al piano *perceptivo* (quante menti riesco a influenzare).

- La tecnologia come livellatore di potenza

Infine, la rivoluzione negli affari militari (RMA)²⁰ e la successiva digitalizzazione hanno completato il superamento del modello convenzionale. Se un tempo solo gli Stati potevano permettersi sistemi di comunicazione o armamenti sofisticati, oggi la tecnologia civile offre a piccoli gruppi o a singoli individui capacità d'offesa globali. Internet e i social media sono diventati i nuovi teatri operativi dove condurre operazioni psicologiche e sabotaggi economici.

permette alle superpotenze di perseguire i propri obiettivi geopolitici, estendere la propria influenza e indebolire gli avversari senza subire perdite dirette, utilizzando paesi terzi o attori non statali come intermediari.

¹⁶ K. Deutsch, *The Analysis of International Relations*, Prentice-Hall, Englewood Cliffs 1968, pp. 110-125.

¹⁷ M. A. Levy, *Asymmetric Warfare: Today's Challenge to US Military Power*, Cass Series on Contemporary Security Studies, London 2001, pp. 8-19.

¹⁸ Il Generale Sir Rupert Smith (1943) è un ufficiale britannico in pensione dell'esercito, noto per il suo servizio di alto livello, la sua esperienza strategica in conflitti come la Guerra del Golfo e la guerra in Bosnia, e per essere stato Vice Comandante Supremo Alleato in Europa (DSACEUR) della NATO; è anche un acclamato autore, noto per il libro “*The Utility of Force*”.

¹⁹ R. Smith, *L'arte della guerra nel mondo contemporaneo. La risposta dei popoli alle crisi di oggi*, Il Mulino, Bologna 2009, pp. 21-45.

²⁰ La Rivoluzione negli Affari Militari (RMA) è un cambiamento radicale e profondo nel modo di condurre la guerra, guidato da nuove tecnologie (come l'informatica e la guerra elettronica) e dottrine, che trasformano la strategia, la tattica e la struttura stessa delle forze armate, passando da conflitti tradizionali a operazioni ad alta intensità informativa e precisione. Si tratta di un'evoluzione continua, spesso legata all'emergere di nuove tecnologie, che ridefinisce il concetto di “dominio” (terra, mare, aria, spazio, cyber) e il rapporto tra efficacia militare e costi

La guerra è uscita dalle caserme per entrare negli smartphone e nelle infrastrutture critiche civili, rendendo la forza militare tradizionale solo una delle tante opzioni disponibili in un arsenale molto più vasto e intangibile²¹.

1.3 LE NUOVE DINAMICHE DEI CONFLITTI NEL CONTESTO CONTEMPORANEO

I conflitti del XXI secolo non sono una mera prosecuzione delle dinamiche passate, bensì il segnale di una profonda mutazione strutturale della geopolitica. Ci troviamo di fronte a una trasformazione dell'essenza stessa della violenza organizzata, che rende ormai obsoleti i parametri di analisi tradizionali. Se il *Secolo Breve*²² è stato l'epopea delle grandi narrazioni ideologiche e degli scontri frontali tra blocchi monolitici, l'era contemporanea ha inaugurato il paradigma della distribuzione del potere tra molteplici poli d'influenza e la sua tendenza a non stabilizzarsi mai in una forma definita.

- Dalla *geopolitica dei blocchi* alla frammentazione del potere

Mentre nel Novecento il conflitto era regolato dalla dottrina della Distruzione Mutua Assicurata (MAD)²³ e da confini chiaramente tracciati dal Trattato di Westfalia, oggi assistiamo alla dissoluzione della sovranità statale come unico attore bellico. Gruppi terroristici transnazionali, milizie private (come il Gruppo Wagner²⁴ o le PMC occidentali²⁵), cartelli della droga e colossi tecnologici (Big Tech) agiscono ora come soggetti politici dotati di capacità

²¹ J. Nye, *Il paradosso del potere americano*. Perché l'unica superpotenza non può fare da sola, Einaudi, Torino 2002, pp. 54-72.

²² Lo storico Eric J. Hobsbawm ha creato la locuzione-concetto di *Secolo breve* per definire (temporalmente) il XX secolo, un secolo di enormi cambiamenti, conquiste, scoperte, ma anche di grandi crisi socio-economiche e naturali. Breve, appunto, perché da un punto di vista storico - anche se non temporale - il Novecento è iniziato nel 1915 alla fine della prima guerra mondiale con la caduta dei grandi imperi, e si è chiuso con la caduta dell'ultimo grande impero, quello del socialismo reale nel 1989.

²³ La Distruzione Mutua Assicurata (MAD, dall'inglese Mutual Assured Destruction) è una teoria strategica nucleare per cui un attacco nucleare su larga scala da parte di un avversario, che possiede capacità di secondo colpo (second-strike capability), causerebbe il completo annientamento sia dell'attaccante che del difensore, creando una deterrenza basata sul terrore reciproco. Questa dottrina, formalizzata durante la Guerra Fredda, assicura una stabilità nucleare impedendo l'uso delle armi atomiche, ma si basa su condizioni rischiose come la perfetta individuazione degli attacchi e la perfetta attribuzione, che potrebbero fallire.

²⁴ Il Gruppo Wagner è di solito descritto come un'entità militare privata (Private Military Company, PMC) non registrata con base in Russia, ma attiva soltanto al di fuori dei suoi confini. In generale, ad oggi le informazioni disponibili su questa entità sono alquanto limitate.

²⁵ Con "PMC occidentali" ci si riferisce alle Private Military Companies (PMC) (Aziende Militari Private) provenienti da paesi occidentali, società che offrono servizi armati di sicurezza e supporto militare a scopo di lucro, come consulenza, addestramento e operazioni di combattimento, spesso reclutando personale con esperienza militare. Queste entità operano globalmente, a volte in parallelo con le forze armate statali, gestendo mercenari (contractors).

belliche autonome. Inoltre è sempre più flebile la separazione tra “fronte” e “retrovie” o tra “civile” e “militare”. La guerra non si dichiara più formalmente ma si vive, si subisce e si alimenta in una zona grigia permanente.

I conflitti moderni si sviluppano attraverso una fusione inscindibile tra forza militare e tattiche asimmetriche. L'obiettivo bellico si è spostato, non si mira più soltanto alla conquista del terreno, ma al dominio strategico delle reti e dei flussi che lo alimentano, dunque si arriva all'uso bellico di ogni cosa: l'energia, i gasdotti, le migrazioni, le catene di approvvigionamento e le sanzioni finanziarie sono diventate oggi armi a tutti gli effetti.

Ulteriore elemento strategico è la manipolazione algoritmica dei social media e le campagne di disinformazione, che mirano a destabilizzare il tessuto sociale del nemico dall'interno, colpendo la percezione della realtà prima ancora dei corpi. Il *cyberspazio*²⁶ è diventato il quinto dominio della guerra (dopo terra, mare, aria e spazio). Una stringa di codice può oggi causare danni paragonabili a un bombardamento aereo, paralizzando infrastrutture critiche come centrali elettriche o sistemi bancari senza che un solo soldato attraversi il confine.

Nel contesto contemporaneo, l'informazione non è più solo un supporto alle operazioni militari, ma è diventata essa stessa un'arma. La cosiddetta Information Warfare (guerra dell'informazione) mira a manipolare la percezione della realtà della popolazione avversaria attraverso l'uso massiccio di fake news, propaganda digitale e operazioni psicologiche (PsyOps²⁷). Parallelamente, la dimensione cyber permette di colpire le infrastrutture critiche di uno Stato, come le reti elettriche, i sistemi bancari, gli ospedali, senza sparare un solo colpo²⁸. Questa forma di ostilità è caratterizzata da un alto grado di “negabilità”: è estremamente complesso attribuire con certezza un attacco cyber a un governo specifico, permettendo agli aggressori di agire nell'ombra²⁹. La superiorità tecnologica non si misura più solo nella gittata

²⁶ Il cyberspazio è lo spazio virtuale globale creato dalle reti informatiche (come Internet) dove avvengono scambi di informazioni, interazioni e transazioni, un dominio immateriale ma con profonde implicazioni nel mondo reale, che unisce hardware, software, dati e utenti. Coniato da William Gibson, oggi indica comunemente l'ambiente digitale interconnesso e viene considerato un dominio strategico, simile agli ambiti militare o fisico, che richiede sicurezza e competenze specifiche.

²⁷ Le PsyOps (Psychological Operations), o operazioni psicologiche, sono attività militari che usano la propaganda e altre tecniche di comunicazione per influenzare le percezioni, le emozioni e i comportamenti di pubblici specifici (nemici, neutrali o amici) a favore degli obiettivi politici e militari di un governo, tramite media, social media, volantini, e comunicazioni faccia a faccia. L'obiettivo è alterare il “valore” o “credenze” del pubblico per ottenere reazioni pianificate, che vanno dal sostegno alla resa, e possono essere tattiche (tra unità militari) o strategiche (a livello governativo).

²⁸ L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano 2017, pp. 210-225.

²⁹ P.W. Singer, A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, Oxford 2014, pp. 67-82.

dei missili, ma nella capacità di proteggere i propri dati e di corrompere quelli del nemico, trasformando ogni dispositivo connesso in un potenziale varco per l'offensiva.

Altro fattore non meno rilevante è l'avvento dell'intelligenza artificiale e l'automazione: L'introduzione di droni autonomi e sistemi d'arma letali guidati dall'IA (LAWS³⁰) sta deumanizzando l'atto bellico, riducendo i tempi di reazione e aumentando l'imprevedibilità dell'escalation.

Ma la caratteristica più inquietante della contemporaneità è la permeabilità dei confini tra pace e guerra. La dinamica più insidiosa dei conflitti contemporanei è la progressiva scomparsa di una linea di demarcazione netta tra lo stato di pace e lo stato di guerra. Ci troviamo in quella che gli esperti definiscono *zona grigia* (Gray Zone), uno spazio concettuale in cui attori statali e non statali competono ferocemente utilizzando tutti i mezzi disponibili, ma mantenendosi deliberatamente al di sotto della soglia che giustificerebbe una risposta militare convenzionale o l'attivazione di trattati di difesa collettiva, come l'Articolo 5 della NATO³¹.

In questa dimensione, le sanzioni economiche, il ricatto energetico, l'uso strumentale delle migrazioni e l'interferenza nei processi elettorali diventano atti di guerra non dichiarati. La pace non è più l'assenza di conflitto, ma una competizione permanente condotta con mezzi non cinetici. Questa guerra senza limiti (come teorizzato dai colonnelli cinesi Qiao Liang³² e Wang Xiangsui³³) trasforma la quotidianità in un campo di battaglia potenziale³⁴. La sfida per la sicurezza contemporanea non è dunque vincere una battaglia finale, ma gestire una condizione di crisi perpetua e multidimensionale, in cui l'avversario è costantemente all'opera per indebolire le basi della convivenza civile e democratica. Siamo immersi in una condizione di conflitto latente e onnipresente con i flussi economici paragonabili a campi di battaglia, le

³⁰ Conosciuti come Killer Robots o LAWS (lethal autonomous weapon system), sono tutte quelle armi in grado di selezionare ed attaccare un obiettivo senza alcun tipo di supporto umano.

³¹ L'Articolo 5 del Trattato NATO stabilisce il principio della difesa collettiva: un attacco armato contro uno Stato membro è considerato un attacco contro tutti, obbligando gli altri a fornire assistenza, compreso l'uso della forza armata, se necessario, per ristabilire la sicurezza. È la base della sicurezza collettiva dell'Alleanza, invocato una sola volta dopo gli attacchi dell'11 settembre 2001 agli Stati Uniti, e prevede che ogni azione sia portata all'attenzione del Consiglio di Sicurezza delle Nazioni Unite.

³² Qiao Liang (1955) è un generale maggiore in pensione dell'Aeronautica dell'Esercito Popolare di Liberazione cinese, teorico militare e autore, famoso per il libro co-scritto "Guerra senza limiti" (1999), che anticipò tattiche di guerra non convenzionali.

³³ Wang Xiangsui (1954) è un professore all'Università Beihang di Pechino e colonnello in pensione dell'Esercito popolare di liberazione. È co-autore di *Unrestricted Warfare*, un libro che impone che nessun paese è in grado di sconfiggere una superpotenza, come gli Stati Uniti, alle sue condizioni. Il libro delinea passi che potrebbero indebolire tali superpoteri, attraverso mezzi non convenzionali, tra cui la manipolazione dei sistemi bancari, il controllo dei media e delle risorse naturali.

³⁴ Q. Liang, W. Xiangsui, *Guerra senza limiti*, Libreria Editrice Goriziana, Gorizia 2001, pp. 45-60.

guerre commerciali non sono più dispute doganali, ma tentativi di strangolamento tecnologico e finanziario volti ad eliminare la competitività sistemica dell'avversario.

Ed ironia della sorte, la stessa globalizzazione che avrebbe dovuto prevenire i conflitti rendendoci interdipendenti è diventata il veicolo della vulnerabilità, un blocco nel Canale di Suez o una crisi informatica in un data center californiano riflettono istantaneamente su scala planetaria.

La globalizzazione ha profondamente alterato la grammatica del conflitto, portando a quella che molti analisti definiscono la *de-territorializzazione* della guerra³⁵. Nella tradizione classica, la geografia era il fattore determinante: conquistare territori, porti e città significava vincere. Oggi, l'interdipendenza economica e la velocità dei trasporti hanno reso le frontiere nazionali estremamente filtranti³⁶.

Il conflitto contemporaneo non si limita ad un'area geografica circoscritta, ma tende a espandersi tramite reti finanziarie e flussi migratori utilizzati come strumenti di pressione. Gli Stati non cercano più solo l'occupazione del suolo nemico ma mirano a destabilizzare i nodi vitali delle reti avversarie. In questo senso, la guerra diventa *reticolare*: un attacco può essere sferrato da un continente all'altro con un clic, allo stesso modo le conseguenze di un conflitto locale possono riflettersi istantaneamente sui mercati globali. La distinzione tra “interno” ed “esterno”, sfuma in un unico teatro operativo globale dove la minaccia può emergere tanto da un esercito straniero quanto da una cellula all'interno dei propri confini.

In questo scenario, la guerra non è più un evento eccezionale che interrompe la normalità, ma una funzione costante dell'interazione umana. L'impossibilità di identificare chiaramente l'inizio e la fine di un conflitto rende le democrazie liberali particolarmente fragili, poiché esse faticano a rispondere a minacce che non si palesano con uniformi e carri armati, ma con byte, investimenti speculativi e narrazioni distorte; siamo passati dalla guerra come “prosecuzione della politica con altri mezzi” (Clausewitz) alla politica come prosecuzione di una guerra invisibile e totale³⁷.

³⁵ Z. Bauman, *Dentro la globalizzazione. Le conseguenze sulle persone*, Laterza, Roma-Bari 2001, pp. 75-90.

³⁶ M. Kaldor, *Le nuove guerre. Violenza organizzata nell'età globale*, Carocci, Roma 1999, p. 108.

³⁷ C. Jean, *Geopolitica*, Laterza, Roma-Bari 1995 (ed. aggiornata 2012), pp. 201-215.

CAPITOLO SECONDO

LA GUERRA IBRIDA: NASCITA E DEFINIZIONE DEL CONCETTO

Dopo aver esaminato nel primo Capitolo la crisi del paradigma classico e l'emergere di nuove forme di conflittualità, il seguente Capitolo si propone di analizzare in modo sistematico la categoria della *guerra ibrida*. Sebbene il termine sia entrato prepotentemente nel lessico giornalistico e politico solo in tempi recenti, in particolare dopo l'annessione russa della Crimea nel 2014, la sua origine dottrinale è più profonda e risponde alla necessità di inquadrare fenomeni bellici che non rientrano più nelle definizioni tradizionali di simmetria o asimmetria.

La guerra ibrida non è semplicemente un'inedita tipologia di guerra, ma piuttosto una modalità d'azione che fonde in un unico schema operativo strumenti cinetici e non cinetici, attori militari e civili, azioni palesi e occulte. Il problema centrale che affronteremo nei seguenti paragrafi riguarda l'ambiguità definitoria: il concetto di "ibrido" è stato spesso criticato per la sua eccessiva genericità, rischiando di diventare una forma di "etichetta-ombrello" sotto la quale ricondurre qualsiasi forma di pressione politica o cyber.

Il percorso di questo capitolo si articolerà in tre passaggi chiave. In primo luogo, nel paragrafo 2.1 dal titolo "Origini del termine e sviluppo nella letteratura", indagheremo appunto l'origine del termine³⁸, rintracciando i primi studi accademici e militari, con un focus particolare sul contributo di Frank Hoffman, considerato il padre accademico del concetto. Successivamente, nel paragrafo 2.2 intitolato "Definizione di guerra ibrida e principali interpretazioni teoriche", analizzeremo le diverse interpretazioni teoriche fornite dalle principali organizzazioni internazionali, come la NATO³⁹ e l'Unione Europea⁴⁰, evidenziando

³⁸ J. J. McCuen, *Hybrid Wars*, in «Military Review», Vol. 88, n. 2, 2008, pp. 107-113.

³⁹ La NATO (North Atlantic Treaty Organization) è un'alleanza politico-militare creata nel 1949 per garantire la difesa collettiva e la sicurezza dei Paesi membri (Europa e Nord America) attraverso strumenti politici e militari, basata sul principio che un attacco a un membro è un attacco a tutti (Articolo 5). Nata come contrappeso all'URSS durante la Guerra Fredda, oggi si occupa di sicurezza, cooperazione e gestione delle crisi, con 32 Stati membri.

⁴⁰ L'UE è un partenariato economico e politico, unico nel suo genere, tra 27 paesi europei. È stata creata nel 1958 come Comunità economica europea da Belgio, Germania, Francia, Italia, Lussemburgo e Paesi Bassi. Da allora, altri 22 paesi si sono uniti per costituire quella che, dal 1993, è nota come Unione europea.

come la percezione del rischio cambi a seconda degli attori coinvolti⁴¹. Infine, nel paragrafo 2.3 denominato “Elementi costitutivi della guerra ibrida”, verranno isolati gli elementi costitutivi della minaccia ibrida, dalla disinformazione al sabotaggio economico, per mappare l’arsenale di strumenti che rendono questo modello di conflitto così insidioso per le moderne democrazie⁴².

L’obiettivo di questa sezione è dunque fornire una base concettuale che permetta di distinguere la guerra ibrida dalle forme di competizione geopolitica ordinaria, definendo i confini di un fenomeno che fa della mancanza di confini la sua arma principale.

2.1 ORIGINE DEL TERMINE E SVILUPPO NELLA LETTERATURA

Il concetto di *guerra ibrida* rappresenta una delle evoluzioni dottrinali più significative degli ultimi vent'anni, ma la sua origine è oggetto di un profondo dibattito tra gli studiosi di studi strategici. Sebbene l'idea di combinare metodi diversi in guerra sia antica quanto il conflitto stesso, la formalizzazione del termine avviene in un contesto storico ben preciso: la crisi delle operazioni militari statunitensi in Iraq e Afghanistan nei primi anni Duemila. È in questo scenario di instabilità che emerge la figura di Frank G. Hoffman⁴³, ricercatore presso il Marine Corps Combat Development Command, il cui lavoro ha segnato il passaggio dalla teoria della *guerriglia* a quella della *conflittualità ibrida*.

Nel suo saggio seminale del 2007, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Hoffman teorizza che le future minacce non saranno più semplicemente classificabili in convenzionali o irregolari. Egli definisce la guerra ibrida come quella che fonde «la letalità degli scontri statali con il fervore fanatico delle forme irregolari di conflitto».

A differenza di molti suoi predecessori, Hoffman non vede la guerra ibrida come una semplice asimmetria, ma come l'integrazione di diversi canali, linguaggi o strumenti che operano simultaneamente per raggiungere un unico obiettivo⁴⁴. Per Hoffman, l'avversario ibrido è in grado di utilizzare contemporaneamente in un unico teatro operativo:

⁴¹ B. Renz, *Russia and 'hybrid warfare'*, in «Contemporary Politics», Vol. 22, n. 3, 2016, pp. 283-300.

⁴² [https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/603918/EPRS_ATA\(2017\)603918_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/603918/EPRS_ATA(2017)603918_EN.pdf)

⁴³ Dr. Frank G. Hoffman, esperto di difesa e ufficiale dei Marines in pensione, ha operato per 43 anni nel settore della difesa, analista e sviluppatore di concetti è un autorevole autore di libri e articoli su strategia e innovazione militare.

⁴⁴ F. G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington 2007, pp. 14-36.

- Forze convenzionali fornite di armamenti moderni;
- Tattiche e formazioni irregolari (guerriglia);
- Atti di terrorismo mirati;
- Disordine criminale per finanziare o coprire le operazioni.

Il caso di studio citato da Hoffman per eccellenza è il conflitto del 2006 tra Israele e Hezbollah⁴⁵. In quell'occasione, un attore non statale riuscì a operare come un esercito regolare, usando missili antinave e comunicazioni criptate, mantenendo però la struttura cellulare e l'invisibilità di una milizia irregolare.

Per comprendere la profondità della letteratura sul tema, è necessario paragonare Hoffman a William S. Lind⁴⁶, il quale, già alla fine degli anni '80, aveva introdotto il concetto di Fourth Generation Warfare (4GW), che rappresenta uno dei pilastri della teoria militare contemporanea per spiegare il superamento del conflitto classico tra Stati⁴⁷. Il termine nasce nel 1989 grazie a un gruppo di analisti americani, tra cui spicca la figura di William S. Lind. L'idea alla base era che la storia militare avesse attraversato quattro fasi distinte:

- Prima fase: Guerre basate sulla massa e sull'ordine (es. l'era napoleonica, linee di fanteria).
- Seconda fase: Guerre di attrito e potenza di fuoco (es. Prima Guerra Mondiale).
- Terza fase: Guerre di manovra e velocità (es. la Blitzkrieg tedesca⁴⁸).
- Quarta fase: Il ritorno a forme di conflitto decentrate dove lo Stato perde il monopolio della forza.

Dunque mentre Hoffman si concentra sulla modalità del combattimento, ovvero il mix di armi e tattiche, Lind si concentra sulla perdita del monopolio statale.

⁴⁵ F. G. Hoffman, Hybrid Warfare and Challenges, in «Joint Force Quarterly», n. 52, 2009, pp. 34-39.

⁴⁶ William S. Lind, (1947) è un autore, teorico militare e commentatore conservatore americano, noto per essere uno dei principali ideatori della teoria della Guerra di Quarta Generazione (4GW), che descrive conflitti non statali e le loro implicazioni, ed è un'importante figura nel conservatorismo americano, spesso critico verso il neoconservatorismo. Ha lavorato come assistente per affari militari per il senatore Gary Hart e scrive e tiene conferenze a livello internazionale su dottrina e teoria militare.

⁴⁷ W. S. Lind et al., The Changing Face of War: Into the Fourth Generation, in «Marine Corps Gazette», Ottobre 1989, pp. 22-26.

⁴⁸ La guerra lampo tedesca (in tedesco Blitzkrieg) fu una tattica militare della Germania nazista nella Seconda Guerra Mondiale, basata su attacchi rapidi e coordinati di carri armati (Panzer), fanteria meccanizzata e aviazione (Luftwaffe) per sfondare le linee nemiche, circondare e annientare le forze avversarie, evitando lunghe guerre di posizione. Fu applicata con successo nelle invasioni di Polonia (1939) e Francia (1940), sfruttando la mobilità e la sorpresa per ottenere vittorie fulminee e schiacciare le resistenze prima che potessero organizzarsi.

La Guerra di quarta generazione non è una semplice evoluzione tecnologica, ma un cambiamento di paradigma politico e sociale, di fatto vi è una scomparsa del fronte, non esiste più, infatti, una distinzione netta tra *fronte* e *retrovie*. Il campo di battaglia è ovunque ed i protagonisti non sono più solo eserciti regolari, ma gruppi terroristici, milizie, cartelli criminali o movimenti religiosi (es. Al-Qaeda, ISIS). Inoltre il nemico si nasconde tra la popolazione e i civili diventano sia bersagli che strumenti di propaganda. E l'obiettivo, a differenza del passato, non è distruggere l'esercito nemico, ma colpire la psiche, la cultura e la coesione sociale dell'avversario per costringerlo alla resa politica.

Secondo Lind, la guerra di quarta generazione è caratterizzata dal ritorno a un mondo pre-vestfaliano in cui entità non statali, combattono contro gli Stati. Dunque vi è una differenza sostanziale tra i concetti di “4GW” e guerra ibrida, sebbene spesso confusi, i due termini hanno sfumature diverse, la 4GW si concentra sulla perdita di potere dello Stato e sul ritorno a conflitti asimmetrici e tribali, mentre la guerra descrive invece come uno Stato utilizzi simultaneamente mezzi convenzionali (carri armati) e non convenzionali (cyber, fake news, economia) per destabilizzare un avversario.

Il paragone tra i due autori rivela una sfumatura fondamentale: per Lind la sfida è politica e identitaria; per Hoffman la sfida è operativa e tecnologica. Hoffman critica parzialmente la 4GW, ritenendola troppo astratta, e propone un modello dove lo Stato rimane un attore centrale, ma impara a *combattere nell'ombra* o a utilizzare *proxy* per i propri scopi.

Un altro pilastro della letteratura contemporanea è il dibattito sulla cosiddetta “dottrina Gerasimov” che si riferisce alla strategia di guerra ibrida russa, teorizzata dal generale capo di stato maggiore russo Valerij Gerasimov⁴⁹, essa integra strumenti militari convenzionali, detti *hard power* con quelli non militari, *soft power*, come attacchi cibernetici, disinformazione, pressioni economiche e operazioni sotto copertura, per alterare la percezione e il processo decisionale dell'avversario e raggiungere obiettivi strategici senza necessariamente ricorrere solo alla forza bruta, creando un conflitto globale e su più livelli. Nel 2013, Gerasimov pubblicò un articolo in cui osservava come le regole della guerra fossero cambiate, il ruolo dei mezzi non

⁴⁹ Valerij Vasil'evič Gerasimov, (1955) è un generale russo, Capo di Stato Maggiore, Generale delle Forze Armate Russe e Vice Ministro della Difesa, nominato nel 2012 da Vladimir Putin, noto per essere considerato l'autore della cosiddetta "dottrina Gerasimov", una strategia militare che integra guerra convenzionale, tecnologica, informativa, diplomatica ed economica per raggiungere obiettivi strategici, sebbene l'interpretazione di questa dottrina sia stata oggetto di dibattito.

militari per raggiungere obiettivi strategici aveva ormai superato, in certi casi, la forza delle armi⁵⁰.

Sebbene molti studiosi occidentali abbiano etichettato questo scritto come il *manifesto russo della guerra ibrida*, autori come Mark Galeotti⁵¹ hanno invitato alla cautela. Galeotti sostiene che Gerasimov non stesse proponendo una nuova dottrina d'attacco⁵², ma stesse descrivendo ciò che la Russia percepiva come una minaccia occidentale, le cosiddette *rivoluzioni colorate*⁵³. Il confronto tra Hoffman e la scuola russa evidenzia una divergenza interpretativa, ovvero se per gli americani l'ibridismo è una complicazione tattica del campo di battaglia, per i russi è una visione strategica totale che abbraccia economia, cultura e informazione come armi permanenti.

Infine, lo sviluppo della letteratura ha visto contributi come quello di John J. McCuen, il quale sottolinea che la guerra ibrida è una lotta per il controllo delle popolazioni in spettri multipli, il piano fisico, quello politico e quello informativo. Egli suggerisce che per vincere una guerra ibrida non basti la superiorità militare, ma sia necessaria appunto una *ibridizzazione* della risposta, integrando sforzi diplomatici e civili⁵⁴. Al contrario, studiosi come Williamson Murray⁵⁵ sono più scettici, avvertendo che il termine “ibrido” rischia di essere una moda passeggera che nasconde realtà antiche: la storia è piena di eserciti che usavano strategie e tecniche *irregolari*⁵⁶. Tuttavia, il consenso accademico odierno riconosce ad Hoffman il merito

⁵⁰ V. Gerasimov, *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations*, trad. it. in «Military Review», Gennaio-Febbraio 2016.

⁵¹ Mark Galeotti (1965) è uno storico, politologo e analista britannico di fama mondiale, specializzato in Russia, sicurezza internazionale e criminalità transnazionale, autore di numerosi libri e consulente per governi ed enti, noto per i suoi studi approfonditi sulla Russia post-sovietica e il potere russo, dirige la società di consulenza Mayak Intelligence e insegna presso il University College London (UCL). Da oltre 30 anni studia la Russia e la sua evoluzione, coprendo politica, sicurezza, criminalità organizzata e spionaggio, Fornisce analisi e consulenza a governi, agenzie di sicurezza e forze dell'ordine in Europa e Nord America. È considerato una delle massime autorità nel campo degli affari russi e della criminalità transnazionale, il suo lavoro spazia dalla storia russa agli aspetti più attuali della geopolitica, come il conflitto in Ucraina e la figura di Putin. È stato bandito dalla Russia nel 2022.

⁵² M. Galeotti, *The 'Gerasimov Doctrine' and Russian Non-Linear War*, in «In Moscow's Shadows», 2014.

⁵³ *Rivoluzioni colorate* è l'appellativo attribuito dai media internazionali e dai soggetti coinvolti a una serie di movimenti simili e correlati tra di loro che si sono sviluppati principalmente in alcuni Stati post-sovietici negli anni 2000.

⁵⁴ J. J. McCuen, *Hybrid Wars*, in «Military Review», Vol. 88, n. 2, 2008, pp. 107-113.

⁵⁵ Williamson Murray (1941-2023) è stato un eminente storico militare e analista di strategia statunitense, professore emerito alla Ohio State University, noto per le sue approfondite analisi delle guerre mondiali e della storia militare, autore di opere fondamentali come *A War to Be Won*, che esamina la Seconda Guerra Mondiale, e consulente per diverse istituzioni di difesa, Le sue ricerche hanno influenzato il pensiero strategico e la comprensione dei conflitti moderni, con un approccio che andava oltre le singole battaglie per comprendere le dinamiche più ampie della guerra.

⁵⁶ W. Murray, P. R. Mansoor (a cura di), *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, New York 2012, pp. 1-15.

di aver compreso che la velocità della tecnologia moderna ha reso questa combinazione non più un'eccezione, ma la norma del XXI secolo.

2.2 DEFINIZIONE DI GUERRA IBRIDA E PRINCIPALI INTERPRETAZIONI TEORICHE

Il passaggio del concetto di guerra ibrida dalle scrivanie dei teorici come Frank Hoffman ai centri di comando strategico della NATO e dell'Unione Europea ha segnato l'istituzionalizzazione di una nuova categoria di minaccia. Non si è trattato di un semplice esercizio accademico, ma di una risposta urgente a eventi geopolitici che avevano dimostrato l'inadeguatezza delle definizioni esistenti. In questo paragrafo analizzeremo come le istituzioni internazionali abbiano recepito e rielaborato il concetto, evidenziando le applicazioni pratiche che hanno trasformato la teoria in una vera e propria politica di difesa attiva.

Per l'Organizzazione del Trattato dell'Atlantico del Nord (NATO)⁵⁷, la guerra ibrida rappresenta una sfida diretta all'Articolo 5⁵⁸, il principio della difesa collettiva. L'insidia principale risiede nell'ambiguità della minaccia: se un attacco non è chiaramente identificabile come *aggressione armata* secondo il diritto internazionale, come può rispondere l'alleanza?

La NATO definisce le minacce ibride come una combinazione di attività militari e non militari, palesi e occulte, che possono includere disinformazione, attacchi cyber, pressione economica e l'impiego di forze irregolari⁵⁹. L'applicazione pratica più eclatante di questa definizione si è avuta nel 2014 con l'annessione della Crimea da parte della Federazione Russa. In quell'occasione, la comparsa dei cosiddetti "omini verdi" (*little green men*)⁶⁰, ovvero soldati professionisti senza insegne nazionali, ha creato un vuoto informativo che ha paralizzato la risposta internazionale nelle prime ore cruciali⁶¹. La NATO ha dovuto quindi sviluppare una strategia costruita attorno al concetto per la *Deterrenza e la Difesa dell'Area Euro-Atlantica* (DDA), che rappresenta il pilastro fondamentale della NATO, focalizzato sul contrasto a

⁵⁷ La NATO (North Atlantic Treaty Organization) è un'alleanza politico-militare creata nel 1949 per garantire la difesa collettiva e la sicurezza dei Paesi membri (Europa e Nord America) attraverso strumenti politici e militari, basata sul principio che un attacco a un membro è un attacco a tutti (Articolo 5). Nata come contrappeso all'URSS durante la Guerra Fredda, oggi si occupa di sicurezza, cooperazione e gestione delle crisi, con 32 Stati membri.

⁵⁸ L'Articolo 5 del Trattato NATO (1949) è il pilastro della difesa collettiva: un attacco armato contro un membro è considerato un attacco contro tutti. Impegna gli alleati a intervenire, incluso l'uso della forza, per ripristinare la sicurezza. Attivato una sola volta (11 settembre 2001). Copre attacchi in Europa o Nord America, ogni paese decide individualmente l'azione necessaria, che può includere la forza armata. Non è automatico e le misure prese devono essere comunicate al Consiglio di Sicurezza ONU e terminano quando questo interviene.

⁵⁹ NATO, Countering Hybrid Threats, in «NATO Topics», aggiornato al 2021 (disponibile su www.nato.int).

⁶⁰ A. Radin, Hybrid Warfare in the Baltics: Threats and Potential Responses, RAND Corporation, Santa Monica 2017, pp. 5-22.

⁶¹ M. Galeotti, The 'Gerasimov Doctrine' and Russian Non-Linear War, in «In Moscow's Shadows», 2014, pp. 1-12.

minacce ibride, convenzionali e cibernetiche, con la Russia considerata la minaccia principale, basata sugli Articoli 5 e 6, mira a proteggere i membri tramite una postura multi-dominio, garantendo prontezza operativa e coordinamento politico. La NATO ha, dunque, riaffermato il suo ruolo centrale nella difesa collettiva, investendo in dissuasione e difesa da minacce ibride, inclusi attacchi cibernetici e spaziali, che potrebbero far scattare l'Articolo 5.

La difesa non è più solo terrestre, aerea o navale, ma integra cyber, spazio e minacce ibride. Il DDA costituisce, quindi, una delle basi della sicurezza europea, lavorando per prevenire conflitti attraverso la gestione delle crisi e il rafforzamento delle capacità militari dei paesi membri, costituendo reparti specializzati come il Counter-Hybrid Support Teams (CHST)⁶², che analizzano l'aggressione ibrida in atto, incontrano istituzioni, militari e ONG per valutare le vulnerabilità e forniscono raccomandazioni concrete per la difesa, agiscono contro avversari atipici che utilizzano strumenti non convenzionali (come attacchi alle infrastrutture critiche o campagne di disinformazione) per destabilizzare un paese senza dichiarare una guerra aperta. Sono strumenti d'emergenza, come dimostrato dal loro invio in Montenegro (2019) e Lituania (2021) per fronteggiare forti pressioni esterne.

Dunque, in sintesi, i CHST rappresentano la risposta attiva e coordinata della NATO contro il *dominio fluido* dei conflitti moderni, con l'obiettivo di fortificare la capacità di reazione dei paesi membri contro minacce che colpiscono sia la sfera pubblica che quella privata.

Mentre la NATO si concentra sulla dimensione militare e di deterrenza, l'Unione Europea ha invece adottato un'interpretazione della guerra ibrida più orientata alla sicurezza interna e alla protezione del tessuto sociale. Dal punto di vista dell'UE, la pericolosità della minaccia ibrida risiede nella sua capacità di sfruttare le vulnerabilità alla base delle società aperte e democratiche.

Nel Joint Framework on countering hybrid threats⁶³ del 2016, l'Europa identifica come strumenti ibridi non solo le armi, ma anche le sanzioni commerciali, il ricatto energetico e

⁶² I Counter-Hybrid Support Teams (CHST) della NATO sono squadre specializzate di esperti, attivate su richiesta, per assistere le nazioni alleate nel rafforzare la resilienza e difendersi da minacce ibride. Combinano competenze civili e militari per analizzare e contrastare attacchi complessi che uniscono cyberwarfare, disinformazione e pressioni economiche.

⁶³ Il Joint Framework on countering hybrid threats è una strategia dell'Unione Europea (lanciata nel 2016) mirata a rafforzare la resilienza e contrastare le minacce ibride, ovvero la combinazione di azioni militari e non militari (cibernetiche, economiche, disinformazione, sabotaggi) utilizzate in modo coordinato da attori statali e non statali. Promuove la cooperazione tra Stati membri e istituzioni UE, migliorando la consapevolezza e la risposta.

l'interferenza nei processi elettorali⁶⁴. Un'applicazione pratica di questa interpretazione è stata osservata durante le campagne di disinformazione volte a influenzare il sentimento pubblico europeo o ad esasperare le divisioni sociali (si pensi ai casi di interferenza digitale denunciati in occasione di referendum o elezioni nazionali).

L'UE ha risposto non con i carri armati, ma con la creazione dello European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)⁶⁵, un'organizzazione internazionale indipendente con sede a Helsinki, inaugurata nel 2017. Funge da hub di competenza per rafforzare la sicurezza di 36 Stati partecipanti, dell'UE e della NATO, supportandoli nel contrastare le minacce ibride attraverso ricerca, formazione ed esercitazioni. L'obiettivo è potenziare la sicurezza dei paesi partecipanti, dell'Unione Europea e della NATO, migliorando la resilienza, la preparazione e le capacità civili-militari. Si basa su una rete di esperti e opera attraverso tre Communities of Interest (COI)⁶⁶, funzioni di ricerca, analisi, formazione ed esercitazioni, e fornisce competenze e networking per affrontare minacce ibride, che combinano mezzi militari e non militari (soft power, cyber, ecc.), sottolineando che in un contesto ibrido, la difesa passa attraverso la resilienza delle infrastrutture critiche e la *media literacy*⁶⁷ dei cittadini.

Oltre alle istituzioni, la letteratura ha approfondito la dimensione della *zona grigia*, interpretandola come lo spazio operativo in cui la guerra ibrida trova la sua massima espressione. Studiosi come Antulio Echevarria hanno sottolineato che le campagne ibride sono progettate per ottenere vantaggi strategici gradualmente, evitando di superare la soglia del conflitto aperto che provocherebbe una ritorsione militare⁶⁸.

Questa interpretazione teorica trova riscontro pratico nelle attività nel Mar Cinese Meridionale. Qui, l'uso di milizie marittime composte da pescherecci civili scortati dalla guardia costiera permette di rivendicare sovranità territoriale senza ingaggiare direttamente le

⁶⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018>

⁶⁵ <https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model-public-version/>

⁶⁶ Una "Community of Interest" (COI) è un gruppo di persone che condividono interessi, obiettivi, passioni o caratteristiche comuni (sociali, economiche, professionali) e si uniscono per scambiare idee, informazioni e supportarsi a vicenda. A differenza delle comunità basate sulla geografia, le COI si formano attorno a temi specifici, spesso online, non richiedendo la vicinanza fisica.

⁶⁷ La *media literacy* (alfabetizzazione mediatica) è la capacità dei cittadini di accedere, analizzare, valutare criticamente e creare contenuti mediatici, inclusi i media digitali e le notizie, per agire in modo consapevole, sicuro ed etico. Fondamentale per la cittadinanza attiva e per contrastare la disinformazione, questa competenza promuove resilienza democratica e inclusione sociale.

⁶⁸ A. J. Echevarria II, *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy*, Strategic Studies Institute, U.S. Army War College, Carlisle 2016, pp. 10-35.

marine militari avversarie⁶⁹. È la cosiddetta *tattica del salame* (salami slicing): una serie di piccoli passi, ognuno dei quali troppo insignificante per scatenare una guerra, ma che nel complesso sono in grado di alterare radicalmente lo status quo geopolitico e consentire di ottenere vantaggi senza provocare reazioni significative o un'opposizione unita, “affettando” (da qui il nome della strategia) il controllo o le concessioni nel tempo. Il termine è stato utilizzato per la prima volta dal politico ungherese Mátyás Rákosi⁷⁰ per descrivere come ha eliminato l'opposizione, fetta dopo fetta. In geopolitica, questa tattica è stata usata per espandere influenze territoriali, come nel caso delle dispute nel Mar Cinese Meridionale o delle manovre russe.

In ultima analisi, le diverse interpretazioni convergono su un punto: la guerra ibrida è una forma di conflitto non lineare. Se nella guerra classica la vittoria è misurata dalla distruzione delle forze nemiche, nelle interpretazioni moderne del conflitto ibrido il successo è misurato dal collasso interno dell'avversario.

Questo ha portato alla nascita di teorie sulla *Guerra cognitiva*, dove l'obiettivo finale è il cervello umano⁷¹, è una strategia non convenzionale che utilizza strumenti tecnologici per alterare i processi mentali, sfruttare i bias cognitivi⁷² e influenzare le decisioni di individui e intere popolazioni.

A differenza della propaganda tradizionale, non mira solo a trasmettere un messaggio, ma a trasformare il cervello umano nel vero campo di battaglia, degradando la razionalità e la capacità critica dell'avversario. L'obiettivo è indebolire una nazione colpendone il morale, la coesione sociale e la fiducia nelle istituzioni, arrivando a vincere il nemico senza combatterlo

⁶⁹ R. D. Kaplan, *Asia's Cauldron: The South China Sea and the End of a Stable Pacific*, Random House, New York 2014, pp. 120-145.

⁷⁰ Mátyás Rákosi (1892–1971) è stato un politico comunista ungherese, leader de facto della Repubblica Popolare d'Ungheria dal 1945 al 1956. Conosciuto come il "miglior discepolo di Stalin", instaurò un regime stalinista repressivo, caratterizzato da un forte culto della personalità e dal terrore della polizia segreta.

⁷¹ G. Gagliano, *Guerra cognitiva. Dalla guerra dell'informazione alle psicotecnologie*, Fuoco Edizioni, Roma 2020, pp. 45-68.

⁷² I bias cognitivi sono distorsioni sistematiche, pregiudizi o errori di valutazione che la mente utilizza come scorciatoie mentali (euristiche) per elaborare informazioni e prendere decisioni rapide. Derivano da percezioni errate e influenzano comportamenti, giudizi e acquisti, portando a una visione soggettiva non aderente alla realtà.

direttamente. Si basa sull'integrazione di cyberwarfare⁷³, guerra psicologica, social engineering⁷⁴ e neuroscienze.

La NATO ha formalizzato la dimensione cognitiva come il sesto dominio delle operazioni (dopo terra, mare, aria, spazio e cyber), considerandolo essenziale per la superiorità strategica.

L'uso dell'Intelligenza Artificiale e dei social network rende inoltre queste operazioni estremamente economiche, scalabili e difficili da rilevare in tempo reale. L'applicazione pratica consiste nell'uso degli algoritmi dei social media per dividere, polarizzandola, l'opinione pubblica, trasformando i cittadini di uno Stato in strumenti inconsapevoli della strategia nemica. In questo senso, la definizione di guerra ibrida si espande arrivando a coprire ogni ambito della socialità: non esiste più una retrovia sicura, poiché ogni individuo connesso alla rete è un potenziale obiettivo e, al tempo stesso, un potenziale vettore di attacco.

2.3 ELEMENTI COSTITUTIVI DELLA GUERRA IBRIDA

La complessità della guerra ibrida risiede nella sua natura sinergica: essa non si affida a un singolo strumento, ma coordina una pluralità di mezzi per colpire le vulnerabilità del bersaglio su più fronti contemporaneamente. Come evidenziato dalla dottrina NATO e dagli studi di Hoffman, analizzati finora, l'efficacia di una campagna ibrida dipende dalla capacità di sincronizzare attacchi cyber, pressioni economiche e operazioni cinetiche sotto un'unica regia strategica⁷⁵. Di seguito analizziamo nel dettaglio i principali elementi costitutivi.

- La dimensione Cyber: dal sabotaggio allo spionaggio infrastrutturale

Lo spazio cibernetico è il catalizzatore della guerra ibrida. Contrariamente a quanto avviene in una guerra tradizionale, l'offensiva cyber permette di colpire il cuore dello Stato nemico senza violarne fisicamente i confini.

⁷³ La cyberwarfare (guerra cibernetica) è un conflitto tra stati che utilizza attacchi informatici per danneggiare o interrompere le infrastrutture critiche (come banche, energia, trasporti) e i sistemi informativi di un avversario, mirando a destabilizzarlo economicamente, socialmente o militarmente, senza l'uso di forze fisiche dirette. Si tratta di operazioni di spionaggio, sabotaggio e disinformazione condotte nel cyberspazio, utilizzando malware (come Stuxnet), attacchi DDoS o ransomware, e rappresenta una componente strategica dei conflitti moderni.

⁷⁴ Il Social Engineering, tradotto in italiano come "ingegneria sociale", è una forma di manipolazione psicologica che coinvolge l'uso manipolativo delle abilità comunicative e psicologiche per ottenere informazioni, accesso o azioni da parte di altre persone.

⁷⁵ M. Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, New York 2007, pp. 88-105.

Un esempio storico essenziale è l'attacco subito dall'Estonia nel 2007⁷⁶. In seguito alla rimozione di un monumento sovietico a Tallinn il paese fu bersaglio di una massiccia ondata di attacchi DDoS (Distributed Denial of Service) che interruppero il servizio di banche, testate giornalistiche e siti governativi. Un attacco DDoS è una minaccia informatica che punta a rendere inaccessibili siti web o risorse di rete, inondandoli di traffico dannoso proveniente da molteplici fonti, spesso *botnet*. Causa rallentamenti o blocchi totali dei servizi provocando downtime⁷⁷ e danni reputazionali. Gli attaccanti utilizzano, come appena detto, una rete di dispositivi infetti (*botnet*), come computer, smartphone, dispositivi IoT (telecamere di sicurezza, router, smart TV) infettati da *malware*⁷⁸ e controllati a distanza da un criminale informatico (*bot-herder*) all'insaputa dei proprietari. Questi dispositivi, chiamati *bot* o *zombie*, vengono utilizzati per attività illecite su larga scala, inclusi attacchi DDoS, invio di spam, furto di dati e attacchi di forza bruta tramite un invio massiccio di richieste al bersaglio, saturando la larghezza di banda⁷⁹ o le risorse del server.

Fu il primo caso in cui una nazione venne quasi interamente “scollegata” dal resto del mondo, dimostrando come il cyber-warfare possa generare caos sociale senza l'uso di esplosivi⁸⁰. Un altro caso di studio cruciale è il malware *Stuxnet*, utilizzato per sabotare le centrifughe nucleari iraniane di Natanz. Secondo quanto riferito, *Stuxnet* bruciò numerose centrifughe nell'impianto di arricchimento dell'uranio causandone la distruzione. Questo episodio ha inaugurato l'era in cui un codice informatico può produrre danni fisici tangibili a infrastrutture critiche, rendendo la distinzione tra attacco digitale e atto di guerra cinetica sempre più sottile. Infatti nel corso del tempo altri gruppi hanno modificato il virus per colpire strutture come impianti di trattamento delle acque, centrali elettriche e gasdotti.

⁷⁶ J. Herzog, *Settling the Estonian Cyber Attacks: Lessons for the United States*, in «Journal of Strategic Security», Vol. 4, n. 1, 2011, pp. 49-74.

⁷⁷ Il downtime è il momento in cui il server è "inattivo", non funziona come previsto e non risponde alle richieste.

⁷⁸ Il malware è un software malevolo progettato per interrompere o rubare dati sensibili dai dispositivi, e rappresenta una minaccia per individui e aziende. I tipi di malware includono ransomware, adware, botnet, cryptojacking, spyware e trojan, ognuno con metodi di attacco e potenziale di danno distinti.

⁷⁹ La larghezza di banda è la capacità massima di trasferimento dati di una connessione di rete in un dato tempo, solitamente misurata in megabit al secondo (Mbps) o gigabit al secondo (Gbps). Determina la velocità di download e upload, influenzando l'efficienza dello streaming, dei giochi online e delle videoconferenze. Una maggiore larghezza di banda equivale a un'autostrada a più corsie, consentendo un flusso di dati più rapido e simultaneo.

⁸⁰ <https://ccdcoe.org/library/publications/the-2007-cyber-attacks-on-estonia-ten-years-on/>

Nonostante la data di scadenza di *Stuxnet* fosse fissata per il giugno 2012 e Siemens avesse prontamente patchato⁸¹ le proprie vulnerabilità, il DNA di questo *worm*⁸² ha dato vita a una stirpe di minacce senza precedenti. I cosiddetti *figli di Stuxnet* hanno ereditato la sua complessità, spostando l'asticella del cyber-spionaggio verso nuovi e pericolosi orizzonti.

I principali discendenti che hanno segnato la storia della sicurezza informatica includono:

Duqu (2011): Considerato il gemello dedito allo spionaggio. Condivideva gran parte del codice di *Stuxnet* ma con uno scopo diverso: agire come un *keylogger*⁸³ avanzato per mappare le infrastrutture industriali e preparare il terreno a futuri attacchi distruttivi

Flame (2012): Uno *spyware*⁸⁴ estremamente sofisticato in grado di sfruttare le porte USB per diffondersi. Oltre a monitorare i tasti premuti, poteva registrare chiamate Skype e catturare screenshot, colpendo prevalentemente enti governativi e accademici nel Medio Oriente.

Havex (2013): Questo malware si è concentrato sull'intelligence industriale, infiltrandosi nei sistemi di aziende energetiche, farmaceutiche e del settore difesa tra Nord America ed Europa.

Industroyer (2016): Concepito con lo scopo specifico di colpire le reti elettriche. È passato alla storia per aver causato il blackout che ha messo in ginocchio parte dell'Ucraina nel dicembre 2016.

Triton (2017): Forse il più inquietante della famiglia, mirava ai sistemi di sicurezza strumentali di un impianto petrolchimico. La sua capacità di manomettere i protocolli di emergenza ha sollevato il timore che l'obiettivo finale fosse causare danni fisici reali alle persone.

A differenza del comune malware domestico, finalizzato spesso all'estorsione di denaro, la famiglia di *Stuxnet* opera su un piano geopolitico. Sebbene l'utente privato non sia il bersaglio

⁸¹ "Patchato" in informatica significa che un software o un sistema è stato aggiornato applicando una "patch", ovvero un piccolo pezzo di codice che corregge bug, vulnerabilità di sicurezza o migliora le prestazioni, rendendo il sistema più sicuro e stabile.

⁸² I worm sono programmi che creano copie di sé stessi in diversi punti di un computer. L'obiettivo di questo tipo di malware è solitamente quello di saturare computer e reti, impedendo che vengano utilizzati. A differenza dei virus, i worm non infettano i file.

⁸³ Un keylogger è un software o hardware malevolo che registra segretamente ogni tasto premuto su un dispositivo, col fine di rubare credenziali, password e dati sensibili. Spesso veicolato tramite phishing o malware, agisce in background trasmettendo informazioni agli hacker. È una grave minaccia alla privacy, configurabile come reato di accesso abusivo.

⁸⁴ Lo spyware è un malware che si installa furtivamente su computer o dispositivi mobili per spiare l'utente, raccogliendo dati sensibili (password, carte di credito, abitudini) e inviandoli a terzi. Spesso nascosto in freeware o allegati e-mail, compromette la privacy, rallenta i sistemi e traccia le attività online senza consenso.

diretto, queste minacce mettono a rischio i servizi essenziali della società moderna: dalla distribuzione elettrica alla sicurezza nazionale. L'obiettivo non è il profitto immediato, ma il sabotaggio o il controllo delle infrastrutture critiche su scala globale.

- L'uso delle "*Proxy Forces*" e degli attori non statali

L'impiego di attori per procura (*proxy*) è l'elemento che garantisce la "*plausible deniability*" all'attaccante. Lo Stato aggressore finanzia, addestra e arma gruppi locali, mercenari o milizie ideologiche allo scopo di condurre operazioni belliche senza apparire direttamente⁸⁵.

L'applicazione pratica più nota è rappresentata dal ruolo della PMC Wagner Group⁸⁶ in vari teatri tra Africa e Ucraina (prima del conflitto su vasta scala del 2022). Utilizzando una compagnia militare privata, uno Stato può proiettare potenza e proteggere i propri interessi economici (come le miniere d'oro in Mali o in Sudan) conservando un distacco formale da aperte violazioni del diritto internazionale⁸⁷. Allo stesso modo il supporto dell'Iran a gruppi come Hezbollah in Libano o gli Houthi in Yemen consente a Teheran di condurre una guerra d'attrito contro i propri rivali nella regione (Israele e Arabia Saudita) senza schierare l'esercito regolare, rendendo così quasi nullo il rischio di una ritorsione diretta sul proprio territorio.

- La manipolazione dell'informazione e la Guerra Cognitiva

La disinformazione (*maskirovka* nella tradizione russa) ha come obbiettivo quello di deteriorare la capacità decisionale del nemico. Non si tratta solamente di diffondere notizie false, ma di inquinare completamente l'ecosistema informativo per far sì che la popolazione non riesca più a distinguere il vero dal falso.

Un esempio pratico è stata l'attività della Internet Research Agency (IRA) di San Pietroburgo, meglio conosciuta mediaticamente come la "fabbrica dei troll" di San Pietroburgo, è stata un'organizzazione russa specializzata in operazioni di guerra psicologica e disinformazione online. Fondata nel 2013, l'IRA è diventata il simbolo moderno della guerra ibrida, operando non con le armi, ma attraverso la manipolazione sistematica dei social media per influenzare l'opinione pubblica globale. L'organizzazione era controllata da Yevgeny

⁸⁵ A. Mumford, *Proxy Warfare*, Polity Press, Cambridge 2013, pp. 30-55.

⁸⁶ Gruppo Wagner è di solito descritto come un'entità militare privata (Private Military Company, PMC) non registrata con base in Russia, ma attiva soltanto al di fuori dei suoi confini (Marten 2019). Nel complesso, le informazioni attualmente disponibili su questa entità sono piuttosto limitate.

⁸⁷ S. Sukhankin, *The 'Hybrid' Role of Russian Private Military Companies*, in «The Jamestown Foundation», 2020.

Prigozhin⁸⁸, l'oligarca russo (defunto nel 2023) noto anche come capo del già citato Gruppo Wagner. L'IRA non era un gruppo di hacker solitari, ma una vera azienda con uffici, dipartimenti (grafica, IT, finanza) e centinaia di dipendenti che lavoravano su turni di 12 ore. Creavano migliaia di falsi account (troll⁸⁹) su *Facebook*, *Twitter* (ora *X*), *Instagram* e *YouTube*. Questi profili fingevano di essere cittadini comuni, attivisti o siti di news locali per seminare discordia e promuovere narrazioni favorevoli al Cremlino⁹⁰.

Durante le elezioni americane del 2016. Attraverso la creazione di migliaia di account fittizi sui social media, sono state alimentate le polarizzazioni esistenti nella società americana (questioni razziali, possesso di armi, diritti civili), trasformando il dibattito democratico in un campo di battaglia fratricida. L'obiettivo ibrido non era far vincere un candidato specifico, ma minare la fiducia dei cittadini nel sistema democratico stesso⁹¹.

Questo fu il caso più celebre, ma anche nel dibattito politico sulla *Brexit*⁹² i ricercatori hanno identificato centinaia di account legati all'IRA impegnati a spingere per l'uscita del Regno Unito dall'UE. Inoltre fin dal 2014, l'agenzia ha lavorato per giustificare l'annessione della Crimea e, successivamente, per delegittimare il governo di Kiev, infatti nelle fasi iniziali del conflitto in Donbass, la disinformazione è stata usata per creare una narrativa di *genocidio dei russi*, fornendo il pretesto morale per l'intervento dei già citati *omini verdi*.

E ancora, diversi studi hanno evidenziato come l'IRA abbia preso di mira anche il dibattito politico italiano, spesso amplificando messaggi populisti o euroscettici.

L'Internet Research Agency è stata formalmente sciolta nel luglio 2023 a seguito del fallito ammutinamento di Prigozhin contro i vertici militari russi. Tuttavia, gli esperti di sicurezza avvertono che molte delle sue tattiche sono state ereditate da nuove entità meno centralizzate ma altrettanto attive.

⁸⁸ Evgenij Prigožin (1961-2023) è stato un imprenditore e mercenario russo, noto come "chef di Putin" per i suoi contratti di catering con il Cremlino. Fondatore e leader del gruppo paramilitare Wagner, ha avuto un ruolo centrale nell'invasione russa dell'Ucraina prima di lanciare una breve e fallita ribellione contro i vertici militari russi nel giugno 2023.

⁸⁹ In ambito internet, un troll è un utente che disturba la convivenza nelle community online (forum, social, chat) inviando messaggi provocatori, irritanti, fuori tema o insensati. L'obiettivo principale è fomentare liti, attirare l'attenzione e disturbare la normale comunicazione, spesso usando ironia o malvagità per causare reazioni stizzite.

⁹⁰ T. Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, Farrar, Straus and Giroux, New York 2020, pp. 320-345.

⁹¹ P. Pomerantsev, *Niente è vero, tutto è possibile*, Minimum Fax, Roma 2015.

⁹² La parola Brexit è una contrazione di 'British exit' e si riferisce all'uscita della Gran Bretagna dall'Unione Europea.

Per concludere, L'IRA non cercava solo di convincere le persone di una “verità” alternativa, ma mirava a distruggere l'idea stessa che esista una verità oggettiva rendendo i cittadini più cinici e diffidenti verso le proprie istituzioni democratiche.

- Il ricatto economico e l'arma energetica

Nella guerra ibrida, il commercio e le risorse naturali diventano armi a tutti gli effetti. Questo strumento sfrutta l'interdipendenza economica globale per piegare la volontà politica di uno Stato.

L'esempio più attuale è la gestione dei flussi di gas naturale verso l'Europa da parte della Russia tra il 2021 e il 2022. Riducendo le forniture e manipolando i prezzi sul mercato, si è cercato di generare inflazione e malcontento sociale nelle nazioni europee per indebolire il loro sostegno militare all'Ucraina⁹³.

In un contesto diverso, la Cina utilizza spesso la cosiddetta *diplomazia del debito* attraverso l'iniziativa Belt and Road⁹⁴.

Il concetto di *diplomazia della trappola del debito* (debt-trap diplomacy) è diventato uno dei temi più caldi della geopolitica moderna. Spesso viene inquadrato come una componente della guerra ibrida, poiché permette alla Cina di ottenere vantaggi strategici, politici e militari senza sparare un solo colpo. Concedendo prestiti ingenti per infrastrutture a paesi strategicamente posizionati (come il porto di Hambantota in Sri Lanka), Pechino ottiene una leva politica che può trasformarsi in controllo territoriale o concessioni militari in caso di insolvenza⁹⁵.

Il processo segue solitamente un copione collaudato nell'ambito della Belt and Road Initiative, la Cina offre ingenti finanziamenti a nazioni in via di sviluppo (spesso con basso rating creditizio) per grandi infrastrutture: porti, ferrovie, autostrade ma a differenza della

⁹³ R. Yergin, *The New Map: Energy, Climate, and the Clash of Nations*, Penguin Books, New York 2020, pp. 115-130.

⁹⁴ La Belt and Road Initiative (BRI), conosciuta in precedenza come “One Belt, One Road” (Una cintura, Una Via) è stata lanciata dal Presidente Xi Jinping alla fine del 2013, inizialmente con lo scopo di rafforzare le interconnessioni fisiche tra la Cina e l'Europa.

⁹⁵ B. Chellaney, *Debt-Trap Diplomacy*, in «Project Syndicate», 2017.

Banca Mondiale⁹⁶ o del FMI⁹⁷, i contratti cinesi sono spesso coperti da clausole di riservatezza e non richiedono riforme democratiche o standard ambientali rigorosi e quando il paese debitore non riesce a ripagare il prestito, Pechino non procede necessariamente al pignoramento, ma rinegozia il debito in cambio di concessioni strategiche.

Si parla di guerra ibrida perché in diversi casi l'economia viene usata per scopi che vanno ben oltre il semplice profitto finanziario: l'esempio più celebre è il porto di Hambantota in Sri Lanka. Incapace di onorare il debito, lo Sri Lanka ha dovuto cedere la gestione del porto alla Cina per 99 anni. Questo trasforma un asset commerciale in un potenziale avamposto logistico-militare nel cuore dell'Oceano Indiano, infatti attraverso il controllo di snodi marittimi e terrestri critici (dal Gibuti al Pireo, dal Pakistan al Montenegro), la Cina crea una rete logistica globale che può essere attivata per scopi militari o per strangolare le rotte commerciali dei rivali in caso di conflitto.

Ed inoltre costituisce anche la base per una vera e propria coercizione politica, il debito agisce come un “guinzaglio” diplomatico. I paesi fortemente indebitati tendono a votare in linea con la Cina presso le Nazioni Unite, per esempio per disconoscere il riconoscimento diplomatico di Taiwan o rimanere in silenzio su questioni sensibili (come la questione sui diritti umani nello Xinjiang o la situazione a Hong Kong).

⁹⁶ Il Gruppo della Banca Mondiale rappresenta una delle maggiori fonti per l'assistenza ai Paesi in via di sviluppo ed agisce attraverso prestiti finalizzati a finanziare investimenti e promuovere la crescita economica per rendere quei Paesi più stabili, efficienti e orientati al mercato.

⁹⁷ Fondo monetario internazionale-Fmi. Il Fondo monetario internazionale (Fmi), con sede a Washington, è un'istituzione internazionale della quale fanno parte 190 paesi, che ha la finalità di promuovere la stabilità economica e finanziaria.

CAPITOLO TERZO

L'EVOLUZIONE DELLA GUERRA IBRIDA NEI CONFLITTI MODERNI

Nel corso dei capitoli precedenti è stata delineata la traiettoria che ha portato dalla cristallizzazione del concetto di guerra classica alla nascita del modello *ibrido*. Tuttavia, la comprensione della guerra ibrida rimarrebbe parziale se non venisse calata nella realtà operativa dei conflitti che stanno ridisegnando gli equilibri del globo nel terzo decennio del XXI secolo. Se inizialmente *l'ibridismo* era percepito come una tattica ausiliaria a disposizione degli attori più deboli per colmare un divario tecnologico, secondo la logica dell'asimmetria, oggi assistiamo ad una sua evoluzione sistemica, di fatto la guerra ibrida è diventata la forma prediletta di scontro tra grandi potenze.

Il presente capitolo si propone di esaminare questa maturazione del concetto, analizzando come la fusione tra strumenti militari e civili sia diventata una condizione permanente e non più legata ad un singolo episodio bellico. Non ci troviamo più di fronte ad una *fase* del conflitto, ma ad una vera e propria metamorfosi degli attori coinvolti e delle loro finalità strategiche⁹⁸.

Lo studio in questo Capitolo procederà seguendo tre distinti percorsi analitici. Nel primo paragrafo (3.1) analizzeremo gli elementi di continuità e discontinuità rispetto alle forme di guerra tradizionali, cercando di capire se l'ibridismo sia una novità assoluta o piuttosto un adattamento iper-tecnologico di antiche arti di inganno e logoramento⁹⁹. Successivamente, nel paragrafo 3.2, esploreremo il radicale mutamento degli attori del conflitto, osservando come la distinzione tra combattente e civile sia ormai definitivamente collassata a favore di figure ibride come i mercenari digitali, le milizie marittime e gli attivisti politici teleguidati. Infine, nel paragrafo 3.3, concluderemo l'analisi proponendo la guerra ibrida non solo come una tecnica,

⁹⁸ M. L. Smith, *Strategy: A History*, Oxford University Press, Oxford 2013, pp. 320-335.

⁹⁹ S. J. Blank, *Russian Information Warfare: Past, Present, and Future*, Strategic Studies Institute, Carlisle 2017, pp. 5-18.

ma come il modello di conflitto dominante del XXI secolo, attraverso una condizione di *crisi perpetua* che sfida le fondamenta stesse del diritto internazionale e della sicurezza collettiva¹⁰⁰.

Attraverso l'esame di casi studio recenti, dalla resistenza ucraina all'assertività cinese, fino alle tensioni nella “zona grigia” del Mediterraneo e del Baltico, vedremo come l'evoluzione della guerra ibrida rifletta la complessità di una società globale interconnessa, dove la vittoria non si ottiene più con la conquista di un territorio, ma con il controllo dei flussi informativi, energetici e cognitivi dell'avversario¹⁰¹.

3.1 CONTINUITÀ E DISCONTINUITÀ RISPETTO ALLE FORME DI GUERRA TRADIZIONALI

Per comprendere l'evoluzione della guerra ibrida, è necessario evitare l'errore prospettico di considerarla un fenomeno privo di radici storiche. Il dibattito accademico si divide tra chi vede nell'ibridismo una *rottura epistemologica*¹⁰² con il passato e chi, invece, lo interpreta come una riproposizione di strategie millenarie. In questo paragrafo analizzeremo come la guerra ibrida si ponga in un rapporto dialettico con la tradizione bellica, identificando ciò che è rimasto immutato e ciò che, a causa della rivoluzione tecnologica e sociale, rappresenta una novità assoluta.

- Gli elementi di continuità: l'inganno, la guerriglia e lo stratagemma

Dal punto di vista della filosofia strategica, la guerra ibrida eredita concetti che risalgono all'antichità. L'idea di vincere senza combattere, o di utilizzare l'inganno per paralizzare l'avversario, trova la sua massima espressione in Sun Tzu¹⁰³. Nel trattato “L'Arte della Guerra” a lui attribuito, composto da 13 capitoli, analizza tattiche, spionaggio, gestione delle risorse e la vittoria tramite l'astuzia piuttosto che la forza bruta, il generale cinese sottolineava che «ogni guerra è basata sull'inganno» e che il vertice della strategia consiste nel piegare la resistenza del

¹⁰⁰ H. Strachan, *The Direction of War: Contemporary Strategy in Historical Perspective*, Cambridge University Press, New York 2013, pp. 15-38.

¹⁰¹ J. L. Gaddis, *On Grand Strategy*, Penguin Books, New York 2018, pp. 210-225.

¹⁰² La rottura epistemologica, concetto introdotto da Gaston Bachelard, indica la discontinuità radicale nel progresso scientifico, che non avviene linearmente ma tramite salti e superamento di “ostacoli epistemologici” (credenze consolidate). Questo cambiamento trasforma i fondamenti di una disciplina, separando la conoscenza scientifica dal senso comune.

¹⁰³ Sun Tzu (VI-V secolo a.C.) è stato un leggendario generale, stratega e filosofo cinese, tradizionalmente riconosciuto come l'autore de “L'arte della guerra”, il più antico e influente trattato di strategia militare. Vissuto durante il periodo delle Primavere e degli Autunni, il suo nome significa “Maestro Sun”.

nemico senza ricorrere alla battaglia campale. I suoi insegnamenti si basano sul taoismo¹⁰⁴ e sul legismo¹⁰⁵, applicando l'equilibrio tra Yin e Yang ed una rigorosa disciplina militare, ed il loro principio cardine è che «la suprema arte della guerra consiste nell'infrangere la resistenza del nemico senza combattere»¹⁰⁶. Questo approccio è la base su cui poggiano le moderne campagne di disinformazione e le operazioni sotto falsa bandiera.

Un altro elemento di forte continuità è il ricorso alla guerriglia e alle forze irregolari in supporto agli eserciti regolari. Storicamente, il coordinamento tra truppe convenzionali e partigiani è stato una costante: si pensi alla Guerra d'indipendenza Spagnola contro Napoleone (1808-1814), che rappresenta un caso studio affascinante perché, pur essendo combattuta nell'era dei moschetti e della cavalleria, presenta elementi che oggi definiremmo *guerra ibrida*.

Napoleone, abituato a battaglie campali simmetriche, si trovò invischiato in un conflitto dove il confine tra soldato e civile era quasi inesistente. Il termine stesso *guerrilla* (piccola guerra) nasce qui, non si trattava solo di imboscate, ma di un ecosistema di resistenza che logorava l'esercito francese (la Grande Armée) senza mai affrontarlo direttamente in campo aperto¹⁰⁷. Vi era un logoramento costante, infatti piccoli gruppi di contadini e disertori attaccavano le linee di rifornimento e i corrieri, i francesi controllavano solo il terreno su cui poggiavano i piedi, appena si spostavano, il territorio tornava ostile, ed inoltre vi era una componente psicologica non indifferente, ovvero la paura costante di attacchi improvvisi che distrusse il morale delle truppe napoleoniche¹⁰⁸. La resistenza spagnola utilizzò la comunicazione come un'arma per mobilitare le masse e demonizzare l'occupante, attraverso un *catechismo civile*, vennero diffusi opuscoli in cui Napoleone era dipinto come l'Anticristo e i francesi come eretici. Questo trasformò la guerra politica in una guerra di religione. Ed inoltre vennero messe in circolo delle *fake news*¹⁰⁹ dell'epoca: venivano diffuse voci esagerate sulle vittorie alleate o su presunte debolezze di Napoleone per mantenere alta la speranza della popolazione.

¹⁰⁴ Il taoismo è un'antica tradizione filosofica e religiosa cinese, basata sul Tao (la Via), il principio cosmico impersonale che regola l'universo. Fondato sul Tao Te Ching di Laozi, promuove l'armonia con la natura, la spontaneità, la semplicità e il wu-wei (azione senza sforzo), cercando equilibrio tra Yin e Yang per longevità e saggezza.

¹⁰⁵ Il legismo era una scuola filosofica cinese incentrata su filosofia politica, diritto, realpolitik e gestione della burocrazia.

¹⁰⁶ Sun Tzu, L'arte della guerra, a cura di L. Maggio, Newton Compton, Roma 1994, pp. 25-40.

¹⁰⁷ B. Liddell Hart, L'arte della guerra nel XX secolo, Mondadori, Milano 1971, pp. 115-130.

¹⁰⁸ T.E. Lawrence, I sette pilastri della saggezza, Bompiani, Milano 1949.

¹⁰⁹ Il termine *fake news* (in italiano "notizie false" o "bufale") si riferisce ad informazioni parzialmente o completamente inventate, ingannevoli o distorte, create appositamente per essere diffuse tramite social media, siti web o media tradizionali.

Vi fu anche una componente di resistenza civile, città come Saragozza e Gerona divennero simboli di resistenza urbana estrema. La popolazione civile partecipava attivamente alla difesa, trasformando ogni casa in una fortezza. Questo costrinse i francesi a lunghi assedi che drenavano risorse immense, spostando il focus dal controllo politico alla mera sopravvivenza militare. La guerra ibrida spagnola, già nei primi anni del 1800 dimostrò che una superpotenza militare può essere sconfitta se non riesce a conquistare i “cuori e le menti” (o almeno a spegnere la volontà di resistenza) di una popolazione profondamente motivata.

Altro esempio storico sono le operazioni condotte da Lawrence d'Arabia (Thomas Edward Lawrence)¹¹⁰ durante la Rivolta Araba (1916-1918) che rappresentano uno dei primi e più brillanti esempi moderni di guerra ibrida. Mentre le grandi potenze si dissanguavano nelle trincee del fronte occidentale, Lawrence sviluppò una strategia che combinava forze irregolari, tecnologia avanzata, guerra psicologica e obiettivi politici a lungo termine. Lawrence non cercava la battaglia campale contro l'Impero Ottomano. La sua intuizione, descritta ne “I sette pilastri della saggezza”, era che la ribellione dovesse essere come un gas: «invisibile, inafferrabile, ma ovunque». Usando i cammelli, le sue forze potevano colpire nel deserto profondo, dove i turchi (legati alle ferrovie e alle basi fisse) non potevano seguirli. Altro stratagemma fu colpire le infrastrutture e non l'esercito: il suo obiettivo principale era la ferrovia dell'Hegiaz. Invece di distruggerla completamente, la sabotava continuamente. Questo costringeva i turchi a mantenere migliaia di soldati a guardia dei binari, immobilizzando forze che avrebbero potuto combattere contro gli inglesi in Palestina.

Inoltre Lawrence fu uno dei primi a capire l'importanza della percezione pubblica, con l'intento della *costruzione di un mito*, collaborò attivamente con il giornalista americano Lowell Thomas per creare un'immagine eroica e romantica della rivolta. Questa “propaganda del successo” serviva a convincere il governo britannico a continuare a finanziare la missione e a dare legittimità internazionale alla causa araba.

Proseguendo nell'associazione con il moderno concetto di guerra ibrida, le operazioni di Lawrence sono il prototipo della *Proxy War* (guerra per procura), attraverso finanziamenti e armi, infatti la Gran Bretagna forniva oro (per pagare i capi tribù), armi e consulenti tecnici, mentre gli arabi fornivano il sangue e la conoscenza del territorio, e coordinamento con le forze

¹¹⁰ Lawrence d'Arabia (Thomas Edward Lawrence) è stato un archeologo, ufficiale, agente segreto e scrittore britannico, diventato famoso per il suo ruolo chiave nella Rivolta Araba contro l'Impero Ottomano durante la Prima Guerra Mondiale, dove organizzò e guidò le tribù arabe, diventando una figura leggendaria e un simbolo dell'indipendenza araba, immortalato anche dal celebre film omonimo.

regolari: Lawrence agiva come elemento di congiunzione tra l'insurrezione irregolare e l'avanzata dell'esercito regolare del generale Allenby¹¹¹. Questo creava un dilemma strategico per gli ottomani: se si concentravano sulla difesa costiera contro gli inglesi, venivano colpiti alle spalle dai guerriglieri di Lawrence; se inseguivano i guerriglieri nel deserto, indebolivano il fronte principale.

La sua stessa immagine, un ufficiale britannico in abiti tradizionali arabi, era un'arma di comunicazione mirata a guadagnare la fiducia totale delle tribù e a terrorizzare e confondere i comandi turchi.

Ma l'elemento più *ibrido* (e controverso) fu la gestione delle promesse politiche, Lawrence giocava su più tavoli, egli prometteva l'indipendenza agli arabi pur essendo a conoscenza degli accordi Sykes-Picot (che spartivano il Medio Oriente tra Francia e Gran Bretagna)¹¹². Raccolse informazioni cruciali sulle dinamiche tribali, usando le rivalità locali per unire i clan sotto un unico obiettivo militare, trasformando una serie di faide interne in un movimento politico nazionale. Pertanto, attraverso varie strategie e diverse componenti, Lawrence d'Arabia trasformò la guerra nel deserto da una questione di forza bruta a una questione di influenza, logistica e intelligence. Come disse lui stesso, la guerra araba era «più simile all'apprendimento di una nuova lingua che alla vittoria di una battaglia».

In questi due casi appena analizzati, l'elemento *ibrido* era già presente sotto forma di sabotaggi e attacchi alle linee di rifornimento volti a logorare un nemico militarmente superiore. La guerra ibrida contemporanea riprende questo schema elevandolo a sistema strategico integrato dove l'irregolare non è più un semplice ausiliario, ma un attore centrale della narrativa bellica.

- Gli elementi di discontinuità: la velocità e la portata globale

Se la strategia di base presenta analogie storiche, la vera discontinuità risiede nei mezzi e nell'intensità. La prima grande differenza è la compressione spaziotemporale. In passato, un'operazione di disinformazione o di sabotaggio richiedeva mesi per essere pianificata ed

¹¹¹ Edmund Allenby (1861 - 1936) è stato un feldmaresciallo britannico, celebre per aver guidato la Forza di spedizione egiziana alla vittoria contro l'Impero Ottomano in Palestina e Siria durante la prima guerra mondiale. Noto come il "liberatore di Gerusalemme" nel 1917, ha svolto un ruolo chiave nella riconfigurazione del Medio Oriente moderno.

¹¹² L'accordo Sykes-Picot (1916) fu un'intesa segreta durante la Prima Guerra Mondiale tra Regno Unito e Francia, con l'assenso della Russia, per spartirsi le sfere d'influenza nel Medio Oriente arabo in caso di crollo dell'Impero Ottomano. Disegnò confini arbitrari che assegnarono il controllo su Siria e Libano alla Francia, e Iraq, Transgiordania e Palestina alla Gran Bretagna.

eseguita, ed i suoi effetti rimanevano spesso localizzati. Oggi, grazie alla digitalizzazione, una campagna di influenza può essere lanciata in pochi minuti e raggiungere milioni di persone contemporaneamente in tutto il mondo.

La seconda discontinuità fondamentale riguarda l'abbattimento della barriera tra ambiti civili e militari. Nella concezione di guerra classica, l'obiettivo era la forza militare dell'avversario; nella guerra ibrida, il bersaglio è la fiducia sociale. La tecnologia moderna permette di colpire il *cuore civile* dello Stato nemico senza dover prima sconfiggere le sue forze armate sul confine. Un attacco ai sistemi di pagamento elettronico di una nazione o alla sua rete elettrica, per esempio, non ha precedenti nella storia della guerra pre-digitale per quanto riguarda la capacità di generare un collasso interno in tempo di pace.

Ma la discontinuità più significativa, tuttavia, riguarda la gestione della soglia di violenza. Tradizionalmente, la guerra era un evento eccezionale che interrompeva la pace. Oggi, l'ibridismo ha creato una condizione di conflittualità permanente che non sfocia mai in un'aggressione palese ma non permette mai una reale distensione. Questa *zona grigia* rappresenta un'innovazione rispetto al passato perché sfida l'ordine giuridico internazionale basato sulla Carta delle Nazioni Unite¹¹³. Mentre in passato l'aggressione era un atto geograficamente e temporalmente definito, oggi siamo di fronte ad una aggressione molecolare, continua e invisibile, che trasforma il commercio, la legge (lawfare¹¹⁴) e la tecnologia in armi di offesa quotidiana.

Un elemento di netta discontinuità rispetto alla guerra classica, e che merita un'analisi specifica nel contesto dell'evoluzione dei conflitti, è il fenomeno del *Lawfare*¹¹⁵. Il termine, derivante dalla fusione di law (legge) e warfare (guerra), è stato reso popolare all'inizio degli anni Duemila dal generale Charles Dunlap e descrive l'uso, o l'abuso, della legge come sostituto dei mezzi militari tradizionali per raggiungere obiettivi operativi e strategici¹¹⁶.

¹¹³ M. Mazziotti di Celso, Il diritto internazionale alla prova dei conflitti ibridi, in «Rivista di Studi Politici», n. 4, 2019, pp. 88-105.

¹¹⁴ Il lawfare è l'uso strategico o l'abuso del sistema legale (leggi, tribunali, regolamenti) come arma per delegittimare, danneggiare o bloccare un avversario (Stati, organizzazioni o individui), sostituendo o integrando i mezzi militari tradizionali. Coniato dal Gen. Charles Dunlap, descrive un conflitto in cui la legge è impiegata per ottenere vantaggi geopolitici o operativi.

¹¹⁵ <https://mwi.westpoint.edu/lawfare-the-use-of-the-law-as-a-weapon-of-war/>

¹¹⁶ C. J. Dunlap Jr., *Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts*, Harvard University Carr Center for Human Rights Policy, Cambridge 2001.

Nel quadro della guerra ibrida, il Lawfare non è una semplice disputa legale, ma un'arma offensiva progettata per delegittimare l'avversario, paralizzare le sue capacità decisionali e rallentare i suoi movimenti sul campo¹¹⁷.

L'applicazione pratica del Lawfare si manifesta in diverse forme. Una delle più comuni riguarda l'uso di contenziosi internazionali per contestare la sovranità territoriale o la libertà di movimento¹¹⁸. Nel contesto del Mar Cinese Meridionale o dei confini marittimi nel Mediterraneo Orientale, gli Stati utilizzano interpretazioni creative della Convenzione delle Nazioni Unite sul Diritto del Mare (UNCLOS)¹¹⁹ per giustificare l'invio di flotte civili o per dichiarare illegittime le operazioni navali avversarie.

In questo scenario, il ricorso a un tribunale internazionale non serve necessariamente a risolvere una controversia, ma a creare un *disturbo* diplomatico che costringe l'avversario a giustificare ogni sua mossa, intaccando il suo consenso politico internazionale. Se uno Stato riesce a far etichettare come illegale una sanzione o un blocco navale nemico, ha ottenuto una vittoria ibrida senza sparare un colpo, poiché ha attivato le pressioni delle organizzazioni internazionali contro il proprio avversario¹²⁰.

Un altro esempio critico riguarda l'uso del diritto commerciale e delle normative ambientali per bloccare progetti infrastrutturali strategici. Nella guerra ibrida, un attore può finanziare gruppi di pressione o organizzazioni non governative nel territorio nemico per avviare lunghe battaglie legali contro la costruzione di gasdotti, porti o basi militari, invocando violazioni normative. Questo *sabotaggio legale* è estremamente efficace perché si muove all'interno delle regole democratiche dello Stato bersaglio, rendendo difficile una risposta coercitiva.

Inoltre, il Lawfare viene impiegato per contrastare il regime delle sanzioni economiche. Gli Stati colpiti da sanzioni spesso avviano procedure legali presso corti internazionali sostenendo la violazione dei diritti umani o dei trattati di libero scambio, con l'obiettivo di congelare i fondi dell'avversario o di creare un'incertezza giuridica che scoraggi gli investitori esteri dal rispettare le sanzioni stesse¹²¹.

¹¹⁷ O. Kittrie, *Lawfare: Law as a Weapon of War*, Oxford University Press, New York 2016, pp. 1-25.

¹¹⁸ D. Kennedy, *Of War and Law*, Princeton University Press, Princeton 2006, pp. 12-34.

¹¹⁹ La Convenzione delle Nazioni Unite sul Diritto del Mare (UNCLOS), firmata a Montego Bay il 10 dicembre 1982 ed entrata in vigore nel 1994, è il trattato fondamentale che disciplina l'uso dei mari e degli oceani. Definisce i diritti e le responsabilità degli Stati, inclusa la zonazione (mare territoriale fino a 12 miglia, zona economica esclusiva fino a 200 miglia), lo sfruttamento delle risorse e la protezione dell'ambiente marino.

¹²⁰ J. Kraska, *Maritime Power and the Law of the Sea: Expeditionary Operations in World Politics*, Oxford University Press, Oxford 2011, pp. 110-145.

¹²¹ S. Neff, *War and the Law of Nations: A General History*, Cambridge University Press, Cambridge 2005.

Infine, il Lawfare agisce sulla percezione morale del conflitto. L'emissione di mandati d'arresto internazionali o l'avvio di indagini per crimini di guerra contro leader politici e militari nemici, spesso basati su prove manipolate in contesti ibridi, serve a limitare la loro libertà di movimento diplomatica e a presentare l'avversario in maniera denigratoria agli occhi dell'opinione pubblica globale. In questo senso, la legge diventa lo scudo dietro cui nascondere operazioni di influenza e lo sferzante con cui colpire la legittimità del potere altrui.

In conclusione, la guerra ibrida rappresenta una *vecchia strategia* ma con *nuovi strumenti*. La continuità risiede nell'obiettivo costante, il potere e la sottomissione dell'altro, mentre la discontinuità risiede nel teatro operativo che non è più solo fisico ma è diventato digitale, psicologico e infrastrutturale, rendendo la difesa un compito non più attribuibile esclusivamente ai militari ma esteso all'intera società¹²².

3.2 GUERRA IBRIDA E MUTAMENTO DEGLI ATTORI DEL CONFLITTO

La trasformazione della guerra nel XXI secolo non riguarda solo le tecnologie impiegate, ma investe profondamente l'identità dei soggetti che la combattono. Nel modello classico clausewitziano, l'attore del conflitto era lo Stato, rappresentato dal suo esercito regolare. Oggi, la scena bellica è affollata da una moltitudine di attori *liquidi*, la cui natura oscilla tra il civile e il militare, tra il pubblico e il privato, tra il legale e l'illegale. Questa frammentazione dell'attore bellico è una scelta strategica precisa: moltiplicare i soggetti coinvolti serve a soffocare la capacità di risposta del difensore e a rendere impossibile l'attribuzione delle responsabilità¹²³.

Il primo grande mutamento risiede nell'ascesa delle Compagnie Militari Private¹²⁴. Non si tratta dei mercenari di sorte del passato, ma di vere e proprie strutture aziendali che offrono servizi di sicurezza, addestramento e, sempre più spesso, combattimento attivo. Il loro status è controverso. Nel diritto internazionale, se catturati, i *contractors* sono generalmente considerati

¹²² Q. Liang, W. Xiangsui, Guerra senza limiti, Libreria Editrice Goriziana, Gorizia 2001, p. 124.

¹²³ <https://www.theguardian.com/world/2022/may/04/the-wagner-group-the-mercenary-army-russia-uses-for-dirty-work>

¹²⁴ Le compagnie militari private (PMC - Private Military Companies), spesso note come contractor, sono società private che offrono servizi specializzati di sicurezza, addestramento, supporto logistico e, talvolta, combattimento diretto per conto di governi, aziende o organizzazioni internazionali. Sono essenzialmente eserciti mercenari moderni, composti da personale altamente qualificato (ex militari o poliziotti) impiegati in zone di conflitto.

combattenti illegittimi e non godono dello stesso status dei soldati regolari, sebbene siano soggetti alle Convenzioni di Ginevra¹²⁵.

L'esempio più emblematico dell'ultimo decennio è rappresentato dal, già citato, Gruppo Wagner¹²⁶. Fondata da Evgenij Prigozhin, la Wagner ha permesso alla Federazione Russa di intervenire in teatri complessi come la Siria, la Libia, il Mali e il Centrafrica, garantendo al Cremlino la cosiddetta *negabilità plausibile*¹²⁷. Se un soldato della Wagner viene catturato o ucciso, lo Stato può dichiarare formalmente di non avere legami con lui, evitando così escalation diplomatiche o responsabilità legali internazionali. In Africa, questi attori non solo combattono, ma gestiscono infrastrutture estrattive (miniere d'oro e diamanti), trasformando la guerra in un'impresa economica ibrida dove il profitto privato e l'interesse geopolitico statale si fondono in maniera intricata¹²⁸.

Un altro attore fondamentale della modernità ibrida è il *combattente digitale*¹²⁹. Gli hacker¹³⁰ non sono più solo individui isolati, ma unità strutturate all'interno dei servizi segreti o dei ministeri della difesa¹³¹.

Un caso di studio rilevante è rappresentato dal gruppo *Lazarus Group*, ampiamente ritenuto un braccio operativo della Corea del Nord, è un collettivo di hacker APT (Advanced Persistent Threat)¹³² sponsorizzato dallo Stato della Corea del Nord. Attivo almeno dal 2009, il gruppo opera sotto la direzione del Reconnaissance General Bureau (RGB), il principale

¹²⁵ Le Convenzioni di Ginevra del 1949, composte da quattro trattati principali, costituiscono il pilastro del diritto internazionale umanitario, proteggendo feriti, prigionieri e civili durante i conflitti armati. Integrati da protocolli aggiuntivi (1977, 2005), impongono il trattamento umano e divieti contro torture e violenze, vincolando quasi tutti gli Stati membri ONU. La distinta Convenzione di Ginevra del 1951 definisce lo status di rifugiato.

¹²⁶ S. Sukhankin, *War, Business and Politics: The Case of the Wagner Private Military Company*, in «Jamestown Foundation», 2019.

¹²⁷ La negabilità plausibile (in inglese *plausible deniability*) è la capacità di un leader o di una figura di alto livello di negare la responsabilità per azioni illecite commesse dai propri subordinati, grazie all'assenza di prove dirette che colleghino il superiore all'evento. Questa strategia crea una "zona grigia" formale, permettendo di dichiararsi estranei ai fatti pur avendoli, in parte o in tutto, favoriti o tollerati.

¹²⁸ A. Gostev, R. Coalson, *Russia's Paramilitary Mercenaries emerge from the Shadows*, in «Radio Free Europe/Radio Liberty», 2016.

¹²⁹ <https://research.checkpoint.com/2022/the-evolution-of-cyber-warfare/>

¹³⁰ In informatica, un hacker è una persona con elevate competenze tecniche capace di esplorare, analizzare e modificare sistemi hardware e software per superarne i limiti o risolverne le criticità. Sebbene nel linguaggio comune sia spesso sinonimo di criminale, il termine nasce negli anni '60 al MIT con un'accezione positiva legata alla curiosità intellettuale e alla condivisione della conoscenza.

¹³¹ J. Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, O'Reilly Media, Sebastopol 2011, pp. 145-160.

¹³² Un "APT hacker" si riferisce a un hacker che fa parte di un gruppo di Advanced Persistent Threat (APT), cioè una minaccia informatica avanzata e persistente, composta da criminali altamente qualificati (spesso legati a stati) che infiltrano segretamente reti per lunghi periodi, rubando dati sensibili o sabotando sistemi, agendo in modo mirato e sofisticato per eludere le difese tradizionali, come antivirus e firewall.

servizio di intelligence militare nordcoreano. È noto con diversi alias, tra cui Hidden Cobra, APT38 e Guardians of Peace e svolge attività di cyber-spionaggio per fini politici e attacchi a scopo di lucro per finanziare il regime di Pyongyang e i suoi programmi missilistici/nucleari, aggirando le sanzioni internazionali. Il gruppo è ritenuto responsabile di alcune delle operazioni cyber più eclatanti della storia, alla Banca del Bangladesh (2016) con un tentativo di furto di quasi un miliardo di dollari tramite il sistema SWIFT¹³³; il *Ransomware WannaCry* (2017), un attacco globale che ha cifrato i dati di centinaia di migliaia di computer in tutto il mondo ed il *Furti Crypto*, tra il 2021 e il 2025, si stima abbiano rubato oltre 5 miliardi di dollari in criptovalute, colpendo piattaforme come Ronin Bridge e Bybit.

Quindi questo gruppo non si limita allo spionaggio militare, ma conduce operazioni di furto finanziario per finanziare il programma nucleare del regime di Pyongyang. Qui l'attore è ibrido per eccellenza: un reparto militare che agisce come un'organizzazione criminale transnazionale. Allo stesso modo, unità come l'Unità 8200 israeliana o il Comando Cyber statunitense operano costantemente in un'area dove il *soldato* siede dietro una scrivania, ma le sue azioni hanno effetti distruttivi superiori a quelli di un bombardamento convenzionale¹³⁴.

Infine, la guerra ibrida ha trasformato le popolazioni civili, o segmenti di esse, in strumenti d'attacco. L'esempio più sofisticato di questo mutamento è la Milizia Marittima Cinese (PAFMM)¹³⁵.

Nel Mar Cinese Meridionale, Pechino utilizza migliaia di pescherecci civili, equipaggiati con sistemi di comunicazione militare e guidati da ufficiali in congedo, per occupare atolli o molestare navi di altri paesi (Filippine, Vietnam)¹³⁶. Se la marina degli Stati Uniti o di altre potenze regionali intervenisse contro queste imbarcazioni, verrebbe accusata di aver attaccato pacifici pescatori civili¹³⁷. È un paradosso tipico della guerra ibrida: l'attore civile viene armato non per combattere una battaglia, ma per fare da scudo umano e legale alle ambizioni territoriali

¹³³ Il sistema SWIFT (Society for Worldwide Interbank Financial Telecommunication) è una rete globale sicura che permette alle banche di scambiarsi messaggi e istruzioni per trasferire fondi internazionali, identificando univocamente le istituzioni tramite il codice SWIFT/BIC, ma non gestisce direttamente i fondi o i conti, agendo solo come mezzo di comunicazione standardizzato per pagamenti sicuri e veloci, essenziale per il sistema finanziario mondiale.

¹³⁴ B. Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Harvard University Press, Cambridge 2020.

¹³⁵ La Milizia Marittima delle Forze Armate Popolari (PAFMM) è una forza para-militare cinese composta da pescherecci civili addestrati ed equipaggiati per sostenere le rivendicazioni territoriali nel Mar Cinese Meridionale. Agisce come "terza forza marittima" (dopo Marina e Guardia Costiera), impiegando tattiche della *zona grigia* per intimidire, monitorare e bloccare imbarcazioni straniere senza causare conflitti militari aperti.

¹³⁶ <https://www.cfr.org/blog/chinas-maritime-militia-what-it-and-why-it-matters>

¹³⁷ A. S. Erickson, C. M. Kennedy, *China's Maritime Militia*, in «CNA Conference Report», 2016.

dello Stato. Questo schema si è ripetuto anche lungo il confine tra Polonia e Bielorussia nel 2021, dove i flussi migratori sono stati strumentalizzati dal regime di Lukashenko come un'arma umana per destabilizzare l'Unione Europea, rendendo i migranti stessi attori inconsapevoli di una pressione ibrida¹³⁸.

In conclusione, il mutamento degli attori ha trasformato la guerra in un fenomeno *totale* dove chiunque può essere un combattente: l'informatico, il mercenario, il pescatore o l'attivista social. Questa frantumazione della figura del soldato rende i tradizionali trattati di pace e le convenzioni di guerra strumenti obsoleti, poiché non sanno più identificare contro chi, e con quali regole, si stia effettivamente combattendo¹³⁹.

3.3 LA GUERRA IBRIDA COME MODELLO DI CONFLITTO DEL XXI SECOLO

L'analisi condotta finora permette di giungere ad una riflessione di carattere sistemico, ovvero che la guerra ibrida non deve essere interpretata come una semplice deviazione dai canoni della guerra convenzionale, bensì come il modello di conflitto dominante del XXI secolo. Se il secolo scorso è stato segnato dalla Guerra Fredda, un equilibrio precario basato sulla deterrenza nucleare tra due blocchi contrapposti, il secolo attuale sembra essere caratterizzato da una *pace ibrida*, ovvero una condizione di competizione geopolitica violenta e incessante che si svolge appena al di sotto della soglia del conflitto armato aperto¹⁴⁰.

Una delle caratteristiche fondamentali di questo modello è la dissoluzione della dimensione temporale del conflitto. Nella tradizione classica, la guerra aveva un inizio (la dichiarazione) e una fine (il trattato di pace). Nel modello ibrido del XXI secolo, il conflitto è permanente. Non esiste un momento di reale distensione, poiché la competizione per il potere si sposta costantemente da un dominio all'altro, quando tacciono le armi cinetiche, si intensificano gli attacchi cyber; quando si raggiunge un accordo commerciale, si attivano le campagne di disinformazione¹⁴¹.

¹³⁸ K. M. Greenhill, *Weapons of Mass Migration: Forced Displacement, Coercion, and Foreign Policy*, Cornell University Press, Ithaca 2010, pp. 12-45.

¹³⁹ M. Walzer, *Guerre giuste e ingiuste. Un discorso morale con esemplificazioni storiche*, Laterza, Roma-Bari 1990, pp. 165-180.

¹⁴⁰ J. Nye, *The Future of Power*, PublicAffairs, New York 2011, pp. 110-125.

¹⁴¹ M. Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, New Haven 2022, pp. 15-40.

Questa *conflittualità permanente* trasforma la società stessa in un campo di battaglia latente. Poiché ogni vulnerabilità (economica, sociale o digitale) può essere sfruttata dall'avversario, lo Stato è costretto ad una mobilitazione difensiva costante¹⁴². Il concetto di sicurezza nazionale si espande fino a comprendere la resilienza delle infrastrutture civili, la stabilità dei mercati finanziari e persino la salute mentale della popolazione, costantemente esposta a operazioni psicologiche.

La guerra ibrida ha avuto la meglio come modello perché ha saputo sfruttare i limiti della deterrenza classica. La NATO e le altre alleanze difensive sono state progettate per rispondere ad invasioni territoriali su larga scala. Tuttavia, di fronte ad un attacco cyber che mette fuori uso il sistema bancario o ad una milizia irregolare che occupa un edificio governativo senza insegne, la risposta militare convenzionale risulta sproporzionata o politicamente impossibile da giustificare.

L'efficacia del modello ibrido risiede proprio in questa capacità di operare nella *zona grigia*. Gli attori ibridi sanno perfettamente dove si trova la *linea rossa* dell'avversario e agiscono con precisione chirurgica per restare appena un millimetro al di sotto di essa. Questo logoramento costante erode la credibilità delle istituzioni internazionali e delle alleanze di difesa, poiché dimostra la loro incapacità di proteggere i cittadini da minacce non cinetiche ma ugualmente devastanti¹⁴³.

In ultima analisi il consolidamento della guerra ibrida come modello globale suggerisce una crisi profonda dell'ordine internazionale liberale basato sulle regole. Se l'uso della forza non è più palese, se gli aggressori rimangono anonimi e se il diritto internazionale viene usato come arma (vedi *Lawfare*), i trattati perdono il loro potere regolatore.

Il XXI secolo si prospetta dunque come un'era di *anarchia ibrida*, in cui il potere viene esercitato attraverso il controllo dei flussi (dati, energia, finanza) piuttosto che dei territori. La vittoria non è più un evento definitivo sancito da una resa, ma una condizione temporanea di superiorità informativa e tecnologica¹⁴⁴. In questo contesto, la sfida per le democrazie moderne non è solo sviluppare nuove armi, ma reinventare il concetto stesso di sovranità e di resilienza

¹⁴² D. Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West*, Oxford University Press, Oxford 2020, pp. 25-50.

¹⁴³ M. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Strategic Studies Institute, U.S. Army War College, Carlisle 2015, pp. 5-32.

¹⁴⁴ P. Khanna, *Connectography: Le mappe del futuro ordine mondiale*, Fazi Editore, Roma 2016.

per sopravvivere ad una guerra che non viene mai dichiarata, ma che non smette mai di essere combattuta.

CONCLUSIONI

Il percorso analitico condotto in questo elaborato ha permesso di evidenziare come la guerra ibrida non rappresenti soltanto una nuova tecnica bellica, ma una vera e propria sfida ontologica alle categorie con cui la modernità ha interpretato il conflitto, la politica e il diritto. Se siamo partiti dalla *trinità* clausewitziana e dal modello vestfaliano di Stato sovrano, siamo giunti ad una realtà in cui la forza viene esercitata nell'ombra, dove i confini sono *fluidi* e dove il nemico è spesso invisibile o non attribuibile.

La prima grande evidenza che emerge dalla ricerca è il superamento definitivo della dicotomia Pace/Guerra. Nel XXI secolo, la pace non è più l'assenza di conflitto, ma una condizione di *pace conflittuale* o *competizione permanente*. La guerra ibrida ha dimostrato che è possibile ottenere vantaggi strategici decisivi, alterare i confini di uno Stato, influenzare le elezioni di una potenza straniera e paralizzare le infrastrutture critiche, senza mai varcare la soglia formale che definisce l'atto di aggressione.

Questa "Zona Grigia" mette in crisi il diritto internazionale, difatti le norme create per regolare l'uso della forza cinetica (lo *Ius ad Bellum*) si rivelano inefficaci di fronte ad un attacco cyber o ad una campagna di disinformazione. Il rischio è che il successo del modello ibrido incentivi una corsa globale all'uso di strumenti occulti in grado di rendere l'ordine internazionale sempre più imprevedibile ed instabile.

Un punto centrale emerso nel corso della tesi riguarda l'asimmetria riscontrabile tra regimi autoritari e democrazie liberali nella gestione della minaccia ibrida. Le democrazie, per loro stessa natura, si fondano sulla libertà d'espressione, sulla trasparenza dei processi decisionali e sulla separazione dei poteri. Questi stessi valori vengono trasformati dall'attore ibrido in vulnerabilità, dove i social media diventano vettori di polarizzazione, il pluralismo dell'informazione diventa lo spazio per la propaganda nemica, e la lentezza dei processi legali viene sfruttata attraverso il *lawfare*.

Di fatto, un aspetto che merita una riflessione conclusiva separata riguarda l'impatto che ha la guerra ibrida sulla struttura legale internazionale. Il sistema di sicurezza collettiva ideato nel secondo dopoguerra si fonda sul presupposto che la forza sia identificabile e che esista un confine netto tra *aggressione* e *legittima difesa*. La guerra ibrida, tuttavia, è programmaticamente costruita per aggirare queste categorie.

Ciò pone le democrazie di fronte ad un dilemma etico senza precedenti: come rispondere a un attacco che non è formalmente un atto di guerra? Se uno Stato risponde militarmente ad un attacco cyber, rischia di essere percepito come l'aggressore originale. Se non risponde, rischia di apparire debole e di invitare a nuove incursioni. E proprio questa *paralisi decisionale* è l'obiettivo ultimo dell'ibridismo. Tuttavia, la risposta a queste minacce non può essere la limitazione delle libertà civili, poiché ciò significherebbe concedere all'aggressore ibrido una vittoria ideologica. La vera prova per il futuro consiste nello sviluppare quella che abbiamo definito resilienza democratica, cioè una combinazione di alfabetizzazione digitale dei cittadini, cooperazione tra pubblico e privato nella cybersecurity ed una rinnovata agilità diplomatica capace di smascherare e attribuire tempestivamente le minacce. La sfida del prossimo decennio sarà quindi la creazione di un nuovo “codice di condotta” per il cyberspazio e la zona grigia, un compito che appare arduo data la mancanza di fiducia tra le grandi potenze.

Guardando oltre l'orizzonte attuale, l'evoluzione della guerra ibrida sembra destinata a legarsi indissolubilmente all'avanzamento dell'Intelligenza Artificiale (IA). L'uso di algoritmi per la creazione di *deepfake*¹⁴⁵ sempre più realistici e la gestione automatizzata di reti di bot per la manipolazione dell'opinione pubblica portano la *guerra cognitiva* ad un livello di precisione chirurgica.

In questo scenario, l'obiettivo ultimo del conflitto ibrido non è più la conquista del territorio, ma la mente umana. Se l'avversario riesce a plasmare la percezione della realtà di una popolazione, lo Stato perde la sua capacità di agire e di difendersi prima ancor prima che un solo colpo venga sparato. La guerra del futuro sarà dunque una guerra di algoritmi e di narrazioni, dove lo sviluppo delle capacità tecnologiche dovrà necessariamente essere accompagnato da una solida etica dell'informazione.

Infine, non si può ignorare il cambiamento dell'uomo all'interno del conflitto. Nella guerra classica il civile era una vittima collaterale o un osservatore passivo. Nella guerra ibrida, il cittadino comune è diventato, spesso a sua insaputa, un attore del conflitto.

Attraverso lo smartphone e l'uso dei social media, ogni individuo può diventare un vettore di propaganda (condividendo notizie false o polarizzanti) o un bersaglio di operazioni psicologiche. Questo significa che la difesa nazionale non può più essere delegata

¹⁴⁵ I deepfake sono media sintetici (video, audio o immagini) creati tramite intelligenza artificiale che sovrappongono o sostituiscono il volto o la voce di una persona con quella di un'altra in modo realistico. Originati dalla fusione di “deep learning” e “fake”, il termine è stato coniato nel 2017 e da allora il fenomeno ha sollevato preoccupazioni a livello globale per il suo potenziale di manipolazione della realtà. Sebbene nati per scopi goliardici, la tecnologia è diventata sempre più accessibile e realistica, sollevando seri dubbi etici e di sicurezza, rappresentando una minaccia crescente per la creazione di bufale, manipolazione politica e frodi finanziarie.

esclusivamente ai generali. La vera *linea del fronte* oggi passa per la consapevolezza critica di ogni singolo cittadino. La resilienza di una nazione si misura, dunque, sulla capacità del suo sistema educativo di formare menti capaci di riconoscere la manipolazione, rendendo la cultura e l'educazione civica i nuovi pilastri della sicurezza nazionale del XXI secolo.

In conclusione, la guerra ibrida ci obbliga a riconsiderare radicalmente il concetto di sicurezza. Non è più sufficiente investire in sistemi d'arma convenzionali per garantire l'integrità di una nazione; è necessario proteggere le reti, i dati e, soprattutto, il consenso sociale.

La tesi ha, dunque, dimostrato che l'ibridismo è la grammatica naturale di un mondo iperconnesso dove tutto, dall'energia ai flussi migratori, dai bit ai tribunali, può essere trasformato in un'arma. La sfida per le autorità politiche e strategiche del futuro non sarà quindi vincere una guerra, ma imparare a navigare in una crisi permanente, mantenendo fermi i principi di legittimità e libertà che la minaccia ibrida mira a distruggere.

BIBLIOGRAFIA E SITOGRAFIA DI RIFERIMENTO

BIBLIOGRAFIA

Aron R., *Il secolo della guerra totale*, Rizzoli, Milano 1954.

Aron R., *Pace e guerra tra le nazioni*, Edizioni di Comunità, Milano 1970.

Bauman Z., *Dentro la globalizzazione. Le conseguenze sulle persone*, Laterza, Roma-Bari 2001.

Blank S. J., *Russian Information Warfare: Past, Present, and Future*, Strategic Studies Institute, Carlisle 2017.

Buchanan B., *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Harvard University Press, Cambridge 2020.

Bull H., *La società anarchica. Uno studio sull'ordine nella politica mondiale*, Vita e Pensiero, Milano 2005.

Carr J., *Inside Cyber Warfare: Mapping the Cyber Underworld*, O'Reilly Media, Sebastopol 2011.

Chellaney B., *Debt-Trap Diplomacy*, in «Project Syndicate», 2017.

Clausewitz Carl von, *Della guerra*, a cura di E. Arbrile, Mondadori, Milano 1970.

Deutsch K., *The Analysis of International Relations*, Prentice-Hall, Englewood Cliffs 1968.

Dunlap Jr. C. J., *Law and Military Interventions: Preserving Humanitarian Values in 21st Century Conflicts*, Harvard University Carr Center for Human Rights Policy, Cambridge 2001.

Echevarria II A. J., *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy*, Strategic Studies Institute, U.S. Army War College, Carlisle 2016.

Erickson A. S., Kennedy C. M., *China's Maritime Militia*, in «CNA Conference Report», 2016.

Floridi L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano 2017.

- Gaddis J. L., *On Grand Strategy*, Penguin Books, New York 2018.
- Gagliano G., *Guerra cognitiva. Dalla guerra dell'informazione alle psicotecnologie*, Fuoco Edizioni, Roma 2020.
- Galeotti M., *The 'Gerasimov Doctrine' and Russian Non-Linear War*, in «In Moscow's Shadows», 2014.
- Galeotti M., *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, New Haven 2022.
- Gerasimov V., *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations*, trad. it. in «Military Review», 2016.
- Gostev A., Coalson R., *Russia's Paramilitary Mercenaries emerge from the Shadows*, in «Radio Free Europe/Radio Liberty», 2016.
- Greenhill K. M., *Weapons of Mass Migration: Forced Displacement, Coercion, and Foreign Policy*, Cornell University Press, Ithaca 2010.
- Herzog J., *Settling the Estonian Cyber Attacks: Lessons for the United States*, in «Journal of Strategic Security», Vol. 4, n. 1, 2011.
- Hoffman F. G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington 2007.
- Hoffman F. G., *Hybrid Warfare and Challenges*, in «Joint Force Quarterly», n. 52, 2009.
- Jean C., *Geopolitica*, Laterza, Roma-Bari 1995 (ed. aggiornata 2012).
- Jünger E., *La mobilitazione totale*, in *Foglie e fiori*, Adelphi, Milano 2003.
- Kaldor M., *Le nuove guerre. Violenza organizzata nell'età globale*, Carocci, Roma 1999.
- Kaplan R. D., *Asia's Cauldron: The South China Sea and the End of a Stable Pacific*, Random House, New York 2014.
- Kennedy D., *Of War and Law*, Princeton University Press, Princeton 2006.
- Khanna P., *Connectography: Le mappe del futuro ordine mondiale*, Fazi Editore, Roma 2016.
- Kilcullen D., *The Dragons and the Snakes: How the Rest Learned to Fight the West*, Oxford University Press, Oxford 2020.

- Kittrie O., *Lawfare: Law as a Weapon of War*, Oxford University Press, New York 2016.
- Kraska J., *Maritime Power and the Law of the Sea: Expeditionary Operations in World Politics*, Oxford University Press, Oxford 2011.
- Lawrence T. E., *I sette pilastri della saggezza*, Bompiani, Milano 1949.
- Levy M. A., *Asymmetric Warfare: Today's Challenge to US Military Power*, Cass Series on Contemporary Security Studies, London 2001.
- Liang Q., Xiangsui W., *Guerra senza limiti*, Libreria Editrice Goriziana, Gorizia 2001.
- Libicki M., *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, New York 2007.
- Liddell Hart B., *L'arte della guerra nel XX secolo*, Mondadori, Milano 1971.
- Lind W. S. et al., *The Changing Face of War: Into the Fourth Generation*, in «Marine Corps Gazette», Ottobre 1989.
- Mazarr M., *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Strategic Studies Institute, U.S. Army War College, Carlisle 2015.
- Mazziotti di Celso M., *Il diritto internazionale alla prova dei conflitti ibridi*, in «Rivista di Studi Politici», n. 4, 2019.
- McCuen J. J., *Hybrid Wars*, in «Military Review», Vol. 88, n. 2, 2008.
- Mumford A., *Proxy Warfare*, Polity Press, Cambridge 2013.
- Murray W., P. R. Mansoor (a cura di), *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, New York 2012.
- Neff S., *War and the Law of Nations: A General History*, Cambridge University Press, Cambridge 2005.
- Nye J., *Il paradosso del potere americano. Perché l'unica superpotenza non può fare da sola*, Einaudi, Torino 2002.
- Nye J., *The Future of Power*, PublicAffairs, New York 2011.
- Pomerantsev P., *Niente è vero, tutto è possibile*, Minimum Fax, Roma 2015.
- Renz B., *Russia and 'hybrid warfare'*, in «Contemporary Politics», Vol. 22, n. 3, 2016.

Schmitt C, Il nomos della terra nel diritto internazionale dello jus publicum europaeum, Adelphi, Milano 1991.

Smith M. L., Strategy: A History, Oxford University Press, Oxford 2013.

Smith R., L'arte della guerra nel mondo contemporaneo. La risposta dei popoli alle crisi di oggi, Il Mulino, Bologna 2009.

Singer P. W., Friedman A., Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, Oxford 2014.

Strachan H., The Direction of War: Contemporary Strategy in Historical Perspective, Cambridge University Press, New York 2013.

Sukhankin S., War, Business and Politics: The Case of the Wagner Private Military Company, in «Jamestown Foundation», 2019.

Sukhankin S., The 'Hybrid' Role of Russian Private Military Companies, in «The Jamestown Foundation», 2020.

Sun Tzu, L'arte della guerra, a cura di L. Maggio, Newton Compton, Roma 1994.

Walzer M., Guerre giuste e ingiuste. Un discorso morale con esemplificazioni storiche, Laterza, Roma-Bari 1990.

Yergin R., The New Map: Energy, Climate, and the Clash of Nations, Penguin Books, New York 2020.

SITOGRAFIA

<https://ccdcoe.org/library/publications/the-2007-cyber-attacks-on-estonia-ten-years-on/>

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018>

<https://mwi.westpoint.edu/lawfare-the-use-of-the-law-as-a-weapon-of-war/>

<https://research.checkpoint.com/2022/the-evolution-of-cyber-warfare/>

<https://www.cfr.org/blog/chinas-maritime-militia-what-it-and-why-it-matters>

[https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/603918/EPRS_ATA\(2017\)603918_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/603918/EPRS_ATA(2017)603918_EN.pdf)

<https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model-public-version/>

<https://www.theguardian.com/world/2022/may/04/the-wagner-group-the-mercenary-army-russia-uses-for-dirty-work>

<https://www.trellix.com/it-it/security-awareness/ransomware/what-is-stuxnet/>

NATO, Countering Hybrid Threats, in «NATO Topics», aggiornato al 2021 (www.nato.int)