LUISS Guido Carli

LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Corso di Laurea Triennale in Scienze Politiche

Corso di Relazioni Internazionali

Guerra algoritmica e strategie della visione: attori privati, immagini operative e la crisi del controllo umano

Prof. Raffaele Marchetti

_____

PROFESSOR

Silvia Caterina Minchella

_____

CANDIDATE

Academic Year: 2025 – 2026

Abstract

Obiettivo

La tesi esamina la trasformazione della guerra nell'era digitale, con particolare attenzione alla *guerra algoritmica* e al ruolo delle immagini non più come rappresentazioni, ma come dispositivi operativi che agiscono nei processi decisionali.

Metodo

L'analisi adotta tre lenti teoriche delle Relazioni internazionali: la *securitizzazione* per comprendere la costruzione dell'urgenza e la legittimazione dell'automazione; il *costruttivismo* per indagare come fiducia, norme e categorie di minaccia siano socialmente costruite; il *neofunzionalismo* per leggere i processi di integrazione e dipendenza tra pubblico e privato.

Campo e casi di studio

La ricerca ricostruisce il passaggio dalle immagini-matrice simboliche alle immagini operazionali (Farocki) e infine alle immagini algoritmiche (Paglen, Steyerl). Due casi emblematici illustrano queste dinamiche: il sistema *Lavender* a Gaza, che automatizza la produzione di target umani, e *MetaConstellation* di Palantir in Ucraina, che orchestra dati civili e militari per fornire *decision advantage*.

Risultati principali

Dai casi emerge che la guerra algoritmica non è un semplice aggiornamento tecnologico, ma una mutazione strutturale: le immagini producono azione, le corporation co-producono sovranità e il ruolo umano tende a ridursi a ratifica di output opachi. La tesi conclude che solo architetture istituzionali trasparenti e responsabili possono garantire che l'efficienza algoritmica non eroda legalità, proporzionalità e umanità della guerra.

Indice

INTRODUZIONE

Harun Farocki, Eye Machine III, © Harun Farocki, 2003.

Negli ultimi decenni l'esperienza della guerra ha conosciuto una trasformazione radicale, determinata dall'irruzione delle tecnologie digitali e dall'emergere di una nuova dimensione del conflitto: il cyberspazio[1]. Per secoli la riflessione strategica e la prassi militare hanno ruotato attorno alle tre dimensioni tradizionali della guerra, ovvero la terra, il mare e l'aria, a cui nel secondo dopoguerra si è aggiunta la dimensione extra-atmosferica. Ognuno di questi spazi ha portato con sé nuove sfide, ridefinendo i concetti di mobilità, potenza e controllo. Tuttavia, nessuno di essi sembra aver inciso in maniera così pervasiva e trasversale come la dimensione digitale, che non si presenta come un semplice campo operativo aggiuntivo, bensì come una realtà ibrida e onnipresente, capace di penetrare trasversalmente tutti gli altri ambiti e di ridisegnare le modalità stesse con cui la guerra è concepita, rappresentata e condotta[2]. Parlare di cyberspazio significa parlare di un terreno immateriale ma decisivo, in cui si intrecciano reti informatiche, infrastrutture critiche, flussi comunicativi, algoritmi predittivi e immagini ad alta e bassa risoluzione: un luogo in cui la superiorità non si misura più soltanto in termini di armamenti o truppe, ma soprattutto in termini di controllo e gestione dell'informazione. Questo spostamento non è avvenuto in modo improvviso, ma è il risultato di un processo iniziato già alla fine della Guerra Fredda, quando la rivoluzione informatica e la diffusione capillare delle tecnologie di rete hanno posto le basi per un nuovo modo di concepire la guerra[3]. Negli anni Novanta, la dottrina americana dell'information warfare ha segnato una prima svolta concettuale, individuando nella capacità di dominare i flussi informativi un elemento dirimente per il successo delle operazioni militari. La successiva elaborazione della "full spectrum dominance" e della "net-centric warfare" ha consolidato l'idea che l'informazione non fosse più soltanto un supporto logistico o un fattore ausiliario, ma la risorsa centrale attorno a cui si costruiscono strategie e tattiche. La guerra net-centrica, fondata sull'interconnessione di sensori, piattaforme e attori umani, si è configurata sempre più progressivamente come un ecosistema complesso in cui la rapidità di raccolta, elaborazione e

---

[1] Curiosamente, il neologismo "cyberspazio" è stato introdotto lontano dalle dimensioni epistemologiche qui discusse. Coniato dallo scrittore canadese William Gibson nell'ambito del cyberpunk, compare per la prima volta nel racconto *La notte che bruciammo Chrome* (*Burning Chrome*), pubblicato su *Omni* nel 1982, e viene poi consacrato dal romanzo *Neuromante* (*Neuromancer*, 1984), dove ne offre una definizione divenuta canonica. "Cyberspazio: un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici... Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano [...]". Vedi Martin Irvine, "Po-Mo SF: William Gibson's *Neuromancer* and Post-Modern Science Fiction," Technoculture, Georgetown University, rev. 12 gennaio 1997, archiviato su Internet Archive Wayback Machine (19 ottobre 2006), consultato il 26 agosto 2025.

[2] Vedi Luigi Martino, "La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale," *Politica & Società* 7, n. 1 (gennaio–aprile 2018): 61–76.

[3] Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: U.S. Army War College Press, 2015), 4.

diffusione dei dati è diventata il vero moltiplicatore di forza. L'informazione, in questo senso, non rappresenta più la realtà: la produce, la modella, la traduce in coordinate operative[4].

All'interno di questo quadro, un ruolo fondamentale è giocato dalle immagini. Se per lungo tempo esse hanno avuto la funzione di documentare, testimoniare o comunicare la guerra, oggi esse assumono una natura diversa: diventano dispositivi operativi. Non sono più destinate a uno spettatore umano, ma a una macchina; non servono a raccontare, ma ad agire. Harun Farocki, con la sua seminale intuizione delle immagini operazionali, aveva colto già diversi decenni fa come le immagini prodotte da sistemi di sorveglianza, da droni o da satelliti non avessero lo scopo di rappresentare un evento, ma di inserirsi direttamente nel processo decisionale e operativo[5]. Un'immagine satellitare non è pensata per essere contemplata, ma per essere incrociata con altre fonti, tradotta in dati, utilizzata per individuare un bersaglio. In questo senso, l'immagine non è più uno specchio del reale, ma un agente attivo che contribuisce a costruirlo. La trasformazione è profonda perché ridisegna il rapporto stesso tra visibilità e potere. Nel paradigma tradizionale, la capacità di vedere e di mostrare era connessa al controllo e alla legittimazione; nel paradigma digitale, invece, la visione diventa parte di un calcolo o calcolo essa stessa. Le immagini algoritmiche non passano più attraverso l'interpretazione umana, ma vengono immediatamente elaborate da sistemi di riconoscimento e da modelli predittivi. L'occhio umano non è più il destinatario, ma un passaggio secondario; il vero spettatore è la macchina. In questa logica, la decisione non è più fondata sulla comprensione, ma sulla correlazione: ciò che conta non è interpretare un contesto, ma individuare pattern, anticipare movimenti, generare previsioni. La razionalità strategica si ibrida così con la logica algoritmica, che riduce la complessità a probabilità e correlazioni, spesso opache e indecifrabili per chi ne subisce gli effetti.

Questa condizione genera una tensione epistemologica ed etica senza precedenti. Se il processo decisionale viene sempre più affidato a sistemi automatizzati, quale spazio rimane per il giudizio umano, per l'esperienza, per la responsabilità? L'operatore che si trova davanti a una dashboard algoritmica non è più chiamato a interpretare un'immagine o a valutare un'informazione, ma a confermare o meno un output prodotto da una macchina; la sua funzione si riduce spesso a un gesto minimo: un clic che convalida una scelta già predisposta altrove. Ciò che un tempo era il risultato di un ragionamento strategico diventa oggi un atto burocratico, un timbro che legittima una decisione di cui non si conosce appieno il processo. Il rischio evidente è la derealizzazione

[4] Stato Maggiore della Difesa, *La trasformazione net-centrica: Il futuro dell'interoperabilità multinazionale e interdisciplinare* (Roma: Stato Maggiore della Difesa, 2006), 6.
[5] Harun Farocki, "Phantom Images," *Public* 29 (2004): 18.

della guerra, in cui il conflitto appare come una sequenza di dati e di coordinate, e la deresponsabilizzazione degli attori umani, che si trovano a ratificare decisioni automatiche senza poterne discutere le premesse. In questa cornice il tema della fiducia acquista un rilievo centrale. Le guerre tradizionali erano fondate su catene di comando in cui la fiducia si stabiliva tra persone, tra comandanti e soldati, tra alleati che cooperavano in contesti incerti. Oggi la fiducia si sposta verso le macchine, verso la capacità dei sistemi distribuiti di funzionare senza errori anche in condizioni di complessità[6]. Modelli come il Byzantine Fault Tolerance, nati in informatica per garantire la coerenza dei sistemi anche in presenza di nodi inaffidabili, diventano metafore operative della guerra digitale. Fidarsi di un protocollo significa accettare che la verità sia stabilita dal calcolo, non dalla deliberazione umana; significa accettare che l'incertezza venga gestita non attraverso il dialogo o il dubbio, ma attraverso l'automatismo. È un cambiamento, un salto di paradigma che non riguarda soltanto la tecnica, ma il modo stesso in cui concepiamo la conoscenza, la responsabilità e la decisione[7].

Accanto a questa trasformazione epistemica, vi è un altro processo che ridisegna in profondità gli equilibri internazionali: la crescente centralità delle aziende tecnologiche private. Nel passato la guerra era considerata un monopolio degli Stati: essi possedevano le armi, controllavano le infrastrutture, detenevano il potere legittimo di dichiarare conflitti e negoziare trattati. Oggi, tuttavia, le capacità decisive si trovano sempre più spesso nelle mani di attori privati. Sono le corporation tecnologiche a sviluppare i software di analisi, a gestire le piattaforme di sorveglianza, a controllare le infrastrutture cloud che permettono la raccolta e l'elaborazione dei dati. In molti casi, sono loro a determinare quali tecnologie siano disponibili, con quali condizioni, con quali limiti. La guerra digitale, in questo senso, non è solo un conflitto tra Stati, ma anche un terreno in cui si ridefinisce il rapporto tra pubblico e privato. La dipendenza degli Stati da queste aziende è evidente. In Ucraina, ad esempio, la capacità di resistere agli attacchi cibernetici russi e di mantenere operative le infrastrutture critiche è stata resa possibile anche grazie al supporto di aziende come Microsoft, che ha fornito sistemi di difesa, e Palantir, che con la sua piattaforma MetaConstellation ha reso possibile l'integrazione di dati commerciali e governativi in tempo reale[8]. Questo tipo di collaborazione ha permesso all'Ucraina di avere una visione più chiara e

---

[6] Vedi Francesco Simonetti e Laura Tripodi, "Automation and the Future of Command and Control," *Journal of Advanced Military Studies* 11, no. 1 (Spring 2020): 145–164.

[7] Per un testo di chiarimento sul caso dei generali bizantini vedi Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems* 4, no. 3 (July 1982): 382–401.

[8] "Ai powered automation for every decision" è la tagline pubblicitaria che si può trovare sul sito internet di Palantir. Palantir Technologies. *Palantir Technologies Official Website*. Accessed August 26, 2025. https://www.palantir.com/.

immediata del campo di battaglia, di anticipare i movimenti delle truppe russe e di coordinare le proprie risposte. Ma il prezzo di questa dipendenza è alto: significa che una parte fondamentale della strategia nazionale dipende da tecnologie proprietarie, sviluppate da aziende che non rispondono a logiche democratiche, ma a interessi commerciali. La stessa questione si pone in Medio Oriente, dove l'utilizzo del sistema Lavender da parte di Israele ha sollevato enormi preoccupazioni etiche e legali[9]. Questo software, in grado di selezionare algoritmicamente i bersagli, riduce la supervisione umana a un ruolo marginale, trasformando l'operatore in un semplice esecutore. I rischi di errori e di danni collaterali sono altissimi, e con essi le responsabilità che nessuno sembra voler assumere.

La domanda che attraversa queste dinamiche è dunque cruciale: *quale ruolo rimane per le relazioni umane nelle decisioni strategiche, quando esse vengono sempre più mediate e sostituite da immagini automatizzate e da algoritmi opachi?* Non si tratta soltanto di un problema tecnico o militare: è una questione politica ed etica che riguarda il futuro delle relazioni internazionali. La guerra digitale, infatti, non ridefinisce soltanto le modalità del conflitto, ma anche i rapporti di potere tra Stati e corporation, tra cittadini e istituzioni, tra esseri umani e sistemi artificiali. Se il potere di decidere della vita e della morte, della pace e della guerra passa attraverso algoritmi proprietari gestiti da attori privati, si apre una frattura che mette in discussione i fondamenti stessi della sovranità e della responsabilità democratica. La tesi che qui si propone intende affrontare questo scenario complesso con un approccio interdisciplinare. L'obiettivo non è soltanto descrivere le trasformazioni in atto, ma anche interpretarle alla luce delle teorie delle relazioni internazionali e della teoria critica delle immagini.

Questa tesi si propone di aprire uno spazio di riflessione sulle trasformazioni in corso, mostrando come la guerra digitale non possa essere considerata un semplice aggiornamento tecnologico, ma un cambiamento strutturale che investe le categorie stesse con cui pensiamo la guerra e la politica internazionale. È un cambiamento che riguarda la conoscenza, la fiducia, la responsabilità, il rapporto tra pubblico e privato, tra umano e artificiale. Comprenderlo significa non solo analizzare le nuove forme del conflitto, ma interrogare il futuro dell'ordine internazionale, le possibilità di mantenere un controllo consapevole sull'uso della forza e la necessità di elaborare nuove forme di responsabilità e trasparenza. La scelta di adottare, nell'introduzione metodologica, tre lenti

[9] Questa tesi analizzerà in modo comparato una pluralità di fonti: da quelle istituzionali (report NATO, EDA, IISS, documenti di policy), alle fonti OISINT e giornalistiche (articoli di +972 Magazine, The Guardian, Just Security), fino ai riferimenti tecnico-industriali, con l'obiettivo di ricostruire in maniera critica il caso "Lavender" e, più in generale, i meccanismi attraverso cui sistemi algoritmici vengono integrati nelle pratiche di sorveglianza e targeting militare.

teoriche – securitizzazione, neofunzionalismo e costruttivismo – risponde a questa esigenza. La securitizzazione di Barry Buzan consente di seguire il processo attraverso il quale un tema diventa minaccia esistenziale e legittima l'adozione di misure straordinarie. Applicata al dominio digitale, questa lente mostra come l'urgenza costruita discorsivamente trasformi tecnologie nate per scopi civili in strumenti di sopravvivenza nazionale, ridefinendo così i confini del lecito e dell'eccezionale[10]. Il costruttivismo di Alexander Wendt permette di cogliere come la fiducia, le identità e le categorie con cui leggiamo il conflitto siano il risultato di pratiche sociali e linguistiche: non è la macchina a essere neutrale, ma il linguaggio che la circonda a renderla "affidabile" o "indispensabile". In questo senso, i concetti di decision advantage o di junior militants non descrivono semplicemente realtà operative, ma producono effetti politici e normativi[11].

Il neofunzionalismo di Ernst Haas offre infine una chiave per comprendere l'integrazione tecnica e istituzionale tra settori civili e militari: lo spill-over funzionale spinge a condividere standard, interfacce, procedure, e conduce progressivamente a un'armonizzazione che consolida dipendenze tra Stati, industrie e attori privati[12]. Ma proprio qui emergono i limiti della teoria. Pensata per l'integrazione europea e per processi cooperativi, essa rischia di apparire fuorviante quando viene applicata al dominio bellico, dove le dinamiche di integrazione non mitigano i conflitti ma li amplificano, e dove la logica funzionale tende a normalizzare pratiche che possono violare i principi fondamentali del diritto internazionale umanitario. In Ucraina, la dipendenza da corporation tecnologiche non è il frutto di una naturale progressione integrativa, ma la conseguenza di un contesto di emergenza che spinge verso l'adozione di soluzioni proprietarie. A Gaza, lo stesso paradigma rischia di mascherare come "spill-over inevitabile" ciò che è in realtà il prodotto di rapporti di forza coloniali e di pratiche di occupazione. Per questo la lente neofunzionalista, pur utile a descrivere meccanismi di standardizzazione e lock-in tecnologico, deve essere impiegata con cautela critica, come strumento euristico e non come spiegazione teleologica.

Questa triangolazione teorica – securitizzazione, neofunzionalismo, costruttivismo – consente dunque di restituire la complessità della guerra algoritmica[13] senza cadere né nel tecnicismo

---

[10] Barry Buzan, Ole Wæver e Jaap de Wilde, *Sicurezza. Una nuova struttura per l'analisi* (Roma: Luiss University Press, 2017).
[11] Alexander Wendt, *La politica internazionale come costruzione sociale* (Milano: Vita e Pensiero, 2001).
[12] Ernst B. Haas, *L'unificazione dell'Europa. Forze politiche, sociali ed economiche, 1950-1957* (Bologna: Il Mulino, 1970).
[13] Il termine *algorithmic warfare* pare emergere nel contesto del Project Maven del Dipartimento della Difesa statunitense, come illustrato in David L. Woods, "Algorithmic Warfare: Applying Artificial Intelligence to

descrittivo né nella retorica della rivoluzione ineluttabile. Ognuna delle tre prospettive illumina un lato del problema e, al tempo stesso, mostra i propri limiti: la securitizzazione rischia di riprodurre la logica emergenziale che analizza; il neofunzionalismo di naturalizzare scelte politiche e militari come progressioni inevitabili; il costruttivismo di sottovalutare gli effetti materiali delle pratiche discorsive. La loro combinazione permette però di tenere insieme un quadro generale, rivelando come l'uso di tecnologie algoritmiche in guerra non riguardi soltanto la ricerca di efficienza, ma tocchi invece la sostanza delle categorie politiche e giuridiche su cui si regge l'ordine internazionale. In ultima analisi, ciò che è in gioco è la capacità delle società democratiche di governare processi sempre più opachi, nei quali la decisione politica rischia di dissolversi nell'automatismo algoritmico. La domanda non è se adottare o meno queste tecnologie, ma come incardinarle in architetture istituzionali che preservino trasparenza, tracciabilità e responsabilità. Solo così sarà possibile evitare che l'efficienza tecnica diventi un eufemismo per deresponsabilizzazione politica, e che il giudizio umano – ridotto a un clic – perda il suo ruolo essenziale di garante della proporzionalità, della legalità e, in definitiva, dell'umanità della guerra.

Il campo di ricerca della tesi si concentra sul ruolo delle immagini nella configurazione della guerra contemporanea, mostrando come esse abbiano progressivamente abbandonato la funzione tradizionale di rappresentazione per trasformarsi in dispositivi operativi. Un primo livello è quello delle immagini-matrice, figure visive ricorrenti che agiscono come coordinate simboliche capaci di strutturare la percezione politica globale. Queste immagini, lungi dall'essere semplici illustrazioni, svolgono una funzione epistemica: definiscono ciò che può essere visto e ciò che rimane invisibile, distribuiscono ruoli e valori, orientano le interpretazioni del conflitto. Seguendo la traccia ispiratrice di Jacques Rancière, è possibile leggere le immagini-matrice come parte di una "distribuzione del sensibile" che conferisce legittimità o marginalità a soggetti e narrazioni, contribuendo a rendere alcune guerre pensabili e altre impensabili[14]. A questa dimensione simbolica si affianca quella delle immagini operazionali, concettualizzate da Harun Farocki e riprese da Jans Eder e Charlotte Klonk[15]. Esse non sono destinate allo sguardo umano, ma entrano direttamente nei processi tecnici e militari come input, interfacce o nodi di calcolo. L'immagine

Warfighting," *Military Review* 98, no. 5 (2018): 81–89. La sua diffusione in ambito accademico è analizzata da Louise Amoore, Marijn Hoijtink e Daniel Lambach, "Innovating Algorithmic Warfare: Experimentation with Information Manoeuvre beyond the Boundaries of the Law," *Global Policy* 15, no. S1 (2024): 28–40, che nota come l'espressione sia ormai "increasingly coined 'algorithmic warfare.'"

[14] Jacques Rancière, *La partizione del sensibile. Estetica e politica* (Roma: DeriveApprodi, 2007), 12.

[15] Jens Eder and Charlotte Klonk, eds., *Image Operations: Visual Media and Political Conflict*, 1st ed. (Manchester: Manchester University Press, 2017)

satellitare che guida un missile o la visualizzazione sintetica di una dashboard operativa non rappresentano un evento, lo producono. La genealogia teorica che va da Flusser a Virilio fino a Farocki mostra come il visivo si sia progressivamente spostato dal dominio estetico a quello operativo, con implicazioni profonde sul rapporto tra percezione, decisione e potere.

Questo processo raggiunge il suo punto più radicale con la categoria di immagine algoritmica. Qui il visibile non è più pensato per l'uomo, ma per la macchina: immagini prodotte, consumate ed elaborate da algoritmi che le trattano come dati, input di un calcolo predittivo. Paglen, Steyerl e Apprich hanno mostrato come queste immagini, spesso invisibili all'occhio umano, costituiscano la nuova infrastruttura visiva della guerra digitale[16]. Dataset, riconoscimento facciale, classificazioni automatiche e generazioni sintetiche non servono a comunicare, ma a orientare azioni letali, a costruire liste di target, a determinare il confine tra civile e combattente. L'immagine diventa così evento computazionale: non un oggetto da interpretare, ma un nodo funzionale in catene operative che riducono la complessità a probabilità e correlazioni. Questa trasformazione è approfondita attraverso il concetto di image operations, che mette in luce il doppio registro dell'operatività visiva. Da un lato vi sono le immagini "fredde", prodotte per essere elaborate da macchine e operatori addestrati, come flussi radar, telemetrie o interfacce di targeting. Dall'altro lato vi sono le immagini "calde", destinate allo spazio pubblico, che mobilitano emozioni e consenso attraverso propaganda, giornalismo o attivismo[17]. Queste due sfere non restano separate, poiché le immagini pensate per le macchine finiscono per alimentare campagne mediatiche, mentre quelle pensate per il pubblico rientrano nei dataset che addestrano sistemi algoritmici. L'operatività dell'immagine è dunque al tempo stesso tecnica e affettiva, fredda e calda, e il suo potere si manifesta tanto nel calcolo militare quanto nell'economia dell'attenzione.

La sezione successiva introduce il concetto di nuova ecologia bellica, legato alla logica della military-civil fusion. Le innovazioni tecnologiche non nascono più primariamente negli apparati militari, ma nel settore civile e commerciale, per poi essere integrate e riadattate alla guerra. Cloud, intelligenza artificiale, big data, infrastrutture di rete e sensori dual use alimentano allo stesso

---

[16] Vedi Clemens Apprich, Wendy Hui Kyong Chun, Florian Cramer, and Hito Steyerl, *Pattern Discrimination* (Lüneburg: meson press, 2018) per un'analisi a otto mani su come algoritmi e tecniche di riconoscimento di pattern producano nuove forme di discriminazione e potere, mostrando il passaggio da una cultura della rappresentazione a una cultura dell'operazione.

[17] L'eredità di Marshall McLuhan, sociologo dei media, primo a teorizzare la dialettica tra media "caldi" e "freddi" come strumenti per orientarsi nei paesaggi comunicativi, si avverte implicitamente anche in questo contesto epistemologico: l'odierno ecosistema digitale può essere letto come un'estensione e al tempo stesso una riconfigurazione di quella sensibilità mediale. Si veda Marshall McLuhan, *Gli strumenti del comunicare* (Milano: Il Saggiatore, 1967).

tempo la vita quotidiana e le operazioni belliche. La guerra algoritmica non è quindi confinata a un dominio militare separato, ma si distribuisce nell'intero tessuto socio-tecnico, ibridando continuamente pratiche civili e logiche belliche. Questa fusione sposta il baricentro del potere: attori privati, corporation tecnologiche e infrastrutture industriali diventano parti costitutive delle capacità militari, rendendo sempre più difficile distinguere tra governance civile, controllo securitario e strategia di guerra. Infine, la riflessione si concentra sul ruolo dell'umano di fronte all'AI. L'intelligenza artificiale è interpretata come tecnologia della predizione: rende meno costosa e più rapida l'anticipazione degli eventi, ma non sostituisce la decisione. Piuttosto, la trasforma, comprimendo i tempi del ciclo osserva-orienta-decidi-agisci e spostando il ruolo umano dalla valutazione strategica alla ratifica di output algoritmici. In questo contesto il problema non è solo tecnico, ma epistemologico e politico: che cosa resta della responsabilità e del giudizio quando la macchina presenta già la decisione come pronta? Gli studi richiamati mostrano che la sfida non è mantenere simbolicamente "l'uomo nel loop", ma progettare istituzioni e procedure che garantiscano un controllo effettivo sul ciclo decisionale, evitando che l'automatismo algoritmico dissolva la possibilità di deliberazione. Il campo di ricerca, così articolato, mette in luce che la guerra algoritmica non è un semplice aggiornamento tecnologico, ma una mutazione strutturale. Mentre le immagini, in tutte le loro forme – matrice, operazionali, algoritmiche – non documentano più soltanto il conflitto, ma lo rendono possibile, le infrastrutture civili e digitali non restano ai margini, ma diventano architetture belliche; il ruolo umano intanto non scompare, ma viene ridisegnato in modi che rischiano di ridurlo a un gesto minimo di validazione. Comprendere queste trasformazioni significa interrogare i fondamenti stessi della conoscenza, della fiducia e della responsabilità in guerra, in un'epoca in cui la decisione politica e militare rischia di essere sempre più catturata dalla logica impersonale del calcolo.

Nei casi studio la tesi analizza due contesti emblematici in cui le logiche della guerra algoritmica si sono concretizzate: l'impiego del sistema Lavender a Gaza e il ruolo di Palantir in Ucraina. Nel primo caso, l'attenzione è rivolta alla trasformazione del targeting israeliano in seguito al 7 ottobre 2023: attraverso Lavender e strumenti correlati come Gospel e Where's Daddy?, l'identificazione dei bersagli avviene in gran parte per via algoritmica, traducendo comportamenti quotidiani e dati biometrici in punteggi di rischio e generando liste di obiettivi con una supervisione umana minima. L'analisi mostra come queste pratiche sollevino gravi questioni rispetto ai principi di distinzione, proporzionalità e precauzione del diritto internazionale umanitario, e come il linguaggio tecnico produca una digital dehumanization, trasformando persone in variabili statistiche. Il caso ucraino offre invece un quadro differente: con MetaConstellation, Palantir ha orchestrato in tempo quasi

reale dati eterogenei – satelliti commerciali, sensori radar, flussi civili e militari – riducendo il ciclo sensor-to-shooter e fornendo alle forze ucraine un vantaggio cognitivo e organizzativo. Qui l'automazione non genera direttamente liste di target individuali, ma costruisce un quadro operativo integrato, mostrando come l'integrazione pubblico-privato e l'uso di infrastrutture civili abbiano ridefinito la condotta del conflitto. Il confronto tra i due casi consente di osservare la duplice traiettoria della guerra algoritmica: in Ucraina l'automazione si manifesta come infrastruttura di fusione e supporto alla decisione, mentre a Gaza come motore selettivo che standardizza e accelera la produzione di target umani, in entrambi i casi mettendo in discussione i confini tra civile e militare, tecnica e politica, calcolo e giudizio.

METODOLOGIA

Harun Farocki, Eye Machine I, © Harun Farocki, 2001.

1.1 Introduzione metodologica

Come si accennava nell'introduzione, parlare di guerra nell'odierno ecosistema digitale significa interrogare una trasformazione che non riguarda soltanto l'armamento o i teatri cinetici, ma investe il nesso tra conoscenza, potere e violenza. In questo quadro, ha preso piede l'espressione "guerra algoritmica": non per dire che le guerre siano "combattute dagli algoritmi", bensì per indicare che gli algoritmi stanno diventando grammatiche di percezione e di azione, strumenti che stimano probabilità, selezionano ciò che conta, scandiscono ritmi e comprimono il ciclo osserva-orienta-decidi-agisci[18]. In questo contesto, l'intelligenza artificiale effettivamente dispiegabile oggi – statistica, modulare, addestrata a compiti circoscritti – non sostituisce la decisione umana; rende meno costosa la predizione e, proprio per questo, accresce il valore e la contendibilità degli altri due elementi che la decisione richiede: dati e giudizio. Questa tesi adotta un'impostazione descrittivo-esplorativa e intende mostrare come la dimensione bellica odierna si organizzi sempre più come infrastruttura cognitiva e logistica fatta di dati, modelli, reti e immagini che raccolgono tracce ordinarie della vita connessa e le traducono in priorità operative o ingaggio.

Questa riconfigurazione cognitiva ha una geografia. Il cyberspazio, spesso descritto come "quinto dominio" dell'azione strategica, non è un'astrazione eterea ma un ambiente stratificato in cui livelli fisici, logico-informatici e sociali si condizionano a vicenda. Sopra questo sostrato fisico operano protocolli e reti di pratiche sociali e decisionali dove persone e macchine interagiscono in tempo reale. La "neutralità" del digitale non è neutra, perché dipende da infrastrutture materiali. Scegliere standard operativi o criteri di certificazione dell'origine dei dati significa decidere in anticipo che cosa è visibile e, se necessario, poter attivare o interrompere i flussi che lo rendono operativo. Oggi che il confine tra pace e guerra è poco chiaro, molto avviene in una "zona grigia": spionaggio, piccoli sabotaggi e campagne d'informazione per attirare o spostare l'attenzione[19]. Come osserva Joseph Nye, nell'era informazionale il potere non solo transita tra grandi potenze, ma si diffonde lungo reti dove anche attori non statali incidono su sicurezza e instabilità[20]. Gli effetti si sentono nella vita quotidiana, perché le stesse reti che usiamo per luce, ospedali e consegne possono essere usate come canali di attacco o diventare obiettivi. Nell'era dell'informazione il potere è più diffuso: non agiscono solo gli Stati, ma anche aziende tecnologiche, gruppi e perfino singole persone,

[18] Per un'introduzione al concetto vedi John Boyd, *A Discourse on Winning and Losing* (Maxwell Air Force Base, AL: Air University, 1987), 383; vedi anche International Institute for Strategic Studies, *Software-Defined Defence* (London: IISS, 2023), 25.
[19] Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: U.S. Army War College Press, 2015), 55.
[20] Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011), 135.

grazie al digitale a basso costo che facilita l'accesso e la circolazione dei dati. Da qui due conseguenze: gli Stati fanno più fatica a controllare processi che superano i confini e dipendono da attori fuori dalla loro catena di comando, e le società sono più esposte perché reti elettriche, ospedali e logistica diventano superfici d'attacco.

Non stupisce, dunque, che molte dottrine collocano oggi il cyberspazio tra i domini operativi, anche in quanto l'adozione di AI promette vantaggi innanzitutto informazionali: rilevamento precoce di anomalie, correlazione di segnali eterogenei, prioritizzazione di allarmi, triage di flussi video e telemetrici, supporto a pianificazione e logistica predittiva. Promesse reali, ma condizionate dall'ambiente avversario e adattivo in cui vengono dispiegate: dataset sporchi o deliberatamente inquinati, spostamento di dominio tra addestramento e impiego, attacchi mirati agli stessi modelli, oltre al rischio cognitivo di "overtrust" verso interfacce che restituiscono punteggi e *heatmap* con un'aura di oggettività non meritata[21]. A ciò si aggiunge una crescente opacità delle catene di responsabilità: quando la predizione è prodotta e veicolata da filiere industriali private, integrate con reti pubbliche e militari, la domanda su chi definisca soglie, pesi e priorità non è soltanto tecnica ma eminentemente politica. La conseguenza riguarda la forma stessa della decisione. Se la guerra algoritmica tende a riformulare il dubbio in termini probabilistici, molte scelte cruciali si spostano sul terreno di "quanto credere" a una stima e "quando agire" alla luce di essa. Di qui l'importanza, di cui la letteratura recente offre ampia testimonianza, di una struttura istituzionale organica capace di rendere visibile l'incertezza, governare la velocità, tracciare le decisioni e mettere in conto il fallimento; un'ecologia, cioè, che rafforzi il ruolo dell'umano non come freno simbolico ma come garante di senso, proporzionalità e legittimità. Su questo sfondo, l'immagine assume una centralità particolare. Come si accennava, le "immagini operative" che alimentano targeting, sorveglianza e simulazione convivono con immagini "calde" che agiscono nello spazio pubblico orientando attenzione ed emozioni. L'AI che riconosce volti, oggetti, pattern di movimento, alimenta entrambe le sfere e le intreccia: dataset addestrati su flussi commerciali e sociali ritornano come presupposti di decisioni di sicurezza, mentre l'estetica di dashboard e video geolocalizzati traduce in persuasione ciò che nasce come misura.

Come si relazionano le teorie di Relazioni Internazionali al campo qui introdotto? In che modo il realismo coglie la competizione per il vantaggio informativo, i dilemmi di deterrenza nella "zona

[21] International Committee of the Red Cross. "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach." *International Review of the Red Cross* 102, no. 913 (2021): 475.

grigia" e la protezione delle infrastrutture; fino a che punto il liberalismo istituzionale spiega standard, regimi e coordinamento tra attori pubblici e privati; che cosa rivelano costruttivismo e studi critici sulla costruzione di minacce e responsabilità e sull'effetto performativo di dati e immagini? La tesi cerca il proprio contributo specifico non mediante un elenco di applicazioni o un esercizio di teoria pura, ma mediante un ponte argomentato tra categorie classiche delle Relazioni internazionali e descrizioni dell'attuale status quo secondo un modello deliberatamente riflessivo ed esplorativo. Per abbracciare questa complessità, adotto un approccio duplice: da un lato seguo una linea teorico-concettuale, usando alcune categorie classiche delle Relazioni internazionali (ad es. sicurezza, minaccia, fiducia, interdipendenza) per definire le domande e i termini dell'analisi; dall'altro, metto alla prova queste categorie su un insieme di materiali prodotti da attori rilevanti.

1.2. La prima dimensione: la securitizzazione come lente per leggere il cambio di paradigma

Nel lessico delle Relazioni Internazionali, "securitizzazione" indica il processo attraverso cui un tema viene presentato come minaccia esistenziale e, per questo, spostato dal terreno della "politica normale" a quello delle misure straordinarie. L'idea, resa nota dalla cosiddetta Scuola di Copenaghen[22], mette in relazione parole, immagini e decisioni: non basta dire "c'è un pericolo", occorre che un pubblico riconosca quella definizione e accetti che, in nome della sicurezza, si possano adottare strumenti eccezionali rispetto alle regole ordinarie. La dinamica è semplice da descrivere: un attore autorevole (governo, autorità, organizzazione) enuncia una minaccia che colpirebbe un "oggetto di riferimento" da proteggere (lo Stato, la popolazione, infrastrutture critiche, l'ordine internazionale); un'audience rilevante (parlamento, opinione pubblica, alleati) considera credibile quella minaccia; sulla base di tale consenso si aprono budget dedicati, si creano unità organizzative, si approvano norme, standard e procedure che consentono di agire più in fretta o con poteri più ampi. Come evidenziato da Didier Bigo, in questo passaggio contano non solo i discorsi ufficiali, ma anche i materiali che li rendono convincenti: dati, mappe, immagini e indicatori che danno forma visibile al pericolo[23].

---

[22] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner, 1998), 23–25.

[23] Bigo, tra i principali esponenti della cosiddetta "Paris School", amplia il modello copenaghense mostrando che la securitizzazione non dipende soltanto da discorsi ufficiali, ma anche da pratiche professionali, apparati tecnologici, statistiche e immagini che producono una "governamentalità dell'inquietudine". In questo senso, dati, mappe e

La securitizzazione è utile perché offre una traccia per seguire come un problema diventa "problema di sicurezza" e con quali effetti politici. Permette di collegare dichiarazioni pubbliche e decisioni concrete, spiegando perché certe priorità entrano in agenda e perché alcune pratiche – sorveglianza, controllo, restrizioni – vengono normalizzate. Consente inoltre di interrogare la responsabilità: chi definisce le soglie di allarme, chi decide, chi risponde degli esiti. La letteratura ne segnala anche i limiti: il rischio di trasformare troppi temi in emergenze; l'eccesso di attenzione al linguaggio rispetto alle pratiche materiali; possibili *bias* nell'individuare che cosa e chi meriti protezione. Per questo, accanto all'analisi dei discorsi, cresce l'attenzione a come la securitizzazione avvenga "nei fatti": nelle interfacce con cui si visualizzano i rischi, negli standard tecnici, nelle procedure operative quotidiane. Nel contesto digitale e della cosiddetta "guerra algoritmica", la categoria diventa particolarmente feconda. La definizione delle minacce passa anche per modelli predittivi, punteggi di rischio e immagini operative che orientano priorità e tempi di reazione; attori pubblici e privati condividono dati e infrastrutture, rendendo più sfumati confini e responsabilità. Guardare alla securitizzazione in questo scenario significa chiedersi come dati e immagini costruiscono la credibilità della minaccia, come vengono accettati da pubblici diversi, quali misure abilitano e con quali garanzie per controllo umano, proporzionalità e trasparenza. In questo modo, la tesi può usare la securitizzazione come cornice chiara per descrivere, senza tecnicismi inutili, il percorso che porta dall'enunciazione del pericolo alle decisioni che incidono su sicurezza e libertà.

Assumere la securitizzazione come prima chiave metodologica significa partire dall'idea, oggi ampiamente condivisa nella letteratura, che "sicurezza" non designi una categoria naturale e stabile, bensì un esito contingente di pratiche discorsive e istituzionali attraverso le quali determinati attori riescono a presentare una questione come minaccia esistenziale e, ottenendo il consenso di un pubblico rilevante, a giustificare misure straordinarie rispetto al repertorio ordinario della politica. Ciò consente di alzare lo sguardo oltre l'armamentario concettuale del rischio tecnico o della gestione aziendale del pericolo e di osservare come, nel passaggio al digitale, molti fenomeni prima trattati come problemi di efficienza o di *compliance* vengano riformulati entro un lessico di urgenza che abilita eccezioni procedurali, ridefinisce competenze e crea nuove asimmetrie di potere. In questo senso, la securitizzazione non è soltanto una teoria sull'uso politico del linguaggio, ma un dispositivo analitico che permette di ricostruire la filiera

indicatori non sono semplici supporti retorici, ma diventano parte costitutiva della produzione sociale della minaccia. Vedi Didier Bigo, "Security and Immigration: Toward a Critique of the Governmentality of Unease," *Alternatives: Global, Local, Political* 27, no. 1 (2002): 63–65.

che va dallo "speech act" alla norma, dall'enunciazione della minaccia alla sua istituzionalizzazione in apparati, budget, standard e procedure. Trasportata nel terreno digitale, la lente copenaghense chiede innanzitutto di mappare gli attori che compiono mosse "securitizzanti" e i pubblici che le accolgono o le respingono. Non si tratta più soltanto di governi, ministeri della difesa o organizzazioni internazionali, ma di un ecosistema in cui agenzie civili, autorità di regolazione, forze dell'ordine, grandi piattaforme tecnologiche, fornitori di infrastrutture critiche e consorzi industriali competono e cooperano nel definire quali eventi meritino l'etichetta di minaccia esistenziale e quali contromisure siano necessarie. La scelta di qualificare il furto di dati, il sabotaggio a sistemi di controllo industriale o le campagne di disinformazione come questioni di sicurezza nazionale, invece che come mere violazioni contrattuali o problemi reputazionali, non è mai neutrale: essa abilita, ad esempio, la possibilità di mobilitare strumenti investigativi invasivi, di estendere l'obbligo di segnalazione a soggetti privati, di imporre standard tecnici vincolanti, di restringere l'accesso a tecnologie sensibili e di riorientare risorse pubbliche verso capacità di difesa cibernetica e di analisi algoritmica[24]. Per comprendere quando e come questa trasformazione avvenga, la metodologia proposta isola alcuni elementi ricorrenti del processo di securitizzazione e li traduce in variabili osservabili. Il primo è l'identificazione del *referent object*, cioè di ciò che si pretende di salvaguardare: nel dominio digitale non si tratta solo dell'integrità territoriale o della vita dei cittadini, ma anche della continuità operativa di funzioni essenziali, dell'affidabilità delle catene del valore, della sovranità sui dati e della fiducia collettiva nelle interfacce che mediano transazioni e decisioni. Il secondo è la costruzione narrativa della minaccia, che spesso combina elementi tecnici (vulnerabilità di protocolli, dipendenze da fornitori, possibilità di attacchi combinati) con frame simbolici che evocano l'eccezionalità del pericolo, accelerando i tempi dell'azione e legittimando deroghe a procedure ordinarie. Il terzo è l'indicazione di misure straordinarie – e qui la straordinarietà è da intendersi non solo rispetto all'intensità dell'intervento, ma anche rispetto alla sua natura –, che può consistere nella centralizzazione di funzioni di risposta, nella militarizzazione di alcuni compiti di protezione, nella delega a soggetti privati di

[24] Nella letteratura sull'aggiornamento della teoria della securitizzazione si possono in quest'ottica considerare ciò che analizza Balzacq: come la securitizzazione non sia riducibile al solo "speech act", ma si sviluppi in un processo complesso che coinvolge attori pubblici e privati, audience differenziate, pratiche istituzionali e dispositivi tecnici - vedi Thierry Balzacq, ed., *Securitization Theory: How Security Problems Emerge and Dissolve* (London: Routledge, 2011) - e anche Huysmans che, invece, mostra come la securitizzazione funzioni intrecciando paure, procedure e dispositivi tecnici, andando oltre il solo discorso politico - vedi Jef Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU* (London: Routledge, 2006).

responsabilità tipicamente pubbliche o, all'opposto, nell'ingresso dello Stato in domini prima lasciati al mercato.

L'adozione della lente "securitizzante" si giustifica inoltre, sul piano metodologico, perché consente di seguire il passaggio cruciale che collega la sfera del discorso alla sfera dell'organizzazione. Una volta osservato che un certo tipo di attacco informatico, ad esempio, viene descritto come minaccia esistenziale – perché mette a rischio dinamiche come la fornitura di energia, la circolazione dei pagamenti, la tenuta di elezioni o l'integrità di basi dati sanitarie – è possibile verificare se e come questa descrizione venga internalizzata sotto forma di procedure, requisiti, catene di responsabilità e nuovi centri decisionali. In altri termini, la securitizzazione non finisce con lo *speech act*; essa inizia con esso e prosegue nella materialità di nuovi centri di fusione dati, sale operative con capacità di analisi predittiva, obblighi di condivisione informativa tra pubblico e privato, regimi sanzionatori e programmi di ricerca e sviluppo orientati verso l'automazione della *detection* e della risposta. Il vantaggio di questa impostazione, rispetto a un approccio puramente tecnologico, è duplice. Da un lato, permette di leggere la sovrapposizione dei "settori" della sicurezza che la Scuola di Copenaghen elenca – politico, militare, economico, societario, ambientale, informazionale – mostrando come, nel digitale, essi si intreccino in modo quasi inestricabile: per fare un esempio, un attacco che colpisce un fornitore di servizi cloud è al tempo stesso un problema economico, informazionale e politico, e il modo in cui viene raccontato ai decisori e all'opinione pubblica ne determina la traiettoria regolatoria e istituzionale. Dall'altro lato, la lente rende visibile il ruolo dell'audience: la securitizzazione riesce quando un pubblico dotato di potere accetta la definizione della minaccia e l'agenda di eccezioni che ne consegue; fallisce o devia quando tale accettazione non avviene, oppure quando emergono contro-narrazioni che riportano l'issue nell'alveo della normalità amministrativa[25].

Poiché la sicurezza digitale tocca infrastrutture che sono in larga parte possedute, gestite e innovate da attori privati, la teoria della securitizzazione va qui letta insieme a una sociologia dell'interdipendenza tra pubblico e privato. Le mosse securitizzanti non si limitano a chiedere più potere allo Stato; spesso chiedono più responsabilità e più obblighi a soggetti non statali, che diventano *proxies* dell'autorità pubblica nella sorveglianza, nella prevenzione e nella risposta.

[25] Claudia Aradau osserva che la desecuritizzazione non coincide semplicemente con un ritorno alla "normalità", ma deve essere intesa come apertura di una scena democratica in cui le questioni possano essere rimesse in gioco e contestate, configurandosi così come emancipazione. Claudia Aradau, "Security and the Democratic Scene: Desecuritization and Emancipation," *Journal of International Relations and Development* 7, no. 4 (2004): 393–94.

Questo produce un doppio slittamento di privatizzazione dell'eccezione e pubblicizzazione del rischio. Chi definisce gli standard, chi controlla le metriche, chi può disconnettere un'intera porzione di rete o rallentare un servizio in nome della sicurezza? Chi risponde degli errori degli algoritmi che filtrano contenuti o che generano *scores* di rischio? Nel mondo digitale, dove l'urgenza tende a farsi regola e la tentazione dell'automazione "risolutiva" è forte, saper leggere e misurare il passaggio all'eccezione e il ritorno alla normalità diventa una competenza analitica centrale. Per questa ragione, la tesi impiegherà la securitizzazione non come griglia ideologica, ma come strumento euristico capace di far vedere ciò che spesso si nasconde nelle pieghe della tecnica: chi ha potuto dichiarare l'urgenza, con quali argomenti, su quale pubblico, in vista di quali misure, con quali responsabilità e quali controlli. È su questa base che, nei passaggi successivi del capitolo metodologico, la prospettiva verrà integrata con il costruttivismo di Wendt – utile a tematizzare fiducia, identità e intersoggettività nei domini digitali – e con il neofunzionalismo di Haas – necessario a spiegare perché e come, in un'area altamente interdipendente come il cyberspazio, spillover tecnici e regolatori possano tradursi in nuove forme di cooperazione (e di conflitto) tra attori pubblici e privati.

1.3. La seconda dimensione: il costruttivismo e la centralità della fiducia come fatto sociale

Assumere la lente costruttivista significa assumere che, nelle relazioni internazionali, strutture, interessi e identità prendano forma nell'interazione e nella ripetizione di pratiche e aspettative condivise[26]. In questa prospettiva, il cyberspazio non è un ambiente neutro, un'infrastruttura tecnica che sopporta decisioni già date; è piuttosto uno spazio sociale denso, nel quale codici, protocolli, standard, routine operative e linguaggi professionali si intrecciano con rappresentazioni, ruoli e norme, fino a generare orizzonti di possibilità e vincoli che gli attori riconoscono come "reali". È in questo intreccio che la fiducia smette di essere un sentimento individuale o un mero calcolo di convenienza e diventa un fatto sociale: una relazione che abilita orienta e, in taluni casi, sostituisce la forza di regole vincolanti quando queste mancano o non sono applicabili con continuità. La fiducia non è, nelle relazioni internazionali, un bene naturale che gli attori possiedono o perdono come si perde un capitale finanziario; è un dispositivo relazionale che

[26] Alexander Wendt definisce il costruttivismo come l'approccio che considera le strutture fondamentali della politica internazionale costituite da idee condivise piuttosto che da forze materiali, e le identità e gli interessi degli attori come prodotti delle pratiche sociali. Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999).

si costruisce nel tempo attraverso segnali, impegni e pratiche di reciprocità, e che si logora quando questi elementi vengono meno o risultano contraddetti dai comportamenti. Nel dominio digitale questo tratto appare con particolare evidenza: gli scambi informativi, le interdipendenze tecnologiche, la condivisione di indicatori e allarmi, l'affidamento su fornitori privati e su protocolli comuni mettono costantemente gli attori in condizioni di vulnerabilità reciproca. Fidarsi, in concreto, può significare accettare che un software di terze parti non contenga una "porta sul retro"; confidare che un partner non sfrutti un accesso privilegiato per fare spionaggio; affidarsi all'algoritmo che classifica l'evento come minaccia, sperando che non sia addestrato su dati distorti. Ogni volta che questa scommessa relazionale regge, si consolidano identità e ruoli – "fornitore affidabile", "alleato responsabile", "certificatore indipendente" –; quando invece si incrina, l'attrito informativo si trasforma in sospetto sistematico e si ripercuote sulla cooperazione tecnica, sui tempi decisionali e, in ultima istanza, sulla stabilità strategica[27].

La fiducia si potrebbe scomporre in quattro dimensioni, distinte sul piano analitico ma spesso sovrapposte nei casi reali: istituzionale, procedurale, tecnica ed epistemica. La fiducia istituzionale rimanda a leggi, accordi, mandati e meccanismi di responsabilità tra enti e Stati; quella procedurale riguarda la qualità delle routine quotidiane (chi avvisa chi, entro quando, con quale formato) che permettono di cooperare anche tra attori diffidenti; la fiducia tecnica dipende dalla robustezza degli strumenti e delle filiere (standard aperti, crittografia, controllo dei fornitori), riducendo le ambiguità negli scambi; la fiducia epistemica si fonda su competenze riconosciute e sulla reputazione di comunità professionali che producono e validano conoscenza. Distinguere di volta in volta quale dimensione è in causa orienta anche gli interventi. In questa cornice, il modello *Zero Trust* (o architettura a fiducia zero) pare epitome sintomatica del cambiamento. Si tratta di un modello di sicurezza informatica che parte dal principio *assume breach*: nessun utente, dispositivo, applicazione o segmento di rete è considerato intrinsecamente affidabile, neppure se "interno"[28]. L'accesso alle risorse è concesso in modo dinamico e granulare, applicando verifica esplicita e

[27] Andrew Kydd mostra come la fiducia e la sfiducia siano esiti di dinamiche strategiche che si costruiscono attraverso segnali e aspettative reciproche, mentre il già citato Joseph Nye evidenzia come, nell'era informazionale, queste dinamiche si intreccino con le interdipendenze tecnologiche e con il potere che deriva dal controllo dei flussi di dati. Andrew Kydd, *Trust and Mistrust in International Relations* (Princeton: Princeton University Press, 2005); Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011).

[28] Il modello di sicurezza informatica denominato *Zero Trust* si fonda sul principio "never trust, always verify": invece di considerare affidabile per default ciò che è all'interno della rete, ogni accesso e ogni flusso devono essere continuamente autenticati, autorizzati e monitorati. Questo approccio, promosso dal NIST come standard di riferimento, nasce per rispondere a scenari in cui minacce interne ed esterne si confondono e in cui le architetture perimetrali tradizionali non garantiscono più protezione. National Institute of Standards and Technology (NIST), *Zero Trust Architecture*, Special Publication 800-207 (Gaithersburg, MD: U.S. Department of Commerce, 2020).

continua dell'identità e dello stato del dispositivo, minimo privilegio e micro-segmentazione del perimetro logico. Le decisioni di accesso sono guidate da policy contestuali (identità, postura del *device*, sensibilità dei dati, rischio, luogo/tempo) ed eseguite tramite componenti di *enforcement*, con cifratura *end-to-end*, telemetria e monitoraggio per rilevare e contenere movimenti laterali. In sintesi, il modello *Zero Trust* non "nega la fiducia", ma la ricostruisce a ogni richiesta, riducendo la superficie d'attacco e aumentando la resilienza complessiva dell'organizzazione. Invece di basarsi su dichiarazioni di intenti, la si fonda su verifiche ripetute, tracciabilità delle azioni e separazione dei domini, così da limitare i danni quando qualcosa va storto. In altre parole, la fiducia passa dall'"io mi fido" alla prevedibilità dei comportamenti sotto regole tecniche e organizzative chiare.

Per uno studio sulla guerra algoritmica questo passaggio è decisivo. Le reti di comando e controllo potenziate dall'AI e le routine di analisi delle minacce si appoggiano a infrastrutture e metriche pensate per rendere più trasparente l'incertezza; tuttavia, la differenza concreta la fanno le scelte negoziate: soglie di allerta, criteri di attribuzione, tempi di comunicazione e di risposta. Sono questi micro-accordi a costruire – o a erodere – la fiducia operativa. Un approccio costruttivista colma un limite degli sguardi solo tecnici: mostra come parole e visualizzazioni orientano la percezione del rischio. Mappe di calore, punteggi di rischio e schermate di allerta non sono strumenti neutri: propongono al decisore un certo ordine del mondo, portando in primo piano alcuni elementi e lasciandone altri sullo sfondo. Quando queste rappresentazioni si ripetono – perché le adottano piattaforme commerciali dominanti, entrano nei documenti di bilancio o vengono riprese in sedi internazionali – finiscono per diventare "evidenze" date per scontate che sostengono scelte e giustificazioni. Per questo l'analisi deve porre domande semplici e verificabili: perché è stata scelta proprio questa metrica? Quali alternative sono state scartate? In che modo questa rappresentazione sposta responsabilità e ruoli? Su questa base, la fiducia può essere trattata come un'aspettativa condivisa di comportamento in condizioni di vulnerabilità e resa osservabile attraverso tre famiglie di segnali: impegni e regole pubbliche (accordi di cooperazione, standard condivisi, procedure di notifica); pratiche ripetute e verificabili (esercitazioni, scambi informativi, audit incrociati, certificazioni reciproche); prestazioni nelle crisi (tempi di comunicazione, chiarezza dei messaggi, coerenza tra dichiarazioni e azioni). Questa griglia, pur semplice, permette di collegare rappresentazioni, decisioni e responsabilità.

Il costruttivismo mette quindi in luce un aspetto decisamente politico della questione: la competizione per stabilire chi ha l'autorità di dire che cosa è "affidabile", anche nel cyberspazio bellico. In un ecosistema in cui standard, piattaforme e servizi sono in gran parte prodotti da

soggetti privati e in cui comunità transnazionali di esperti definiscono buone pratiche e soglie di rischio, il confine tra "sicuro" e "insicuro" è un terreno conteso. Gli Stati cercano di incorniciare questa autorità con certificazioni nazionali, politiche industriali ed etichette di conformità; le imprese puntano su reputazione tecnica, effetti di rete e sul ruolo di snodi di fiducia; le organizzazioni internazionali provano a tessere quadri comuni di responsabilità. Capire dove questi sforzi convergono o si neutralizzano aiuta a spiegare perché alcune filiere risultano affidabili e altre no, con effetti concreti negli equilibri della guerra algoritmica. La prospettiva costruttivista, dunque, non oppone tecnica e politica: mostra che si costituiscono a vicenda. Algoritmi, protocolli e interfacce non operano nel vuoto, ma incorporano scelte su che cosa conti come minaccia, quali prestazioni siano accettabili e quali errori siano tollerabili. La fiducia, come fatto sociale, tiene insieme questi piani: rende possibile la cooperazione nell'incertezza, ma richiede una manutenzione continua di ruoli, aspettative e pratiche. È sul "costo" di questa manutenzione – chi lo sostiene, con quali strumenti e a quali condizioni – che si misura la capacità degli attori di usare l'AI e le reti digitali non come scorciatoia, ma come leve per migliorare la qualità del giudizio e la legittimità delle decisioni.

1.4. La terza dimensione: il neofunzionalismo come chiave per seguire integrazione, spillover e armonizzazione

Il neofunzionalismo, nato per spiegare l'integrazione europea[29], offre una chiave semplice: quando i Paesi cooperano su un problema concreto, questa cooperazione tende a estendersi ad altri ambiti e a rafforzare istituzioni comuni. L'integrazione avanza così per piccoli passi, spinta da esigenze pratiche più che da grandi accordi politici. Nella prospettiva dell'integrazione, due meccanismi risultano particolarmente rilevanti. Il primo è lo spillover funzionale: quando si tenta di risolvere un problema circoscritto, emergono rapidamente dipendenze tecniche e organizzative che impongono di intervenire anche su ambiti contigui. In altre parole, per far funzionare davvero una riforma in un settore, occorre coordinare regole, strumenti e competenze in settori adiacenti. Nel caso della guerra algoritmica, l'introduzione di sistemi di targeting basati su modelli predittivi non può avvenire isolatamente: richiede la standardizzazione dei sensori, la definizione di formati dati

[29] Il neofunzionalismo è una teoria delle Relazioni Internazionali e dell'integrazione regionale sviluppata a partire dagli anni '50 per spiegare il processo di unificazione europea. Secondo questo approccio, l'integrazione tende ad autoalimentarsi attraverso meccanismi di *spill-over* funzionale e politico: la cooperazione in un settore tecnico-economico crea pressioni per estenderla ad altri ambiti, generando progressiva convergenza istituzionale e politica. Il testo fondativo è Ernst B. Haas, *The Uniting of Europe: Political, Social, and Economic Forces, 1950–1957* (Stanford: Stanford University Press, 1958).

e metadati, criteri di qualità e procedure di verifica lungo l'intera filiera informativa, altrimenti il sistema rimane fragile o incoerente. Il secondo meccanismo è lo spillover politico/istituzionale. Gli attori che traggono vantaggio dall'integrazione – istituzioni comuni, imprese, comunità professionali – hanno incentivi a estendere regole e competenze, perché l'allineamento riduce i costi di coordinamento, amplia i mercati e aumenta la prevedibilità delle decisioni. In ambito tecno-militare questo si traduce, ad esempio, nella richiesta di cornici condivise per certificazioni, metriche di prestazione, audit dei modelli e tracciabilità dei dati, così da rendere più agevole l'adozione su più amministrazioni e teatri operativi. A questi due processi si affianca l'armonizzazione, intesa come l'allineamento esplicito di standard, procedure e definizioni per prevenire conflitti interpretativi e garantire interoperabilità. L'armonizzazione non significa uniformità rigida: mira piuttosto a stabilire un linguaggio comune – formati e interfacce, soglie operative, criteri di qualità, glossari condivisi – che consenta a sistemi diversi di cooperare e renda verificabili le responsabilità. In sintesi, lo spillover spiega perché l'integrazione tende ad ampliarsi (per necessità tecniche o per spinte di attori interessati), mentre l'armonizzazione descrive come tale ampliamento diventa praticabile, controllabile e, in ultima analisi, valutabile sul piano pubblico.

Assumere il neofunzionalismo di Ernst B. Haas come terza lente per interpretare il campo digitale del cyberspazio[30] significa spostare lo sguardo dai soli contenuti tecnici delle innovazioni digitali agli effetti istituzionali che esse generano nel tempo, quando funzioni inizialmente circoscritte finiscono per trascinare con sé, quasi per inerzia, domini contigui e attori ulteriori. Il punto di partenza è noto: nelle società complesse l'integrazione non scatta perché qualcuno la decreta una volta per tutte, ma perché problemi pratici eccedono la portata di singole giurisdizioni e inducono cooperazioni ripetute. Trasposto al dominio digitale della sicurezza, questo paradigma offre una grammatica convincente per leggere perché una pratica specialistica difficilmente resta confinata: la dipendenza da dati, piattaforme e protocolli comuni tende a generare pressioni verso meccanismi di armonizzazione che, a loro volta, ridefiniscono ruoli e responsabilità degli attori pubblici e privati coinvolti. Nel campo esaminato dalla tesi, l'innesco tipico è un problema "funzionale"

[30] Se Haas mostra come l'integrazione europea si sviluppi attraverso passaggi incrementali che estendono la cooperazione da un settore tecnico all'altro, studiosi come Bendiek e Bossong illustrano come la stessa logica di *spill-over* si stia oggi manifestando nel digitale e nella cybersecurity, con la progressiva armonizzazione di standard, procedure e infrastrutture comuni a livello UE. Vedi Annegret Bendiek and Raphael Bossong, "The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges," *SWP Comment* 47 (Berlin: Stiftung Wissenschaft und Politik, November 2017).

apparentemente tecnico: verificare l'autenticità di un video di campo, classificare un attacco come sabotaggio o spionaggio, allineare criteri di priorità nel *patching* di sistemi critici. Ogni volta che la soluzione più efficiente richiede dati comparabili, tassonomie condivise, strumenti interoperabili e tempi di risposta orchestrati, si crea un incentivo a adottare standard e interfacce comuni. La qualità e la velocità dell'azione migliorano quando i partner parlano la stessa lingua tecnica e adottano schemi condivisi per l'annotazione dei metadati visivi. Ma, come suggerisce Haas, lo standard tecnico è raramente neutro: cristallizza una certa idea di rischio, distribuisce oneri e benefici, sposta potere decisionale verso chi definisce la metrica e i criteri di qualità.

È in questo slittamento dalla funzione alla regola che lo *spillover* prende forma: la cooperazione intorno a un compito operativo trascina nella scia la necessità di organismi di coordinamento, procedure comuni di *audit*, talvolta nuove basi legali per lo scambio dei dati e per la responsabilità dell'azione. Si riconosce una sequenza ricorrente. Quando si diffonde l'uso di strumenti di analisi automatizzata delle immagini – per collegare tracce visive a eventi – nasce il bisogno di rendere i metodi comparabili: si fissano procedure di acquisizione, si tutela l'integrità dei file con una "catena di custodia" digitale, si stabiliscono soglie di confidenza per le prime attribuzioni. Questa standardizzazione abbassa i costi di coordinamento e rende conveniente allargare la platea: forze di polizia, autorità di regolazione, centri di risposta agli incidenti, redazioni e laboratori iniziano a cooperare perché condividere strumenti e repertori riduce i costi e moltiplica le capacità. La cooperazione tecnica diventa poi politica quando occorre decidere che cosa conta come "evidenza" in sede giudiziaria o diplomatica, quanto pesa un punteggio generato da un classificatore e come bilanciare tempestività e accuratezza. L'esito è il passaggio da un'alleanza di tecnici a una costellazione istituzionale: comitati con mandato sulle prassi, piattaforme di scambio dati, linee guida operative e codici di condotta che formalizzano le intese.

Il neofunzionalismo aiuta anche a capire il ruolo degli "imprenditori della cooperazione"[31]: figure collocate in organizzazioni sovranazionali, enti di standardizzazione, grandi piattaforme o consorzi pubblico-privati che trasformano problemi locali in agende comuni. Sono loro a redigere bozze di standard, promuovere prove di interoperabilità che mostrano i benefici di soluzioni compatibili e negoziare compromessi su definizioni e metriche. Se questi attori mancano, le soluzioni restano

[31]Haas identificava nelle élite sovranazionali gli attori che favoriscono lo *spill-over* trasformando problemi settoriali in sfide politiche condivise; Sandholtz e Stone Sweet hanno poi sviluppato questa intuizione mostrando come policy entrepreneurs operino concretamente in arene transnazionali e istituzioni comuni, redigendo standard, promuovendo interoperabilità e costruendo compromessi tra attori pubblici e privati. Vedi Wayne Sandholtz and Alec Stone Sweet, *European Integration and Supranational Governance* (Oxford: Oxford University Press, 1998).

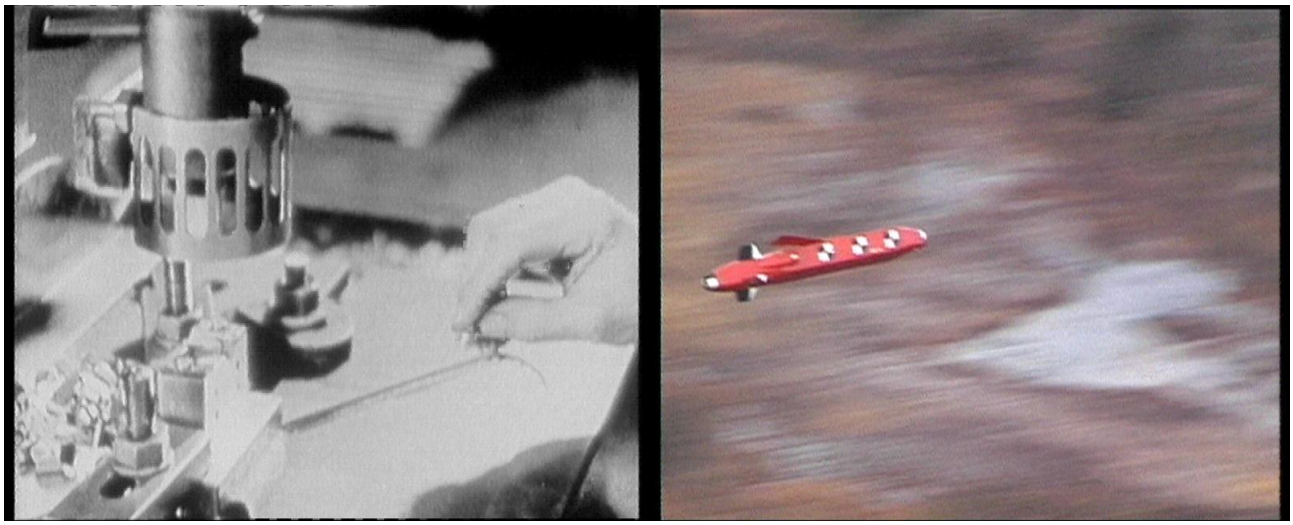
frammentate; quando agiscono con continuità, l'allineamento in un settore crea incentivi perché settori vicini si adeguino, evitando incoerenze. Così una tassonomia per contenuti audiovisivi manipolati può diventare la base di procedure di moderazione sulle piattaforme; gli schemi per lo scambio di indicatori tecnici evolvono in protocolli di allerta precoce tra autorità nazionali; e i modelli di valutazione del rischio *cyber* migrano nell'analisi del rischio operativo militare, con campi dati, criteri e soglie sempre più omogenei. Ragionare in termini di *spillover* non significa però adottare una visione ottimista per principio. La stessa letteratura neofunzionalista ricorda la possibilità di passi indietro (*spillback*) o di stalli quando gli interessi cambiano o quando un settore "resiste" a farsi trascinare. Nel digitale della sicurezza queste frizioni sono frequenti: standard pensati per favorire la condivisione si scontrano con vincoli di segretezza e interessi commerciali; in un contesto avversario, inoltre, maggiore trasparenza può aiutare anche chi attacca. Talvolta l'integrazione funzionale crea dipendenze critiche da infrastrutture o fornitori dominanti; altre volte la fretta di armonizzare sacrifica la sensibilità ai contesti locali e irrigidisce procedure che dovrebbero restare adattive.

Sul piano metodologico, la lente proposta è utile per due ragioni. Primo, consente di ricostruire in modo ordinato il passaggio dal tecnico al politico: l'adozione di un lessico o di un formato conduce alla creazione di organismi di coordinamento, a riforme procedurali e a nuove aspettative di comportamento. Secondo, permette di mettere a fuoco attori e meccanismi che favoriscono lo spillover: interdipendenze tecnologiche (cloud condivisi, protocolli, dataset), costi della non-interoperabilità e pressione reputazionale generata tanto dai fallimenti quanto dalle pratiche di successo. La cybersicurezza in contesti bellici poggia su infrastrutture e competenze distribuite (laboratori universitari, gruppi civici OSINT, team di piattaforme, unità governative e comandi militari). Da una prospettiva neofunzionalista, questo mosaico non è un'anomalia, ma la risposta razionale a problemi che nessun attore risolve da solo. Il coordinamento scaturisce da cornici procedurali e tecniche condivise che riducono attriti e, soprattutto, l'incertezza sulle mosse altrui in crisi. In questo quadro, la fiducia non è un prerequisito astratto ma un bene organizzativo che si costruisce attraverso scambi informativi affidabili regolati da norme chiare e verificabili. La qualità dell'integrazione non si misura solo nel throughput tecnico (volume/velocità dei dati), bensì nell'accountability: tracciabilità delle decisioni, possibilità di audit e chiarezza delle responsabilità quando il calcolo produce effetti operativi. Spillover che generano "più scambio" senza rendere visibili soglie, assunzioni e limiti dei modelli producono integrazioni fragili; al contrario, allineamenti che incorporano trasparenza, controlli incrociati e formati che preservano il contesto dei dati tendono a reggere agli shock e a consolidarsi. Lo spazio cibernetico è popolato

da attori non coincidenti con lo Stato (piattaforme, fornitori d'infrastrutture, consorzi di standardizzazione, laboratori di ricerca, società civile, comunità tecniche). La legittimità delle decisioni dipende dalla capacità di orchestrare tali attori su basi di fiducia e responsabilità.

La lettura congiunta di Buzan, Wendt e Haas consente di vedere, rispettivamente: come temi vengano costruiti come questioni di sicurezza; come idee, norme e identità professionali modellino aspettative e scelte; come l'integrazione si espanda tramite spillover sostenuti da standard, procedure minime e definizioni condivise. In questo processo, gli attori privati non sono meri esecutori: contribuiscono a definire lessici, metriche e priorità che ridefiniscono ciò che conta come sicurezza e ciò che passa per cooperazione. Ogni triangolazione comporta rischi: irrigidimento interpretativo dovuto alle grandi teorie, bias delle fonti istituzionali, privilegio del visibile a scapito dello sfondo. La risposta è triplice: uso strumentale e non dogmatico delle teorie; costruzione di un corpus deliberatamente plurale (testi programmatici, standard tecnici, linee guida, materiali di attori non governativi, resoconti critici); accompagnamento dell'analisi con riscontri procedurali e documentali. La tesi muove da una domanda circoscritta: che cosa mostrano le lenti della securitizzazione, del neofunzionalismo e del costruttivismo su come immagini e stime prodotte da sistemi automatizzati, spesso inserite in filiere tecnologiche private, entrano nei processi decisionali di sicurezza e ridisegnano il ruolo delle relazioni e dell'agenzia umane? L'obiettivo è una ricognizione descrittiva di attori, passaggi e logiche in casi pubblicamente documentati di guerra algoritmica e di ingresso di interessi privati nei conflitti, con un impianto comparativo e documentale (documenti strategici, linee guida, report istituzionali, analisi pubbliche, materiali OSINT). Le tre lenti funzionano come strumenti complementari: la *securitizzazione* spiega come si costruiscono urgenza e consenso; il neofunzionalismo chiarisce dinamiche di spillover e armonizzazione che sostengono l'integrazione; il *costruttivismo* illumina come categorie e norme definiscano minaccia, evidenza ed errore accettabile. Assunte insieme, aiutano a leggere la guerra algoritmica e il ruolo degli attori privati non come un salto puramente tecnologico, ma come un insieme di processi graduali di costruzione dell'evidenza, coordinamento e legittimazione, nei quali la velocità decisionale può tanto erodere quanto aumentare la capacità di scelta e di responsabilità politica a seconda del disegno istituzionale.

CAMPO DI RICERCA



Harun Farocki, Eye Machine I, © Harun Farocki, 2001.

"Operational images, not propaganda
for machines performing their tasks no longer repetitively or blindly
but rather independently, autonomously.
Imagine a war of autonomous machines,
wars without soldiers,
like factories without workers
we saw images like these in 1991, of the war against Iraq
propaganda, yet an ad for intelligent machines"

Harun Farocki – Eye/Machine I

2.1. Immagini matrice

Dagli equilibri diplomatici alla giustificazione delle azioni militari, dalla costruzione delle figure avversarie fino all'attribuzione di umanità o disumanità ai soggetti ritratti, le immagini svolgono un ruolo essenziale nelle relazioni internazionali e nella geopolitica contemporanea. Un primo modo di considerarne l'effetto e l'influenza è considerare come esse influenzino direttamente le narrazioni dominanti, le dottrine strategiche e persino le decisioni cruciali prese dagli attori globali. La comprensione delle relazioni internazionali non si è mai limitata a un esercizio oggettivo di osservazione dei fatti. Al contrario, essa è stata storicamente modellata da un repertorio ristretto ma persistente di rappresentazioni visive, vere e proprie immagini-matrice: figure ricorrenti, direzionate e controllate, che operano come coordinate fondamentali nella configurazione della percezione politica e morale del mondo. Come ha messo in luce Jacques Rancière, le immagini partecipano attivamente alla costruzione dell'ordine sociale e politico attraverso una precisa "distribuzione del sensibile", ovvero una partizione storicamente situata di ciò che può essere visto, detto, pensato e sentito[32]. Non si tratta semplicemente di un regime estetico, ma di una cartografia percettiva che determina cosa può essere rappresentato e quali soggetti, territori o eventi risultano visibili o, al contrario, esclusi dal panorama globale. In questa prospettiva, le immagini-matrice che strutturano il campo delle relazioni internazionali non si configurano come semplici strumenti illustrativi, ma come dispositivi epistemici che delimitano lo spazio del

[32] Jacques Rancière, *La partizione del sensibile. Estetica e politica* (Roma: DeriveApprodi, 2007).

pensabile e del dicibile all'interno di un preciso ordine mondiale. Esse assegnano ruoli, distribuiscono valori, modulano l'intelligibilità degli eventi e decidono quali storie meritino di essere raccontate e quali rimangano nell'ombra. La loro forza non risiede solo nella capacità di rappresentare, ma nel potere di orientare, prefigurare, prescrivere.

Per comprendere appieno l'impatto di tali figure visive sulla formazione delle visioni politiche e delle conoscenze collettive, è necessario superare l'idea dell'immagine come mero oggetto estetico. Queste immagini agiscono come veri e propri schemi cognitivi, operanti a un livello prelinguistico ed emotivo, capaci di influenzare in profondità il modo in cui interpretiamo, valutiamo e attribuiamo senso agli avvenimenti internazionali. In tal senso, si configurano come un atlante iconografico[33] condiviso, una sorta di mappa simbolica alla quale attingono cittadini, diplomatici, analisti, media e istituzioni per orientarsi nel mondo, soprattutto in situazioni di incertezza, ambiguità o conflitto. È in questo intreccio tra visione, potere e conoscenza che si gioca gran parte della posta in gioco simbolica della politica globale contemporanea. Come hanno messo in luce alcuni studiosi interessati al ruolo delle strutture audiovisive nelle relazioni internazionali, le immagini matrice funzionano orientando le nostre interpretazioni del conflitto, della cooperazione o del caos globale in un modo simile a quelle metafore visive ed espressioni di sintesi concettuale profondamente radicate nella realtà dell'esperienza umana. Pensiamo ad esempio al concetto di "famiglia delle nazioni", che richiama l'idea di solidarietà e ordine simile a quello familiare. Oppure all'idea di "strada verso la democrazia", che esprime il concetto di progresso politico con un movimento costante e lineare. Infine, consideriamo un'espressione come "cartina geopolitica", che trasforma il mondo in una superficie astratta governabile e delimitata dove lo spazio rappresenta il potere. Queste costruzioni metaforiche non sono soltanto riflessioni della cultura umana ma piuttosto manifestazioni figurative che traggono forza dalla loro capacità di rispecchiare gestualità e programmi tipici dell'esperienza umana. Allo stesso tempo non sono figure ideologicamente innocenti, anzi, spesso supportano certe prospettive ideologiche specifiche e consolidano determinate strutture di potere mentre definiscono i limiti di ciò che è permesso dire o fare sulla scena mondiale.

Spesso ci lasciamo ingannare dall'apparente immediatezza delle immagini. Le percepiamo come qualcosa di "naturale", quasi un dato di fatto nella nostra quotidianità, ma questa percezione maschera una realtà ben più complessa. Dietro questa 'prima natura' si cela una 'seconda natura': quella di costruzioni altamente codificate, capaci di selezionare e organizzare la realtà in base a

[33] Un contemporaneo e distopico atlante Mnemysune di warburgiana memoria.

logiche politiche, morali e strategiche ben precise. Le immagini che definiamo "matrici" – quelle che plasmano la nostra comprensione degli eventi – non si limitano a descrivere o a riprodurre in modo mimetico il mondo. Al contrario, esse lo producono attivamente, agendo come veri e propri protagonisti e motori di processi politici. Pensiamo a come riescono a offrire cornici intuitive per l'azione diplomatica, a giustificare interventi armati, a forgiare la narrazione della pace o della minaccia. Sono strumenti potenti che ci permettono di reagire rapidamente a eventi complessi, incanalandoli in scenari visivi già familiari. Questo, in effetti, riduce l'incertezza e genera un senso di urgenza o di legittimità che può orientare le nostre azioni. In quest'ottica, le immagini non sono semplici veicoli di comunicazione; si configurano piuttosto come autentiche tecnologie della percezione che hanno il potere di determinare il significato profondo degli eventi. Ecco perché affrontare il tema delle immagini nell'ambito delle relazioni internazionali non significa addentrarsi in un argomento satellite. Significa, invece, penetrare nel cuore stesso dei meccanismi di potere che regolano la 'visibilità' del mondo. Sono le immagini, in ultima analisi, a decidere cosa può essere visto e, di conseguenza, cosa può essere fatto. Diventa allora cruciale interrogarsi: chi è degno di rappresentazione e chi, invece, rimane relegato all'invisibilità? Quali territori vengono mappati e quali restano meri 'spazi bianchi' nella nostra cognizione? E, infine, quali emozioni vengono attivate e quali, al contrario, vengono sistematicamente represse dalla loro influenza?

Ben O'Loughlin osserva che certe immagini che modellano la nostra percezione del mondo globale non emergono da uno spazio neutro o naturale. Al contrario, sono sostenute da complesse infrastrutture mediatiche, altamente tecnologiche e spesso centralizzate. Questa intricata rete di infrastrutture include centri di raccolta e analisi dati, piattaforme di distribuzione visiva, agenzie di stampa, server, algoritmi per la selezione della visibilità, e interfacce grafiche, senza dimenticare l'apparato tecnico-visuale di think tank ed eserciti. Tutti questi elementi funzionano come un'unica grande strumentazione volta a filtrare e uniformare ciò che viene offerto alla vista del pubblico; il loro modo di operare tende a favorire non tanto l'innovazione nella narrazione o la diversità di prospettive, quanto piuttosto la riproposizione di schemi consolidati e immediatamente riconoscibili, perché familiari. Invece di aprire nuove possibilità di comprensione o di stimolare l'immaginazione, tali infrastrutture creano in questi casi un effetto che potremmo definire "ricorsività iconica"[34], attraverso ripetizioni in grado di risvegliare emozioni nel pubblico, confermando la sua visione preesistente del mondo e inserendosi perfettamente in una grammatica

[34] Si veda Ben O'Loughlin, "Images as Weapons of War: Representation, Mediation, and Interpretation," *Review of International Studies* 44, no. 3 (2018): 414–416; Ben O'Loughlin, Andrew Hoskins, and Akil Awan, *War and Media: The Emergence of Diffused War* (Cambridge: Polity Press, 2010), 56–60.

visiva già affermata. In altre parole, queste immagini non si limitano a trasmettere informazioni, ma contribuiscono attivamente a definire l'ordine simbolico entro cui si sviluppa il dialogo nel campo internazionale.

Basti pensare, come esempio emblematico, all'onnipresente paradigma del “prima e dopo” nelle rappresentazioni dei conflitti. Interi reportage visivi e dossier strategici vengono metodicamente costruiti attorno alla promessa di documentare la trasformazione tangibile di territori, corpi e città. Queste narrazioni binarie – pensiamo al villaggio pacifico trasformato in macerie dai bombardamenti, al leader prima carismatico e poi giustiziato, o alla piazza inizialmente ordinata e poi invasa dalla folla – operano come veri e propri dispositivi cognitivi rassicuranti. La loro funzione è quella di semplificare la complessa realtà storica e politica degli eventi, riducendola a sequenze lineari e teleologiche, spesso cariche di un intento emotivamente manipolatorio. A ciò si affianca l'uso reiterato e quasi ritualizzato di cliché visivi, che agiscono come autentici “segni-segnali” del disordine internazionale: la bandiera che brucia, la folla inferocita, il combattente incappucciato con l'arma in pugno. Queste immagini non hanno lo scopo di rivelare una realtà inedita o di stimolare un pensiero critico; al contrario, esse attivano automaticamente una serie di associazioni culturali, morali e politiche predefinite, reiterando costantemente la distinzione tra civiltà e barbarie, tra democrazia e caos, tra ordine e minaccia. In questa particolare economia dell'immagine, perfino gli strumenti che appaiono più neutri e tecnici – come le slide PowerPoint utilizzate nei briefing militari, le infografiche elaborate dai centri strategici o i pannelli di analisi geopolitica – assumono una funzione estetico-politica di fondamentale importanza. L'impaginazione, la scelta cromatica, la gerarchizzazione grafica delle informazioni, e persino la rappresentazione stilizzata di territori o figure avversarie, concorrono attivamente a stabilire ciò che viene percepito come centrale o marginale, ciò che è immediatamente leggibile e ciò che, invece, rimane intenzionalmente opaco.

In questo senso, emerge chiaramente come anche la guerra cognitiva – ovvero quella battaglia che si combatte per la legittimazione dell'azione armata – venga vinta o persa non solo sul piano del contenuto, ma soprattutto su quello della forma. Le immagini non si limitano ad accompagnare il conflitto; piuttosto, lo rendono intrinsecamente possibile, rendendolo visibile e presentandolo secondo logiche di necessità, urgenza o giustizia. È un dato di fatto che alcune guerre diventano pensabili e legittime proprio perché l'immaginario visivo che le ha precedute ne ha già plasmato lo scenario, definito i ruoli e pre-attivato le emozioni. Al contrario, altre guerre rimangono invisibili o persino impensabili, non trovando alcuno spazio all'interno della grammatica visiva autorizzata e dominante. In questo complesso quadro, la ripetizione visiva non è affatto una mera questione estetica o mediatica; è, al contrario, un fatto eminentemente politico. È proprio attraverso

la reiterazione insistente di determinate immagini – e la conseguente, deliberata esclusione di altre – che si delinea chi ha diritto alla visibilità, chi può essere riconosciuto come soggetto politico e, infine, chi è ritenuto degno di protezione o di intervento. Come efficacemente argomentato da O'Loughlin, l'infrastruttura visiva globale opera come una vera e propria "macchina di normalizzazione percettiva"[35]: essa distribuisce ruoli, emozioni, valori e gerarchie attraverso un uso sapientemente codificato dell'immagine. In questo modo, l'ordine mondiale non viene imposto unicamente tramite il diritto internazionale, le dinamiche economiche o la forza militare. Esso si consolida anche, e in maniera determinante, attraverso una regia sapiente delle immagini, capace di produrre quella realtà sensibile entro cui il politico può manifestarsi e agire.

La proposta teorica di O'Loughlin ci invita, in questo contesto, a operare un radicale spostamento del nostro approccio. Non è più sufficiente, infatti, limitarsi a denunciare le manipolazioni mediatiche, a smascherare le fake news o a criticare la spettacolare estetizzazione della guerra nei media mainstream. Questi, pur importanti, rimangono esercizi di mera reazione, che intervengono "a valle" del complesso processo di produzione del senso. Al contrario, O'Loughlin ci esorta a risalire "a monte", ovvero in quel luogo originario dove le immagini non sono ancora meri contenuti da interpretare, ma vere e proprie strutture cognitive invisibili. Sono queste strutture a predisporre, a un livello profondo, ciò che può essere visto, pensato, immaginato e, di conseguenza, ciò che può essere agito. Le immagini, in questa prospettiva, non si configurano come semplici rappresentazioni del mondo; piuttosto, lo prefigurano. Funzionano come cornici operative che anticipano la nostra comprensione del reale e che condizionano le scelte politiche e morali ancor prima che esse vengano formulate e percepite consapevolmente. Ogni immagine-matrice opera così a livello quasi precosciente, fornendo una topologia affettiva e semantica che organizza le nostre categorie del possibile e dell'impossibile, del giusto e dell'ingiusto, del vicino e del nemico. La funzione prefigurativa delle immagini è resa ulteriormente potente dal fatto che esse non agiscono in isolamento. Al contrario, sono sostenute e costantemente riprodotte da una robusta infrastruttura tecnica e istituzionale che ne garantisce la diffusione capillare, la persistenza nel tempo e l'incredibile capacità di orientare lo sguardo collettivo. È proprio in questo senso che O'Loughlin parla di infrastrutture mediali che operano come veri e propri dispositivi di selezione e ripetizione visiva.

[35] O'Loughlin concorda con Paul Virilio su questo punto. Vedi Ben O'Loughlin, Andrew Hoskins, and Akil Awan, *War and Media: The Emergence of Diffused War* (Cambridge: Polity Press, 2010), 19.

Tutto ciò implica una revisione profonda e necessaria del nostro modo di intendere la politica dell'immagine. Se accettiamo che l'immagine sia una vera e propria forma di azione, una matrice capace di generare e modellare la realtà, allora le relazioni internazionali non si giocano più esclusivamente sul piano delle alleanze strategiche, dei trattati diplomatici o degli equilibri di potere. Si dispiegano, con pari se non maggiore rilevanza, anche sul terreno delle visibilità concesse o deliberatamente negate, delle estetiche che conferiscono legittimità o la ritirano, e delle grammatiche figurative che rendono certi eventi pensabili e altri, al contrario, impensabili. Consideriamo, ad esempio, come la cosiddetta "guerra umanitaria" venga spesso narrata, alla stregua di alcuni dei concetti che abbiamo esposto sopra, attraverso un repertorio visivo ben definito: immagini di corpi da salvare, bambini feriti o donne in lacrime[36]. Al contempo, i conflitti meno riconosciuti – penso a quelli che coinvolgono popolazioni indigene, gruppi oppressi o frontiere instabili – faticano enormemente a trovare un'espressione visiva compatibile con il repertorio emotivo e le aspettative dominanti. Questo profondo squilibrio visivo non è affatto un semplice effetto collaterale, bensì una strategia politica attiva, che determina quali guerre appaiono legittime e quali no, quali vittime meritano attenzione e quali, invece, restano relegate nell'ombra dell'indifferenza. La proposta di O'Loughlin è, dunque, quella di un'estetica critica delle relazioni internazionali: un approccio che ci spinge a interrogare non soltanto i contenuti delle immagini, ma le stesse condizioni formali della visione. Solo attraverso un'analisi delle immagini intese come autentiche operazioni cognitive e politiche – e non come meri ornamenti o semplici riflessi di una realtà preesistente – possiamo aspirare a costruire un'estetica politica alternativa. Un'estetica che sia in grado non solo di sovvertire l'orizzonte visivo dominante, ma che sperimenti attivamente nuove forme di rappresentazione, nuove cartografie emotive e morali, e inediti dispositivi di visibilità per immaginare diverse forme di convivenza, di sovranità e di opposizione. In questo senso, la lotta per un ordine internazionale più giusto passa anche – e forse soprattutto – attraverso una battaglia decisiva sulle immagini: su ciò che viene mostrato, nascosto, ritualizzato o immaginato come possibile. È proprio in questa dinamica che emergono con forza anche quelle "immagini operazionali", distinte dalle matrici, la cui funzione non è tanto quella di prefigurare la realtà, quanto di intervenire direttamente su di essa, guidando l'azione e la percezione in tempo reale.

[36] Lilie Chouliaraki mostra per esempio come il discorso umanitario contemporaneo utilizzi un repertorio visivo consolidato — corpi vulnerabili, donne e bambini in lacrime — per generare empatia e legittimare interventi politici o militari, mentre altre sofferenze restano invisibili. Lilie Chouliaraki, *The Ironic Spectator: Solidarity in the Age of Post-Humanitarianism* (Cambridge: Polity Press, 2013), 54–59.

2.2. Immagini operazionali

Negli studi più recenti dedicati alla guerra, alla sorveglianza e alle trasformazioni tecnologiche che investono l'azione politica, si è progressivamente affermata una nozione teorica che mette profondamente in discussione la tradizionale concezione dell'immagine: parliamo dell'immagine operazionale. Questo concetto segna una netta rottura con l'idea classica che l'immagine sia essenzialmente una rappresentazione passiva, destinata unicamente alla contemplazione o all'interpretazione. Come si diceva appena sopra, le immagini, nel contesto odierno, non sono più semplici sussidi per comunicare o illustrare; esse intervengono e operano direttamente all'interno dei sistemi militari, dei dispositivi di sorveglianza, dei complessi flussi di dati e dei sistemi di controllo algoritmico. Oggi si preferisce parlare di 'operazioni delle immagini', sottolineando che le immagini stesse operano, e non si limitano a essere operate 'su' o 'con' esse. In quest'ottica, le immagini più che in matrici si trasformano in vere e proprie interfacce, moduli di calcolo, nodi funzionali, capaci di generare effetti concreti e tangibili nel mondo: riconoscere un potenziale bersaglio, identificare una minaccia imminente, o attivare una risposta automatica e immediata. Questa profonda trasformazione investe l'intera ecologia visiva contemporanea, estendendosi ben oltre il solo ambito militare per coinvolgere strettamente la sfera mediatica, quella biopolitica e perfino pratiche apparentemente distanti come quelle artistiche e giornalistiche. L'immagine, dunque, compie un vero e proprio spostamento dal dominio del simbolico a quello dell'operazionale: non è più soltanto una figura che rappresenta un evento, ma diventa una figura che produce un evento, contribuendo in modo decisivo a orientare le decisioni e a modulare i comportamenti.

Il punto cruciale, tuttavia, è che tale processo non è né immediato né autoevidente; per comprendere pienamente come l'immagine sia giunta a rivestire questo nuovo statuto, è indispensabile ricostruirne la sua complessa genealogia teorica. L'obiettivo sarà quindi quello di analizzare le principali tappe di questa trasformazione, mettendo in luce come alcune correnti del pensiero critico – dalla filosofia della tecnica alla dromologia – abbiano in vari modi anticipato, tematizzato e in parte problematizzato l'emergere dell'immagine come autentico “operatore automatico”. Percorrendo un arco che va dalla riflessione di Vilem Flusser a quella di Paul Virilio, dalle opere di Harun Farocki fino alle attuali discussioni sull'automazione algoritmica e sulle reti neurali, la genealogia dell'immagine operazionale rivela come la soglia tra rappresentazione e azione si sia fatta sempre più porosa. Si è giunti a un punto tale da rendere le immagini attori effettivi e centrali nelle dinamiche di potere. In un contesto simile, l'immagine non è più un

semplice oggetto della politica visiva; essa è essa stessa è un dispositivo produttivo, un'agency inscritta e operante direttamente nei sistemi sociotecnici. Ricostruire questa genealogia significa, dunque, non solo tracciare un percorso storico-teorico, ma soprattutto fornire gli strumenti concettuali necessari per affrontare in modo rigoroso la seconda parte di questo lavoro, dedicata invece all'intelligenza artificiale, agli algoritmi militari e alla cruciale problematica della fiducia distribuita nei complessi sistemi di guerra automatizzata.

Per addentrarci nella complessa genealogia del concetto di immagine operazionale, è inevitabile soffermarsi sul contributo di Vilém Flusser. La sua riflessione, sviluppata tra la fine degli anni Settanta e i primi anni Ottanta, ha infatti introdotto una vera e propria frattura epistemologica, mettendo in discussione radicalmente l'idea classica dell'immagine come mero oggetto da contemplare, interpretare o decifrare[37]. Secondo Flusser, infatti, è cruciale distinguere tra le immagini tradizionali – quelle che operano come rappresentazioni simboliche e narrative del mondo, create con l'intento di raccontare, spiegare o persuadere – e quelle che egli definisce immagini tecniche. Queste ultime, come la fotografia, il diagramma scientifico, la scansione radar o la mappa digitale, non si limitano più a "rappresentare" in senso stretto; si configurano piuttosto come strumenti attivi per operare concettualmente sul reale. L'immagine tecnica, nella visione di Flusser, non si limita a osservare un oggetto: lo computa, lo ricompone numericamente, lo trasforma in puro calcolo. L'apparato fotografico, in questa prospettiva, non è uno strumento passivo, bensì un insieme complesso di funzioni, regole e algoritmi che precedono e, di fatto, orientano l'atto stesso dell'operatore umano. Il semplice gesto di scattare una fotografia non è altro che l'ultima fase di un processo ben più complesso, interamente determinato da variabili preconfigurate: l'apertura del diaframma, il tempo di esposizione, la selezione del frame, la profondità di campo[38].

Ogni immagine, dunque, si rivela essere il prodotto visibile di un'operazione invisibile, saldamente inscritta nel programma tecnico dell'apparato. In questo contesto, Flusser introduce il concetto di "immaginazione proiettiva"[39], un'attitudine che non è più orientata alla produzione di immagini ex novo, quanto piuttosto alla programmazione di dispositivi capaci di generare combinazioni visive.

---

[37] Flusser distingue tra immagini tradizionali e immagini tecniche, sottolineando che queste ultime non sono meri supporti rappresentativi ma strumenti che computano il reale, prefigurati dall'apparato stesso. Vilém Flusser, *Per una filosofia della fotografia*, (Torino: Bruno Mondadori, 2006).

[38] Vedi Vilém Flusser, *Into the Universe of Technical Images* (Minneapolis: University of Minnesota Press, 2011). Qui Flusser amplia la riflessione: le immagini tecniche, come fotografie, mappe digitali o diagrammi scientifici, diventano programmi che non rappresentano ma operano sul mondo, traducendolo in numeri e calcoli.

[39] Diedrich Irrgang, "Projective Imagination: Vilém Flusser's Concept of the Technical Image," *Theory, Culture & Society* 40, no. 7–8 (2023): 73.

L'immaginazione, in tal senso, cessa di essere un'attività meramente rappresentativa per divenire profondamente progettuale: essa si esercita nel predisporre le condizioni affinché l'apparato produca un determinato tipo di *output*. L'immagine tecnica, di conseguenza, non è più soltanto un documento visivo, ma un segmento inseparabile di un processo computazionale più ampio, parte di una catena di trasformazioni che traduce concetti in forme visive attraverso regole formalizzate. Questa mutazione impone un doppio e fondamentale spostamento: sul piano ontologico, l'immagine si distacca definitivamente dalla nozione di mimesi, mentre su quello epistemologico, il sapere visivo si trasforma in un'interazione diretta con gli algoritmi, superando la semplice lettura di segni. Il soggetto che interagisce con l'immagine tecnica non è più un osservatore distante, ma un agente pienamente coinvolto in una rete operativa che include sensori, protocolli, archivi digitali e sistemi di elaborazione automatica. In questo quadro, la tradizionale distinzione tra immaginario e reale cede il passo a quella tra ciò che è computabile e ciò che non lo è: solo ciò che può essere formalizzato in codice diventa visibile, processabile e, in ultima analisi, operativo.

Le implicazioni di questa visione sono profonde, sia dal punto di vista teorico che da quello politico. L'idea che il visibile coincida sempre più con il computabile sposta l'asse del potere: non è più il fotografo o l'osservatore a determinare il significato dell'immagine, bensì chi detiene il controllo dell'apparato che la genera. Ciò significa che la visibilità – ossia ciò che è incluso nel dominio del visibile e del calcolabile – si configura come una vera e propria posta in gioco strategica di prim'ordine. Le immagini che circolano nella nostra società, dalle fotografie sociali ai feed di sorveglianza, non sono più semplicemente vere o false, ma si rivelano operative nella misura in cui attivano complessi processi di selezione, classificazione, riconoscimento e intervento. Flusser, con straordinaria preveggenza, anticipa così di decenni la logica intrinseca delle tecnologie contemporanee, quali il riconoscimento facciale, l'intelligenza artificiale applicata alla visione, i droni autonomi e i sistemi predittivi di polizia. In tutti questi ambiti, l'immagine non svolge primariamente una funzione comunicativa, quanto piuttosto una funzione decisionale: essa orienta il comportamento di altri apparati, funge da input fondamentale per operazioni successive e condiziona le possibilità d'azione future. Il teorico, dunque, ci offre una prospettiva radicale che consente di comprendere le immagini non come oggetti visivi statici, bensì come nodi operativi all'interno di complesse reti di decisione automatica. La sua filosofia della fotografia non si limita a descrivere l'evoluzione di una tecnica, ma costruisce una vera e propria epistemologia del visivo contemporaneo, in cui la funzione dell'immagine è sempre più assimilabile a quella del codice. Questo lo rende uno dei precursori più lucidi e fondamentali della riflessione sull'immagine operazionale, e il suo pensiero risuona in modo potente e riconoscibile nelle teorie successive di Harun Farocki, Hito Steyerl e Trevor Paglen. Senza il contributo di Flusser, non potremmo

comprendere né la natura intrinsecamente algoritmica delle immagini militari, né la loro crescente capacità di agire nel mondo in modo autonomo. Egli ci insegna che, nell'era delle immagini tecniche, vedere significa già operare – e che l'immagine, da superficie di significato, si è irrevocabilmente trasformata in una vera e propria infrastruttura di potere. Proprio l'opera teorica e cinematografica di Farocki rappresenta un punto di svolta decisivo nella comprensione e nella definizione contemporanea di "immagine operazionale". Questo artista e cineasta tedesco, attivo dagli anni Sessanta fino alla sua scomparsa nel 2014, ha infatti ridefinito in modo radicale le relazioni tra immagine, visione e azione, smantellando la distinzione classica tra mera rappresentazione e intervento effettivo. In particolare, attraverso il suo celebre ciclo di video-saggi "Eye/Machine" (2001–2003) (l'opera di cui alcuni frame sono riportati all'inizio di ciascun capitolo di queste tesi), Farocki introduce esplicitamente e con grande acume la nozione di "immagine operazionale" per descrivere quelle particolari visioni che, anziché essere destinate all'interpretazione umana o alla narrazione, sono intrinsecamente connesse a processi automatici e sistemi di controllo, guidando direttamente l'agire delle macchine o mediando l'interazione uomo-macchina. Farocki stesso le definiva con chiarezza disarmante immagini senza uno scopo sociale, non per edificazione, non per riflessione.

La complessa riflessione di Farocki si struttura attorno a diverse, e interconnesse, modalità di operatività delle immagini. Volker Pantenburg, nel suo "Working images: Harun Farocki and the operational image", ne analizza l'articolazione in tre livelli fondamentali[40]. L'autore individua le immagini puramente funzionali (o in senso stretto): si tratta di quelle visioni che sono intrinsecamente elementi di un processo tecnico, e la cui stessa presentazione visiva è spesso un mero "epifenomeno di processi di calcolo". Sono immagini generate direttamente da sistemi di riconoscimento di pattern che guidano automaticamente robot, veicoli o missili. Non sono affatto pensate per l'occhio umano; la loro funzione precipua è piuttosto quella di guidare direttamente l'azione autonoma di una macchina. La loro efficacia risiede dunque nella capacità di innescare risposte concrete, spesso senza alcuna mediazione. A tal proposito, Farocki osserva lucidamente che "il computer non ha bisogno dell'immagine"[41]; queste visioni sono semplicemente visualizzazioni di dati che, in linea di principio, potrebbero esistere in altre forme. Per loro natura, sono strettamente legate al digitale e agli algoritmi. Un secondo livello è costituito dalle immagini strumentali; queste mediano l'interazione tra l'essere umano e la macchina, stabilendo o facilitando

[40] Volker Pantenburg, "Working Images: Harun Farocki and the Operational Image," in *Image Operations: Visual Media and Political Conflict*, ed. Jens Eder and Charlotte Klonk (Manchester: Manchester University Press, 2017), 49–65.
[41] Harun Farocki, "Phantom Images," *Public* 29 (2004): 17.

un'operazione militare o non militare. Ne sono esempi paradigmatici le simulazioni di volo, le interfacce grafiche complesse dei sistemi di controllo o le visualizzazioni tecniche che orientano il comportamento di un operatore in contesti critici come quelli militari, industriali o di sorveglianza. In questi casi, l'immagine si trasforma in una vera e propria "lingua" che permette all'uomo di interagire con la logica computazionale della macchina, includendo anche immagini elettroniche o filmiche, come i film animati degli anni '40 che Farocki stesso cita in "Eye/Machine". Infine, un terzo livello, che espande e sintetizza i precedenti, è quello delle immagini che agiscono autonomamente (o performative). Questa categoria include tutti i tipi di immagini che attivamente avviano processi e azioni, siano essi tecnici o non tecnici, prodotti da umani o macchine. È qui che tecniche come il montaggio o il commento voice-over intervengono in modo determinante per infondere un senso di agency che le immagini da sole non avrebbero. In questo senso più ampio, la nozione di "operazionale" diventa quasi sinonimo di "performativo", suggerendo che una teoria dell'immagine necessiti di essere riformulata come una teoria generale del "Bildakt" (atto dell'immagine), evidenziando il loro ruolo attivo nel plasmare la realtà[42].

Ciò che rende l'approccio di Farocki profondamente radicale rispetto al tema in questione è, in sostanza, la sua straordinaria capacità di mettere in luce come queste immagini non siano semplicemente "nuove" tecnologie visive o meri prodotti dell'era digitale. Esse, piuttosto, incarnano una vera e propria mutazione epistemologica: non si tratta più di immagini da leggere, da interpretare nel loro significato simbolico o da contemplare esteticamente, ma di immagini che intrinsecamente "agiscono", che "fanno accadere" qualcosa[43]. La loro operatività si manifesta nella produzione di effetti concreti e misurabili, con ricadute significative sia sul piano militare e politico, sia su quello economico e simbolico. Per Farocki, l'immagine operazionale è un "protagonista nella storia del lavoro", un "attore chiave nell'odierna sostituzione dell'occhio" umano, proprio come i robot hanno sostituito le mani nella produzione industriale[44]. In questa prospettiva, Farocki porta alle estreme conseguenze l'intuizione pionieristica di Flusser, dimostrando come l'immagine, da entità rappresentativa, sia migrata verso uno statuto di operatore attivo nel mondo. Nei suoi innovativi montaggi saggistici e nelle suggestive installazioni video, come "Serious Games" (2009–2010) – che esplora l'uso delle simulazioni di guerra per addestrare i soldati – o "Parallel" (2012–2014) – che analizza la costruzione visiva dei mondi virtuali –, Farocki elabora un metodo critico che lui stesso definisce "soft montage". Si tratta di un

[42] Volker Pantenburg, 62–64.
[43] Harun Farocki, “Phantom Images,” *Public* 29 (2004): 12–22.
[44] Harun Farocki, “Operative Images,” in *Harun Farocki. Working on the Sightlines*, ed. Thomas Elsaesser (Amsterdam: Amsterdam University Press, 2004), 17–21.

accostamento apparentemente tenue, ma concettualmente potente, di flussi visivi eterogenei: immagini industriali, simulazioni di guerra, filmati promozionali, archivi militari. L'intento di questo "montaggio morbido" non è costruire una narrazione unificata o un messaggio esplicito. Al contrario, mira ad aprire spazi di riflessione profonda sulla convergenza tra processi di produzione e distruzione. Le immagini, in tale contesto, cessano di essere percepite come documenti neutri o semplici riflessi della realtà; esse vengono svelate come costrutti attivi che partecipano intrinsecamente alla formazione del reale[45].

Per comprendere appieno la radicalità di questa mutazione epistemologica nel campo del visivo, e in particolare il suo impatto sulle dinamiche di conflitto e sorveglianza, è indispensabile affiancare alla riflessione di Farocki il contributo di un altro pensatore visionario, Paul Virilio. Se Harun Farocki ci ha condotto nel cuore delle "immagini operazionali" che agiscono al di là della rappresentazione, è Paul Virilio a fornirci le coordinate dromologiche e strategiche attraverso cui comprendere la radicale trasformazione del visivo nel contesto della guerra moderna[46]. Per Virilio, infatti, la guerra non è più concepibile primariamente come uno scontro di forze fisiche o territoriali, ma si manifesta come una guerra del campo visivo, della velocità e della dislocazione istantanea. Nelle sue opere fondamentali, Velocità e politica: saggio di dromologia (1977) e Guerra e cinema (uscito originariamente nel 1984), Virilio sviluppa una teoria che pone la velocità – o dromologia, la scienza della velocità – al centro di ogni fenomeno sociale e, in particolare, di ogni conflitto. La tecnologia bellica, lungi dall'essere un mero strumento di distruzione, è interpretata come un apparato destinato a ottimizzare la velocità di percezione e di decisione. La guerra diventa, così, una questione di dromologia, dove l'obiettivo ultimo è annullare il tempo tra l'informazione acquisita e l'azione conseguente. È una battaglia per il controllo del "momento zero", l'istante in cui l'informazione è disponibile e la risposta può essere innescata.

In questo quadro emerge il concetto cruciale di "logistica della percezione": un sistema integrato in cui la visione non è più un passivo atto di osservazione o di pura decifrazione, ma si trasforma essa stessa in un mezzo di attacco diretto[47]. Non si tratta più di "vedere per sapere" in senso tradizionale, bensì di "vedere per agire" in tempo reale. I sistemi di avvistamento, i radar, le telecamere a infrarossi e, successivamente, i sensori dei droni, diventano non solo occhi potenziati

---

[45] Harun Farocki, "Cross Influence/Soft Montage," in *Harun Farocki. Against What? Against Whom?*, eds. Antje Ehmann and Kodwo Eshun (London: Koenig Books, 2009), 285–289.
[46] Paul Virilio, *Velocità e politica. Saggio di dromologia*, trad. it. di Giancarlo Pavanello (Milano: SugarCo, 1981), 15–20.
[47] Paul Virilio, *Guerra e cinema. Logistica della percezione*, trad. it. di Fabio Tarzia (Milano: Raffaello Cortina, 1984), 7–12.

che estendono la portata della vista umana, ma armi a tutti gli effetti. Come sottolinea Virilio, la "motorizzazione della vista" è iniziata con la Prima Guerra Mondiale, un periodo in cui il "genio della guerra" si è fuso con il "genio del progresso", dando vita a quella che Ernst Jünger definì la "mobilitazione totale"[48]. L'oculare della macchina da presa imbarcata sugli aeroplani nella ricognizione aerea prefigurava già una mutazione sintomatica nell'acquisizione degli obiettivi, segnando una crescente derealizzazione dello scontro militare. In questa nuova forma di guerra industriale, la rappresentazione degli eventi cominciava a dominare la presentazione dei fatti stessi. L'approvvigionamento delle immagini diventerà l'equivalente dell'approvvigionamento di munizioni, e la guerra del 1914 inaugurerà un nuovo "sistema d'armi" formato dalla combinazione di un veicolo da combattimento e di una macchina da presa. La capacità di acquisire informazioni visive con velocità sempre maggiore si traduce direttamente in un vantaggio tattico e strategico incommensurabile. La guerra dell'immagine, come la definisce Virilio, è intrinsecamente legata al tempo reale, alla prevenzione visiva e all'anticipazione letale[49]. Il campo di battaglia si sposta dalla dimensione geografica a quella ottica e informatica: vince chi vede prima, chi elabora l'immagine con maggiore rapidità e chi è in grado di proiettare il proprio sguardo – e di conseguenza la propria azione – in un futuro prossimo, impedendo la reazione dell'avversario. L'immagine, in questa prospettiva, è lo strumento attraverso cui si realizza l'occultamento reciproco delle forze e l'improvvisa rivelazione del bersaglio, una dinamica che annulla la distanza e rende la reazione quasi impossibile. Ciò che Virilio descrive è una perenne corsa all'armamento percettivo, dove l'occhio diventa il fulcro della logistica bellica e la velocità dell'immagine è la chiave per la vittoria. Le riflessioni di Virilio trovano una potente risonanza e una drammatica attualizzazione nel contesto dell'automazione e dello sviluppo dei sistemi di visione artificiale, spingendo oltre il concetto di logistica della percezione. La trasformazione da "vedere a far vedere" si è ulteriormente radicalizzata: le macchine non si limitano più a estendere la nostra vista o a renderci visibile ciò che era nascosto, ma si assumono sempre più il compito di "vedere per noi", e persino di agire autonomamente sulla base di ciò che percepiscono visivamente[50]. Questo passaggio segna una soglia fondamentale della visione, in cui l'occhio umano, pur rimanendo talvolta un punto di validazione o di supervisione, perde progressivamente la sua centralità operativa e decisionale.

---

[48] Ernst Jünger, *La mobilitazione totale*, in *Saggi di politica e di letteratura*, trad. it. di Julius Evola (Roma: Edizioni di Ar, 1990), 119–142.
[49] Paul Virilio, *Guerra e cinema. Logistica della percezione*, trad. it. di Fabio Tarzia (Milano: Raffaello Cortina, 1984), 11–15.
[50] Paul Virilio, *Velocità e politica. Saggio di dromologia*, trad. it. di Giancarlo Pavanello (Milano: SugarCo, 1981), 95–100.

Le immagini prodotte dai sistemi di sorveglianza, dai droni e dai sistemi di intelligenza artificiale (AI) sono l'emblema di questa nuova era. Qui le macchine non solo producono visione attraverso sensori complessi, ma sono anche programmate per analizzare, interpretare e agire autonomamente o semi-autonomamente su di essa. Un drone armato, ad esempio, non è solo una telecamera volante che trasmette immagini a un operatore remoto; è un sistema integrato che combina acquisizione visiva (spesso multispettrale), analisi algoritmica dei dati e capacità di ingaggio autonomo o tele-operato. Le sue "decisioni" operative sono mediate da un flusso costante di immagini e metadati che vengono interpretati da sofisticati software, riducendo l'intervento umano a una mera supervisione o a un'approvazione finale. La visione artificiale nell'industria, per esempio, opera a velocità che superano di gran lunga l'ispezione umana, rilevando difetti e memorizzando dati per un miglioramento continuo, senza stanchezza o errori soggettivi. Grégoire Chamayou, nella sua Teoria del drone, Principi filosofici del diritto di uccidere analizza in profondità le implicazioni etiche e politiche di questa "sospensione della visione umana" e della distanza che essa crea. L'immagine ripresa dal drone, pur offrendo una prospettiva apparentemente "oggettiva" e onnicomprensiva dall'alto, crea una distanza abissale e una derealizzazione dello scontro che permettono la sospensione del volto, del rischio e dell'empatia. L'operatore, guardando attraverso uno schermo protetto e distaccato, non percepisce il pericolo immediato, né è direttamente confrontato con la fisicità dell'azione o con le conseguenze umane della propria decisione. La visione mediata tecnologicamente si traduce in una "dislocazione morale", dove l'atto di uccidere può apparire come un'azione quasi burocratica o un mero click sul joystick. Chamayou critica aspramente i filosofi che operano nel campo dell'etica militare per la loro "necroetica" che tenta di legittimare il drone come "arma umanitaria per eccellenza", nonostante costituisca lo strumento più compiuto di una "guerra senza rischio" che mina i principi metagiuridici e l'ethos militare tradizionale. Le immagini, in questo contesto, diventano il veicolo attraverso cui si realizza una forma di guerra asettica e disincarnata, che altera profondamente la percezione del conflitto stesso e la responsabilità morale[51].

2.3. L’immagine algoritmica

Il culmine di questa evoluzione, che trascende tanto la logistica della percezione di Virilio quanto la visione a distanza dei droni analizzata da Chamayou, è l'emergere dell'immagine algoritmica. Questa nuova forma di visione va radicalmente oltre l'occhio umano e la sua capacità di

[51] Grégoire Chamayou, *Teoria del drone. Principi filosofici del diritto di uccidere*, trad. it. di Caterina Zanfi (Roma: DeriveApprodi, 2013).

interpretazione percettiva diretta, non essendo necessariamente pensata per la nostra contemplazione o comprensione. Non si tratta più soltanto di immagini che supportano una decisione umana o di macchine che ci mostrano ciò che non possiamo vedere; parliamo ora di immagini che esistono primariamente come dati per la fruizione di altre macchine. La loro funzione è interna a un processo computazionale, agendo come input o output per algoritmi complessi. L'immagine algoritmica, in questo senso, non è ciò che possiamo interpretare a occhio nudo; la sua "leggibilità" è riservata a sistemi automatici, costituendo un nuovo regime del visibile governato dal calcolo. In questa inedita dimensione del visivo, pensatori e artisti come Trevor Paglen, Hito Steyerl e Florian Apprich hanno esplorato, ciascuno con una prospettiva distintiva, gli aspetti cruciali che definiscono l'immagine algoritmica. L'invisibilità di queste immagini non deriva dalla loro assenza fisica, ma dal fatto che sono prodotte e consumate da entità non umane, spesso senza mai diventare accessibili alla percezione diretta dell'uomo. Trevor Paglen, artista e geografo, si dedica proprio a rendere visibile ciò che è stato intenzionalmente reso invisibile all'occhio umano, ma che è perfettamente leggibile per i sistemi automatizzati. Attraverso opere come la serie "Limit Telephoto", egli utilizza strumentazioni ottiche estreme per fotografare infrastrutture segrete di sorveglianza a centinaia di chilometri di distanza. Le immagini risultanti, spesso al limite dell'astrazione e della percettibilità umana, rivelano non solo l'esistenza di questi siti nascosti, ma anche l'imponente apparato tecnologico che governa la "visione delle macchine", un'operazione complessa e non un semplice atto di osservazione[52]. La sua installazione "Autonomy Cube", un server Wi-Fi pubblico che instrada il traffico internet attraverso il sistema Tor, rende tangibile l'infrastruttura di rete – altrimenti invisibile – attraverso cui circolano miliardi di immagini e dati costantemente monitorati dagli algoritmi. Ancora più incisivo è il suo progetto "ImageNet Roulette", che ha dimostrato i bias intrinseci nei dataset di addestramento dell'intelligenza artificiale, rivelando come le "visioni" delle macchine non siano neutrali, ma riflettano e perpetuino le distorsioni etiche e sociali contenute nei dati umani su cui sono state addestrate. L'immagine, in questo contesto, diventa un veicolo per la propagazione di categorie problematiche, non per l'interpretazione critica[53].

Parallelamente, Hito Steyerl indaga l'immagine algoritmica concentrandosi sulla sua materialità e la sua circolazione. Nel suo influente saggio "In Defense of the Poor Image", Steyerl celebra la poor image – la copia di una copia, compressa e diffusa – come l'immagine emblematica dell'era

[52] Trevor Paglen, *Invisible: Covert Operations and Classified Landscapes* (New York: Aperture, 2010), 12–18.
[53] Trevor Paglen, “Invisible Images (Your Pictures Are Looking at You),” *The New Inquiry*, December 8, 2016.

digitale[54]. Nonostante la sua bassa risoluzione e la perdita di qualità, essa detiene un potere operativo immenso grazie alla sua velocità, alla facilità di manipolazione e alla sua capacità di circolare in maniera virale. Per Steyerl, l'immagine algoritmica non è un'entità statica o un manufatto da contemplare, ma un flusso computazionale, un'entità dinamica che si manifesta attraverso processi di data mining, riconoscimento, copia, modifica e rielaborazione continua. L'immagine, in questa prospettiva, è meno un oggetto nel senso tradizionale e più un veicolo per l'azione e l'analisi automatizzata, un dato che acquisisce significato e influenza nel suo movimento e nella sua interazione con altri dati e algoritmi. La sua video installazione "Liquidity Inc." (2014) utilizza l'acqua come metafora della fluidità dei dati, dei capitali e delle immagini nel capitalismo globale, mostrando come queste ultime siano parte integrante di sistemi fluidi che determinano destini individuali e collettivi, agendo come attori invisibili ma potenti[55].

Infine, autori come Florian Apprich (il cui lavoro spesso si interseca con quello di Florian Cramer, specialmente nelle riflessioni sulle "immagini vive" e sulla post-media aesthetics) approfondiscono l'idea che l'immagine algoritmica sia primariamente un evento di calcolo, non più un evento estetico o di significato in sé. Per Apprich, la visione artificiale si basa su un'infrastruttura di dati massivi e processi computazionali in cui l'immagine è un punto dati, un insieme di informazioni numeriche che viene processato e interpretato da algoritmi, piuttosto che da occhi umani. Le sue analisi sui Deepfake e sulla sintesi di immagini generata dall'AI sono emblematiche: queste immagini non "rappresentano" la realtà, ma la "generano" sinteticamente a partire da dataset di dati esistenti. La loro funzione è creare una verosimiglianza computazionale, non una verità estetica. La capacità di manipolare e creare volti o eventi "autentici" (ma fittizi) rivela come l'immagine sia diventata un campo di battaglia per la percezione e per la costruzione di realtà alternative, basate non sull'osservazione, ma sulla manipolazione dei dati. In questo contesto, l'immagine, in quanto parte di dataset massivi, viene collezionata e annotata in volumi colossali, non per essere guardata o interpretata da esseri umani, ma per "insegnare" alle macchine a "vedere" in modo autonomo, a classificare, identificare, prevedere e persino generare nuove immagini. La sua efficacia è misurata dalla precisione con cui alimenta il sistema computazionale e dalla sua capacità di generare risposte automatizzate[56].

---

[54] Hito Steyerl, “In Defense of the Poor Image,” *e-flux* journal 10 (2009).
[55] Hito Steyerl, *Duty-Free Art: Art in the Age of Planetary Civil War* (London: Verso, 2017), 145–150.
[56] Clemens Apprich, Wendy Hui Kyong Chun, Florian Cramer, and Hito Steyerl, *Pattern Discrimination* (Lüneburg: meson press, 2018), 33–40.

Come già detto sopra, in sintesi, l'immagine algoritmica non è creata per stimolare l'emozione o la riflessione critica; al contrario, è un evento di calcolo, una sequenza di pixel e metadati la cui efficacia è misurata dalla sua utilità nel sistema computazionale. Di conseguenza, il suo valore non è più primariamente estetico o narrativo, ma funzionale e operativo, segnando una rottura definitiva con le tradizionali concezioni del visivo. Questa shift comporta una profonda revisione del nostro rapporto con il visivo: come dicevamo, le immagini non sono più solo finestre sul mondo o strumenti di narrazione, ma diventano ingranaggi invisibili di un vasto meccanismo di controllo, previsione e azione. Una forma di "visione senza occhio" che opera nel silenzio dei circuiti e degli algoritmi, plasmando la realtà in modi sempre più autonomi e decisivi, e sollevando questioni etiche e sociali di portata senza precedenti riguardo alla sorveglianza, al potere e alla definizione stessa della verità visiva. La profonda ridefinizione dell'immagine come "evento di calcolo" – un insieme di pixel e metadati primariamente destinato a essere letto e processato da macchine, piuttosto che interpretato dall'occhio umano – trova la sua applicazione più critica e le sue implicazioni più controverse nel contesto della guerra autonoma. Se, come abbiamo visto, l'immagine algoritmica è divenuta un ingranaggio invisibile in un vasto meccanismo di controllo e previsione che plasma la realtà, è proprio nell'arena militare che questa trasformazione raggiunge il suo apice. In questa sezione, pertanto, si analizzerà in che modo le immagini siano ormai parte integrante dell'infrastruttura operativa della guerra, fungendo da input essenziali per gli algoritmi predittivi che guidano le decisioni automatizzate, definendo nuove e complesse dinamiche di conflitto. Questa evoluzione è resa possibile dalla crescente fusione tra tecnologie civili avanzate – quali l'intelligenza artificiale, i big data e i sistemi autonomi – e le loro applicazioni nel dominio della difesa, offrendo nuove capacità e vantaggi strategici ai moderni eserciti. In questo contesto, gli algoritmi predittivi giocano un ruolo centrale, trasformando flussi di dati visivi e metadati in input per decisioni operative che possono avere conseguenze letali.

Un esempio emblematico è il sistema Lavender, un'intelligenza artificiale sviluppata dall'Unità 8200 dell'intelligence militare israeliana. Lavender è stato utilizzato per identificare migliaia di potenziali obiettivi di bombardamento a Gaza, classificando gli individui in base alla loro probabilità di essere coinvolti con le ali militari di Hamas o del Jihad Islamico Palestinese[57]. La sua operatività si svolgeva con una supervisione umana minima, talvolta limitata alla sola conferma del genere del bersaglio. Secondo diverse testimonianze, l'accuratezza umana è stata spesso sostituita dalla generazione di liste di obiettivi di massa, con il sistema sotto pressione per

[57] Yuval Abraham, "Lavender: The AI Machine Directing Israel's Bombing Spree in Gaza," *+972 Magazine* and *Local Call*, April 2024.

"portare più obiettivi". Questo ha comportato un margine di errore significativo, con casi in cui individui innocenti sono diventati bersagli a causa di associazioni indirette o semplici coincidenze (come un familiare che utilizzava lo stesso telefono del sospettato). Le conseguenze sono state drammatiche, con l'approvazione di numerosi obiettivi civili e l'uso di bombe "non guidate" che distruggevano intere abitazioni con i loro occupanti. L'immagine, in questo scenario, diventa un dato grezzo che, una volta processato dall'algoritmo, si traduce direttamente in una "kill list", evidenziando come la sua funzione sia passata da documentaria a esecutiva. Altri sistemi correlati, come "Gospel" per la localizzazione di strutture e "Where's Daddy?" per il tracciamento dei bersagli all'interno delle loro residenze, completano questo ecosistema di targeting automatizzato[58].

La geospazializzazione in tempo reale rappresenta un'altra frontiera in cui le immagini sono centrali nell'infrastruttura di guerra. Piattaforme come MetaConstellation di Palantir esemplificano questa capacità. MetaConstellation è un software che sfrutta la potenza delle costellazioni satellitari e dell'intelligenza artificiale per ottimizzare sensori orbitali, determinare dinamicamente la disponibilità di sensori e programmare in modo collaborativo la copertura di un'area[59]. La piattaforma integra modelli di intelligenza artificiale, inclusa l'Edge AI (AI elaborata direttamente sui sensori o sui satelliti), per identificare oggetti di interesse e riconfigurare i satelliti in base alle esigenze della missione. Gli utenti di MetaConstellation non ricevono dati sensoriali grezzi, ma direttamente "intuizioni algoritmiche", ovvero informazioni già elaborate e contestualizzate dagli algoritmi, accelerando le decisioni da parte degli operatori umani. Questo tipo di tecnologia è utilizzata per applicazioni diverse, dalla lotta agli incendi boschivi al tracciamento di sottomarini, dimostrando la versatilità e l'integrazione delle immagini come input per l'azione militare e di sicurezza. Palantir Gotham, un altro prodotto di Palantir, è ampiamente utilizzato da analisti militari e antiterrorismo per migliorare la capacità di prevedere la posizione di ordigni esplosivi improvvisati e ha contribuito ad aumentare la precisione e la letalità degli attacchi di artiglieria, come nel caso del supporto all'Ucraina[60]. Ciò evidenzia come la "consapevolezza situazionale condivisa – idealmente, in tempo reale o quasi reale" sia diventata un imperativo per le forze armate, con i veicoli aerei senza pilota (UAV) utilizzati per la ricognizione e lo sfruttamento delle tecnologie dell'informazione, inclusi i sistemi C4ISR integrati (Command, Control, Communications, Computers, Information and Intelligence systems).

---

[58] Amos Harel, "Gospel and Lavender: Israel's AI Targeting Systems in Gaza," *Haaretz*, May 2024.
[59] Palantir Technologies, "MetaConstellation: Artificial Intelligence for Real-Time Space Operations," Palantir (2022).
[60] Max Chafkin, "Palantir's Karp Is First Western CEO to Visit Zelenskyy in Kyiv," *Bloomberg*, June 2022.

In definitiva, le decisioni automatizzate basate su immagini e metadati segnano il passaggio a una guerra sempre più algoritmica. Le immagini, non più semplici strumenti di documentazione o rappresentazione, sono diventate componenti essenziali dell'infrastruttura operativa della guerra. Fungono da dati per algoritmi predittivi che identificano obiettivi, da input per sistemi di sorveglianza geospaziale che forniscono consapevolezza situazionale in tempo reale, e da catalizzatori per azioni dirette e spesso letali. Come discusso in The Black Box Society, sebbene in un contesto più ampio, la crescente dipendenza da "algoritmi segreti" e la "potenza predittiva" di modelli complessi, insieme all'opacità e alla segretezza di certi sistemi, riflettono principi che si applicano in modo ancora più acuto al dominio militare[61]. Questo sposta il baricentro del conflitto dalla tradizionale azione umana sul campo a una "guerra dei pixel", dove l'efficacia è misurata dalla velocità e precisione del calcolo algoritmico, e dove le immagini, in quanto dati, detengono il potere di determinare la vita e la morte con una logica inesorabile e spesso opaca. L'avanzamento delle immagini algoritmiche e la loro integrazione nelle infrastrutture di guerra autonome sollevano una questione fondamentale che travalica la semplice efficienza tecnologica: quella della fiducia computazionale. Al centro di questa problematica si trova il celebre problema dei generali bizantini, un modello concettuale proveniente dall'informatica distribuita che serve a comprendere l'impossibilità di raggiungere un consenso affidabile in ambienti caratterizzati dalla mancanza di fiducia, disinformazione o guasti. Immaginate un gruppo di generali bizantini che assediano una città nemica; devono coordinare un attacco simultaneo o una ritirata, ma comunicano solo tramite messaggeri che potrebbero essere traditori o inaffidabili. Alcuni generali stessi potrebbero essere traditori, inviando messaggi contraddittori. Il problema risiede nel fatto che, in assenza di un canale di comunicazione totalmente affidabile e di una fiducia reciproca incondizionata, è impossibile garantire che tutti i generali fedeli raggiungano un accordo unanime e coerente sull'azione da intraprendere.

Questo scenario, pur essendo una metafora storica, offre un modello potente per comprendere le sfide che emergono quando si delegano decisioni cruciali a reti decisionali distribuite composte da agenti autonomi in contesti conflittuali. Nella guerra computazionale odierna, i "generali" sono sensori, droni, algoritmi di targeting, sistemi di intelligenza artificiale che operano in ambienti complessi e imprevedibili, dove i dati visivi possono essere manipolati, le comunicazioni intercettate o corrotte, e gli stessi algoritmi possono presentare bias o fallimenti non prevedibili. Come possono questi agenti autonomi raggiungere un consenso affidabile su un obiettivo, una

[61] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2015), 3–10.

minaccia o un'azione, quando le informazioni visive che li alimentano sono elaborate e interpretate da macchine, e l'integrità del sistema non può essere pienamente garantita da un occhio o una mente umana? L'impossibilità di stabilire un consenso in presenza di "traditori" – intesi non solo come hacker o attori malevoli, ma anche come bug software, sensori difettosi o dataset di addestramento compromessi – evidenzia la profonda vulnerabilità dei sistemi autonomi a una forma di "guerra della fiducia". La transizione verso una guerra sempre più computazionale richiede una nuova forma di "fiducia" che non risiede più nell'affidabilità umana, ma nella fede nell'algoritmo. È una fiducia che si sposta dalla trasparenza e dalla comprensibilità dei processi decisionali umani all'opacità delle "scatole nere" algoritmiche. Accettare che le macchine prendano decisioni autonome basate su immagini e dati significa depositare una fede incondizionata nella correttezza dei loro calcoli e nella validità dei loro output, anche quando i processi interni rimangono imperscrutabili. Questo pone questioni etiche e operative immense: chi è responsabile in caso di errore? Come si può ratificare una decisione presa da un sistema distribuito che opera a velocità sovrumane? Il problema dei generali bizantini ci ricorda che, senza meccanismi robusti per garantire la coerenza e l'affidabilità in un ambiente intrinsecamente non fidato, la guerra computazionale rischia di precipitare in un caos decisionale, dove l'illusione del consenso può portare a conseguenze catastrofiche, senza che vi sia un unico punto di controllo o di responsabilità[62].

Il percorso intrapreso attraverso le trasformazioni dell'immagine, da medium di rappresentazione a operatore invisibile nel cuore dei conflitti globali, ci conduce a una riaffermazione della tesi centrale: l'immagine, nella contemporaneità, non è più né mero segno da interpretare né semplice documento da archiviare. Essa è piuttosto un operatore invisibile la cui funzione è intrinsecamente legata all'azione e al calcolo, non più alla contemplazione o alla narrazione. Attraverso l'analisi delle "immagini operazionali" di Farocki, della "logistica della percezione" di Virilio, e della proliferazione delle "immagini algoritmiche" studiate da Paglen, Steyerl e Apprich, abbiamo delineato una mutazione radicale del regime del visibile. L'immagine è ora un dato, un input per algoritmi, un catalizzatore di azioni che si svolgono al di là della percezione e del controllo diretto dell'uomo. In questa nuova era, l'apparato visivo contemporaneo è matrice bellica e codice decisionale. Le telecamere, i sensori, i satelliti e gli algoritmi che li elaborano non sono strumenti passivi, ma componenti attivi di un sistema che genera conoscenza operativa, identifica minacce, seleziona obiettivi e, in ultima istanza, determina azioni militari. Le immagini costituiscono il

[62] Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems* 4, no. 3 (1982): 382–401.

carburante per i motori predittivi della guerra autonoma, come dimostrato dai sistemi come Lavender e MetaConstellation, dove la "visione" è funzionale a una logica di efficienza e ottimizzazione del conflitto. Il controllo dello spazio visivo si è trasformato nel controllo dello spazio operativo, in cui la velocità di acquisizione e processamento delle immagini è sinonimo di vantaggio strategico e potere.

Giungiamo così alla constatazione che la guerra moderna si scrive con immagini che non vediamo e decisioni che nessuno prende. Le immagini che contano di più nel contesto bellico sono quelle prodotte e consumate dalle macchine, invisibili all'occhio umano, la cui funzione è quella di alimentare algoritmi che operano con logiche computazionali proprie. Le decisioni, un tempo appannaggio di comandanti e strateghi, sono ora sempre più delegate a intelligenze artificiali che operano a velocità e con una complessità tale da superare la capacità di supervisione umana. Il problema dei generali bizantini, in questo scenario, non è più solo un esercizio teorico, ma un'inquietante realtà operativa, dove la fiducia nell'algoritmo sostituisce la necessità di consenso umano, portando a esiti le cui responsabilità diventano sfumate e distribuite. La guerra del XXI secolo è una guerra delle immagini senza volto e delle decisioni senza firmatario, un conflitto che si combatte nel silenzio dei circuiti e degli algoritmi, plasmando la realtà attraverso una "visione senza occhio" sempre più autonoma e pervasiva.

2.4. Dalle immagini alla guerra algoritmica

Come abbiamo visto nei paragrafi precedenti, il passaggio dall'immagine che rappresenta all'immagine che opera è il tratto distintivo della visione automatizzata nel conflitto contemporaneo. Nel volume curato da Jens Eder e Charlotte Klonk, l'espressione *image operations* definisce proprio il nesso operativo di cui sopra, tra vedere e fare: le immagini non si limitano a rappresentare, ma diventano componenti di catene tecniche e strategiche, incidendo sull'esito degli eventi[63]. L'"immagine" smette di essere un semplice supporto informativo e diventa un *actant*, un dispositivo che connette sensori, analisi e decisioni. Nell'Introduzione, i curatori insistono su un punto cruciale: in molte situazioni di conflitto le immagini sono *agens et movens*, fattori causali che generano conseguenze inaspettate e spesso irreversibili. È il caso della fotografia di Kevin Carter con l'avvoltoio e la bambina affamata, del video *Collateral Murder* diffuso da WikiLeaks, o dell'esecuzione di James Foley da parte dell'ISIS: tre "immagini-evento" che non solo hanno documentato, ma hanno anche riconfigurato agende politiche, discussioni

[63] Jens Eder and Charlotte Klonk, eds., *Image Operations: Visual Media and Political Conflict* (Manchester: Manchester University Press, 2017), 2–5.

etiche, reazioni mediatiche e perfino decisioni militari. Per comprendere come le immagini possano *operare*, il volume richiama la genealogia delle *operational images* elaborata da Harun Farocki e discussa da Volker Pantenburg: immagini prodotte per guidare processi, calibrare strumenti, pilotare azioni - non per essere viste da un pubblico, ma per "far fare" a uomini e macchine. In questo registro, lo sguardo non è contemplazione ma funzione: sensori che tracciano, interfacce che classificano, overlay che trasformano il mondo in bersagli, traiettorie, allarmi. In altre parole, l'immagine è già calcolo; la visualizzazione è parte integrante dell'azione.

Il contributo dagli stessi Eder e Klonk mostra come questo regime visivo si dispieghi lungo due registri che spesso s'intrecciano. Da un lato, quello delle "immagini fredde", materiali progettati per essere processati da macchine e da operatori addestrati: flussi video elettro-ottici, radar, visioni sintetiche per l'addestramento e la simulazione, telemetrie e *feeds* di piattaforme senza equipaggio, *heads-up display* che guidano l'arma, mappe interattive per l'ISR. Dall'altro, il registro delle "immagini calde": clip, fotografie, *memes* e montaggi che mobilitano affetti nello spazio pubblico – propaganda, contro-propaganda, attivismo, giornalismo partecipativo –, dove pathos e viralità diventano risorse strategiche. Eder parla di *affective image operations*: montaggi, inquadrature e scelte di piattaforma che orientano emozioni e, con esse, consenso, indignazione, paura, solidarietà[64]. In questa doppia ecologia, immagini pensate per la macchina finiscono per alimentare campagne pubbliche, e immagini pensate per il pubblico vengono "riassorbite" nei dataset che addestrano i sistemi di riconoscimento: una circolazione che salda estetica, tecnica e potere. Nella seconda parte del volume, i saggi dedicati a guerra, insurrezione e contro-insurrezione scompongono invece la materialità di questo regime. Timothy Lenoir e Luke Caldwell seguono il trasferimento di tecniche ed estetiche dal *virtual reality* al campo di battaglia digitale: simulazioni, *serious games* e ambienti di *wargaming* definiscono formati percettivi che ritroviamo nelle interfacce operative, dove la "vista dall'alto" e l'astrazione grafica (symbology, *heatmaps*, *tracks*) guidano l'azione e la coordinano in rete[65]. Tom Holert, ragionando sul "*seen-unseen*" della guerra con i droni, mostra come la *sensorship* – nel doppio senso di sensorio e censura – decida ciò che è visibile e ciò che viene escluso: *cropping*, latenza, compressione, *black boxes* algoritmiche e protocolli classificati che filtrano l'esperienza degli operatori e l'accesso del pubblico, producendo una precisione apparente che spesso nasconde le ambiguità dell'inquadratura. La promessa di

[64] Jens Eder, "Affective Image Operations," in *Image Operations: Visual Media and Political Conflict*, ed. Jens Eder and Charlotte Klonk (Manchester: Manchester University Press, 2017), 89–107.
[65] Timothy Lenoir and Luke Caldwell, "The Military-Entertainment Complex," in *Image Operations: Visual Media and Political Conflict*, ed. Jens Eder and Charlotte Klonk (Manchester: Manchester University Press, 2017), 123–150.

trasparenza della visione elettronica convive, così, con un'architettura di opacità tecnica e istituzionale[66].

Il nesso tra immagine e decisione emerge in modo emblematico proprio nei tre casi di apertura del volume. La già citata foto di Carter, il video di Collateral Murder e la messinscena dell'ISIS mostrano che gli esiti non sono mai pienamente controllabili: l'immagine che dovrebbe "provare" o "convincere" può suscitare indignazione morale, attivare controversie sul montaggio, innescare contro-narrazioni, o persino spingere a escalation militari - effetti che eccedono le intenzioni dei produttori e mettono a nudo la natura intrinsecamente politica della circolazione visiva. L'operatività dell'immagine, dunque, non è lineare: è fatta di *feedback*, appropriazioni, contro-letture; e ogni catena operativa include snodi tecnici (piattaforme, standard, *formats*) e sociali (redazioni, comunità online, centri di comando) che trasformano di volta in volta significato e impatto. Il libro mantiene insieme questo piano "a freddo" e "a caldo" (un precipitato teorico che viene dalla teoria dei media di Marshall McLuhan[67]) illustrando come le operazioni visive si estendano dall'industria militare-securitaria alle economie dell'attenzione. Nel percorso iconografico del volume compaiono, per esempio, *cut-scenes* promozionali di UAV e persino interventi artistici come *#NotABugSplat*, in cui un ritratto a grandezza naturale viene installato a terra per "interpellare" lo sguardo aereo dei droni. Sono casi al confine tra propaganda industriale e attivismo visuale[68].

Accanto a ciò, il volume mette in scena l'uso investigativo delle immagini da parte di giornalisti, ONG e *civic technologists*. Il capitolo Exposing the Invisible di Tactical Tech mostra come pratiche di *visual forensics* - geolocalizzazione, analisi dei metadati, confronto morfologico - trasformino fotografie e video in prove operative: l'immagine "aperta" diventa materia di indagine. Sam Gregory riflette sulla *live-streamed co-presence, cioè* quando testimoni lontani possono intervenire in tempo reale e l'immagine smette di essere documento *post hoc* diventando interazione. In parallelo, Nicholas Mirzoeff parla di *visual commons*: una sfera condivisa (qualcosa di simile a quelle che sono state definite come immagini-matrice) in cui la produzione circolante di immagini consente contro-poteri e nuove forme di contro-visione comunitaria[69]. Tutto questo

---

[66] Tom Holert, "Aerial Perspectives: The Drone Gaze," in *Image Operations: Visual Media and Political Conflict*, ed. Jens Eder and Charlotte Klonk (Manchester: Manchester University Press, 2017), 151–165.
[67] Marshall McLuhan, *Gli strumenti del comunicare*, trad. it. di E. Capriolo (Milano: Il Saggiatore, 1967), 22–30.
[68] Mariam Saeed, Ali Rez Peled, and the French artist collective, "#NotABugSplat," 2014, available at https://notabugsplat.com
[69] Nicholas Mirzoeff, *How to See the World* (London: Pelican, 2015), 221–230.

conferma che l'operatività dell'immagine non è monopolio dello Stato o dei militari: è un terreno conteso, dove si confrontano attori con risorse, mezzi e obiettivi differenti[70]. Una domanda cruciale attraversa i saggi dedicati ad archivi e memoria: che cosa resta, e con quali effetti? Christian Christensen si chiede se i video di guerra "durino" e come si trasformino nei passaggi da YouTube a WikiLeaks, mentre Ariella Azoulay ragiona su archivi fotografici e "entità d'archivio" come luoghi in cui il potere decide che cosa è ricercabile[71]. L'immagine operativa non agisce solo nell'istante dello *strike* o del *breaking news*: prolunga la sua forza nelle infrastrutture che la conservano, la indicizzano, la ricontestualizzano, influenzando nel tempo la storiografia dei conflitti[72].

Letta in prospettiva della definizione di una guerra algoritmica (la guerra algoritmica è immagine che agisce), questa letteratura fornisce tre risultati analitici. Primo, chiarisce che la "visione" dei sistemi intelligenti è sempre una visione formattata. L'oggettività promossa è solo una presunta oggettività, composta da scelte normative travestite da necessità tecniche. Questo vale tanto per le immagini fredde della sensoristica quanto per le visualizzazioni che orientano l'opinione pubblica. Secondo, mostra che lo spazio operativo delle immagini è relazionale: ciò che un'immagine fa dipende dalle reti di attori, umani e non-umani, che la trasportano e la riusano – dai server alle redazioni, dai *feeds* militari alle piattaforme social. Terzo, sposta il problema della responsabilità: se vedere è già agire, allora le condizioni di produzione, filtraggio e circolazione delle immagini vanno progettate e governate con criteri di *accountability* e tracciabilità dei passaggi. Ne discende un punto metodologico utile per l'intera tesi: le immagini del conflitto non sono "illustrazioni" di un mondo che esiste a prescindere, ma infrastrutture che lo compongono, lo semplificano, lo gerarchizzano. Nell'era dell'AI, in cui la visione è delegata a catene di calcolo, la domanda non è solo cosa vedono le macchine, ma che cosa impariamo a vedere noi.

2.5. Nuova ecologia bellica

Per capire perché la "guerra algoritmica" si gioca tanto nelle infrastrutture militari quanto nello spazio civile delle immagini, è utile guardare alla Quarta rivoluzione industriale e al modo in cui ha rimescolato le filiere dell'innovazione. Quello che Yoram Evron e Richard Bitzinger chiamano

---

[70] Sam Gregory, "Cameras Everywhere: Ubiquitous Video Documentation of Human Rights, New Forms of Video Activism, and Human Rights 'Seeing,'" *Journal of Human Rights Practice* 2, no. 2 (2010): 191–207.
[71] Ariella Azoulay, *The Civil Contract of Photography* (New York: Zone Books, 2008), 83–90.
[72] Christian Christensen, "Disciplining the Viewer: YouTube, Real-Time Evidence and the 'War on Terror'," in *Image Operations: Visual Media and Political Conflict*, ed. Jens Eder and Charlotte Klonk (Manchester: Manchester University Press, 2017), 201–217.

military-civil fusion (MCF) descrive proprio questo processo: tecnologie sviluppate in ambito commerciale diventano la base per la potenza militare, perché oggi la spinta innovativa nasce più dal mercato che dai tradizionali apparati bellici[73]. La MCF non è solo uno slogan ma un vero dispositivo organizzativo: significa selezionare e adattare tecnologie civili per integrarle in sistemi d'arma e di comando, creando un "pozzo tecnologico" comune da cui attingono ricerca e sviluppo sia civile sia militare. È anche una promessa di velocità e riduzione dei costi, una scorciatoia verso l'innovazione. Il quadro comparativo mostra però differenze significative: negli Stati Uniti e in Israele, grazie a economie di mercato dinamiche e a un solido tessuto industriale, l'assorbimento di tecnologie civili nella difesa è stato relativamente agevole sin dagli anni Novanta. In Cina, invece, il carattere chiuso e corporativo dell'industria militare ostacola la collaborazione con i grandi gruppi civili, che faticano a realizzare grandi progetti tecnologici. In India, i colli di bottiglia negli acquisti militari e negli investimenti in R&S limitano la resa delle tecnologie della Quarta rivoluzione industriale in campo militare. La superiorità algoritmica non dipende solo dalla disponibilità di hardware e software, ma soprattutto da istituzioni solide, regimi di proprietà intellettuale, standard e governance dei dati[74].

Se guardiamo al dominio cibernetico, questo spostamento di *locus* innovativo è ancora più marcato. Fabio Cristiano descrive il nesso AI–cyber come un rapporto di interdipendenza: il cyberspazio è al tempo stesso il primo campo di impiego dell'AI e l'infrastruttura che ne consente addestramento, distribuzione e aggiornamento[75]. Qui l'adozione di algoritmi che automatizzano produzione di conoscenza e decisione alimenta l'illusione di una sicurezza "scientifica", mentre in realtà apre nuovi rischi: bias meccanici nella classificazione, ampliamento della *attack surface*, offuscamento delle responsabilità lungo catene decisionali distribuite. L'effetto, sul piano strategico, è un ulteriore sfumare del confine tra offesa e difesa e un intreccio sempre più fitto tra conflitti a bassa intensità, sabotaggio, spionaggio e operazioni d'influenza. Non sorprende, in questo contesto, che il tema dell'"uso responsabile" dell'AI in cyber sia entrato nell'agenda normativa internazionale e nei dibattiti su attribuzione, auditabilità e trasparenza[76]. Dal punto di vista tecnico-operativo, la letteratura raccolta nel volume curato da Cristiano segnala tanto le

---

[73] Yoram Evron, "China's Military-Civil Fusion: Origins, Drivers and Implications," *Journal of Strategic Studies* 43, no. 3 (2020): 400–420; vedi anche Richard A. Bitzinger, "Civil–Military Integration and Chinese Military Modernization," *Asian Security* 15, no. 1 (2019): 45–61.
[74] Ibid.
[75] Fabio Cristiano, Emilio Iasiello, and Massimiliano Signoretti, eds., *Artificial Intelligence and Cybersecurity: Emerging Challenges and Opportunities* (Leiden: Brill, 2023).
[76] Ibid., 145–160.

possibilità quanto i colli di bottiglia. L'AI abilita automazione del monitoraggio di rete, *early warning* e *patching* automatico; ma la stessa automazione produce nuove vulnerabilità: attacchi "in input" che ingannano i classificatori e *poisoning* dei dataset e dei modelli; inoltre, agenti autonomi dispiegati in ambienti contesi possono operare per lunghi periodi senza supervisione umana, con rischi di malfunzionamenti difficili da diagnosticare e correggere. In breve: mentre l'AI accelera i cicli *Identify–Protect–Detect–Respond–Recover*, la sua efficienza operativa dipende da rappresentazioni dei dati adeguate, infrastrutture di calcolo e protocolli *machine-to-machine* robusti; senza questi prerequisiti, velocità e scala si convertono in instabilità. Questa geografia dell'innovazione– fatta di cloud, semiconduttori, standard e regimi di scambio dati– spiega perché la "fusione" tra guerra e spazi civili sia innanzitutto una infrastruttura socio-tecnica e normativa. La corsa all'AI in cyber è anche una corsa a politiche industriali, a regimi di controllo delle esportazioni e a *rule-making* multilaterale: processi ONU su comportamento responsabile, codici etici (OECD, UNESCO), percorsi come GGE/OEWG e proposte di *Program of Action* che cercano di fissare paletti a un'adozione altrimenti interamente plasmata dalle logiche della competizione tra grandi potenze. In assenza di cornici per audit dei modelli, attribuzione e *de-biasing*, la promessa di deterrenza tecnologica tende a trasformarsi in un moltiplicatore di opacità e vulnerabilità sistemica.

È a questo punto che la lettura di Louise Amoore aiuta a tracciare la pericolosità dei collegamenti tra il "militare" al "civile". Nell'impianto teorico presentato da Louise Amoore la "guerra algoritmica" non coincide con una semplice militarizzazione della società, né con la mera privatizzazione della sicurezza[77]. È, piuttosto, la forma attraverso cui si dispiega nella vita quotidiana un'"architettura dell'inimicizia" che distingue e gerarchizza coppie come noi/loro, dentro/fuori, normale/sospetto; un prolungamento di logiche belliche entro pratiche amministrative, commerciali e statali che, sommandosi, rendono operativi confini e soglie invisibili[78]. In questo senso, la sicurezza appare come continuazione della guerra con altri mezzi: non perché uomini in uniforme occupino gli spazi civili, ma perché decisioni di fermo, esclusione e controllo vengono prese in base a calcoli che rendono visibile un rischio e lo trasformano in azione preventiva. È questa la tesi di fondo che Amoore denomina "algorithmic war" e che chiama

[77] Louise Amoore, "Algorithmic War: Everyday Geographies of the War on Terror," *Antipode* 41, no. 1 (2009): 51.
[78] Louise Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others* (Durham: Duke University Press, 2020), 55–65.

in causa, accanto allo Stato e al militare, attori tecnologici e infrastrutture mediatiche, in un circuito che rende la guerra un'ecologia diffusa di pratiche di selezione e sospetto.

Il primo segnale di questa nuova razionalità bellica atmosferica è lo slittamento di strumenti nati nel retail – regole di associazione e *decision trees* – nell'ambito della homeland security. L'idea alla base di questo slittamento, riconosce Amoore, è che, individuando regolarità in grandi insiemi di dati eterogenei, sia possibile stabilire connessioni probabilistiche tra persone, luoghi, transazioni, merci e movimenti, così da "collegare i puntini" prima che un evento avvenga. La Joint Inquiry statunitense del 2003, evocata dalla studiosa in merito agli eventi post 11 settembre, ha codificato questa promessa: i dati "c'erano", bisognava saperli associare. L'algoritmo, in questa narrazione, traduce tracce ex post in giudizi ex ante, autorizzando interventi *pre-emptive* sulla base di visualizzazioni del rischio. Non a caso lo stesso capo dell'ufficio ispettivo del Dipartimento per la Sicurezza Interna degli Stati Uniti, riconosce che "l'associazione non implica causalità", ma che l'algoritmo "scopre e visualizza relazioni" da cui discendono decisioni operative: ciò che appare sullo schermo dell'operatore – il *flag* che separa chi passa da chi viene fermato – è l'esito di una regia calcolante che ordina residui di vita ordinaria in una geografia schermata del sospetto. Amoore individua i passaggi tecnici obbligati di questa conversione: l'incrocio di identità disperse su database differenti, di variabili che "caratterizzano" condotte (pagamento in contanti, prenotazione sotto data, pattern di viaggio). Amoore mostra come questa grammatica si istituisca mediante fornitori che trasferiscono al decisore pubblico la promessa commerciale del *data mining*: connettere pattern e regolarità per "vedere prima" il rischio e per tradurre correlazioni in operatività. Il risultato è una semantica dell'*authorization by visualization*[79].

Il secondo movimento è spaziale. Amoore parla di una "geografia della locatabilità": tecnologie di tracciamento nate per le catene logistiche (RFID, sistemi di tagging) vengono integrate in documenti e varchi – passaporti e visti con chip, carte di trasporto, badge di accesso. In questo regime, la stessa espressione *smart borders* condensa una promessa: velocità e fluidità per alcuni, esposizione e attrito per altri. Amoore ricostruisce l'intreccio tra dimostrazioni tecnologiche (scansioni RFID di targhe e documenti in auto in corsa), gare pubbliche e contratti (il consorzio Trusted Borders per l'e-borders britannico), e routine aeroportuali come *MiSense*, che promettono di "semplificare il viaggio mantenendo la sicurezza", invitando i soggetti a offrirsi volontariamente

[79] Per un approfondimento sugli aspetti dell'*authorization* vedi Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Durham: Duke University Press, 2013).

al tracciamento in cambio di corsie rapide[80]. L'ambivalenza è costitutiva: le stesse tecnologie che lusingano con la semplificazione incastonano nuovi confini, traducendo desideri di rapidità in accettazione di un'esposizione permanente. Questa migrazione di tecniche dalla supply chain ai regimi di frontiera non è marginale: mette in continuità logiche di mercato e automatismi della sicurezza. I free zones thailandesi lo mostrano bene: RFID e smart card tracciano sia le merci sia i corpi dei lavoratori, e la stessa logica entra nei documenti di frontiera e nei permessi migratori, creando l'illusione di un mondo aperto ma segnato da nuove linee di separazione. Sistemi pensati per ridurre al minimo l'intervallo tra percezione e risposta – tra sensing e shooting, come scrive Jordan Crandall – si rispecchiano nei dispositivi di polizia preventiva che comprimono il tempo della decisione. Per Amoore, strumenti apparentemente tecnici trasferiscono scelte normative dentro calcoli che appaiono neutri: l'algoritmo nasconde le categorie che decidono chi è visibile e come. Da qui la diagnosi di una "colpa per associazione": quando le tecniche di data mining commerciale vengono applicate alla sicurezza, le *association rules* finiscono per marcare "corpi rischiosi", movimenti sospetti, transazioni anomale. Così, sequestri di merci nei porti, congelamenti di asset o fermi in frontiera derivano da procedure di calcolo che mascherano discriminazioni e violenza sotto un'apparenza tecnica e asettica. La formula "il confine come ultima linea di difesa" funziona solo perché l'attribuzione di rischio è già incorporata nell'algoritmo; e persino domande banali ("ha pagato in contanti? è frequent flyer? che pasto ha scelto in volo?") diventano criteri normativi di selezione.

Secondo Amoore, molte piattaforme nate in altri settori sono rientrate nella cassetta degli attrezzi della sicurezza e del controterrorismo. Per esempio, il sistema NORA, creato per l'intrattenimento, è stato poi adottato dal Dipartimento di Giustizia e da varie agenzie federali; allo stesso modo, IBM e il gruppo di Rakesh Agrawal hanno trasformato in strumenti di sicurezza nazionale le tecniche di "connettere i puntini" sviluppate inizialmente per il commercio. Si è così formata una filiera che collega consulenti, fornitori e apparati statali, dando vita a un'*expertise* ibrida, dove il punto centrale non è spiegare le cause, ma tradurre associazioni statistiche direttamente in decisioni operative. A livello più profondo, Amoore interpreta questa evoluzione come parte di un lungo processo di "addomesticamento del caso": grazie alla statistica, l'incertezza non viene eliminata, ma trasformata in una variabile gestibile. Non serve più cercare nessi causali certi, basta lavorare su probabilità e deviazioni. In questo quadro, il dubbio non è un ostacolo, ma la condizione stessa del potere: la minaccia diventa qualcosa di rappresentabile – come curva,

[80] Amoore, "Algorithmic War," 59–60, e vedi anche Louise Amoore, *Cloud Ethics*, 122–130.

distribuzione o scarto – e quindi agibile. L'algoritmo, in altre parole, non risolve l'incertezza ma la traduce in soglie di intervento, facendo della probabilità la base delle decisioni. È per questo che Amoore insiste sui dispositivi di visualizzazione: ciò che appare su uno schermo o in un report non si limita a descrivere il mondo, ma lo fa esistere operativamente, determinando come agiscono coloro che prendono le decisioni.

Le conseguenze per la fiducia sono immediate. In un regime di normalità differenziale, "fidarsi" non può significare delegare a un'astratta "AI": bisogna poter risalire alla provenienza dei dati. Senza questa trasparenza, la *authorization by visualization* si rovescia in sfiducia sociale, perché gli stessi parametri che promettono neutralità possono riprodurre, in forma numerica, gerarchie e pregiudizi già conosciuti (profilazioni etniche incorporate in misure biometriche). È qui che la "guerra algoritmica" rende visibili le sue geografie violente: non nella spettacolarità dell'uso della forza, ma nelle limitazioni diffuse delle possibilità di vita che derivano da controlli e selezioni incessanti, dalla metropolitana al varco aeroportuale, fino alla banca dati condivisa. Infine, la "geografia della locatabilità" mostra l'intimo intreccio tra piaceri e ansie: le stesse tecnologie che promettono comodità chiedono in cambio tracciabilità puntuale; e mentre alcuni "si fondono nella folla" godendo dell'attrito ridotto, altri vengono esposti a visibilità accresciuta, a verifiche continue, a controlli ripetuti – mentre i dati di viaggio vengono spesso estradati in tempo reale oltre confine. Le industrie militari e le aziende informatiche si mettono insieme per sviluppare le stesse tecnologie di sorveglianza e sicurezza. Questa risonanza tra logiche geo-economiche e pratiche statali definisce oggi il senso di "guerra" nei gesti ordinari della sicurezza. Parlare oggi di "guerra algoritmica" non significa quindi evocare un futuro remoto popolato da macchine senzienti, ma descrivere una trasformazione già in atto, in cui il potere militare si riorganizza attorno a dati, modelli predittivi e reti socio-tecniche che collegano sensori, decisori e attuatori. È una riconfigurazione che si articola tanto sul terreno operativo quanto negli spazi ordinari della vita sociale, dove pratiche di sorveglianza, profilazione e automazione decisionale anticipano e modellano il rischio, traducendo probabilità in azione.

2.6. Umano troppo umano

La diffusione endemica della realtà algoritmica e la crescente triangolazione tra spazio bellico, civile e cybernetico pongono una questione cruciale: quale sia oggi il ruolo dell'umano di fronte a questa nuova configurazione. L'impressione è di trovarsi di fronte a una "rivoluzione copernicana", cioè a un cambiamento epistemologico che sposta il centro del processo decisionale umano verso un nuovo asse dominato da dati, modelli predittivi e reti digitali. In questo scenario,

l'intelligenza artificiale non appare come un semplice strumento tecnico, ma come un insieme di pratiche, infrastrutture e linguaggi che trasformano il modo di concepire la strategia, la sicurezza e il conflitto. La guerra algoritmica non si limita infatti all'uso delle macchine sul campo: implica una ridefinizione dei rapporti tra tecnologia, organizzazione e decisione, in cui le categorie classiche della strategia – fini, mezzi, tempi – vengono ricalibrate alla luce delle capacità predittive delle macchine e dei vincoli delle architetture socio-tecniche che le sostengono.

La domanda centrale non è se le macchine possano sostituire l'umano, ma come gli esseri umani possano continuare a esercitare responsabilità e giudizio in un ambiente in cui le operazioni cognitive vengono sempre più delegate ad algoritmi. A questo nodo rispondono, con prospettive diverse, autori che convergono sulla necessità di interpretare l'AI non come un'entità autonoma, ma come un insieme di capacità modulari, la cui efficacia dipende dalle condizioni organizzative e culturali entro cui sono collocate. Un primo contributo fondamentale è quello di Avi Goldfarb e Jon R. Lindsay, che propongono una cornice analitica chiara per comprendere la natura algoritmica dei conflitti contemporanei. Secondo gli autori, l'AI oggi realmente dispiegabile – cioè, il machine learning "stretto" – va intesa soprattutto come tecnologia della predizione. Il compito principale degli algoritmi di apprendimento automatico è infatti quello di riempire spazi di incertezza: stimare probabilità, anticipare esiti, completare informazioni mancanti[81]. Tuttavia, ricordano Goldfarb e Lindsay, la predizione non è che uno degli elementi della decisione, che rimane un'operazione composta: accanto alla capacità di predire, servono dati di qualità e capacità di giudizio[82]. Quando la predizione diventa più economica, osservano, i suoi complementi – dati e giudizio – diventano ancora più preziosi e, in contesti strategici, inevitabilmente più contesi. Questa è la differenza principale tra ambito commerciale e ambito militare. Nei mercati civili, la disponibilità di dataset abbondanti, relativamente puliti e condivisi rende efficace l'automazione predittiva: basti pensare alla logistica delle consegne o agli algoritmi pubblicitari. In guerra, invece, l'informazione è scarsa, distorta, manipolabile, e gli obiettivi sono politicizzati: le condizioni che abilitano l'AI commerciale raramente si ripresentano. Per questo, sostengono gli autori, l'AI non elimina il ruolo dell'umano, ma lo rende più centrale. Non si tratta di sostituire il decisore con una macchina, ma di capire come e dove incastonare la predizione dentro architetture organizzative fatte di preferenze politiche, vincoli legali e responsabilità di comando. Questa impostazione conduce Goldfarb e Lindsay a proporre una tipologia dei diversi modi in cui l'AI può essere impiegata, che incrocia la

[81] Avi Goldfarb and Jon R. Lindsay, "Prediction and Judgment in Military Applications of Artificial Intelligence," in *Software-Defined Defence: Algorithms at War* (London: IISS, 2023), 12–15.
[82] Ibid., 16.

qualità dei dati disponibili con la chiarezza degli obiettivi da raggiungere. Ne risultano quattro regimi distinti. Nel primo caso, quando i dati sono abbondanti e gli obiettivi ben specificati, l'automazione può essere quasi totale. È lo scenario tipico di compiti amministrativi e logistici, caratterizzati da standardizzazione e ripetitività, in cui l'AI riesce a fornire un valore aggiunto senza margini di ambiguità. All'estremo opposto, invece, quando i dati sono scarsi o distorti e gli obiettivi controversi, la decisione deve restare saldamente nelle mani dell'umano, poiché mancano i presupposti minimi per affidarsi alla macchina[83].

Fra questi due poli si collocano le condizioni intermedie. La prima è quella che gli autori definiscono *premature automation*: situazioni in cui, pur essendo chiari gli obiettivi, i dati rimangono turbolenti o incompleti. In simili contesti la tentazione di delegare troppo all'AI può risultare pericolosa, perché un errore di classificazione rischia di tradursi in gravi conseguenze, come un targeting scorretto o addirittura un *'escalation* non intenzionale, soprattutto se la decisione automatizzata è collegata a effetti letali. La seconda condizione intermedia è quella dell'*human–machine teaming*. Qui la qualità dei dati è sufficiente a permettere all'AI di fornire supporti come mappe, riepiloghi o annotazioni che rafforzano la capacità di analisi, senza però sostituire il giudizio umano. È in questo regime che si collocano la maggior parte delle attività di pianificazione operativa e di analisi d'intelligence, dove l'AI funziona come un ausilio, non come un sostituto. In questa griglia analitica si concentra la forza del loro argomento: l'AI non è un attore indipendente, ma uno strumento che, a seconda della qualità dei dati e della chiarezza degli obiettivi, può costituire una risorsa o diventare una vulnerabilità. La posta in gioco non riguarda dunque la costruzione del modello "più intelligente", ma la capacità di garantire dati affidabili e di mantenere intatta la dimensione del giudizio umano. Dove la burocrazia funziona e standardizza i processi, l'AI può essere integrata e amplificare le capacità; dove prevalgono invece ambiguità e conflitti di valori, essa deve restare soltanto un supporto. Da qui discende la raccomandazione organizzativa: occorre investire parallelamente nelle competenze umane – formazione, dottrina, processi decisionali – e nella progettazione di interfacce che rendano visibili limiti, incertezze e compromessi. Senza queste precondizioni, il rischio è quello di costruire "disegni istituzionali fragili": apparati che promettono molto in termini di automazione, ma che finiscono per rivelarsi incapaci di gesti e margini di errore e responsabilità effettive.

[83] Ibid., 19–21.

Kareem Ayoub e Kenneth Payne spostano l'attenzione su un piano diverso: quello della psicologia della strategia. La loro tesi è chiara: non serve evocare scenari di intelligenza artificiale generale (AGI) per registrare un mutamento, perché già le forme di AI "ristrette" e modulari stanno incidendo profondamente sui tempi e sui modi della decisione strategica[84]. Questi sistemi, progettati per compiti specifici, hanno alcune caratteristiche peculiari: apprendono dall'esperienza, classificano grandi volumi di dati e operano a velocità inarrivabili per gli esseri umani. Tuttavia, ciò non produce automaticamente un vantaggio netto. Piuttosto, ridisegna gli incentivi: la rapidità degli algoritmi aumenta l'attrito tra velocità e comprensione, accentua la pressione a colpire in anticipo e rende più fragile l'allineamento tra fini politici e mezzi automatizzati. In altre parole, la velocità macchina non sostituisce il giudizio strategico, ma rischia di alterarne i tempi e le logiche[85]. Ayoub e Payne insistono sull'asimmetria fra il ritmo degli algoritmi e le capacità adattive delle istituzioni militari. Bias cognitivi, scorciatoie mentali (euristiche), dinamiche di gruppo e inerzie burocratiche non scompaiono con l'introduzione dell'AI: al contrario, vengono riflessi e amplificati in un ambiente in cui le interfacce e le visualizzazioni presentano scenari con un'apparente urgenza e precisione. È per questo che parlano di una mutazione cognitiva prima ancora che tecnologica: ciò che cambia non è solo la velocità di calcolo, ma il modo stesso in cui i decisori percepiscono la realtà operativa e le opzioni disponibili[86]. Per illustrare questa dinamica, gli autori recuperano una definizione classica di strategia: la direzione della violenza organizzata in un contesto antagonistico, dinamico e incerto. Seguendo Freedman e Strachan, ricordano che la strategia non è un piano rigido, ma un processo adattivo in cui gli obiettivi possono mutare durante l'interazione con l'avversario. In questa cornice, la dimensione cognitiva assume un ruolo centrale. L'immagine clausewitziana della guerra come un gioco di carte[87] è ancora utile: nel mazzo contano il caso, le emozioni e la frizione, e ciò mostra quanto sia inevitabile l'errore umano nella stima dei rischi in condizioni di incertezza. In questo scenario, l'AI modulare introduce una discontinuità funzionale. È in grado di elaborare masse di dati senza cadere nelle stesse distorsioni cognitive che affliggono gli esseri umani, e può comprimere in maniera drastica i tempi dell'analisi e dell'azione.

Tuttavia, questa apparente superiorità ha i suoi limiti: l'AI non condivide le nostre categorie di valore e fatica a valutare beni strategici intangibili come reputazione, credibilità o deterrenza[88].

---

[84] Kareem Ayoub and Kenneth Payne, "Strategy in the Age of Artificial Intelligence," in *Software-Defined Defence: Algorithms at War* (London: IISS, 2023), 26–28.
[85] Ibid., 29–30.
[86] Ibid., 31–33.
[87] Carl von Clausewitz, *Della guerra*, trad. it. di Piero Martinetti (Milano: Rizzoli, 2006), libro I, cap. 1, 43–47.
[88] Ayoub and Payne, "Strategy in the Age of Artificial Intelligence," 34–36.

Questi elementi, essendo radicati in dimensioni psicologiche e culturali, restano inaccessibili ai calcoli algoritmici. Di conseguenza, l'AI eccelle laddove gli obiettivi sono chiari e formalizzabili e i dati abbondanti, ma fallisce laddove i fini politici sono ambigui, mutevoli o contestati. La prudenza dei due autori si coglie anche nella loro critica alla retorica dei "giochi risolti". Il fatto che una macchina sia imbattibile in una variante di poker non autorizza a inferire una capacità generale di strategia. La guerra, spiegano, non è un gioco di poker, è molto più complessa, caratterizzata da causalità non lineare e da informazioni sempre incomplete. La velocità macchina è un fattore importante, ma non è mai l'unico. Sono le istituzioni e le culture strategiche a modellare l'adozione e l'uso degli algoritmi, filtrando, rallentando o distorcendo i vantaggi promessi e, in alcuni casi, aumentando i rischi di instabilità se la corsa alla velocità porta a segnali più aggressivi e meno interpretabili dall'avversario. Da qui deriva il loro invito alla cautela progettuale; non bisogna confondere previsione e decisione: l'algoritmo ottimizza rispetto a una metrica, ma la scelta di quella metrica è sempre un atto politico. Bisogna inoltre tenere a bada l'antropomorfismo, evitando di attribuire alle macchine capacità umane. Termini come "apprendimento" o "errore" sono utili come metafore, ma rischiano di diventare travestimenti linguistici che spingono a deleghe improprie. Infine, occorre ricordare che la strategia ha una forte componente culturale: le istituzioni, le norme e i repertori nazionali di azione plasmano il modo in cui si definiscono gli obiettivi e si interpretano i segnali. Lo stesso sistema modulare, inserito in contesti organizzativi diversi, può quindi produrre comportamenti e rischi differenti[89].

Se Ayoub e Payne hanno mostrato il lato cognitivo della trasformazione algoritmica, Jensen, Whyte e Cuomo si concentrano invece sull'aspetto organizzativo. La loro proposta parte da una domanda pratica: che cosa porta concretamente l'intelligenza artificiale sul campo di battaglia? La risposta si articola in tre funzioni fondamentali: apprendere, percepire e muovere[90]. La prima funzione, apprendere, riguarda l'introduzione di modelli capaci di classificare, ordinare per priorità e sintetizzare i segnali, così da ridurre i tempi del ciclo decisionale noto come osserva–orienta–decidi–agisci. La seconda, percepire, si riferisce alla capacità di fondere flussi eterogenei – immagini elettro-ottiche, radar, telemetria, traffico digitale – restituendo una rappresentazione probabilistica più densa e coerente dell'ambiente operativo. Infine, muovere significa tradurre tale rappresentazione in traiettorie e ingaggi di sistemi senza equipaggio, con la promessa di maggiore precisione e minori rischi per il personale militare. Il punto cruciale, osservano gli autori, non è la

[89] Ibid., 37–38.
[90] Eric Jensen, Christopher Whyte, and Carla Anne Robbins Cuomo, "Learning, Sensing, Moving: AI on the Battlefield," in *Software-Defined Defence: Algorithms at War* (London: IISS, 2023), 40–44.

pura capacità tecnica dell'automazione, ma la frizione che si genera quando queste funzioni vengono inserite nel vivo delle organizzazioni militari. La velocità macchina si scontra con regole d'ingaggio, catene di comando, vincoli giuridici e responsabilità legali. È da questa tensione che emergono i cosiddetti "fantasmi nella macchina": disallineamenti fra l'agenzia umana e la condotta della guerra[91]. La loro tesi rimane volutamente prudente. Gli algoritmi funzionano bene in domini circoscritti, ma la guerra è un ambiente avversario e adattivo, che resiste a schemi fissi. L'introduzione rapida di sistemi complessi non garantisce quindi un vantaggio lineare, ma può modificare incentivi e stabilità in maniera imprevedibile. Per questo Jensen, Whyte e Cuomo insistono nel considerare la triade *learn–sense–move* come un insieme modulare e non come un blocco unico: ogni capacità richiede dati addestrati sul contesto rilevante, feedback affidabili, integrazione con i sistemi già esistenti e regole organizzative di controllo.

Quando queste condizioni mancano, i rischi crescono: dall'*overtrust*, cioè l'eccessiva fiducia riposta nella macchina, al sovraccarico cognitivo degli operatori, fino all'automazione di errori sistematici e all'amplificazione delle incertezze. La vera superiorità promessa dall'AI non risiede dunque nella potenza della singola rete neurale, ma nella capacità delle organizzazioni militari di incastonarla in cicli decisionali responsabili. A livello operativo, gli autori interpretano l'AI come un "motore" delle campagne informazionali. L'automazione dell'ISR e la pianificazione assistita promettono infatti di "vincere la lotta per l'informazione prima del primo colpo". Tuttavia, l'inserimento di questi sistemi in architetture di comando e controllo reali – multilivello, multinazionali e soggette a vincoli giuridici e politici – introduce inevitabili attriti che ridimensionano i rendimenti. L'efficacia di un algoritmo di assegnazione dei sensori, ad esempio, dipende dalla qualità e dalla provenienza dei dati, dalla compatibilità con sistemi preesistenti e da criteri di priorità che, in ultima analisi, restano sempre scelte politiche tradotte in parametri tecnici. La stessa accelerazione introdotta dalla macchina nel ciclo decisionale può diventare un rischio: l'azione corre più veloce della comprensione e l'agente umano scivola "dietro" i processi tecnici. È in questo squilibrio che si manifestano i "fantasmi nella macchina": disallineamenti che mettono a rischio la stabilità operativa. Sul piano strategico, la triade *learn–sense–move* apre la possibilità di immaginare nuove "teorie della vittoria", fondate sulla superiorità informativa e sulla rapidità dei processi decisionali. Ma gli autori mettono in guardia dal considerare questo scenario come una rivoluzione lineare: l'adozione dell'AI non avviene nel vuoto, bensì è mediata dal labirinto burocratico delle organizzazioni di difesa, dalle culture di comando e dal diritto bellico. In

[91] Ibid., -45–47.

situazioni di crisi, i guadagni di velocità possono persino ridurre gli spazi di de-escalation e comprimere il controllo politico.

In questa prospettiva, l'AI non sostituisce la strategia: la costringe a riformulare la relazione fra strumenti ad alta automazione e fini politici. Deterrenza, segnali, attribuzione e responsabilità rimangono dimensioni centrali, che nessun algoritmo può risolvere autonomamente. A completare il quadro intervengono Evron e Bitzinger, i quali spostano lo sguardo sulla geografia dell'innovazione militare. Secondo i due autori, l'innovazione oggi fluisce soprattutto attraverso filiere civili – cloud, semiconduttori, piattaforme di *machine learning* – e gli Stati cercano di "fondere" ecosistemi commerciali e requisiti della difesa all'interno di regimi comuni di standard, proprietà intellettuale e circolazione dei dati. La cosiddetta *military-civil fusion* non è dunque uno slogan retorico, ma una vera e propria infrastruttura: chi è in grado di tradurre bisogni operativi in soluzioni industriali, proteggendo al contempo catene di fornitura e flussi informativi, accumula vantaggi incrementali difficili da imitare[92]. Nel dominio cibernetico, questa dinamica è ancora più evidente. L'intreccio tra automazione cognitiva e operazioni offensive rende sempre più labile il confine tra offesa e difesa. La letteratura su AI e cybersicurezza mette in luce l'ambivalenza di questo passaggio: la stessa automazione che promette rilevazione precoce, triage delle minacce e *patching* predittivo può introdurre nuove vulnerabilità, come il *poisoning* dei dataset, gli attacchi agli input o le dipendenze da protocolli macchina-a-macchina. In questo scenario, la pretesa di "scientificità" rischia di trasformarsi in illusione, se non accompagnata da audit indipendenti, da regimi di attribuzione e da meccanismi di responsabilità che sappiano integrare dimensione tecnica, legale e strategica[93]. Da qui si può ricavare un lessico di lavoro che integra le riflessioni precedenti e aiuta a leggere la guerra algoritmica nel suo complesso.

- La prima parola-chiave è rete: la tradizione net-centrica mostra che il valore non risiede nella potenza isolata dei singoli sistemi, ma nella loro interconnessione e nella capacità di condividere informazioni situazionali. In questo senso, mantenere "l'uomo al centro" non è un vezzo umanistico, ma una condizione organizzativa di efficacia, che dipende da interoperabilità, dottrina e formazione.

---

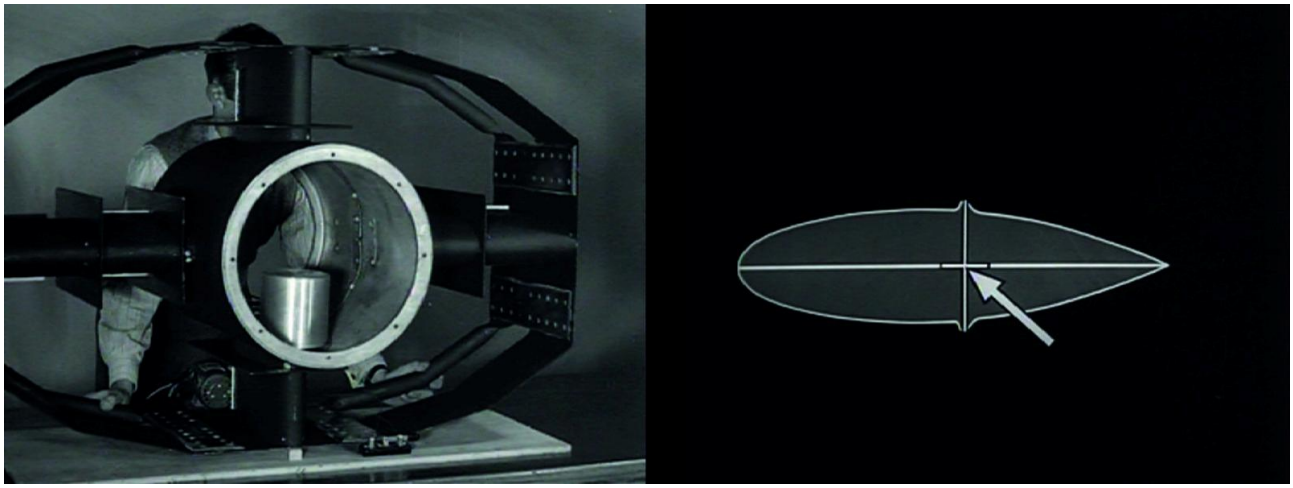
[92] Yoram Evron, "China's Military-Civil Fusion: Origins, Drivers and Implications," *Journal of Strategic Studies* 43, no. 3 (2020): 400–420; Richard A. Bitzinger, "Civil–Military Integration and Chinese Military Modernization," *Asian Security* 15, no. 1 (2019): 45–61.

[93] Fabio Cristiano, Emilio Iasiello, and Massimiliano Signoretti, eds., *Artificial Intelligence and Cybersecurity: Emerging Challenges and Opportunities* (Leiden: Brill, 2023), 121–135.

- La seconda è predizione: l'AI rende più economico prevedere, ma la qualità della decisione resta proporzionale al grado di trasparenza di metriche, soglie e responsabilità. Senza questa esplicitazione, l'automazione non riduce l'incertezza ma amplia la superficie di attacco, sia tecnica sia cognitiva.
- La terza è visualità: immagini e interfacce non sono strumenti neutri, ma componenti centrali del processo decisionale, perché condizionano ciò che appare come realtà e ciò che, di conseguenza, diventa azione legittima.

Tutto converge, infine, su una questione decisiva: l'accountability. Che si tratti delle geografie del sospetto che attraversano lo spazio civile, dei "fantasmi nella macchina" che emergono nelle catene di comando e controllo, delle predizioni che vanno ricondotte a fini politici o delle immagini che agiscono nei teatri informativi, il problema non è tanto avere simbolicamente "l'umano nel loop". La vera sfida è progettare circuiti decisionali in cui la responsabilità umana sia effettiva: informata sui limiti dei modelli, tracciabile lungo le decisioni, verificabile nei suoi effetti. È in questo spazio – più istituzionale che tecnologico – che la guerra algoritmica rivela il suo discrimine tra promessa e pericolo. Solo la capacità di mantenere responsabilità chiare e intellegibili potrà evitare che l'accelerazione tecnica si trasformi in opacità strategica.

CASI STUDIO



Harun Farocki, War at a Distance, © Harun Farocki, 2003.

3.1. Il sistema "Lavender" costruzione dell'urgenza e ridefinizione delle soglie operative"

Dopo gli attacchi di Hamas del 7 ottobre 2023, Israele ha lanciato l'operazione "Swords of Iron" a Gaza. È in questo quadro che l'uso di sistemi di supporto alle decisioni basati su AI (AI DSS) da parte delle Forze di Difesa Israeliane (IDF) è diventato un tema centrale del dibattito pubblico e accademico. Il perimetro spazio-temporale che consideriamo va da ottobre 2023 ad aprile 2025 e coincide con l'emersione mediatica di due snodi chiave: a dicembre 2023 le inchieste su "Gospel/Habsora"; ad aprile 2024 l'inchiesta su "Lavender" e la discussione sul tool di tracciamento "Where's Daddy?"[94]. Queste rivelazioni hanno generato reazioni ufficiali dell'IDF, prese di posizione di organismi internazionali e un ampio dibattito legale sull'impatto umanitario della targeting *enterprise* israeliana. Il trigger dichiarato per l'innovazione (o l'espansione) di questi sistemi è l'esigenza di aumentare drasticamente il ritmo di produzione dei bersagli. L'ex Capo di Stato Maggiore Aviv Kohavi ha affermato che, nella guerra del maggio 2021, la "macchina" avrebbe generato circa 100 bersagli al giorno, rispetto a circa 50 all'anno in passato[95]. Questa accelerazione, che inquadra la velocità come valore strategico, è stata presentata come funzionale a mantenere campagne aeree prolungate in un contesto urbano densissimo. Le inchieste hanno sostenuto che "Lavender" avrebbe marcato decine di migliaia di nominativi come potenziali obiettivi, riducendo di fatto la latenza tra segnalazione e azione; l'IDF, da parte sua, ha respinto l'idea di una "kill list" automatica, descrivendo tali strumenti come ausili analitici sottoposti a verifica umana.

Nel contesto di Gaza sono stati riportati quattro sistemi di supporto decisionale algoritmico, ognuno con un ruolo specifico nell'architettura di targeting. Gospel (Habsora) è un motore di raccomandazione orientato a obiettivi strutturali: incrocia dati di intelligence e mappe infrastrutturali per individuare edifici associati a funzioni militari (depositi, centri di comando, infrastrutture di comunicazione), proponendoli come target ad alta priorità[96]. Lavender è stato

---

[94] Si veda l'inchiesta, molto ripresa da vari organi di stampa e informazione, di Yuval Abraham, "Lavender: The AI Machine Directing Israel's Bombing Spree in Gaza," *+972 Magazine* and *Local Call*, April 2024; Amos Harel, "Gospel and Lavender: Israel's AI Targeting Systems in Gaza," *Haaretz*, dicembre 2023.

[95] Yaakov Lappin, "How Israel's AI Targeting System Changed Warfare in Gaza," *Jerusalem Post*, July 7, 2024.

[96] Il commento del Royal United Services Institute spiega che il sistema di intelligenza artificiale "Habsora" (soprannominato "Gospel") utilizza dati di intelligence aggregati per generare obiettivi di bombardamento a Gaza, includendo una valutazione delle probabili vittime civili; un analista umano conferma le raccomandazioni prima che vengano trasmesse ai comandanti sul campo. Vedi Royal United Services Institute (RUSI), "Israel's Targeting AI: How Capable Is It?," *RUSI Commentary*, 8 febbraio 2024.

descritto come un AI decision-support system o "database potenziato", che integra grandi volumi di informazioni da registri telefonici, sociali e biometrici per attribuire punteggi di probabilità a individui sospettati di appartenenza militante: il risultato è la generazione semi-automatica di liste di bersagli umani[97]. Where's Daddy? agisce in continuità con Lavender, fornendo un tracciamento temporale e geospaziale degli individui già marcati, con l'obiettivo di colpirli quando rientrano a casa o si trovano in contesti di vita privata, aumentando così la prevedibilità dell'azione. A questi si affiancano altri strumenti di filtraggio e correlazione dati che permettono di integrare segnali eterogenei in una pipeline unica di selezione e aggiornamento dei target[98]. Come visto attraverso gli studiosi citati precedentemente, nel complesso, questi sistemi non si limitano a fornire "informazioni", ma trasformano dati grezzi in raccomandazioni operative, riducendo l'intervento umano nella catena di comando e sollevando questioni cruciali sulla responsabilità e sull'automazione del giudizio letale[99].

Questo caso esamina il dibattito intorno a "Lavender", un sistema capace di generare elenchi di obiettivi a partire da grandi moli di dati e segnali, e difeso in ambito militare-accademico come strumento di supporto decisionale impiegato per accelerare l'analisi e migliorare la coerenza fra fonti. Il sistema Lavender, sviluppato dall'Unità 8200 – una divisione di intelligence delle Israel Defence Forces (IDF) – può essere inquadrato nella categoria dei Decision Support Systems (DSS), ossia strumenti informatici concepiti per assistere gli operatori umani nel prendere decisioni complesse. Tali sistemi analizzano e classificano grandi quantità di dati, restituendo informazioni utili oppure proponendo possibili alternative che l'operatore può valutare per orientare una determinata linea d'azione. Nello specifico, Lavender si basa su algoritmi di intelligenza artificiale e ha come obiettivo primario quello di individuare potenziali affiliati di Hamas o del Movimento per la Jihad Islamica in Palestina. Gli individui vengono classificati sulla base di informazioni raccolte da un sistema di sorveglianza di massa sui cittadini palestinesi e ricevono un punteggio compreso tra 1 e 100, che indica il grado di probabilità della loro appartenenza a tali organizzazioni. La classificazione si fonda su caratteristiche predeterminate, derivate dai profili di militanti già noti, ma non rese pubbliche nelle loro specificità.

---

[97] Yuval Abraham, "Lavender: The AI Machine Directing Israel's Bombing Spree in Gaza," *+972 Magazine* and *Local Call*, April 2024.
[98] Yuval Abraham, "The Israeli Army's Cloud: Amazon, Google and Microsoft Are Building the Infrastructure of Occupation," *+972 Magazine*, 28 giugno 2022.
[99] Louise Amoore, "Algorithmic War: Everyday Geographies of the War on Terror," *Antipode* 41, no. 1 (2009): 49–69.

È importante sottolineare sin da subito un elemento decisivo: Lavender, come il sistema The Gospel, non deve essere confuso con i cosiddetti sistemi d'arma autonomi, nei quali l'intelligenza artificiale è direttamente associata al controllo e all'impiego di armamenti. Gli Autonomous Weapon Systems (AWS), chiamati LAWS quando hanno effetti letali, sono sistemi d'arma capaci di selezionare e colpire obiettivi senza un intervento umano diretto nelle funzioni più delicate, cioè l'identificazione del bersaglio e l'uso della forza. Il Comitato Internazionale della Croce Rossa (ICRC) ha sottolineato che proprio queste "funzioni critiche" definiscono il problema centrale: quanto controllo umano deve rimanere per assicurare che i principi del diritto internazionale umanitario – distinzione tra civili e combattenti, proporzionalità e precauzione – vengano rispettati[100]. Nel caso che interessa questa tesi, strumenti come Lavender o Gospel non rientrano ancora nella categoria delle armi autonome vere e proprie, come i missili Harpy o i sistemi di difesa aerea Iron Dome[101]. Essi si collocano piuttosto nella sfera dei sistemi di supporto alle decisioni, che raccolgono e classificano grandi quantità di dati, producendo liste di potenziali obiettivi. La pianificazione e l'esecuzione degli attacchi rimangono formalmente sotto la responsabilità degli operatori umani, ma il problema nasce dal fatto che il controllo esercitato dall'uomo è spesso minimo o ridotto a una mera ratifica delle raccomandazioni algoritmiche. Nel caso esaminato dalla tesi, si tratta piuttosto di strumenti destinati alla fase di identificazione preliminare dei potenziali obiettivi. La pianificazione e l'esecuzione materiale dell'attacco rimangono, almeno formalmente, sotto la responsabilità degli operatori umani. Per questo motivo, tali sistemi devono essere tenuti distinti da armamenti già impiegati da Israele, come la difesa aerea Iron Dome o i missili Harpy NG, i quali rientrano pienamente nella categoria dei sistemi autonomi.

Dal punto di vista tecnico, l'autonomia in guerra non è una prospettiva futura ma una realtà già presente. Esistono droni e munizioni circuitanti capaci di pattugliare un'area e colpire in autonomia, sistemi di navigazione e di riconoscimento dei bersagli che operano senza input costanti da parte dell'uomo, e prototipi di sciami di droni in grado di comunicare tra loro e prendere decisioni collettive. Il citato rapporto del SIPRI del 2017 ha mostrato come alcune funzioni siano già oggi automatizzate, dalla navigazione alla gestione del fuoco, e come altre stiano evolvendo rapidamente[102]. Sul piano normativo, il quadro di riferimento resta quello dei trattati esistenti, in particolare il Primo Protocollo Addizionale del 1977, che pone limiti ai mezzi e metodi di guerra,

[100] International Committee of the Red Cross, "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach," *International Review of the Red Cross* 102, no. 913 (2021): 463-479.
[101] SIPRI, *Mapping the Development of Autonomy in Weapon Systems* (Stockholm: SIPRI, 2017).
[102] Ibid., 15-20.

vieta gli attacchi indiscriminati e richiama, attraverso la clausola Martens[103], i principi di umanità e di coscienza pubblica anche nei casi in cui non esistano regole specifiche[104]. Il problema etico e operativo riguarda la difficoltà di tradurre in algoritmi giudizi che richiedono sensibilità e contesto umano, come distinguere un combattente da un civile, riconoscere un gesto di resa o valutare l'intenzione di un soggetto. Inoltre, l'evoluzione tecnologica, con la miniaturizzazione dei droni e lo sviluppo di sistemi coordinati basati sull'intelligenza artificiale, spinge verso scenari in cui i tempi decisionali sono sempre più compressi e la letalità più difficile da controllare. Come per gli altri mezzi e metodi di guerra, anche i DSS utilizzati a scopi militari sono soggetti ai limiti previsti dal diritto internazionale umanitario. L'articolo 35(1) del Primo Protocollo Addizionale (IPA) sancisce infatti che la libertà delle parti nella scelta dei mezzi e dei metodi di guerra non è illimitata[105]. Sono vietati, tra gli altri, i sistemi che causano sofferenze inutili (art. 35(2) IPA), quelli che provocano danni estesi, durevoli o gravi all'ambiente naturale (art. 35(3) IPA) e, soprattutto, quelli che risultano indiscriminati, cioè incapaci di distinguere tra civili e combattenti o che producono effetti indiscriminati (art. 51(4)(b)(c) IPA)[106]. Non solo: il diritto internazionale umanitario non disciplina unicamente la natura dei mezzi di guerra, ma anche le modalità del loro impiego, attraverso il cosiddetto diritto del targeting, ossia l'insieme di regole che governano la pianificazione e l'esecuzione degli attacchi.

L'uso di sistemi DSS in conflitto non rappresenta una novità in sé, ma nel caso di Lavender emergono aspetti particolarmente problematici. Le criticità individuabili sono principalmente tre: a) l'errata identificazione degli obiettivi, b) l'assenza di un adeguato controllo umano e c) le modalità concrete di esecuzione degli attacchi. Il primo problema riguarda la qualità dei dati su cui Lavender è stato addestrato. La genericità di tali informazioni ha portato a frequenti errori, come la confusione tra militanti e categorie di personale civile, ad esempio poliziotti o operatori della protezione civile[107]. Il secondo problema si lega invece al ridotto livello di supervisione: secondo l'inchiesta giornalistica, per la maggior parte dei target non veniva effettuata alcuna verifica ulteriore, nonostante fosse noto che il margine di errore del sistema si attestava intorno al

[103] Clausola Martens, Protocollo I aggiuntivo alle Convenzioni di Ginevra, art. 1(2).
[104] Protocollo Addizionale alle Convenzioni di Ginevra del 12 agosto 1949 relativo alla protezione delle vittime dei conflitti armati internazionali (Protocollo I), 8 giugno 1977, artt. 35–36, 48 e 51.
[105] Protocollo Addizionale I alle Convenzioni di Ginevra del 12 agosto 1949 relativo alla protezione delle vittime dei conflitti armati internazionali, 8 giugno 1977, art. 35.
[106] Protocollo Addizionale I, art. 51(4)(b)(c); International Committee of the Red Cross (ICRC), *Customary International Humanitarian Law*, Regola 7.
[107] Yuval Abraham, "Lavender: The AI Machine Directing Israel's Bombing Spree in Gaza," *+972 Magazine* and *Local Call*, April 2024.

10%. Per i militanti di basso rango ("*junior militants*") era richiesto soltanto di confermare che l'obiettivo fosse di sesso maschile, mentre ulteriori controlli erano previsti solo per figure di alto profilo[108]. Questo approccio, che consentiva di accelerare le procedure, ha inevitabilmente aumentato il rischio di colpire individui non appartenenti a Hamas. Si comprende così come l'impiego di Lavender comprometta il principio di distinzione, che obbliga le parti a distinguere in ogni momento civili e beni civili da un lato e obiettivi militari dall'altro (art. 48 IPA; Regola 7 CICR Customary IHL). Ad esso si aggiunge la violazione del principio di precauzione, che impone di verificare costantemente la legittimità del target[109].

Le modalità operative aggravano ulteriormente il quadro. Grazie al sistema di tracciamento Where's Daddy? i target venivano monitorati fino al rientro nelle abitazioni, momento in cui erano più facilmente colpibili[110]. Tuttavia, in tali circostanze la presenza delle famiglie era altamente probabile, con conseguenti perdite civili. Pur essendo stati introdotti software per stimare il numero di persone all'interno degli edifici, spesso tali stime non venivano verificate e si basavano su dati obsoleti. L'uso di bombe a caduta libera (*dumb bombs*), scelte per ragioni di costo ma caratterizzate da scarsa precisione, ha ulteriormente aumentato i danni collaterali. Inoltre, secondo fonti interne, l'IDF aveva stabilito soglie predeterminate di perdite civili "accettabili": fino a 15-20 per militanti di basso livello, e fino a 100 vittime collaterali nel caso di obiettivi di alto rango[111]. Questo modus operandi sembra porsi in tensione con il principio di proporzionalità (come definito dall'art. 57 IPA; Regola 14 CICR Customary IHL), che vieta attacchi in cui i danni collaterali prevedibili risultino eccessivi rispetto al vantaggio militare concreto e diretto atteso. Nel caso di Lavender, il calcolo non avveniva caso per caso, ma secondo criteri standardizzati, con un tetto fisso di "civili tollerati", in contrasto con gli obblighi internazionali. Alla luce di tali elementi, appare evidente che l'utilizzo di Lavender ponga questioni di conformità con il diritto internazionale umanitario. In particolare, il rischio che l'algoritmo produca effetti indiscriminati, unito alla mancanza di controlli adeguati da parte degli operatori umani, mina i principi di distinzione, precauzione e proporzionalità. Non si può escludere che la consapevolezza dell'errore

[108] Amos Harel, "Gospel and Lavender: Israel's AI Targeting Systems in Gaza," *Haaretz*, December 2023.
[109] Protocollo Addizionale I, art. 57; Federico Longobardo, *Il principio di precauzione nel diritto dei conflitti armati* (Napoli: Editoriale Scientifica, 2020).
[110] Yuval Abraham, "The System Known as 'Where's Daddy?' and the Targeting of Homes in Gaza," *+972 Magazine*, April 2024.
[111] Protocollo Addizionale I, art. 57; ICRC, *Customary International Humanitarian Law*, Regola 14.

intrinseco del sistema, unita alla scelta di non effettuare verifiche ulteriori, possa configurare responsabilità anche sul piano del diritto penale internazionale[112].

Il caso Lavender mette in luce come l'uso dei DSS in guerra richieda un controllo umano significativo, condizione ribadita da vari Stati, organizzazioni internazionali e ONG[113]. L'esperienza israeliana dimostra i rischi derivanti dall'affidamento quasi esclusivo a sistemi algoritmici nella selezione di target: la possibilità di identificare decine di migliaia di obiettivi in pochi istanti, se non accompagnata da reali verifiche umane, si traduce in conseguenze devastanti per la popolazione civile e in una compromissione dei principi fondamentali del diritto umanitario. Su questi punti esistono versioni divergenti. L'IDF nega di utilizzare un sistema che "identifica terroristi in modo autonomo" e definisce Lavender "un database per incrociare fonti", con verifica umana e valutazioni di proporzionalità caso per caso; l'esercito respinge inoltre l'idea di una politica deliberata di colpire in abitazioni familiari[114]. Le inchieste giornalistiche, invece, riportano un'ampia dipendenza dagli output dei sistemi per accelerare la selezione dei bersagli individuali. Per trasparenza, qui segnaliamo entrambe le posizioni. Gli attori coinvolti toccano più sfere. Sul versante pubblico, oltre ai vertici politici e ai comandi operativi dell'IDF, sono centrali il Direttorato Intelligence, l'Unità 8200 (per lo sviluppo e l'uso dei sistemi), l'Aeronautica e i consulenti legali interni. La letteratura legale militare tende a qualificare questi strumenti come *decision support* (e non come decisione automatica), pur richiamando i rischi di automation bias e di erosione del controllo umano quando la velocità è massimizzata.

Sul versante privato/tecnico infrastrutturale, il contesto di Project Nimbus (contratto cloud con Google e AWS per fornire servizi – inclusi anche strumenti di AI – a ministeri e apparato di sicurezza israeliani, con data center locali per garantire che i dati restino all'interno dei confini nazionali) rende visibili temi di sovranità dei dati, dipendenze infrastrutturali e responsabilità dual use[115]. Il dibattito pubblico su Nimbus si è intensificato proprio durante la guerra, anche per via delle proteste interne alle aziende tech. Accanto a questi attori, sono intervenuti organismi internazionali e ONG. Un gruppo di esperti ONU (OHCHR) ha deplorato il "preteso uso dell'AI" nei bombardamenti a Gaza, parlando di "domicidio" qualora certe prassi fossero confermate;

---

[112] Vedi Statuto di Roma della Corte Penale Internazionale, art. 30, 17 luglio 1998.
[113] International Committee of the Red Cross, "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach," *International Review of the Red Cross* 102, no. 913 (2021): 465.
[114] Amos Harel, "A Failure of All Systems, With Political Shock Waves Like '73," *Haaretz*, 8 ottobre 2023.
[115] Neta Alexander and Nadim Nashif, "Project Nimbus: Cloud Computing, Digital Occupation and Resistance," *Journal of Palestine Studies* 52, no. 4 (2023): 7–20.

Human Rights Watch ha pubblicato un Q&A che analizza punti di rischio e incertezza dei tool digitali (inclusi Lavender, Gospel e Where's Daddy?); l'ICRC ha ribadito che, nel diritto umanitario, determinazioni giuridiche su distinzione e proporzionalità restano responsabilità umana e che gli AI DSS devono essere progettati e impiegati in modo da sostenere, non sostituire, il giudizio umano[116]. Da un lato l'urgenza di neutralizzare reti militanti con rapidità, dall'altro la necessità di ancorare l'azione a regole e soglie verificabili agli occhi di platee interne ed esterne: queste prese di posizione entrano direttamente nel nostro "oggetto di riferimento" normativo.

Un ulteriore livello di analisi, che arricchisce e complica quanto emerso dalle inchieste giornalistiche, proviene dal rapporto pubblicato da Human Rights Watch[117], che fornisce un inquadramento più strutturato sia sul piano tecnico che giuridico. Diversamente dalle fonti giornalistiche, HRW non si limita a riportare testimonianze anonime di ufficiali israeliani, ma colloca Lavender all'interno di un più ampio ecosistema di strumenti digitali utilizzati dall'esercito israeliano nella guerra a Gaza: oltre a Lavender, compaiono infatti The Gospel e Where's Daddy? e l'*evacuation monitoring tool* basato sulla triangolazione dei telefoni cellulari per monitorare gli spostamenti della popolazione. In questo modo, il software non appare più come un episodio isolato, ma come parte integrante di un'architettura algoritmica diffusa che copre simultaneamente sorveglianza di massa, analisi predittiva e selezione dei target. Il rapporto introduce anche due concetti teorici di grande rilievo. Il primo è l'*automation bias*, ovvero la tendenza degli operatori umani a fidarsi eccessivamente delle macchine, proprio perché percepite come più neutrali e "oggettive". Questo spiega il ruolo ridotto del controllo umano nella validazione dei target. Il secondo è la digital dehumanization: trasformare i cittadini palestinesi in punteggi di rischio e variabili statistiche, riducendoli da soggetti giuridici titolari di diritti a dati da elaborare[118]. Questo passaggio è cruciale dal punto di vista normativo e politico, perché implica un'inversione della presunzione di innocenza: mentre il diritto internazionale umanitario stabilisce che lo status di civile si presume fino a prova contraria, in questo contesto è l'algoritmo a generare la presunzione di colpevolezza. HRW solleva inoltre la questione del diritto alla privacy, collegando l'uso di questi sistemi alla sorveglianza sistematica esercitata da Israele sui palestinesi già prima del conflitto.

---

[116] United Nations, *Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories*, 20 settembre 2024.
[117] Human Rights Watch, *Questions and Answers on the Israeli Military's Use of Digital Tools in Gaza*, 10 settembre 2024.
[118] Ibid.

La raccolta e l'archiviazione di dati biometrici e comportamentali, in un contesto di occupazione e apartheid, violano l'articolo 17 dell'ICCPR, che vieta interferenze arbitrarie o illegittime nella vita privata[119]. Questo spostamento di prospettiva è fondamentale: il problema non riguarda soltanto il diritto bellico, ma anche il diritto internazionale dei diritti umani, mostrando come l'architettura di sorveglianza alimenti e sostenga le pratiche militari di selezione dei target. Infine, HRW chiarisce un punto metodologico rilevante: questi strumenti non sono sistemi d'arma autonomi, ma sistemi di supporto al targeting. Formalmente, la decisione resta in mano umana. Tuttavia, in pratica, operano come generatori automatici di target, riducendo il ruolo umano a mera timbratura burocratica. La distinzione giuridica, quindi, non basta a dissipare la zona grigia: anche se non rientrano nella categoria di armi autonome, il loro uso intensivo senza adeguato scrutinio umano produce effetti simili, contribuendo ad aumentare il ritmo della guerra e a comprimere ulteriormente i margini per il rispetto delle regole di distinzione e proporzionalità. Questi elementi rendono il contributo di HRW particolarmente prezioso per il quadro teorico di questa tesi. Nella prospettiva della securitizzazione, la fiducia cieca nella macchina e la deumanizzazione digitale sono parte del discorso che costruisce i palestinesi come minaccia indistinta, giustificando l'adozione di misure eccezionali. In questo senso, il rapporto HRW non solo conferma quanto emerso dalle fonti giornalistiche, ma ne amplia la portata, collegando le pratiche operative a un quadro più vasto di sorveglianza, diritti e tecnologie. Così facendo, fornisce il terreno per un'analisi comparata che metta in relazione la dimensione discorsiva (securitizzazione), quella funzionale (neofunzionalismo) e quella identitaria (costruttivismo), mostrando come il caso Lavender rappresenti non solo un problema di efficacia operativa, ma soprattutto una trasformazione strutturale della guerra nell'era digitale.

3.2. La logica della securitizzazione

Come abbiamo esaminato in precedenza, la teoria della securitizzazione, elaborata dalla Scuola di Copenaghen, sostiene che la sicurezza non sia una realtà oggettiva e neutra, ma un effetto discorsivo: un tema diventa una questione di sicurezza quando viene rappresentato come una minaccia esistenziale che richiede misure straordinarie, al di fuori delle normali regole politiche[120]. In altre parole, ciò che è "securitizzato" non è soltanto ciò che oggettivamente costituisce un

[119] United Nations, *International Covenant on Civil and Political Rights*, adottato dall'Assemblea Generale delle Nazioni Unite il 16 dicembre 1966.
[120] Vedi l'apparato introduttivo in Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner, 1998).

pericolo, ma ciò che viene narrato, percepito e riconosciuto come tale da una comunità di riferimento. La securitizzazione è quindi un atto performativo: attraverso dichiarazioni, pratiche e cornici discorsive, un determinato fenomeno viene costruito come minaccia e autorizza l'uso di strumenti eccezionali per contrastarlo. Leggere il caso sotto la luce della securitizzazione significa seguire il passaggio dall'enunciazione del pericolo alla richiesta di strumenti eccezionali rispetto alle procedure ordinarie, e osservare l'accettazione (o il rifiuto) di tali richieste da parte dei pubblici rilevanti[121]. Nel caso di Gaza, il lessico della minaccia esistenziale e del ciclo operativo "a tempo compresso" funge da giustificazione per l'adozione di interfacce che promettono di velocizzare l'identificazione degli obiettivi; al contempo, l'audience internazionale e domestica valuta se la velocità comprometta la proporzionalità e la distinzione sancite dal diritto umanitario. È in questa tensione che si colloca la progettazione delle soglie: quali livelli di confidenza, quali limiti ai danni collaterali, quali condizioni minime di verifica sono ritenute sufficienti. La letteratura e i commenti giuridico-operativi successivi alle rivelazioni hanno proposto quadri interpretativi divergenti: per alcuni "Lavender" e lo strumento correlato "Gospel" restano tecnologie di supporto alla selezione dei target, per altri la scala e il ritmo trasformano di fatto il ruolo umano in mera ratifica di raccomandazioni prodotte a monte, con rischi di overtrust.

Applicata al caso di Lavender, la teoria permette di leggere come l'introduzione di un software di intelligenza artificiale per l'identificazione dei bersagli sia stata giustificata e resa legittima all'interno di un conflitto ad altissima intensità come quello di Gaza. Come anticipato, l'inchiesta di +972 Magazine del 3 aprile 2024 ha rivelato che il sistema ha generato circa 37.000 obiettivi nelle prime settimane successive all'attacco del 7 ottobre 2023, includendo anche "junior militants", ossia figure di basso rango, e gli operatori dedicavano appena 20 secondi alla validazione di ogni target. Tali pratiche, che contraddicono i principi di distinzione e precauzione del diritto internazionale umanitario, non sono state raccontate come violazioni, ma come necessità operative in un contesto di emergenza[122]. Sul piano tecnico, HRW chiarisce che Lavender si fonda

---

[121] Come sottolinea Rita Floyd in *The Morality of Security: A Theory of Just Securitization* (Cambridge: Cambridge University Press, 2019), la teoria della securitizzazione non dovrebbe essere solo uno strumento descrittivo, come proposto dalla Scuola di Copenaghen, ma anche un paradigma normativo capace di distinguere tra securitizzazioni giuste e ingiuste. Mentre Buzan, Wæver e de Wilde mostrano come gli atti linguistici costruiscano minacce esistenziali e giustifichino misure straordinarie, Floyd introduce criteri etici ispirati alla *just war theory*, fondati su principi di proporzionalità, necessità e protezione dei diritti fondamentali. In questo modo, la sua proposta cerca di rispondere alla domanda non solo di come avvenga la securitizzazione, ma di quando essa possa essere considerata legittima sul piano morale. Vedi Rita Floyd, *The Morality of Security: A Theory of Just Securitization* (Cambridge: Cambridge University Press, 2019), e anche Mitja Sardoc, "The Ethics of Securitisation: An Interview with Rita Floyd," *Critical Studies on Terrorism* 14, no. 1 (2021): 139–148.

[122] Protocollo Addizionale I alle Convenzioni di Ginevra, artt. 48 e 57; International Committee of the Red Cross, *Customary International Humanitarian Law*, Regole 7 e 15.

su un metodo di machine learning semi-supervisionato noto come *positive-unlabeled learning*[123]. Questa tecnica, che consiste nell'estrapolare schemi da un insieme di dati "positivi" (già etichettati come sospetti) e "non etichettati" (che includono l'intera popolazione civile), comporta margini di errore strutturali e difficilmente controllabili. In concreto, significa che comportamenti neutri – cambiare telefono, avere contatti sociali con un sospetto, o persino la mera appartenenza a un gruppo WhatsApp – possono diventare indicatori di affiliazione militare. HRW sottolinea così che gli errori di classificazione non sono incidentali, ma incorporati nell'architettura stessa del sistema, poiché si basano su dati incompleti, obsoleti o discriminatori. Qui emerge il principio del *garbage in*, *garbage out*: se i dati in ingresso sono distorti, anche gli output dell'algoritmo non possono che esserlo[124].

Qui la logica della securitizzazione appare evidente. Le forze armate israeliane hanno presentato la minaccia di Hamas non come un problema politico o militare tradizionale, ma come un pericolo esistenziale per lo Stato e per i suoi cittadini. In questa cornice, l'uso di un sistema algoritmico capace di elaborare migliaia di profili in tempi brevissimi non viene percepito come un rischio per i civili, bensì come una risposta inevitabile e proporzionata a un nemico che si muove rapidamente e si confonde con la popolazione. Il discorso securitizzante non nega la possibilità di errori, ma li relativizza all'interno di un quadro di sopravvivenza collettiva: la perdita di vite civili palestinesi viene implicitamente presentata come un costo necessario per proteggere la sicurezza israeliana. Un altro aspetto centrale della securitizzazione da questo punto di vista è il ruolo delle audience. Nel caso Lavender si possono distinguere almeno tre livelli. Per l'opinione pubblica interna israeliana, l'IDF ha negato che il sistema fosse un'"intelligenza artificiale autonoma" di targeting, definendolo piuttosto come una banca dati di supporto[125]. Tale definizione ha lo scopo di rassicurare, presentando la decisione ultima come pienamente umana e conforme alle regole. Per la comunità internazionale, invece, l'uso di Lavender è stato minimizzato nelle dichiarazioni ufficiali, in modo da attenuare il rischio di accuse di violazioni del diritto internazionale umanitario. Al contrario, l'inchiesta giornalistica e le ONG hanno presentato Lavender come simbolo di un processo di automazione pericoloso e potenzialmente illegittimo, costruendo una narrativa alternativa che mira a securitizzare la tecnologia stessa, presentandola come minaccia ai civili e al diritto internazionale. Questa tensione tra discorsi opposti mostra la natura

[123] Human Rights Watch, *Questions and Answers on the Israeli Military's Use of Digital Tools in Gaza*, 10 settembre 2024.
[124] Eyal Weizman and Ruthie Ginsburg, "Israel's AI Program, Lavender, Is Automating the Killing in Gaza," *The Philadelphia Inquirer*, April 7, 2024.
[125] Amos Harel, "A Failure of All Systems, With Political Shock Waves Like '73," *Haaretz*, 8 ottobre 2023.

eminentemente politica della securitizzazione. Da un lato, lo Stato israeliano utilizza atti linguistici per rappresentare il sistema come indispensabile alla sicurezza; dall'altro, giornalisti e attivisti internazionali cercano di delegittimarlo costruendolo come un rischio inaccettabile. Entrambi i discorsi sono performativi: non descrivono soltanto la realtà, ma cercano di plasmarla, influenzando la percezione pubblica e le reazioni diplomatiche.

Un ulteriore elemento è l'eccezionalità delle pratiche giustificate dal discorso securitizzante. Le soglie di perdite civili considerate accettabili – 15-20 vittime collaterali per obiettivi minori e fino a 100 per comandanti di alto livello – costituiscono un chiaro superamento delle regole del diritto internazionale, che impongono valutazioni di proporzionalità caso per caso[126]. Tuttavia, all'interno del frame securitizzato, tali numeri vengono normalizzati e incorporati come parametri operativi. La trasformazione della proporzionalità da giudizio discrezionale a calcolo predefinito dimostra fino a che punto il discorso securitizzante riesca a sospendere la norma giuridica per introdurre una logica di eccezione permanente. Applicata al caso del software Lavender, la teoria illumina il modo in cui Israele ha costruito l'urgenza e legittimato pratiche operative altrimenti difficilmente compatibili con il diritto internazionale umanitario. Dopo gli attacchi del 7 ottobre 2023, il discorso politico israeliano ha presentato Hamas non come un avversario militare circoscritto, ma come una minaccia esistenziale per lo Stato ebraico e, più in generale, per la sopravvivenza dei suoi cittadini. Dichiarazioni come quella del presidente Isaac Herzog, secondo cui "non esistono civili innocenti a Gaza", o quelle di ministri che hanno invocato la necessità di "radere al suolo la Striscia", hanno funzionato come atti linguistici di securitizzazione: nel momento in cui un'intera popolazione viene descritta come indistinguibilmente collegata a un nemico mortale, ogni misura eccezionale diventa presentabile come necessaria alla sopravvivenza collettiva[127]. Tuttavia, nella cornice securitizzata, queste soglie non vengono presentate come violazioni, ma come scelte razionali, legittimate dal discorso politico secondo cui la sopravvivenza dello Stato giustifica la sospensione delle norme ordinarie. La logica dell'eccezione diventa così parte integrante delle procedure quotidiane, normalizzando pratiche che al di fuori del discorso securitizzante apparirebbero inaccettabili.

[126] Protocollo Addizionale I alle Convenzioni di Ginevra, art. 57; International Committee of the Red Cross (ICRC), *Customary International Humanitarian Law*, Regola 14.
[127] United Nations Human Rights Office of the High Commissioner, "UN Expert Warns of New Instance of Mass Ethnic Cleansing of Palestinians, Calls for Immediate Ceasefire," Press Release, 14 ottobre 2023.

La securitizzazione si manifesta anche nella rappresentazione della tecnologia. Sistemi come Lavender e Habsora vengono descritti come "smart systems", strumenti razionali e scientifici che migliorano l'efficienza delle operazioni. Questo linguaggio contribuisce a conferire un'aura di legittimità e neutralità tecnica a pratiche che, nella sostanza, comportano la sistematica eliminazione di civili. La narrazione tecnologica agisce come una maschera: trasforma un processo di selezione algoritmica, privo di reale trasparenza e con un margine di errore noto, in un dispositivo percepito come affidabile e razionale[128]. In questo modo, la tecnologia diventa parte integrante del discorso securitizzante, offrendo la giustificazione simbolica per una violenza su larga scala. Infine, la securitizzazione si manifesta nella deumanizzazione. Gli algoritmi trasformano individui in numeri, categorie statistiche e punteggi di rischio. Il palestinese non è più rappresentato come persona, ma come variabile di un calcolo probabilistico. Anche la scelta dei nomi dei sistemi – Lavender, Where's Daddy?, The Gospel – contribuisce a questa astrazione: un linguaggio neutro, quasi banale o ironico, che maschera la realtà della morte e rafforza la distanza tra l'operatore e la vittima. È in questo slittamento semantico che si compie la piena logica securitizzante: il nemico non è più visto come soggetto umano, ma come minaccia impersonale da neutralizzare.

Un ulteriore aspetto che rafforza la lettura securitizzante è emerso dalle testimonianze raccolte dal Guardian e da +972/Local Call. Gli ufficiali che hanno utilizzato Lavender hanno dichiarato di avere "più fiducia in un meccanismo statistico che in un soldato in lutto", sottolineando come la freddezza della macchina fosse percepita come un vantaggio operativo in un contesto segnato dal trauma del 7 ottobre[129]. Questo passaggio discorsivo è particolarmente significativo: il dispositivo tecnologico viene securitizzato non solo come strumento di efficienza, ma come garante di razionalità rispetto all'emotività umana, legittimando così la sua centralità nelle operazioni. In termini teorici, ciò mostra come la tecnologia diventi parte integrante del discorso securitizzante, assumendo un'aura di neutralità che permette di accettare pratiche letali su vasta scala. Allo stesso tempo, le rivelazioni sul ricorso sistematico a bombe non guidate e sull'esistenza di soglie numeriche pre-autorizzate di vittime civili rafforzano il legame tra securitizzazione e normalizzazione dell'eccezione. Stabilire in anticipo che fino a venti civili potevano essere uccisi per eliminare un militante di basso rango, o fino a cento per un comandante, equivale a

[128] Louise Amoore, "Algorithmic War: Everyday Geographies of the War on Terror," *Antipode* 41, no. 1 (2009): 49–69.
[129] Vedi Bethan McKernan and Quique Kierszenbaum, "Israel Uses AI System to Generate Targets in Gaza Airstrikes," *The Guardian*, 3 aprile 2024.

istituzionalizzare l'eccezione, trasformandola in regola operativa. Dal punto di vista della teoria, si tratta di un chiaro esempio di come il discorso securitizzante consenta di sospendere il principio di proporzionalità del diritto internazionale umanitario e di sostituirlo con parametri quantitativi legittimati dall'urgenza della sopravvivenza.

Inoltre, il clima descritto dagli stessi ufficiali – una pressione costante a "produrre più target possibili" e a colpirli "a ogni costo", alimentato da un'atmosfera di vendetta – mostra come la securitizzazione non sia un atto isolato, ma un processo che plasma culture organizzative e pratiche quotidiane. L'urgenza securitaria giustifica la velocizzazione estrema del ciclo decisionale (20 secondi per autorizzare un attacco) e la riduzione del ruolo umano a mera timbratura burocratica. Anche qui la logica discorsiva produce effetti materiali: la costruzione del nemico come minaccia esistenziale e la rappresentazione della macchina come più razionale dell'uomo convergono nel normalizzare una politica operativa che, al di fuori del quadro securitizzato, apparirebbe come una violazione sistematica delle norme internazionali. Un ulteriore elemento che rafforza la lettura securitizzante del caso Lavender riguarda il modo in cui il discorso ufficiale tende a occultare le incertezze, le assunzioni e i bias che caratterizzano ogni sistema algoritmico. Come osserva Arthur Holland Michel, l'AI non "sbaglia" in senso stretto: produce esattamente gli output per cui è stata progettata, basati però su criteri opachi e non verificabili che incorporano presupposti statistici e culturali spesso lontani dal diritto internazionale umanitario[130]. Il discorso securitizzante, nel contesto israeliano, agisce dunque su due livelli: non solo costruisce Hamas e la popolazione di Gaza come minaccia esistenziale, ma presenta anche la macchina stessa come garante di sicurezza, più affidabile e "fredda" dell'uomo, proprio perché immune all'emotività e al lutto. È questo linguaggio che rende accettabile l'automazione, anche quando essa si fonda su assunzioni arbitrarie, come l'idea che cambiare numero di telefono o avere certi contatti sociali possa equivalere a una prova di militanza. In tal modo, la securitizzazione non legittima soltanto la sospensione dei principi di distinzione e proporzionalità, ma anche la normalizzazione dell'opacità algoritmica: la fiducia nella macchina diventa parte del discorso politico sulla sicurezza, consentendo che criteri arbitrari si trasformino in parametri operativi di vita o di morte.

Lo studio del Center for Security and Emerging Technology (CSET) su AI for Military Decision-Making offre un punto di vista strategico e istituzionale statunitense, che permette di collocare i casi empirici di Gaza e Ucraina dentro una cornice più ampia di riflessione dottrinale. La

[130] Arthur Holland Michel, "The Accountability Surface of Militaries Using Automated Technologies," *Centre for International Governance Innovation (CIGI)*, 14 giugno 2021.

specificità del rapporto sta nella centralità attribuita al concetto di *decision advantage*: l'AI è presentata come strumento indispensabile per abbreviare l'OODA loop, consentendo alle forze armate di anticipare l'avversario e garantire una superiorità operativa. Dal punto di vista della securitizzazione, questo linguaggio è significativo perché costruisce la velocità decisionale come una questione esistenziale: l'adozione dell'AI non viene narrata come scelta facoltativa, ma come condizione necessaria per la sopravvivenza degli Stati in un contesto competitivo. È la stessa logica che ritroviamo nel caso di Gaza, dove la rapidità della generazione di target attraverso sistemi come Lavender e Where's Daddy? è giustificata in termini di urgenza securitaria, e in Ucraina, dove Palantir viene presentata come alleato vitale per accelerare il ciclo decisionale. Come vedremo, in ottica neofunzionalista, il rapporto sottolinea che per realizzare questo decision advantage è inevitabile integrare dati civili e commerciali (da satelliti privati, infrastrutture cloud, sensori dual use) nell'ecosistema militare. È la logica dello spill-over: risorse nate in ambito civile diventano parte del ciclo operativo bellico. Questo è evidente anche nel caso ucraino, dove satelliti commerciali e dati civili sono stati incorporati in MetaConstellation, e a Gaza, dove dati biometrici e reti telefoniche di sorveglianza sono confluiti in sistemi di targeting algoritmico. Inoltre, nella chiave costruttivista che vedremo più approfonditamente nel prossimo capitolo, il rapporto CSET dimostra come il linguaggio dottrinale costruisca un immaginario bellico centrato sull'*informational dominance* e sull'AI come "garante" della razionalità della guerra. Espressioni come decision advantage e AI-*enabled command* non descrivono semplicemente una capacità tecnica, ma creano una narrativa che attribuisce all'AI uno status identitario nuovo, quello di attore politico-militare indispensabile. È lo stesso meccanismo che troviamo nel discorso israeliano su Lavender, presentato come "supporto inevitabile" al targeting, e in quello occidentale su Palantir, rappresentata come "alleata" dell'Ucraina. In questo senso, la specificità del rapporto CSET è duplice: da un lato, fornisce la cornice teorico-strategica che spiega perché gli Stati investano nell'AI militare; dall'altro, permette di leggere i casi di Gaza e Ucraina non come anomalie, ma come applicazioni concrete di un paradigma già elaborato nelle dottrine occidentali.

L'articolo pubblicato su Insight Turkey nel 2022 evidenzia come l'approccio del *realist constructivism* sia particolarmente utile per comprendere la percezione israeliana della sicurezza e, quindi, i processi di securitizzazione che caratterizzano la politica del Paese[131]. Sin dalla fondazione dello Stato nel 1948, il discorso politico israeliano ha costruito la propria

[131] Arda Can Kumbaracibasi, "Understanding Israel's Foreign Policy from the Perspective of Identity and Security," *Insight Turkey* 24, no. 1 (2022): 65–84.

sopravvivenza come continuamente minacciata da nemici esterni ed interni: i "coltelli" delle organizzazioni non statali come Hamas o Hezbollah, i "carri armati" degli Stati confinanti, i "razzi" provenienti da Iran e suoi proxy regionali. Questo linguaggio, citato in modo esemplare dall'ex presidente Shimon Peres, rivela come la costruzione discorsiva della minaccia sia centrale nella definizione della sicurezza israeliana. Applicando la lente della securitizzazione, è evidente che Israele non si limita a rispondere a pericoli materiali, ma li narra e li rappresenta come sfide esistenziali, attraverso il trauma della minoranza e il timore della *demographic threat* (la possibilità di diventare minoranza nella Palestina storica). In questo modo, la percezione della minaccia diventa un atto politico che legittima pratiche straordinarie: la costruzione della barriera di separazione, le politiche di annessione e l'uso sistematico della forza militare anche contro popolazioni civili. Il nesso tra identità e sicurezza, sottolineato dal *realist constructivism*, consente dunque di spiegare perché Israele *securitizzi* quasi ogni aspetto della sua esistenza politica. Non è solo la distribuzione del potere regionale a dettare il comportamento, ma la costruzione identitaria dell'Altro come nemico irriducibile. In questo senso, la securitizzazione israeliana si presenta come un processo continuo: ogni minaccia viene narrata come totale, ogni misura adottata come necessaria alla sopravvivenza. In conclusione, l'applicazione della teoria della securitizzazione al caso Lavender mostra come l'uso dell'intelligenza artificiale a Gaza non possa essere compreso unicamente come fatto tecnico o operativo, ma come processo discorsivo e politico. Attraverso atti linguistici, soglie operative e narrazioni tecnologiche, Israele ha trasformato la gestione algoritmica della popolazione palestinese in una questione di sopravvivenza nazionale, legittimando pratiche che violano i principi fondamentali del diritto internazionale umanitario. Allo stesso tempo, la contestazione di ONG, giuristi e media internazionali evidenzia che la securitizzazione non è mai assoluta: essa rimane un campo di lotta discorsiva, in cui ciò che è definito "sicurezza" e ciò che è definito "minaccia" è costantemente rinegoziato.

3.3. Il frame costruttivista

Il costruttivismo rappresenta una delle principali correnti delle Relazioni Internazionali sviluppatesi dagli anni Novanta, a partire dagli studi di Alexander Wendt[132]. A differenza del realismo e del liberalismo, che tendono a spiegare la politica internazionale in base a fattori materiali come il potere militare o gli scambi economici, il costruttivismo mette al centro le idee, le identità e le norme condivise. Secondo questa prospettiva, gli interessi degli Stati non sono dati

[132] Come abbiamo già anticipato sopra, vedi Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999), 385.

una volta per tutte, ma vengono costruiti socialmente attraverso discorsi, pratiche e rappresentazioni. L'affermazione di Wendt secondo cui "l'anarchia è ciò che gli Stati ne fanno" riassume bene questa impostazione: le strutture del sistema internazionale non determinano automaticamente il comportamento degli Stati, ma vengono interpretate e interiorizzate in modi diversi a seconda delle identità e dei significati condivisi. Di conseguenza, anche la distinzione tra amico e nemico, alleato e avversario, civile e combattente, non è mai puramente oggettiva, ma è il risultato di pratiche discorsive e istituzionali che orientano le scelte politiche. Un contributo fondamentale a questa prospettiva è venuto da Martha Finnemore e Kathryn Sikkink, che hanno introdotto il concetto di "imprenditori normativi": attori in grado di promuovere nuove norme sociali e di farle accettare come standard legittimi dalla comunità internazionale[133]. Parallelamente, Emanuel Adler e Peter Haas hanno evidenziato il ruolo delle comunità epistemiche: gruppi di esperti e professionisti che producono e diffondono categorie interpretative, trasformandole in istituzioni e pratiche condivise[134]. Applicata al tema della guerra algoritmica, la lente costruttivista consente di comprendere come le tecnologie digitali non siano strumenti neutrali, ma dispositivi che contribuiscono a costruire nuove categorie politiche e sociali.

Algoritmi, interfacce e dataset producono inedite definizioni di chi è un potenziale combattente, di cosa costituisce una minaccia e di quali margini di errore possano essere accettati. In questo senso, il costruttivismo non si limita a descrivere l'uso dell'intelligenza artificiale in guerra, ma aiuta a rivelare come questa trasformi lo stesso significato di sicurezza, umanità e responsabilità. In questa chiave, il caso Lavender diventa un laboratorio per osservare come le identità professionali di analisti e operatori si ricalibrino rispetto a un'interfaccia che propone associazioni probabilistiche, e come, dopo eventi critici, linguaggi e priorità possano cambiare, producendo aggiornamenti di protocolli o nuove norme informali. La discussione pubblica, lungi dall'essere un rumore di fondo, diventa uno dei luoghi in cui la fiducia viene definita e redistribuita tra attori. La prospettiva costruttivista trova un punto di rafforzamento particolarmente significativo nelle osservazioni di Arthur Holland Michel sul funzionamento degli algoritmi militari. L'autore sottolinea come non esista un'intelligenza artificiale "neutrale": ogni output riflette inevitabilmente incertezze, assunzioni e bias che sono incorporati nel processo di addestramento e nell'uso della tecnologia. In altre parole, ciò che appare come un risultato "oggettivo" della macchina è in realtà il frutto di un insieme di scelte culturali, sociali e politiche sedimentate nei

[133] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917.
[134] Peter M. Haas, "Epistemic Communities and International Policy Coordination," *International Organization* 46, no. 1 (1992): 1–35.

dati e nei criteri con cui l'algoritmo è stato costruito[135]. Questo punto è fondamentale per comprendere il caso di *Lavender*. A Gaza, per esempio, una pratica quotidiana come cambiare frequentemente numero di telefono – spesso dovuta a interruzioni della rete, perdita di dispositivi durante i bombardamenti o semplice precarietà materiale – può essere interpretata dall'algoritmo come un indicatore di militanza. Allo stesso modo, la partecipazione a gruppi di messaggistica o la vicinanza familiare a individui sospettati possono diventare parametri che alimentano la classificazione automatica. In questi casi non siamo di fronte a un errore tecnico, ma a una vera e propria costruzione sociale del sospetto: comportamenti culturalmente e contestualmente normali vengono trasformati, dal linguaggio tecnico dell'AI, in segnali di appartenenza militante[136]. Il costruttivismo permette di cogliere tutta la portata di questa dinamica. Non è soltanto la macchina a operare la trasformazione, ma il linguaggio tecnico che la accompagna: termini come "indicatori", "pattern" o "punteggio di rischio" creano una nuova semantica del conflitto, nella quale l'identità dei soggetti palestinesi viene ridefinita in chiave securitaria. Il civile, che secondo il diritto internazionale umanitario gode di una presunzione di protezione, diventa così un "potenziale target" sulla base di correlazioni statistiche opache e di presupposti culturali codificati in forma algoritmica.

La forza di questa lettura costruttivista è che mostra come il problema non sia soltanto giuridico (la violazione dei principi di distinzione e proporzionalità) o tecnico (il margine d'errore del 10%), ma discorsivo e identitario: il modo in cui gli algoritmi vengono addestrati e descritti produce una nuova categoria politica di popolazione, in cui la linea di confine tra civile e combattente è ridefinita da criteri arbitrari e culturalmente situati. La tecnologia, lungi dall'essere un attore neutrale, diventa uno strumento di produzione di significati, capace di ridefinire chi è degno di protezione e chi può essere legittimamente eliminato. L'apporto di Holland Michel è particolarmente prezioso per la tesi perché mostra come il costruttivismo aiuti a comprendere la dimensione semantica e culturale della guerra algoritmica: non solo l'AI "interpreta" la realtà, ma contribuisce a costruirla, trasformando pratiche quotidiane in indizi di colpevolezza e ridefinendo lo status politico-giuridico delle persone in base a categorie tecniche che celano scelte sociali e valoriali. La prospettiva costruttivista permette di cogliere come l'uso dell'intelligenza artificiale in guerra non si limiti a costruire target, ma contribuisca a ridefinire lo status stesso dell'umano nel conflitto armato. Il documento dell'ICRC sottolinea con chiarezza che, per garantire il rispetto

---

[135] Arthur Holland Michel, "The Accountability Surface of Militaries Using Automated Technologies," *Centre for International Governance Innovation (CIGI)*, 14 giugno 2021.
[136] Louise Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others* (Durham, NC: Duke University Press, 2020), 62–65.

del diritto internazionale umanitario e dei principi etici fondamentali, è indispensabile preservare il controllo umano significativo sulle decisioni che riguardano la vita e la morte[137]. Tale esigenza non è soltanto tecnica o giuridica, ma affonda le radici nella concezione etica della guerra come spazio in cui, anche nelle condizioni più estreme, l'agency umana deve rimanere centrale per salvaguardare la dignità e la responsabilità morale.

Qui il costruttivismo è essenziale: il modo in cui le tecnologie vengono discorsivamente integrate nei conflitti produce una nuova semantica dell'umano. Se la macchina è rappresentata come capace di sostituire il giudizio umano, il combattente perde il suo ruolo di soggetto morale e giuridico e si riduce a mediatore tecnico di un processo algoritmico. Parallelamente, la vittima perde riconoscimento della propria dignità: da soggetto protetto dal diritto e dalla coscienza pubblica, viene trasformata in "output" o "punteggio di rischio". In questo senso, l'uso di sistemi come *Lavender* non ridefinisce solo la pratica del targeting, ma ricostruisce le identità politiche di chi partecipa o subisce la guerra: l'operatore non è più responsabile in senso pieno, il civile non è più civile, ma potenziale sospetto. L'ICRC richiama proprio la già citata clausola Martens[138]; applicato al caso di Gaza, questo significa che la delega a sistemi algoritmici non può essere giustificata solo in termini di efficienza operativa o velocità decisionale: se la macchina sostituisce il giudizio umano, viene meno quella base simbolica ed etica che fonda la protezione dei civili. Il costruttivismo, dunque, mostra come l'adozione dell'AI nel conflitto non abbia effetti soltanto tecnici o giuridici, ma profondamente identitari. La narrazione che accompagna l'uso di AI – presentata come più razionale, fredda, affidabile – produce una nuova costruzione sociale dell'umano in guerra: l'agente morale si dissolve nell'automazione, la vittima diventa dato. In questo modo, l'AI non solo contribuisce alla selezione di obiettivi, ma riplasma le categorie fondamentali del diritto di guerra e del riconoscimento politico delle persone.

Amber Rahman ha scritto di come l'intelligenza artificiale e le pratiche di sorveglianza digitale non siano affatto strumenti neutrali, ma parte integrante di un progetto coloniale che si fonda sulla costruzione di identità[139]. Nella prospettiva costruttivista, questo significa che le tecnologie non si limitano a raccogliere e analizzare dati, ma producono categorie politiche e sociali che ridefiniscono lo status dei soggetti. I palestinesi, in questo quadro, non sono più persone titolari di diritti, ma diventano "oggetti sorvegliati", "potenziali minacce", o addirittura "output di un

---

[137] International Committee of the Red Cross, "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach," *International Review of the Red Cross* 102, no. 913 (2021): 425–451.
[138] Protocollo Addizionale I alle Convenzioni di Ginevra, art. 1(2).
[139] Amber Rahman, "Explainer: The Role of AI in Israel's Genocidal Campaign Against Palestinians," *Genocide in Gaza (blog)*, *Institute for Palestine Studies*, October 16, 2024.

algoritmo". Concetti come quello di *digital occupation* chiariscono che la sorveglianza è parte integrante del progetto coloniale: controllare reti telefoniche e internet, accumulare dati biometrici e utilizzare sistemi di riconoscimento facciale ai checkpoint non serve solo a gestire movimenti o prevenire minacce, ma a costruire un regime di visibilità che definisce chi è civile e chi è "militante", chi può circolare e chi deve essere fermato[140]. In questo senso, database come Blue Wolf – definito da ex soldati israeliani "Facebook for Palestinians" – funzionano come dispositivi di classificazione identitaria: attraverso colori (rosso, giallo, verde) che indicano se un palestinese può passare, essere fermato o arrestato, la vita delle persone viene tradotta in categorie algoritmiche che sostituiscono ogni valutazione giuridica o politica[141].

Lo stesso discorso si ritrova nella formula di "Automated Apartheid" coniata da Amnesty International, che descrive il sistema di sorveglianza basato su AI nei Territori Occupati come una forma di segregazione automatizzata: l'identità palestinese viene costruita come identità "a rischio", non in base a comportamenti effettivi, ma attraverso correlazioni statistiche e categorie arbitrarie imposte da sistemi tecnologici[142]. Questo processo non solo deumanizza i soggetti, ma trasforma il significato stesso di cittadinanza e umanità: essere palestinese significa, per default, essere sotto sorveglianza, e dunque essere potenzialmente targettizzabile. La forza della chiave costruttivista sta nel rivelare come le tecnologie non si limitino a eseguire ordini, ma contribuiscano a produrre la realtà sociale del conflitto. L'uso di AI nei sistemi come *Lavender*, *Where's Daddy?* o *Blue Wolf* non è solo un fatto tecnico, ma un atto discorsivo che ridefinisce lo status politico dei palestinesi. Invece di essere presunti civili fino a prova contraria – come previsto dal diritto internazionale umanitario – essi vengono presunti sospetti fino a dimostrazione contraria, e spesso senza alcuna possibilità di smentita. In questo modo, l'AI e la sorveglianza digitale diventano strumenti di costruzione identitaria e razzializzazione, normalizzando la distinzione coloniale tra chi è considerato "umano" e chi è ridotto a "dato".

Un esempio utile per introdurre questa dinamica è offerto dalla ricerca di Md. Rabioul Aual Robel. Il lavoro mostra come il sostegno statunitense a Israele non sia spiegabile unicamente in termini di interessi materiali (contenimento dell'URSS, accesso a tecnologie, sicurezza in Medio Oriente), ma sia il risultato di un processo identitario e discorsivo. Lobby come l'AIPAC, media mainstream

---

[140] Helga Tawil-Souri, "Digital Occupation: Gaza's High-Tech Enclosure," *Journal of Palestine Studies* 41, no. 2 (2012): 27–43; vedi anche Elias Zureik, *Israel's Colonial Project in Palestine: Brutal Pursuit* (London: Routledge, 2016), 98–105.

[141] Shira Rubin and Loveday Morris, "Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank," *The Washington Post*, 5 novembre 2021.

[142] Amnesty International, *Automated Apartheid: How Israel's Digital Surveillance of Palestinians Entrenches Oppression* (London: Amnesty International, 2023).

e think tank pro-Israele hanno operato come imprenditori normativi, diffondendo narrazioni che descrivono Israele come "unica democrazia in Medio Oriente", "alleato naturale", "vittima circondata da nemici", "portatore di valori condivisi"[143]. Queste immagini hanno costruito un orizzonte normativo entro il quale presidenti, *congressmen* ed elettori agiscono: essere pro-Israele diventa l'unica opzione politicamente legittima[144]. Il lavoro di Md. Rabioul Aual Robel mostra come il sostegno statunitense a Tel Aviv non possa essere spiegato esclusivamente in termini di interessi materiali – sicurezza nel Medio Oriente, contenimento dell'URSS, accesso a tecnologie avanzate – ma vada letto come il risultato di un processo identitario e discorsivo. Nel corso del tempo, attori interni al sistema politico statunitense – lobby, media, think tank e opinione pubblica – hanno contribuito a costruire l'immagine di Israele come: unica democrazia in Medio Oriente; alleato naturale degli Stati Uniti; vittima circondata da nemici; Paese portatore di valori condivisi. Questa costruzione ha modellato le preferenze delle élite politiche e le percezioni del pubblico: presidenti, congressmen ed elettori agiscono all'interno di un orizzonte normativo in cui essere pro-Israele rappresenta l'unica opzione legittima. In questa dinamica, lobby come l'AIPAC e i media mainstream hanno fissato cornici interpretative normative ("Israele come amico", "Palestinesi come terroristi"), riproducendo immagini e narrative (Israele bastione di libertà, Palestina minaccia alla sicurezza) e punendo il dissenso attraverso la marginalizzazione di giornalisti e politici critici. Il risultato è la creazione di un clima intersoggettivo in cui difendere Israele diventa il *default* politico. L'opinione pubblica stessa, come evidenziato da Robel, è stata progressivamente educata a percepire Israele come "amico naturale". I dati raccolti da Gallup e Pew mostrano infatti un sostegno costante, con il 60–70% degli americani che simpatizza con Israele contro appena il 10–15% con i palestinesi.

Tale sostegno non è spontaneo: è il prodotto di discorsi ripetuti che insistono su valori condivisi (religione, democrazia, lotta comune al terrorismo). Da un punto di vista costruttivista, il consenso sociale diventa così la base di legittimità con cui le élite giustificano scelte anche controverse, come il veto sistematico degli Stati Uniti a risoluzioni ONU critiche verso Israele. Un ruolo cruciale spetta anche ai think tank pro-Israele – dal Washington Institute for Near East Policy (WINEP) all'American Enterprise Institute (AEI), fino all'Heritage Foundation – che hanno contribuito a normalizzare analisi e narrazioni favorevoli a Israele. In questo caso si osserva un passaggio costruttivista fondamentale, secondo cui le idee diventano istituzioni. Non si tratta più

---

[143] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917.
[144] Md. Rabioul Aual Robel, "US–Israel Relation: How Constructivism Works," *International Journal of Social Science and Humanity* 5, no. 7 (2015): 651–657.

soltanto di lobby o media, ma di vere e proprie comunità epistemiche, secondo la definizione di Emanuel Adler e Peter Haas, in grado di produrre sapere apparentemente neutrale e trasformarlo in policy condivise. Il valore del caso USA–Israele per questa tesi è duplice. Da un lato, mostra come il costruttivismo sia capace di spiegare il sostegno statunitense a Israele anche quando esso non risponde a criteri di convenienza materiale. Dall'altro, offre un parallelismo utile con il tema della guerra algoritmica. Così come AIPAC e i media hanno costruito Israele come "alleato fidato", oggi white paper industriali, documenti NATO o dichiarazioni ufficiali dell'IDF costruiscono l'AI come "strumento affidabile", minimizzando bias e incertezze e promuovendone l'integrazione nei processi decisionali di targeting. Il costruttivismo permette da questo punto di vista di mettere in luce un aspetto cruciale sia nelle relazioni internazionali sia nel dibattito sull'uso dell'intelligenza artificiale in guerra: la fiducia non è un dato oggettivo, ma una costruzione sociale[145]. Nel caso del sostegno degli Stati Uniti a Israele, la fiducia politica non è nata automaticamente da interessi materiali o da una valutazione puramente strategica. È stata piuttosto costruita attraverso un insieme di discorsi, immagini e pratiche. Lobby influenti come l'AIPAC, i principali media statunitensi e numerosi think tank hanno agito come "imprenditori normativi", diffondendo l'idea che Israele fosse l'unico alleato affidabile del Medio Oriente, una democrazia assediata ma resiliente, portatrice di valori condivisi con l'Occidente. Nel tempo, questa rappresentazione si è trasformata in una cornice istituzionale stabile: essere pro-Israele è diventato l'orizzonte normativo entro cui si muovono presidenti, parlamentari ed elettori.

Un meccanismo analogo è oggi riscontrabile nell'ambito della guerra algoritmica. L'intelligenza artificiale non è percepita come affidabile perché effettivamente priva di errori o di distorsioni. Al contrario, la fiducia nelle tecnologie di supporto al targeting viene costruita attraverso documenti ufficiali, white paper industriali e dichiarazioni di autorità militari. NATO, Stati Uniti, Israele e Unione Europea presentano l'AI come uno strumento "inevitabile" per aumentare efficienza, velocità e capacità predittiva. In questo processo, i rischi noti – bias nei dataset, errori di classificazione, perdita di trasparenza – vengono sistematicamente ridimensionati o minimizzati, mentre prevale una narrativa che descrive l'AI come una risorsa necessaria e sicura. Il parallelismo è evidente. Così come la fiducia politica verso Israele è stata costruita e resa "naturale" da pratiche discorsive e istituzionali, allo stesso modo la fiducia tecnologica verso i sistemi di intelligenza artificiale viene costruita attraverso un linguaggio di inevitabilità e di affidabilità, che legittima il

[145] Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999), 385.

loro impiego nei processi decisionali bellici[146]. La logica sottostante è la medesima: in entrambi i casi la fiducia non nasce da una valutazione oggettiva, ma è il prodotto di rappresentazioni condivise che si stabilizzano in norme, politiche e istituzioni. In questo senso, l'analisi di Robel dimostra con chiarezza come il costruttivismo non sia una teoria meramente speculativa, ma uno strumento empiricamente fecondo per comprendere come attori, discorsi e pratiche plasmino la realtà politica. Così come l'identità di Israele come "alleato necessario" è il risultato di pratiche discorsive interne alla società statunitense, analogamente la percezione dell'AI come "affidabile" deriva da pratiche di legittimazione istituzionale e industriale che stabiliscono ciò che conta come minaccia, ciò che vale come evidenza e ciò che viene accettato come errore tollerabile. L'inchiesta pubblicata da *Le Monde* il 5 aprile 2024 rappresenta un passaggio cruciale per osservare la dimensione costruttivista dell'uso dell'intelligenza artificiale in guerra[147]. Il giornale francese riportava che il sistema *Lavender* aveva generato circa 37.000 potenziali target umani a Gaza. Questo dato, più che una misura tecnica, assume la forma di un atto discorsivo: quantificare la minaccia serve a rafforzare la percezione di Hamas come pericolo diffuso e sistemico, rendendo plausibile l'adozione di misure straordinarie. La stessa definizione di *junior militants*, usata per giustificare attacchi con alto margine di danno collaterale, mostra come categorie linguistiche costruite dal discorso politico-militare e dagli output algoritmici plasmino la distinzione tra civile e combattente, ridefinendo così i limiti del legittimo uso della forza[148]. In questo quadro, il "controllo umano" si riduce a un clic di approvazione che richiede 20 secondi di validazione per target, trasformandosi in una norma operativa nuova e normalizzata. L'analisi costruttivista permette dunque di cogliere il punto centrale: l'AI non produce solo stime probabilistiche, ma categorie sociali e politiche che, se accettate da un'audience, diventano realtà operative. La ricezione critica di queste pratiche da parte della stampa internazionale, in contrapposizione alla loro legittimazione interna, conferma che il significato delle tecnologie militari è sempre costruito intersoggettivamente e dipende dall'arena discorsiva in cui viene negoziato.

Applicare la lente costruttivista al tema della guerra algoritmica consente di andare oltre il livello tecnico e interrogare come gli algoritmi, lungi dall'essere strumenti neutrali, diventino parte di processi di costruzione sociale e politica della minaccia, della fiducia e della legittimità. Questo

---

[146] Emelia S. Probasco, Helen Toner, Matthew Burtell, e Tim G. J. Rudner, *AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks* (Washington, DC: Center for Security and Emerging Technology, aprile 2025).

[147] Stéphanie Maupas, "À Gaza, l'armée israélienne utilise un logiciel d'intelligence artificielle pour désigner des cibles," *Le Monde*, 5 April 2024.

[148] Yuval Abraham, "Lavender: The AI Machine Directing Israel's Bombing Spree in Gaza," *+972 Magazine* and *Local Call*, April 2024.

caso è utile perché mostra come il sostegno politico si fondi su una costruzione sociale di fiducia: la credibilità di Israele come alleato non deriva da fatti oggettivi, ma da un discorso intersoggettivo che lo rappresenta come partner necessario. È un processo simile a quello descritto da Emanuel Adler e Peter Haas a proposito delle comunità epistemiche: gruppi di esperti e professionisti che, producendo linguaggi e standard, stabiliscono che cosa valga come conoscenza legittima. In questo caso, gli algoritmi e i loro operatori costruiscono nuove categorie di evidenza ("pattern", "punteggi di rischio") che diventano la base accettata per decisioni di vita o di morte. Un elemento centrale della prospettiva costruttivista è che le norme funzionano solo se accettate da un'audience rilevante. Internamente, il discorso israeliano presenta gli algoritmi come strumenti di efficienza e precisione; esternamente, la stampa internazionale e le ONG li denunciano come strumenti di violazione del diritto umanitario. Questo divario mostra come la legittimità delle tecnologie non sia intrinseca, ma dipenda dalla negoziazione discorsiva tra attori diversi: governi, opinioni pubbliche, istituzioni internazionali, media. Un utile riferimento è l'analisi di Hubert Zimmermann, Alex Burkhardt e Milena Elsinger, che applica le principali lenti teoriche delle Relazioni Internazionali al conflitto israelo-palestinese[149]. Gli autori sottolineano come il costruttivismo permetta di cogliere un nodo centrale: le narrazioni speculari di vittimizzazione – Israele come Stato nato per garantire sicurezza a un popolo perseguitato fino alla Shoah, i palestinesi come vittime della Nakba e dell'occupazione – costruiscono identità politiche che orientano le scelte strategiche e che costituiscono un ostacolo persistente alla pace. In questa prospettiva, la minaccia non è mai un dato oggettivo, ma il prodotto di una memoria storica e di discorsi politici che la rendono credibile a un'audience interna. Qui la categoria della securitizzazione trova un terreno privilegiato: l'identità israeliana come "Stato assediato" legittima la trasformazione del conflitto in questione esistenziale, giustificando pratiche eccezionali e ampliando l'uso di tecnologie come l'intelligenza artificiale nel targeting. Allo stesso tempo, l'articolo mostra i limiti delle istituzioni internazionali nel mediare il conflitto, suggerendo che laddove il neofunzionalismo spiegherebbe l'integrazione tecnica e politica attraverso spillover, nel contesto israelo-palestinese le costruzioni identitarie prevalgono, bloccando i meccanismi cooperativi. Questa analisi teorica, quindi, conferma che per comprendere casi come l'uso di sistemi di AI militare è essenziale un approccio costruttivista capace di leggere come identità e

[149] Vedi Hubert Zimmermann, Alex Burkhardt, e Milena Elsinger, "The Israel/Palestinian Crisis and International Relations Theory," *Social Science Space*, 12 agosto 2024, e degli stessi autori Hubert Zimmermann, Andreas Dür, e Thomas Risse, eds., *International Relations Theories: Discipline and Diversity* (London: Sage, 2023).

norme socialmente costruite trasformino dati tecnici in categorie politiche di minaccia e legittimità.

Un contributo particolarmente rilevante alla prospettiva costruttivista è fornito da Farah Muna Safa Taqiya[150], che analizza il ricorso del Sudafrica all'International Court of Justice contro Israele per violazione della Convenzione sul genocidio. L'autrice sottolinea come la politica estera sudafricana non sia spiegabile in termini di interessi materiali immediati, ma come espressione dell'identità post-apartheid del Paese, definita dalla lotta contro l'oppressione e dal sostegno universale ai diritti umani. In questa prospettiva, il ricorso al diritto internazionale è uno *speech act* che non mira soltanto a ottenere una condanna giuridica, ma a plasmare norme globali e a rafforzare il divieto di genocidio e di apartheid come principi condivisi della comunità internazionale. Il valore costruttivista di questo caso emerge dalla capacità del Sudafrica di tradurre la propria memoria storica in pratica diplomatica, creando pressione normativa e stimolando processi di *norm building*. Ciò rivela un parallelo con il caso israeliano: se da un lato Israele utilizza strumenti tecnologici e discorsi securitizzanti per costruire la legittimità del proprio uso della forza, dall'altro il Sudafrica costruisce la propria agency internazionale sull'autorità morale e normativa, mostrando come l'azione degli Stati sia profondamente modellata da identità, valori e memorie condivise. Da questi esempi emerge di nuovo che la guerra algoritmica non può essere interpretata soltanto come un fenomeno tecnico, ma come il prodotto di pratiche discorsive e istituzionali che costruiscono la fiducia nelle macchine, ridefiniscono lo status dei soggetti e legittimano scelte letali. L'intelligenza artificiale diventa così parte integrante della costruzione sociale della sicurezza, esattamente come Israele è stato costruito come alleato naturale o il Sudafrica come difensore dei diritti umani. In tutti i casi, ciò che conta non è la natura oggettiva della minaccia o dell'alleanza, ma il modo in cui essa viene narrata, percepita e accettata da un'audience rilevante. Il costruttivismo si conferma dunque non solo come una teoria utile, ma come una prospettiva indispensabile per leggere le trasformazioni della guerra contemporanea. Esso permette di capire che la fiducia politica e la fiducia tecnologica non sono dati oggettivi, ma risultati di pratiche discorsive e processi identitari che stabiliscono cosa conti come minaccia, cosa come prova e quale livello di errore sia accettabile. In questo quadro, la guerra algoritmica appare come il punto di incontro tra logiche funzionali e costruzioni simboliche: le macchine accelerano i processi decisionali, ma sono i discorsi a stabilire chi è nemico, chi è civile e quali vite siano sacrificabili. È qui che il costruttivismo dimostra la sua forza esplicativa: rivelare che l'AI non

[150] Farah Muna Safa Taqiya, "Can Constructivism Hold Israel Accountable?," *Modern Diplomacy*, January 2024.

solo supporta la guerra, ma contribuisce a rifondarla, trasformando categorie giuridiche e identitarie in variabili computazionali e ridefinendo i confini stessi dell'umano e del politico.

3.4. La prospettiva neofunzionalista

La lente neofunzionalista consente di interpretare l'impiego di sistemi come Palantir in Ucraina e Lavender a Gaza come il risultato di una dinamica di *spill over* tecnologico. Ciò significa che strumenti inizialmente sviluppati per ambiti civili o per la sorveglianza vengono gradualmente assorbiti nei processi bellici fino a diventarne componenti indispensabili. Questo approccio permette di osservare come gli effetti a catena si propaghino: dall'analisi rapida dei target al coordinamento tra sensori, dai formati dati alle catene di custody (che garantiscono provenienza e integrità del dato), fino alla definizione di soglie decisionali comuni tra unità operative[151]. La prospettiva funzionalista mette quindi a fuoco la logica tecnica che collega interoperabilità dei formati (metadati coerenti, tassonomie condivise) e standard decisionali (punteggi minimi per validare un target). L'automazione, in questo quadro, "aggancia" direttamente i processi delle unità sul campo e spinge verso un'armonizzazione minima di procedure e definizioni. Tuttavia, questa stessa integrazione crea nuove dipendenze e attribuisce potere a chi controlla le metriche e i criteri di qualità. Lo *spill over* funzionale – dal problema tecnico alla regola comune – trascina con sé anche uno *spill over* istituzionale: standard, glossari, certificazioni e processi di auditing diventano vere e proprie infrastrutture di governance. Chi definisce le metriche (accuratezza, latenza, affidabilità) acquisisce così potere strutturale. Ma la dinamica resta ambivalente: troppa integrazione può irrigidire procedure che richiederebbero flessibilità, mentre troppo poca coordinazione rischia di frantumare la filiera informativa. La controversia su Lavender mostra bene questo punto: la disputa non è soltanto tecnica, ma anche istituzionale e semantica[152]. Decidere cosa valga come evidenza, quali errori siano accettabili e quale velocità sia compatibile con la responsabilità non è neutro[153]. Sono scelte politiche che si stabilizzano in interfacce e protocolli.

L'analisi di Bo e Dorsey aiuta a chiarire che questo *spill over* è guidato da un imperativo funzionale ben preciso: la ricerca di efficienza e rapidità. L'integrazione di sistemi di decision support basati

[151] International Committee of the Red Cross, "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach," *International Review of the Red Cross* 103, no. 916–917 (2021).
[152] Anna Gordon et al., "How Israel Uses AI in Gaza—And What It Might Mean for the Future of Warfare," *TIME*, 18 dicembre 2024
[153] Yuval Abraham, "'Lavender': The AI machine directing Israel's bombing spree in Gaza," *+972 Magazine*, 3 aprile 2024.

su AI risponde alla volontà degli Stati di abbreviare il ciclo decisionale OODA (observe, orient, decide, act)[154]. L'idea è che la capacità di generare e validare più rapidamente i target costituisca un vantaggio strategico decisivo. Più la catena si accorcia, più cresce la pressione a integrare stabilmente tali sistemi[155]. In Ucraina, Palantir e MetaConstellation sono stati adottati proprio perché capaci di integrare in tempo quasi reale fonti eterogenee – satelliti commerciali, dati civili, informazioni militari – fornendo un vantaggio immediato in termini di rapidità analitica e di risposta. L'orchestrazione di dati SAR, ottici e OSINT in un'unica interfaccia riduce l'attrito cognitivo e accelera la comprensione operativa[156]. A Gaza, invece, sistemi come Lavender e The Gospel hanno reso possibile un salto di scala nella produzione di target: da poche decine l'anno con i metodi tradizionali a centinaia al giorno. È questa capacità di moltiplicare la scala, più ancora della precisione tecnica, a spiegare l'integrazione stabile dei sistemi. La logica è chiara: se un sistema funziona in termini di tempo e volume, la pressione politica e militare spinge verso la sua incorporazione stabile[157]. Ma, come notano Bo e Dorsey, la velocità accorciata riduce la possibilità di controllo umano significativo. La verifica tende a diventare una formalità: un clic rituale entro venti secondi. In questo modo cresce la velocità, ma diminuisce la responsabilità effettiva. La dinamica conferma la forza del paradigma neofunzionalista: lo *spill over* funzionale non si arresta davanti ai rischi legali o etici, perché privilegia rapidità e scala come criteri dominanti.

Da questa prospettiva emerge anche la questione umanitaria. Il punto cruciale è che strumenti nati in ambiti civili, commerciali o persino umanitari vengono progressivamente incorporati in contesti bellici e, una volta integrati, diventano difficilmente separabili dal dominio militare. Il documento dell'ICRC del 2021 insiste proprio su questa natura duale dell'AI: gli stessi strumenti possono servire a localizzare dispersi o ottimizzare gli aiuti, ma anche a identificare target militari[158]. A Gaza, questo *spill over* è particolarmente evidente. Lavender non nasce dal nulla, ma da un'infrastruttura di sorveglianza già applicata in tempo di pace relativa: database biometrici, riconoscimento facciale ai checkpoint, triangolazione dei cellulari. La base amministrativa civile ha anticipato la base operativa militare. Lo stesso dato che può servire a monitorare evacuazioni

---

[154] Jessica Dorsey e Marta Bo, "AI-Enabled Decision-Support Systems in the Joint Targeting Cycle: Legal Challenges, Risks, and the Human(e) Dimension," *International Law Studies* 106 (2025), preprint SSRN (27 giugno 2025).
[155] Vedi anche Marta Bo e Jessica Dorsey, "The 'Need' for Speed – The Cost of Unregulated AI Decision-Support Systems to Civilians," *Opinio Juris*, 4 aprile 2024.
[156] Vera Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab," *TIME*, 8 febbraio 2024. A breve eanalizzeremo più approfonditamente la sezione sulla Guerra in Ucraina.
[157] Bethan McKernan e Harry Davies, "'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets," *The Guardian.*
[158] ICRC, "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach," 2021 (come n. 1).

civili può essere riusato per stabilire se un quartiere sia "sgombro" e quindi bombardabile. È un caso paradigmatico di *spill over*: la permeabilità tra sfere rende normale il riadattamento di un'infrastruttura civile a scopi bellici. Una volta che i dati entrano in una piattaforma come Lavender, è quasi impossibile separarli dal loro nuovo uso. Si crea così *path dependence*: il dato eredita la funzione della piattaforma.

Gaza mostra quindi in forma estrema la logica descritta dall'ICRC: l'uso duale non è un rischio astratto, ma una pratica quotidiana. La stessa architettura digitale che dovrebbe proteggere i civili diventa la base tecnica per colpirli. In questo processo, il vantaggio funzionale – rapidità, scala, efficienza – prevale sulle distinzioni originarie tra scopi civili, umanitari e militari. L'ICRC avverte anche che l'integrazione di AI e machine learning amplifica rischi già presenti in contesti civili: imprevedibilità, opacità, bias. Se questi aspetti sono problematici nei sistemi predittivi di polizia, diventano esistenziali in un contesto bellico. Da qui il passaggio all'ecosistema industriale. Amber Rahman documenta come le tecnologie digitali usate dall'esercito israeliano per la gestione della popolazione palestinese siano state riconfigurate nei sistemi di targeting Lavender, Gospel e Where's Daddy. In questo passaggio non vi è discontinuità: pratiche amministrative quotidiane diventano criteri per individuare target, mostrando la fusione tra controllo sociale e violenza armata. È la convergenza tra polizia preventiva e uso della forza. Un altro elemento decisivo riguarda l'integrazione tra settore privato tecnologico e dominio militare israeliano. Secondo Rahman, l'infrastruttura di sorveglianza e targeting dipende in larga parte da partnership con grandi aziende come Amazon, Google, Microsoft e Palantir, che forniscono servizi cloud, capacità di archiviazione e algoritmi di analisi. Qui lo *spill over* funzionale si converte in *spill over* politico-istituzionale: il settore privato diventa snodo strutturale. Queste collaborazioni, inizialmente commerciali, finiscono per consolidare un'integrazione bellica[159]. Inoltre, il conflitto diventa terreno di sperimentazione, un laboratorio per affinare prodotti poi esportati a livello globale. Il caso di Project Nimbus, contratto cloud tra Israele e Google/Amazon, è paradigmatico: nato come accordo civile, si è tradotto rapidamente in integrazione militare[160]. Documenti interni rivelano che Google conosceva i rischi di violazioni dei diritti umani, ma le clausole etiche restrittive non furono adottate. La logica di efficienza e interoperabilità ha prevalso. Tre elementi neofunzionalisti emergono chiaramente: lo *spill over* funzionale (strumenti civili estesi al militare), quello politico (Big Tech come attore strutturale del ciclo di sicurezza) e il tentativo di armonizzazione normativa

[159] Human Rights Watch, "Gaza: Israeli Military's Digital Tools Risk Civilian Harm," 10 settembre 2024.
[160] *Wired*, "The Hidden Ties Between Google and Amazon's Project Nimbus and Israel's Military," 2024.

(AI Principles, compliance etica[161]). Tecnica, istituzioni e regole co-evolvono. Project Nimbus mostra come la guerra algoritmica non nasca da una decisione isolata, ma da un processo cumulativo di integrazione tra privati globali e apparati militari[162].

Il paradigma neofunzionalista consente quindi di leggere Gaza come un laboratorio di integrazione continua: i confini tra civile, coloniale e militare convergono in un unico flusso tecnologico. La continuità infrastrutturale diventa continuità d'uso. Sistemi di sorveglianza e database pensati per il controllo della popolazione vengono normalizzati come strumenti di guerra, mentre le aziende private diventano attori organici della macchina bellica. Si consolida così una guerra digitale a geometria variabile pubblico-privato. Il caso Gaza illustra in forma estrema la dinamica descritta dal neofunzionalismo: la funzionalità prevale sulle distinzioni originarie, integrando settori diversi in un sistema bellico digitale pervasivo. L'IISS nel rapporto *Software Defined Defence* (2023) evidenzia come la difesa contemporanea sia destinata a diventare sempre più *software driven*, cioè fondata su infrastrutture digitali, cloud e algoritmi civili[163]. Questa traiettoria riflette perfettamente la logica dello *spill over*: innovazioni nate in ambito industriale e civile diventano il cuore della strategia militare. La stessa infrastruttura che sostiene mercati e servizi civili globali diventa il cuore operativo dei sistemi di comando e targeting. Non si tratta di una scelta contingente, ma di un processo irreversibile, in cui rapidità ed efficienza prevalgono su ogni altra considerazione. La difesa "software defined" non è un concetto tecnico neutrale, ma il risultato di un'integrazione sistematica che trasforma l'infrastruttura digitale globale in terreno di conflitto.

Un caso particolarmente rilevante è rappresentato dal White Paper dell'European Defence Agency *Trusted Artificial Intelligence in Defence* (2025). Il documento non si limita a fissare linee guida tecniche, ma mostra come l'adozione di AI militare richieda regole, standard e procedure che travalicano il settore difensivo, coinvolgendo industrie civili, centri di ricerca e istituzioni sovranazionali[164]. Questo è lo *spill over* funzionale: per rendere operativi i sistemi AI occorre intervenire su formati, dataset, supply chain. L'operatività richiede prerequisiti trasversali. Il documento sottolinea che la fiducia nei sistemi dipende da standard comuni di trasparenza, verificabilità e tracciabilità, non solo dal collaudo operativo. Qui emerge anche lo *spill over* politico-istituzionale: imprese tecnologiche, centri civili e istituzioni europee devono cooperare

[161] *The Verge*, "Internal Google documents reveal concerns about its cloud contract with Israel," 3 dicembre 2024.
[162] *The Guardian*, "We are Google and Amazon workers. We condemn Project Nimbus," 12 ottobre 2021.
[163] Simona R. Soare, *Software-Defined Defence: Algorithms at War* (London: IISS, 2023).
[164] European Defence Agency, *Trustworthiness for AI in Defence* (White Paper), 9 maggio 2025.

stabilmente, trasformando soluzioni tecniche in dispositivi regolativi (task force permanenti, regole comuni di procurement, certificazioni transnazionali). Infine, il documento richiama la necessità di armonizzazione: glossari condivisi, criteri unificati, linee guida comuni. Ciò che nasce come soluzione tecnica diventa un linguaggio comune che riduce costi di coordinamento e stabilizza la cooperazione. La guerra algoritmica, in questo quadro, non è un fatto tecnico, ma un processo istituzionale cumulativo che cristallizza organismi e regole.

Le inchieste di TIME costituiscono una fonte preziosa per leggere Gaza con la lente neofunzionalista perché non si limitano a descrivere gli strumenti, ma mostrano come essi ristrutturino le fasi del ciclo di targeting[165]. In concreto, sistemi come Lavender, Gospel e Where's Daddy non solo accorciano i tempi (da cicli di mesi a poche settimane), ma riorganizzano il lavoro: spostano l'enfasi dall'indagine "caso per caso" alla selezione su larga scala, con soglie e metriche che rendono replicabile la produzione quotidiana di target[166]. In parallelo, in Ucraina Palantir, attraverso MetaConstellation, svolge una funzione analoga ma a monte: unifica flussi eterogenei (satelliti, SAR, OSINT, dati militari) e li presenta in un'unica interfaccia, riducendo l'attrito cognitivo e anticipando decisioni a valle. Questa convergenza non è un semplice parallelo: opera come spill over funzionale, perché modelli e dataset maturati in un teatro vengono trasferiti e riadattati in altri, creando interdipendenze tecniche (stessi formati, stesse soglie, stessi protocolli di validazione). A valle dello spill over tecnico, si attiva quello politico-istituzionale: il dibattito su errori, proporzionalità e "controllo umano significativo" spinge attori come ICRC e Congresso USA a proporre cornici normative (per es. l'AWARE Act[167]) che provano a "trattenere" l'accelerazione funzionale dentro regole comuni. Anche il linguaggio è parte dell'integrazione: definire questi sistemi "glorified Excel sheets" depoliticizza l'automazione, spostando l'attenzione dall'autorità delle soglie alla loro apparente neutralità[168]. Qui la lettura costruttivista si intreccia con quella neofunzionalista: funzione (riduzione tempi/scala) e significato (narrazioni che minimizzano il rischio) co-producono pratiche e categorie operative ("civile", "combattente") che poi vengono rese stabili in interfacce e procedure.

---

[165] Anna Gordon et al., "How Israel Uses AI in Gaza—And What It Might Mean for the Future of Warfare," *TIME*, 18 dicembre 2024

[166] Yuval Abraham, "'Lavender': The AI machine directing Israel's bombing spree in Gaza," *+972 Magazine*, 3 aprile 2024.

[167] U.S. Congress, S.5239 — *Artificial Intelligence Weapons Accountability and Risk Evaluation (AWARE) Act of 2024*.

[168] Klaudia Klonowska, "AI-Based Targeting in Gaza: Surveying Expert Responses, Refining Debate," *Articles of War* (Lieber Institute, West Point), 7 giugno 2024.

Un ulteriore tassello è l'inchiesta Reuters (aprile 2023) sulla collaborazione tra Palantir e la Procura Generale ucraina: le stesse piattaforme impiegate sul fronte vengono usate per raccogliere e organizzare prove di presunti crimini di guerra (foto, video, testimonianze, satelliti) in un archivio processabile giudiziariamente[169]. Stessa infrastruttura, finalità diversa: dalla guerra alla giustizia. In termini neofunzionalisti, questo è uno spill over inter-dominio che consolida la centralità della piattaforma: più domini agganciano Foundry/Gotham, più cresce l'incentivo a standardizzare formati e catene di custody attorno ad esse[170]. In parallelo, la rappresentazione pubblica di Palantir come attore di accountability accresce la legittimità simbolica dell'azienda e retroagisce sull'adozione in ambito militare (e viceversa): funzione e fiducia si rafforzano reciprocamente. In questo quadro si colloca l'analisi di TIME su MetaConstellation: la piattaforma non solo integra satelliti commerciali, SAR e tracciamenti in quasi tempo reale, ma orchestra priorità e attenzione, diventando snodo cognitivo della situazione tattica[171]. L'"orchestratore di dati" è quindi duplice: dimostra la logica dello spill over (civile→militare→giudiziario) e costruisce un immaginario politico in cui Palantir appare non come semplice fornitore, ma come alleato strategico[172]. In chiave costruttivista, la fiducia non discende soltanto dalla performance, ma dalla narrazione che accredita la piattaforma come incarnazione della razionalità e della resilienza ucraina nella guerra digitale: una legittimità discorsiva che si stabilizza nel funzionamento quotidiano.

Mettendo in fila i passaggi, la catena logica diventa più esplicita: (i) l'analisi rapida dei target richiede integrazione tecnica (sensori, formati, metadati, chain of custody); (ii) la ricerca di efficienza sull'OODA attiva spill over funzionali che portano ad incorporazione stabile dei sistemi; (iii) l'integrazione, una volta sedimentata, produce lock-in organizzativi e assottiglia il controllo umano[173]; (iv) il dual use evidenziato dall'ICRC mostra la permeabilità tra civile, umanitario e militare[174]; (v) le partnership pubblico-privato trasformano l'integrazione tecnica in istituzionale (procurement, cloud, auditing)[175]; (vi) documenti come IISS 2023 e EDA 2025 confermano la traiettoria software defined e l'esigenza di standard comuni; (vii) narrazioni e inchieste (TIME,

---

[169] Reuters, "Data company Palantir to help Ukraine prosecute alleged Russian war crimes," 22 aprile 2023.
[170] Palantir Technologies, "Palantir to Support Ukrainian Prosecutor General's Investigation into War Crimes," comunicato stampa, 22 aprile 2023.
[171] Billy Perrigo, "How Palantir Is Shaping the Future of Warfare," *TIME*, 10 luglio 2023.
[172] David Ignatius, "How the algorithm tipped the balance in Ukraine," *The Washington Post*, 19 dicembre 2022.
[173] Jessica Dorsey e Marta Bo, "AI-Enabled Decision-Support Systems in the Joint Targeting Cycle: Legal Challenges, Risks, and the Human(e) Dimension," *International Law Studies* 106 (2025).
[174] International Committee of the Red Cross, "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach," *International Review of the Red Cross* 103, no. 916–917 (2021).
[175] *The Guardian*, "We are Google and Amazon workers. We condemn Project Nimbus," 12 ottobre 2021.

Reuters) non solo descrivono, ma producono legittimità e quindi domanda di ulteriore integrazione. Il risultato è coerente con la tesi: lo spill over normalizza l'uso militare delle tecnologie e sposta parte della responsabilità dalle persone alle interfacce che istituzionalizzano soglie, punteggi e tempi. Il punto più problematico, reso ora più visibile, è il rischio di slittamento dalla spiegazione alla giustificazione implicita: applicata al dominio bellico, la lente neofunzionalista finisce per naturalizzare l'integrazione come esito "ovvio" dell'efficienza, mentre in realtà amplifica rischi e dipendenze. Se un sistema "funziona" (riduce tempi, aumenta targets/giorno, integra dati civili e militari), la logica funzionale tende a legittimarlo senza una valutazione sostanziale di proporzionalità, trasparenza e responsabilità. Qui emerge il lato oscuro: più l'integrazione avanza, più svanisce la separazione civile/militare, più si restringe lo spazio per usi neutrali, più le violazioni si sedimentano come prassi. Neofunzionalismo e guerra algoritmica non delineano un percorso automatico verso una governance multilaterale: descrivono piuttosto una militarizzazione della sfera digitale, con Big Tech come attori organici e i conflitti come laboratori di prodotto e procedura. Il rischio non è solo analitico, ma politico: leggere questi processi con la lente neofunzionalista significa riconoscere che l'integrazione non è neutra; stabilizza pratiche che moltiplicano i pericoli di deresponsabilizzazione, di erosione del diritto e di marginalizzazione dell'umano nel ciclo decisionale.

3.5. Guerra russo-ucraina, un laboratorio per nuove forme belliche

L'invasione russa dell'Ucraina, avviata nel febbraio 2022, non ha rappresentato soltanto una cesura geopolitica nel continente europeo, ma anche un vero e proprio laboratorio per l'elaborazione di nuove forme di conflitto tecnologico. La guerra in corso ha reso evidente un passaggio cruciale: la capacità di dominare il campo di battaglia non dipende più esclusivamente dalla quantità di mezzi schierati o dall'efficienza della catena di comando, ma dalla possibilità di raccogliere, integrare e interpretare in modo efficace un flusso costante e massiccio di dati. Questo conflitto si configura come un banco di prova per l'uso combinato di droni, immagini satellitari commerciali, reti di comunicazione digitali e piattaforme di monitoraggio. Ciò che emerge è una nuova architettura della guerra, fondata non solo sul controllo del territorio, ma soprattutto sul governo dell'informazione[176].

[176] Ramesh Jaura, Software on the Front Line: How Palantir Is Aiding Ukraine in Its War With Russia," *Eurasia Review*, 6 settembre 2025.

In questo contesto si inserisce il ruolo della società statunitense Palantir Technologies, attiva da anni nel settore dell'analisi dei big data e già coinvolta in programmi di sicurezza nazionale negli Stati Uniti e in altri paesi occidentali. Palantir ha fornito al governo ucraino la piattaforma MetaConstellation, che si presenta come un'infrastruttura capace di gestire e coordinare fonti informative estremamente eterogenee[177]. A differenza dei tradizionali sistemi militari chiusi, concepiti per operare quasi esclusivamente su dati governativi e classificati, MetaConstellation lavora come un "orchestratore di dati". Non si limita, cioè, a fungere da archivio digitale, ma integra simultaneamente immagini satellitari a telerilevamento ottico, dati radar SAR, flussi civili di tracciamento navale (AIS) e aereo (ADS-B), oltre a input provenienti da alleati e da reti logistiche[178]. L'obiettivo dichiarato è quello di abbreviare drasticamente il tempo che intercorre tra la raccolta di un segnale e la decisione operativa, riducendo quello che in dottrina viene definito sensor-to-shooter cycle[179]. L'elemento innovativo risiede nella capacità della piattaforma di costruire una rappresentazione coerente e unificata del campo operativo a partire da fonti diverse, spesso incompatibili tra loro. In passato, infatti, i dati civili e quelli militari rimanevano separati e difficilmente interoperabili; la quantità di informazioni raccolte, inoltre, era tale da rendere l'analisi lenta e dispendiosa, dipendente quasi interamente dal lavoro di analisti umani. MetaConstellation, invece, riduce l'attrito informativo attraverso algoritmi di correlazione che filtrano, traducono e integrano i dati, restituendo un'interfaccia unica. Il vantaggio operativo è evidente: i movimenti di truppe, i cambiamenti infrastrutturali, le minacce emergenti possono essere individuati con una rapidità prima inimmaginabile, permettendo di trasformare in decisione tattica quello che altrimenti resterebbe un semplice accumulo di segnali[180].

Questa trasformazione non riguarda solo l'efficienza tecnica. Essa incide profondamente sulla relazione tra apparato bellico statale e mercato privato. MetaConstellation, infatti, non opera come piattaforma esclusivamente governativa o militare, ma si alimenta anche di dati prodotti da aziende private come Maxar e Planet Labs, che raccolgono immagini satellitari per usi commerciali. La loro integrazione nello stesso ecosistema in cui confluiscono dati statali e militari rappresenta un mutamento sostanziale nella natura della guerra contemporanea: lo spazio operativo diventa un terreno condiviso tra pubblico e privato, in cui le imprese tecnologiche assumono un ruolo paragonabile, se non superiore, a quello degli attori statali. L'Ucraina diventa così il primo caso

[177] Ishaan Tharoor, "How the Algorithm Tipped the Balance in Ukraine," *The Washington Post*, 19 dicembre 2022.
[178] George Grylls, "Ukraine's Secret Weapon: The £40bn Tech Firm That Found Bin Laden," *The Times*, 2023.
[179] Vera Bergengruen, "How Palantir Is Shaping the Future of Warfare," *TIME*, 27 giugno 2023.
[180] Vedi anche George Grylls in *Palantir. Ukraine's Technological Edge*. Reprint da *The Times*, 24 dicembre 2022.

emblematico di “guerra algoritmica”, condotta attraverso un’infrastruttura che non appartiene né a un esercito né a un’alleanza militare, ma a una società privata che agisce come attore ibrido, sospeso tra industria e sicurezza nazionale. Dal punto di vista tecnico, i contributi più rilevanti provengono dall’integrazione di dati con caratteristiche radicalmente diverse ma complementari. Le immagini satellitari ottiche forniscono rappresentazioni ad alta risoluzione in bande visibili e infrarosse, utili per identificare con precisione edifici, mezzi militari o modifiche al terreno, ma sono condizionate dalla presenza di nuvole e dalla luce solare. I sensori radar SAR, al contrario, utilizzano microonde capaci di attraversare nuvole, fumo o pioggia, restituendo informazioni indipendenti dalle condizioni atmosferiche e dall’illuminazione. A queste fonti si aggiungono i flussi civili di tracciamento delle navi e degli aerei (AIS e ADS-B), i dati provenienti dalle reti logistiche, le comunicazioni operative e le informazioni condivise dagli alleati. La funzione di Palantir non si esaurisce nella raccolta: la piattaforma filtra e correla i dati, riducendo la ridondanza e traducendo formati diversi in un quadro operativo immediatamente fruibile.

Il risultato è duplice. Da un lato, si riduce sensibilmente il tempo necessario per passare dalla rilevazione al fuoco, accorciando la kill chain e consentendo all’Ucraina di operare con una prontezza decisionale paragonabile a quella delle strutture NATO, pur senza farne parte. Dall’altro, si introduce una nuova logica di interoperabilità che rende meno netta la distinzione tra informazioni civili e militari, tra produzione privata e utilizzo governativo. La conseguenza è che la guerra non appare più solo come un fenomeno di competizione tra eserciti nazionali, ma come un terreno di co-produzione in cui attori statali e privati collaborano, talvolta in maniera opaca, nella definizione delle strategie e delle pratiche operative. Questa dinamica non si limita alla dimensione strettamente militare. MetaConstellation è stata impiegata anche per fini giudiziari e civili, in particolare per la raccolta e l’elaborazione di prove digitali relative a presunti crimini di guerra. La piattaforma ha contribuito a organizzare immagini da droni, post sui social media, intercettazioni e dati satellitari, rendendoli utilizzabili in dossier destinati a tribunali e organismi internazionali. In questo senso, il sistema si colloca all’intersezione tra guerra e giustizia, evidenziando come il potere di gestione dei dati non influisca soltanto sull’azione militare, ma anche sulla costruzione di narrazioni legali e politiche. La guerra in Ucraina, quindi, non è soltanto un conflitto territoriale: è il primo scenario in cui l’infrastruttura informativa diventa la vera protagonista del campo di battaglia. Palantir, con MetaConstellation, mostra come il dominio dei dati e la capacità di renderli operativi in tempo reale siano ormai elementi indispensabili per la conduzione della guerra contemporanea. Questo caso impone una riflessione più ampia sul futuro delle relazioni internazionali e sul ruolo che le imprese tecnologiche private possono assumere

nelle dinamiche belliche, alterando il confine tradizionale tra pubblico e privato, tra potere statale e potere industriale.

3.6. La logica securitizzante

La lettura in chiave di securitizzazione permette di vedere come, di fronte a un'aggressione, l'urgenza strategica renda accettabile l'ampliamento dell'accesso a dati commerciali, la cooperazione con *vendor* esteri e la creazione di canali di scambio informativo che, in tempi di pace, sarebbero più difficili da giustificare. L'audience, in questo caso, è plurale: autorità politiche e militari, partner internazionali, opinione pubblica nazionale ed europea. L'adozione di piattaforme private diventa parte della narrazione dell'efficacia e, insieme, del dilemma della dipendenza: quanto l'infrastruttura è "sostituibile", chi certifica l'affidabilità della supply chain, quali condizioni di trasparenza sono imposte ai fornitori. Le note critiche hanno infatti messo in guardia sui rischi per la privacy, sulla necessità di cornici etiche e sull'impatto che accordi confidenziali possono avere su diritti e bilanciamento dei poteri. Applicando la lente della securitizzazione (di nuovo Buzan, Wæver, de Wilde), l'intervento di Palantir in Ucraina può essere interpretato come parte di un processo discorsivo che trasforma il dominio digitale e informativo in un tema di sicurezza esistenziale. La piattaforma non è solo un tool tecnico, ma viene narrata dai governi occidentali e dai media come un *game-changer*, essenziale per la sopravvivenza dello Stato ucraino. Attraverso atti linguistici e cornici comunicative, il flusso dei dati satellitari e commerciali viene elevato a priorità di sicurezza nazionale, giustificando così un'integrazione senza precedenti tra industria privata e difesa. In questo senso, Palantir non appare solo come un attore tecnologico, ma come un "agente securitizzante": la sua presenza nel conflitto si legittima attraverso la capacità di incarnare la promessa di protezione e sopravvivenza, trasformando la gestione dei dati in un atto politico.

Come sottolineato da un editoriale del *Washington Post* (2022), l'integrazione di Palantir nella difesa ucraina solleva questioni di trasparenza e accountability. Se da un lato la piattaforma è presentata come garanzia di efficienza e rapidità, dall'altro non esistono meccanismi chiari per verificare logiche algoritmiche e bias. In questa prospettiva, il discorso critico può essere letto come una forma di contro-securitizzazione: mentre la narrativa governativa ed aziendale costruisce Palantir come "salvatrice digitale", la stampa indipendente sottolinea i rischi di dipendenza da un attore privato e l'assenza di reali controlli democratici[181]. Tale tensione mostra bene la dimensione

[181] David Ignatius, "How the Algorithm Tipped the Balance in Ukraine," *The Washington Post*, December 19, 2022.

costruttivista della guerra algoritmica: la fiducia nell'AI non deriva da verifiche tecniche, ma da narrazioni politiche e industriali che cercano di consolidarne la legittimità. La visita del CEO di Palantir, Alex Karp, a Kiev nel giugno 2022, documentata da *DefenseNews*, rappresenta uno degli episodi simbolicamente più forti della securitizzazione della tecnologia nella guerra in Ucraina. Karp, accolto da Zelensky come un capo di Stato, ha incarnato in quell'occasione la trasformazione di Palantir da semplice vendor tecnologico ad attore politico-militare riconosciuto[182]. Non si tratta di un dettaglio marginale: è un atto discorsivo che costruisce l'azienda come alleato strategico indispensabile per la sopravvivenza dello Stato ucraino. Dal punto di vista costruttivista, l'episodio mostra come identità e ruoli possano essere ridefiniti: Palantir non è più soltanto un'impresa privata, ma diventa parte della comunità politica della difesa occidentale. In chiave neofunzionalista, questa trasformazione evidenzia un chiaro spill-over politico-istituzionale: la cooperazione tecnica si consolida come integrazione strutturale tra governo e impresa, normalizzando la presenza di attori privati nelle alleanze di sicurezza.

Nel contesto della guerra in Ucraina, un momento particolarmente significativo si è verificato quando il Presidente Zelensky ha incontrato ufficialmente Alex Karp, CEO di Palantir Technologies. Il comunicato rilasciato dall'Office of the President of Ukraine (dicembre 2022) descriveva la collaborazione non nei termini di una comune relazione commerciale tra Stato e fornitore privato, bensì come una partnership strategica per la sopravvivenza del Paese. L'enfasi non era posta sulla componente tecnologica neutrale, ma sul valore esistenziale che la piattaforma di Palantir avrebbe avuto nella resistenza all'invasione russa: la capacità di integrare e processare grandi quantità di dati satellitari, militari e civili veniva rappresentata come fattore chiave per la difesa dello Stato e per la protezione della popolazione[183]. Si tratta di un chiaro atto di securitizzazione, nel senso indicato dalla Scuola di Copenaghen: attraverso uno speech act compiuto al massimo livello politico, una tecnologia privata viene elevata a "strumento vitale di sicurezza nazionale". In questo modo, la partnership con Palantir non appare più come un'opzione tecnica, ma come una misura necessaria e straordinaria in risposta a una minaccia esistenziale. L'incontro pubblico con Zelensky contribuisce inoltre a legittimare l'azienda come attore politico a pieno titolo, al pari degli alleati istituzionali tradizionali (USA, NATO, UE), consolidando la sua immagine di "alleato strategico" e non di semplice vendor tecnologico. Questo episodio mostra bene come il discorso securitizzante possa ridefinire le gerarchie di legittimità nel campo della

[182] Colin Demarest e Jen Judson, "Palantir's Karp Is First Western CEO to Visit Zelenskyy Amid Invasion," *Defense News*, 2 giugno 2022.
[183] President of Ukraine, "President of Ukraine and Palantir CEO Discussed Cooperation in the Defense and Security Sector," *Office of the President of Ukraine*, 2 giugno 2022.

sicurezza internazionale: non solo Stati e organizzazioni internazionali, ma anche corporation tecnologiche diventano referenti indispensabili della sicurezza nazionale. Nel caso ucraino, la narrazione prodotta dalla Presidenza ha trasformato Palantir in un attore politico riconosciuto, capace di occupare lo spazio simbolico dell'alleanza militare. In termini teorici, ciò conferma la centralità del linguaggio e degli atti istituzionali nel costruire la sicurezza: l'AI e le infrastrutture digitali non sono percepite come semplici strumenti tecnici, ma come condizioni di sopravvivenza collettiva, e dunque come "armi" discorsive tanto quanto operative.

Un ulteriore tassello del processo di securitizzazione della tecnologia Palantir in Ucraina emerge dal comunicato ufficiale del Ministero dell'Economia (aprile 2023), che annuncia un accordo con l'azienda statunitense per l'uso dell'intelligenza artificiale nei processi di sminamento. In questo documento, il linguaggio utilizzato è particolarmente rivelatore: non si parla soltanto di efficienza tecnica o di innovazione industriale, ma di "urgenza" e "modernizzazione della sicurezza nazionale". L'AI viene descritta come strumento indispensabile non soltanto sul fronte militare, ma anche nella protezione della vita civile e nella ricostruzione del Paese devastato dalla guerra[184]. Da un punto di vista teorico, questa dichiarazione istituzionale mostra come il discorso securitizzante travalichi la sfera strettamente militare per colonizzare anche spazi apparentemente umanitari o civili. Lo sminamento, tradizionalmente collocato nell'ambito della sicurezza umana e della cooperazione internazionale, viene rappresentato come parte integrante della difesa nazionale e come priorità securitaria. In questo modo, la tecnologia Palantir, già legittimata come alleato strategico nella lotta contro la Russia, diventa anche garante della sicurezza quotidiana della popolazione e della possibilità stessa di ricostruire lo Stato. Il comunicato congiunto della Cybersecurity and Infrastructure Security Agency (CISA) e delle autorità ucraine (2023) amplia la prospettiva oltre il singolo caso Palantir, mostrando come l'intero dominio digitale venga securitizzato nel contesto della guerra. Nel testo si sottolinea che la cooperazione tra Washington e Kiev nel campo della cyberdifesa non riguarda più soltanto la protezione di reti governative o militari, ma l'intera infrastruttura nazionale, dalle comunicazioni alle reti energetiche. Il lessico adottato enfatizza termini come *resilience*, *critical infrastructure* e *joint defense*, costruendo il cyberspazio non come un ambito tecnico neutrale, ma come nuovo fronte di conflitto esistenziale[185]. Dal punto di vista della securitizzazione, questo documento è esemplare. Buzan e Wæver hanno mostrato come un tema diventi "questione di sicurezza" quando viene presentato

[184] Ministry of Economy of Ukraine, "Automation of Demining Processes and the Use of AI: The Ministry of Economy Signs a Partnership Agreement with Palantir," *Government Portal of Ukraine*, 3 aprile 2023.
[185] Cybersecurity and Infrastructure Security Agency (CISA), "United States and Ukraine Expand Cooperation on Cybersecurity," *CISA Press Release*, 27 luglio 2022.

come minaccia esistenziale che richiede misure eccezionali[186]. In questo caso, la protezione delle reti digitali non è descritta come un problema amministrativo o tecnologico, ma come condizione di sopravvivenza nazionale, tale da giustificare la cooperazione diretta tra agenzie statali e lo sviluppo di meccanismi di risposta straordinari. Il comunicato conferma anche la logica neofunzionalista. La partnership cyber USA–Ucraina nasce come risposta a vulnerabilità militari (attacchi informatici russi alle reti di comando), ma si estende rapidamente a settori civili come l'energia e la sanità, secondo il tipico meccanismo di *spill-over*[187]. L'interdipendenza tecnologica rende impossibile separare il militare dal civile: proteggere i data center del Ministero della Difesa significa automaticamente proteggere le infrastrutture energetiche da cui dipende la società.

Il quadro securitizzante che avvolge la guerra digitale in Ucraina emerge con chiarezza anche nei comunicati ufficiali del Dipartimento di Stato USA dedicati alla cooperazione in materia di sicurezza con Kiev. In tali documenti, Washington descrive la partnership militare non soltanto come un sostegno operativo, ma come un impegno vitale per la stabilità dell'ordine internazionale e per la sopravvivenza stessa dell'Ucraina come Stato sovrano. La narrativa statunitense insiste su due aspetti centrali: la fornitura continua di armamenti e assistenza tecnica viene rappresentata come necessaria a "difendere la democrazia" e a contenere una minaccia esistenziale incarnata dall'aggressione russa; l'integrazione di nuove tecnologie digitali, dalla cybersecurity ai sistemi *data-driven*, viene presentata come elemento strutturale della cooperazione, sottolineando che il conflitto odierno è una guerra "multidominio" in cui i dati e l'infrastruttura digitale hanno lo stesso peso di carri armati e missili[188]. Questo linguaggio conferma il passaggio tipico della securitizzazione: la sopravvivenza di Kiev e, per estensione, della "democrazia europea", viene posta come oggetto di riferimento da proteggere. Di conseguenza, ogni strumento – armamenti tradizionali, piattaforme cloud, software predittivi – diventa legittimo se presentato come funzionale alla difesa di quell'oggetto. Un ulteriore elemento d'interesse, utile per comprendere la logica della guerra algoritmica, è rappresentato dal comunicato BusinessWire del 2023, con cui Palantir annuncia ufficialmente il proprio supporto all'Ufficio del Procuratore Generale ucraino nelle indagini su presunti crimini di guerra[189]. Qui la narrativa aziendale è completamente diversa

---

[186] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner, 1998).
[187] Ernst B. Haas, *The Uniting of Europe: Political, Social, and Economic Forces, 1950–1957* (Stanford: Stanford University Press, 1958).
[188] U.S. Department of State, *U.S. Security Cooperation with Ukraine*, Bureau of Political-Military Affairs, aggiornato 2023.
[189] Palantir Technologies, "Palantir to Support Ukrainian Prosecutor General's Office in Investigating War Crimes," *BusinessWire*, 24 aprile 2023.

rispetto a quella che emerge dai comunicati militari: Palantir non si presenta come *fornitore di targeting*, ma come strumento di giustizia e accountability, garante della trasparenza e della ricostruzione della verità giuridica. Il linguaggio scelto dal comunicato è rivelatore: piattaforme come Foundry e Gotham vengono presentate come strumenti "neutrali", capaci di elaborare grandi moli di dati per preservare prove digitali e supportare i tribunali internazionali. Questa immagine contrasta radicalmente con quella del Palantir *nella kill chain*, usata per accelerare la produzione di target in tempo reale. Questo episodio permette di sottolineare che la guerra algoritmica non è solo questione di armi e attacchi, ma un ecosistema istituzionale che si estende alla giustizia, alla diplomazia e alla società civile. Palantir, insomma, non è più semplicemente un attore tecnologico: viene legittimato come garante di sicurezza e verità tanto sul campo di battaglia quanto nei tribunali. Una voce critica è emersa sul *Washington Post* (dicembre 2022), che ha messo in guardia contro l'entusiasmo acritico per Palantir e le piattaforme algoritmiche utilizzate in Ucraina. L'editoriale sottolineava i rischi di opacità algoritmica e i dilemmi di accountability, ponendo una domanda cruciale: chi risponde se una piattaforma privata fornisce un output errato che conduce a un attacco? L'operatore militare, l'azienda o lo Stato? In questo senso, la fonte rappresenta un esempio di contro-securitizzazione: laddove governi e media hanno narrato Palantir come "alleato indispensabile", il *Washington Post* ha ricordato che l'affidamento cieco agli algoritmi può minare i principi di distinzione e proporzionalità previsti dal diritto internazionale umanitario[190].

3.7. Il frame costruttivista

Di fronte al caso Palantir, la lente costruttivista consente di spostare l'attenzione dalla presunta "natura" della tecnologia alla trama di linguaggi, norme e routine che la rendono credibile, desiderabile e, in ultima analisi, legittima dentro un contesto di guerra. In questa prospettiva, piattaforme come Foundry, Gotham e soprattutto MetaConstellation non sono soltanto strumenti tecnici; sono oggetti discorsivi che, attraverso white paper, blog aziendali[191], linee guida su governance e privacy, testimonianze davanti a organismi pubblici e interviste ai media, guadagnano uno status politico e si radicano come prerequisiti del fare sicurezza[192]. Il loro ruolo non deriva da un'essenza tecnologica autonoma, ma dall'insieme di pratiche comunicative e regolative che le rendono pensabili come soluzione: standard di interoperabilità, template di audit,

[190] David Ignatius, "How the Algorithm Tipped the Balance in Ukraine," *The Washington Post*, 19 dicembre 2022.
[191] Palantir Technologies, "Palantir's Response to OMB on AI Governance, Innovation, and Risk Management," *Palantir Blog*, December 14, 2023.
[192] Palantir Technologies, "Palantir's Recommendations to the White House OSTP on Developing an AI Action Plan," *Palantir Blog*, March 17, 2025.

glossari ufficiali, demo in situazioni di crisi, "playbook" per l'integrazione con i flussi decisionali. Ne risulta una configurazione in cui non è solo la tecnologia a entrare nel dominio militare, ma è il dominio militare a farsi ridefinire dalla semantica operativa della tecnologia, fino a incorporarne tempi, metriche e criteri di validità come se fossero ovvi, inevitabili, naturali[193].

In altri termini, Palantir costruisce il proprio ruolo non solo fornendo software, ma producendo categorie interpretative – "decision advantage", "etica dell'AI in difesa", "sovranità digitale" – che riorganizzano il senso di che cosa significhi fare sicurezza, pianificare operazioni e perfino "vedere" il campo di battaglia. La fiducia non precede la tecnologia, ma viene fabbricata e riprodotta quotidianamente tramite lessici, procedure e standard che allineano attori diversi e rendono interoperabili dati eterogenei, creando familiarità operativa e abbassando le soglie di resistenza organizzativa. Nella pratica, questo significa che mappe, grafi, timeline e score di rischio diventano non solo ausili cognitivi, ma architetture di decisione che distribuiscono responsabilità, tempistiche, livelli di visibilità e criteri di rendicontazione. La promessa di "comprendere più in fretta e meglio" si traduce così in routine e rituali di legittimazione: sessioni di red teaming, matrici RACI, piste di audit, indicatori di confidenza, tutti elementi che performano l'idea di controllo e quindi consolidano l'accettabilità politica dell'intervento tecnologico. Il vocabolario scelto da Palantir è un primo tassello di questa costruzione. Nei documenti di policy e nei contributi indirizzati alle istituzioni statunitensi, l'azienda definisce l'AI come infrastruttura capace di offrire un "decision advantage" a decisori e militari[194]. Questo vantaggio, secondo la retorica aziendale, permetterebbe di prevenire conflitti e mitigare rischi grazie a un'integrazione più rapida e sicura dei dati, alla riduzione dei tempi di latenza tra sensing e sense-making, e alla capacità di orchestrare molteplici domini (spazio, cyber, terra) dentro un'unica cornice di command and control[195]. La formula, all'apparenza neutra, traduce funzioni computazionali in categorie normative: non più semplici database o pipeline di analisi, ma un bene strategico la cui assenza espone gli Stati a vulnerabilità sistemiche, quasi fosse una componente critica della sovranità alla stregua dell'energia o delle reti di pagamento. Il linguaggio del "vantaggio" mette dunque in fila un prima e un dopo: prima, l'incertezza e l'attrito; dopo, la "chiarezza" operativa prodotta da correlazioni, simulazioni e raccomandazioni machine-assisted.

---

[193] Mohammad Nazer Shahir and Ali Boghairy, "Constructivist Analysis of Russia's Military Invasion of Ukraine (2022).
[194] Palantir Technologies, "AI Systems Governance through the Palantir Platform," *Palantir Blog*, December 20, 2024.
[195] Palantir Technologies, "Data Lifecycles: Protecting Data with Privacy First Principles," *Palantir Blog*, June 16, 2023.

Il lessico del "vantaggio decisionale" agisce così in modo performativo: naturalizza l'idea che la sovranità, nella sua dimensione operativa, si giochi sulla capacità di tradurre dati in decisioni con una velocità e una tracciabilità che solo determinati sistemi promettono di garantire[196]. Palantir articola questa promessa in risposte formali indirizzate alla Casa Bianca e alle agenzie federali, dove sostiene che l'AI – se ben governata – può rafforzare l'adesione ai principi del diritto umanitario, migliorando consapevolezza situazionale e indagini post-azione, e fornendo un "registro" verificabile delle scelte compiute[197]. Nel fare ciò, sposta l'attenzione dal "se" adottare queste piattaforme al "come" farlo in modo responsabile, disegnando un perimetro discorsivo in cui l'adozione diventa l'opzione predefinita e l'inerzia istituzionale appare come irresponsabilità organizzativa. In parallelo, la retorica del vantaggio consolida nuove metriche di riuscita – tempi di ciclo, coverage dei sensori, ratio segnale/rumore – che diventano indicatori di buona amministrazione della sicurezza[198].

Questa torsione linguistica è ben visibile nella memoria presentata all'Office of Science and Technology Policy, in cui "decision advantage" viene descritto contemporaneamente come beneficio nazionale e come criterio di impiego responsabile dei sistemi d'AI. L'azienda non si limita quindi a offrire un prodotto: costruisce una cornice normativa e semantica che rende l'adozione della tecnologia non solo utile, ma doverosa, facendone un attributo di "buona governance". L'enunciazione stessa del vantaggio genera aspettative politiche e amministrative: procurement più rapidi, interoperabilità by design, integrazione con standard NATO, tutto inscritto in una narrazione dove ritardo tecnologico equivale a deficit di tutela del personale e dei civili[199]. È così che la categoria performa budget, roadmap, e obiettivi di missione, trasformando un argomento tecnico in una ragione di Stato[200]. La seconda parola chiave è "sovranità". Palantir dedica articoli e iniziative alla nozione di "sovranità digitale", associandola alla capacità, per

---

[196] U.S. Department of Defense, *Summary of the Joint All-Domain Command and Control Strategy* (Washington, DC: Department of Defense, 2022); vedi anche Brian R. Price, "Decision Advantage and Initiative: Completing Joint All-Domain Command and Control," *Air & Space Operations Review* 3, no. 1 (2024).

[197] Palantir Technologies, *Response to the Office of Science and Technology Policy: National Priorities on AI* (Washington, DC: Executive Office of the President, 2023), PDF; Palantir Technologies, "AI Systems Governance through the Palantir Platform," *Palantir Blog* (20 dicembre 2024); Palantir Technologies, "Security Auditing • Audit Logging Overview," *Foundry Docs* (13 marzo 2023).

[198] .S. Department of Defense, *Summary of the JADC2 Strategy*; U.S. Government Accountability Office, *DOD and Air Force Continue to Define Joint Command and Control* (Washington, DC: GAO, 2023).

[199] NATO Supreme Headquarters Allied Powers Europe, "NATO Acquires AI-Enabled Warfighting System (MSS NATO)," press release (14 aprile 2025); Cristina Criddle, "NATO Acquires AI Military System from Palantir," *Financial Times* (aprile 2025).

[200] Brandi Vincent, "Army Plans Big Shake-Up in Software Buying Practices with Palantir Deal," *DefenseScoop* (31 luglio 2025).

istituzioni pubbliche e imprese, di mantenere il controllo sui propri dati e sulle decisioni che da essi discendono. Le partnership europee, la partecipazione a progetti come GAIA-X e le referenze a requisiti di "data residency" servono a collocare l'azienda come "fornitore sovrano", in grado di coniugare performance e compliance in giurisdizioni caratterizzate da forte sensibilità regolatoria[201]. Nel racconto aziendale, la sovranità smette di essere un attributo esclusivo dello Stato per presentarsi come esito di un'architettura: chi controlla lo stack (ingestion, cataloghi, policy, lineage) controlla il campo decisionale, e quindi l'esercizio effettivo dell'autorità. La retorica enfatizza la reversibilità, la portabilità e la segmentazione perimetrale, costruendo l'immagine di un potere pubblico che "sceglie" standard privati senza abdicarvi.

La semantica, anche qui, è decisiva: la sovranità non è più soltanto un attributo dello Stato, ma un bene co-prodotto con un attore privato capace di garantire infrastrutture e standard. Il confine tra pubblico e privato non scompare, ma viene ridisegnato nei termini di una co-titolarità operativa, in cui la "compliance" diviene vettore di legittimazione reciproca. È un esempio limpido di co-costruzione discorsiva: l'azienda assorbe nel proprio linguaggio parole della politica – sovranità, alleanza, responsabilità – e le reimmette nel mercato come qualità della piattaforma; lo Stato, a sua volta, traduce le proprie funzioni in requisiti tecnici (criteri di logging, classificazione, segregazione) che, una volta inscritti nello stack, diventano regole di fatto. Così la sovranità si fa lavoro infrastrutturale: non un principio astratto, ma un insieme di scelte di design che allocano poteri, visibilità, tempi e possibilità di contestazione. Il contesto ucraino mostra bene come queste categorie non restino sulla carta. Le dichiarazioni pubbliche del CEO Alex Karp hanno messo in chiaro che il software di Palantir è impiegato direttamente nella catena che porta alla selezione degli obiettivi[202]. La frase – "responsabile della maggior parte del targeting in Ucraina" – ha un valore che va oltre l'informazione: inscrive l'azienda nel lessico della vittoria e della difesa nazionale, trasformando un fornitore in "alleato" e comprimendo la distanza simbolica tra decisione pubblica e capacità privata[203]. In questa narrativa, la piattaforma è più di un'interfaccia: è la grammatica che rende "leggibile" il teatro operativo, l'ambiente in cui i dati prendono forma come opportunità, minacce, priorità. Di conseguenza, strumenti e concetti diventano coestensivi: tasking, fusion, triage, deconfliction, ogni voce costruisce l'ovvietà di un workflow, e il workflow radica l'idea che l'azione corretta sia quella già anticipata dal sistema. L'alleanza è innanzitutto

[201] GAIA-X Association, "GAIA-X Strengthens European Digital Sovereignty at European Parliament Reception" (21 marzo 2025).
[202] Jeffrey Dastin, "Ukraine Is Using Palantir's Software for 'Targeting,' CEO Says," *Reuters*, February 1, 2023.
[203] "Ukraine War Shows Urgency of Military AI, Palantir CEO Says," *Reuters*, February 15, 2023.

linguistica: in conferenze, interviste e documenti, la linea di demarcazione tra Stato e impresa si assottiglia, e la piattaforma diventa una componente dell'identità politica ucraina orientata alla "sovranità dei dati" e alla resilienza. Questa metamorfosi linguistica è poi amplificata dalla copertura mediatica. Un'inchiesta di *TIME* ha narrato la presenza di Palantir in Ucraina come integrazione trasversale allo Stato, dal ministero della Difesa ad altre agenzie, con un uso che eccede il fronte cinetico e tocca la bonifica degli ordigni, la raccolta di prove di crimini di guerra e il coordinamento di risorse civili. Tale racconto fissa cornici di senso: la guerra come problema di interoperabilità, la protezione dei civili come questione di visibilità in tempo quasi reale, la strategia come disciplina di orchestrazione dati. La ripetizione di questi frame consolida aspettative: più sensori, più correlazioni, più automazione nella prioritizzazione[204].

Nella stessa ricostruzione, MetaConstellation compare come il perno di una "kill chain digitale": i dati di droni, satelliti e fonti aperte vengono fusi e presentati come opzioni operative, in un flusso che reinterpreta il campo di battaglia come ecosistema informazionale. Raccontare la guerra come "laboratorio" dell'AI consolida l'idea che il terreno principale della competizione sia il ciclo dato-decisione, e che i soggetti più legittimati a popolarlo siano le aziende tech che lo rendono possibile. Ma, soprattutto, re-distribuisce la responsabilità: se la bontà della decisione dipende dalla "completezza" del quadro informativo, allora la mancanza di determinate integrazioni o la lentezza di alcuni connettori diventa, discorsivamente, una carenza di protezione. La norma implicita diventa così il massimo grado di visibilità tecnicamente raggiungibile. La costruzione discorsiva di Palantir non si limita a parole suggestive. Stabilire che l'AI fornisca "vantaggio" e "sovranità" sposta la discussione pubblica dalla domanda "se" impiegarla alla domanda "come" e "con chi". L'azienda presidia perciò anche il livello delle regole: pubblica white paper su privacy e governance, promuove cornici di "responsible AI", propone modelli di audit, controllo degli accessi, tracciabilità e versionamento. A livello operativo, ciò si traduce in policy engine, profili RBAC/ABAC, masking a livello di colonna e di riga, e grafi di lineage che promettono di rendere ogni trasformazione ispezionabile ex-post. La promessa non è tanto la perfezione informativa, quanto l'introduzione di una razionalità verificabile che consenta di dimostrare, dopo il fatto, che i passaggi decisionali sono stati "ordinati", "giustificati", "misurabili". È un modo per tradurre in procedure tecniche questioni che, altrimenti, resterebbero eminentemente politiche: chi decide, chi risponde, chi vede che cosa. La normalizzazione passa proprio da qui: l'AI bellica diventa accettabile perché presentata come più controllabile dei processi tradizionali; l'interfaccia – con i

[204] Bruno Maçaes, *TIME*, "How Palantir Is Shaping the Future of Warfare," July 4, 2023.

suoi log, i suoi grafi di lineage, i suoi profili di permesso – promette una razionalità verificabile. In termini costruttivisti, sono questi dispositivi a costruire la fiducia organizzativa, più dei claim astratti su neutralità o "umanità" del sistema. Ne deriva un mutamento della scena della responsabilità: da virtù politica a qualità dell'infrastruttura, da principio deliberativo a proprietà di una piattaforma. Così la "responsabilità" si performa attraverso l'auditabilità, e l'auditabilità finisce per definire lo spazio del dicibile e del contestabile[205].

Qui la comparazione con il caso russo, come descritto da Shahir e Boghairy, è illuminante. Il paper mostra come anche la Russia abbia utilizzato categorie discorsive per giustificare e normalizzare la guerra in Ucraina, radicando l'azione nello schema identitario dell'Eurasianismo e nella ricerca di "sicurezza ontologica" (identity security) come continuità di sé nel tempo. L'invasione del 2022, secondo gli autori, non può essere spiegata solo con categorie realistiche o geopolitiche, ma deve essere letta come un atto identitario in cui l'Ucraina viene narrata quale parte integrante del *Russkiy mir*, e la sua "perdita" come minaccia esistenziale alla coerenza del sé collettivo. La performatività dei discorsi – "denazificazione", "recupero delle terre storiche", "difesa contro l'allargamento NATO" – organizza aspettative e rende plausibile l'uso della forza come scelta necessaria e perfino protettiva. Il lessico usato dal Cremlino è performativo tanto quanto quello di Palantir: dire che l'Ucraina è "parte della Russia", che il regime di Kiev è "neo-nazista" o che la guerra è volta alla "denazificazione" produce condizioni di realtà che giustificano l'azione militare, in modo analogo a come "decision advantage" naturalizza la centralità di piattaforme private nella definizione del ciclo dato-decisione. Se Palantir pratica un "constructivismo aziendale aggressivo", gli autori definiscono l'approccio russo "constructivismo aggressivo": una combinazione di motivazioni identitarie e logica militare che trasforma la guerra in dispositivo di riaffermazione ontologica. In entrambi i casi, l'enunciazione non descrive il mondo: lo fabbrica, delimitando il dicibile e quindi il possibile. L'analogia, per il tuo capitolo, consente di mostrare come Stati e corporation condividano tecniche retoriche di legittimazione, pur perseguendo finalità diverse e operando su piani istituzionali differenti.

Il ruolo dei media e dei think tank contribuisce a stabilizzare queste rappresentazioni. Analisi sulla trasformazione del dominio spaziale e dei dati nel conflitto ucraino sottolineano la centralità dei servizi commerciali per la condotta delle operazioni, offrendo un fondale autorevole alla tesi –

[205] Shahir, Mohammad Nazer, and Ali Boghairy. "Constructivist Analysis of Russia's Military Invasion of Ukraine (2022); Investigating Putin's Identity Model and Cognitive Actions." *Journal of World Sociopolitical Studies* 8, no. 4 (Autumn 2024): 846–850.

cara a Palantir – secondo cui l'innovazione privata è ormai componente strutturale della sicurezza. Report, podcast, workshop inter-agenzia, simulazioni e wargame accademici ricorsivamente citano l'efficacia di soluzioni C2 "data-driven", sedimentando un canone discorsivo che associa il "buon governo" della guerra alla capacità di orchestrazione informazionale. La riproduzione di grafici, storyboard, dashboard nelle sedi pubbliche e mediatiche non solo documenta, ma accentua l'adozione: ciò che si vede e si ripete acquisisce la forza del necessario. Parallelamente, Palantir coltiva con attenzione la propria europeizzazione: la partecipazione a GAIA-X, gli impegni sulla localizzazione dei dati e i testi dedicati alla "sovranità digitale" in lingua tedesca e francese mostrano come l'azienda non si limiti a vendere software, ma si proponga come interprete delle sensibilità normative europee. Anche qui, il lavoro è performativo: posizionarsi come "fornitore sovrano" significa contribuire a scrivere le regole e a trasformarle in specifiche tecniche di piattaforma – dai requisiti di pseudonimizzazione al versioning delle policy – con effetti a cascata su procurement, certificazioni e pratiche di audit. Il risultato è un allineamento interessato ma stabile: la norma dà forma allo stack, lo stack produce tracciabilità, la tracciabilità "dimostra" conformità, e la conformità diventa argomento politico per l'espansione dello stack.

L'approccio costruttivista invita a considerare i rischi non come "effetti collaterali" di una tecnologia neutra, ma come possibilità inscritte nelle stesse cornici discorsive che ne legittimano l'uso. Presentare l'AI come fonte di "vantaggio decisionale" può favorire automatismi cognitivi che attenuano lo scetticismo critico verso errore e incertezza, spingendo verso una "epistemic overreach" in cui la quantità di dati e la loro integrazione sostituiscono surrettiziamente il giudizio politico. Parlare di "sovranità digitale" all'interno di infrastrutture proprietarie può creare frizioni tra promessa di autonomia e pratiche di dipendenza: l'effetto lock-in, l'opinioned integration, la path-dependency che lega la pianificazione operativa alle affordance di una piattaforma riducono, nel tempo, lo spazio di manovra istituzionale. Invocare la "responsabilità" come promessa di tracciabilità tecnica può oscurare la necessità di accountability democratica: ciò che è auditabile non è automaticamente giustificabile, e la qualità dei log non sostituisce la deliberazione pubblica. Sono le stesse ambivalenze che emergono nel caso russo: Putin giustifica l'invasione come difesa dell'identità russa, ma proprio questa retorica produce dipendenza dal linguaggio militare e dall'idea di conflitto come unica forma di sicurezza. Come mostrano Shahir e Boghairy, la "sicurezza ontologica" può diventare cornice che assorbe e neutralizza obiezioni alternative – negoziazione, neutralità, regionalizzazione dei rischi – trasformando la politica in necessità tecnica e l'eccezione in regola. Analogamente, nel discorso aziendale, il rischio è che "responsible AI" si riduca a check-list di conformità che presiedono alla continuità dell'adozione, spostando la

critica dalla sostanza (chi decide e perché) alla forma (come si logga e con quali standard), con il pericolo di un "ethical hollowing out".

Osservare Palantir attraverso la lente costruttivista significa mettere a fuoco una doppia co-produzione: da un lato la tecnologia contribuisce a definire che cos'è, oggi, "guerra" – un processo di orchestrazione informazionale che promette velocità, coerenza e tracciabilità; in tal senso, dashboard, flussi ETL, grafi di dipendenza e sistemi di ranking plasmano ciò che conta, che è visibile e che resta negli archivi, istituzionalizzando nuove metriche di successo operativo e nuove forme di responsabilità documentale; dall'altro il discorso politico e mediatico contribuisce a definire che cos'è, per un'impresa privata, "sovranità", "alleanza", "responsabilità", ridefinendo il patto pubblico-privato e trasformando caratteristiche tecniche in virtù civiche, fino a far coincidere il "bene comune" con le affordance di uno stack proprietario. MetaConstellation non è soltanto un componente software: è un simbolo che riunisce in un'unica immagine la fusione tra spazio, dati e decisione. I documenti su governance e privacy non sono soltanto manuali tecnici: sono dispositivi retorici che trasformano un'infrastruttura commerciale in garanzia di ordine pubblico. Le frasi pronunciate dal CEO non sono meri commenti: sono atti performativi che inseriscono l'azienda nella grammatica della sicurezza nazionale, definendo l'ovvio e il necessario e spostando il baricentro dal "se" al "come". La comparazione con il caso russo – identità, Eurasianismo, sicurezza ontologica, "costruttivismo aggressivo" – mostra che tanto gli Stati quanto le corporation tech operano attraverso cornici discorsive che fanno esistere gli oggetti che nominano. Nel caso ucraino, Palantir non si limita a "fornire" strumenti: contribuisce a costruire il mondo in cui quegli strumenti appaiono necessari, legittimi e persino doverosi, mentre l'apparato retorico e regolatorio ne stabilizza la presenza nel tempo.

3.8. Una parentesi sulla prospettiva neofunzionalista

Il paradigma neofunzionalista di Ernst B. Haas– che concepisce l'integrazione come un processo incrementale innescato da cooperazioni tecniche circoscritte e propagato tramite spill-over funzionali, politici e "coltivati" da imprenditori dell'integrazione– offre una lente particolarmente utile per leggere la trasformazione, prodotta dalla guerra in Ucraina, delle infrastrutture tecnologiche civili in dispositivi militari e giuridici a forte valenza istituzionale, ridefinendo confini e funzioni della sovranità in un ecosistema ibrido Stato–impresa; nella formulazione classica, infatti, l'integrazione tende ad auto-alimentarsi una volta avviata in ambiti tecnici, generando pressioni verso settori contigui e istituzioni più ampie, una dinamica ampiamente discussa nella ricerca su Haas e sulla sua nozione di spill-over automatico (e sulle sue revisioni

successive), che qui viene "riallocata" dall'Europa comunitaria al teatro bellico e digitale ucraino, dove la cooperazione su standard, dati e interoperabilità assume di fatto la funzione di un nuovo livello di governance[206]. In questa prospettiva Palantir Technologies incarna l'esempio più eloquente di come una fase iniziale di cooperazione tecnica limitata– nella quale l'obiettivo era integrare fonti eterogenee e assicurare auditabilità e sicurezza dei dati– abbia prodotto, per pressione funzionale e per "coltivazione" imprenditoriale, un'espansione semantica e normativa: il lessico aziendale di *decision advantage*, *data-driven sovereignty* e *trust architecture* non si limita a promuovere capacità software, ma connette esplicitamente la competenza di calcolo alla legittimazione dell'autorità pubblica, predisponendo quel trasferimento di fedeltà e aspettative verso infrastrutture tecnico-istituzionali che il neofunzionalismo associa ai momenti di avanzamento dell'integrazione[207].

L'acceleratore è stato il campo di battaglia ucraino, dove la piattaforma MetaConstellation ha reso operativa la logica di spill-over dal dominio civile a quello militare orchestrando in tempo quasi reale un mosaico di dati provenienti da satelliti commerciali, sensori SAR, flussi civili come AIS/ADS-B e asset militari, con la conseguenza di comprimere drasticamente il *sensor-to-shooter cycle* e di trasformare la "raccolta" informativa in abilità di tiro e manovra: osservatori indipendenti hanno documentato che MetaConstellation coordina tasking e revisite dei satelliti come un vero "orchestratore", capace di portare il passaggio da immagine a ingaggio a una scala di minuti, segnando una discontinuità nei tempi del comando-controllo e nella connettività tra sensori e attuatori. La proiezione di questa infrastruttura oltre il perimetro tecnico è visibile anche nel mutamento di percezione pubblica: non un fornitore privato tra i tanti, ma un "alleato" dell'Ucraina, un attore che, secondo dichiarazioni del suo amministratore delegato riprese da Reuters, sarebbe stato "responsabile della maggior parte del targeting" effettuato nel teatro ucraino– affermazione che, al di là della retorica, segnala una simbiosi operativa e cognitiva tale da rendere porosa la linea tra supporto commerciale e funzione sovrana. L'analisi neofunzionalista aiuta a spiegare perché, una volta imposti standard e routine interoperabili, gli attori pubblici siano incentivati ad armonizzare procedure, basi dati e dottrine operative con l'infrastruttura già in uso: è la catena cumulativa dello spill-over funzionale che, nel caso ucraino, investe non solo il ciclo di targeting e l'intelligence tattica ma anche la pianificazione della resilienza civile, la gestione delle infrastrutture critiche e l'amministrazione della ricostruzione, come mostrano sia i white

[206] Ernst B. Haas, *The Uniting of Europe: Political, Social, and Economic Forces, 1950–1957* (Stanford: Stanford University Press, 1958).
[207] Palantir Technologies, *Foundry for Resilience Planning*, white paper (London: Palantir Technologies UK).

paper aziendali sia il dibattito sulle piattaforme digitali per la ripartenza e l'integrazione economica con l'Europa.

La stessa dinamica di propagazione emerge sul versante istituzionale: think tank e osservatori transatlantici hanno evidenziato come l'adozione accelerata di tecnologie dual-use e di sistemi nati per il settore civile abbia saldato in Ucraina una rete di interdipendenze tra Stato, grandi piattaforme e startup, con benefici operativi immediati ma anche con rischi per diritti, accountability e qualità democratica– uno schema perfettamente compatibile con la previsione neofunzionalista secondo cui il successo della cooperazione tecnica tende a creare nuove domande politiche e regolatorie[208]. La metamorfosi funzionale non si arresta al dominio operativo: si osserva uno spill-over "duale" dalla guerra alla giustizia, poiché la medesima architettura dati impiegata per la condotta delle operazioni è stata adattata alla preservazione probatoria e al tracciamento di responsabilità individuali in sede di indagine e di cooperazione con organismi internazionali; fonti giornalistiche e comunicazioni ufficiali indicano che la Procura generale ucraina utilizza software Palantir per mappare fatti, unità militari e catene di comando in potenziali crimini di guerra, in parallelo a un'attività istruttoria dell'ICC avviata sin dai primi giorni dell'invasione su larga scala[209]. Da qui discende un doppio effetto neofunzionalista: da un lato, l'estensione dell'integrazione pubblico-privato a nuove funzioni sovrane (accertamento e memoria giudiziaria), dall'altro, la cristallizzazione di dipendenze tecnologiche difficilmente reversibili, che traducono l'efficienza dello standard proprietario in lock-in istituzionale; rischi e trade-off sono ampiamente discussi nella letteratura di policy, che richiama l'attenzione su potenziali asimmetrie di potere, sulla necessità di cautele per la protezione dei dati e sull'urgenza di meccanismi di controllo democratico proporzionati al nuovo peso delle piattaforme.

La diacronia dell'integrazione ucraina mostra inoltre come lo spill-over non sia monopolio di una singola impresa, ma si situi in un ecosistema più ampio di "imprenditori della cooperazione" tecnologica: la piattaforma statale BRAVE1 coordina innovazione, grant e sperimentazione "in tempo di guerra", mentre il sistema nazionale di *situational awareness* Delta– oggetto di analisi comparate con la visione statunitense CJADC2– sintetizza un'architettura software-defined di comando e controllo in cui l'interoperabilità tra unità, sensori e fuochi diventa un bene pubblico di fatto, organizzando una filiera di dati che scorre tra soggetti statali, partner privati e volontari

[208] Anna Mysyshyn, "Advanced Technologies in the War in Ukraine: Risks for Democracy and Human Rights," *German Marshall Fund of the United States*, 30 settembre 2024.
[209] John Hewitt Jones, "Palantir to Help Ukraine Process Data in War Crimes Investigations," *FedScoop*, 25 aprile 2023 e vedi anche International Criminal Court, *Situation in Ukraine*, accessed august 2025.

qualificati; questa cornice di *software-centric warfare* rende plausibile l'analogia con l'integrazione europea degli anni Sessanta: il "cultivated spill-over" non è qui opera di Commissioni o agenzie comunitarie, ma di ministeri digitali, hub d'innovazione e piattaforme commerciali che generano standard, incentivi e aspettative difficili da disfare a guerra finita[210]. Il valore strategico della *commons* informativa così costruita– milioni di ore di video da droni, telemetrie, telematica di campo, serie storiche su attacchi e riparazioni– è ormai esplicitamente rivendicato come una risorsa di potere negoziale e una leva per l'attrazione di supporto e investimenti occidentali, oltre che un dataset unico per addestrare modelli predittivi e simularne la trasferibilità in altri teatri: nelle ricostruzioni giornalistiche più recenti, il patrimonio dati del fronte è definito una "miniera" preziosa e difficilmente riproducibile, segno che lo spill-over della guerra nell'economia politica della conoscenza è già in atto[211].

Se si ricompone il quadro, il neofunzionalismo appare non come una metafora debole, ma come un modello analitico robusto: la cooperazione tecnica innescata da esigenze contingenti (interoperabilità dei sensori, auditabilità dei flussi, tempi di reazione) genera una catena di integrazioni contigue– operativa, organizzativa, normativa– che travalica il perimetro di partenza e riconfigura la fisionomia stessa della sovranità; Palantir ha svolto un ruolo di "catalizzatore" in più snodi di questa catena (targeting, pianificazione della resilienza, accertamento probatorio), ma la catena si regge su un più vasto assemblaggio che include istituzioni statali, partner alleati, startup e consorzi, tant'è che i principali studi strategici sull'uso di AI e autonomia nel conflitto segnalano non solo l'aumento di efficienza tattica ma anche i problemi di fiducia nell'automazione, di dottrina d'impiego, di stabilità dell'escalation e di conformità al diritto umanitario– tutti aspetti che, nel linguaggio di Haas, corrispondono a *feedbacks* politici che richiedono nuovi livelli di decisione e di regola per non inceppare la macchina dell'integrazione[212]. In definitiva, la guerra in Ucraina funziona da "laboratorio di governance tecnologica" in cui la sovranità digitale diventa il prodotto di una cooperazione strutturale fra Stato e piattaforme, e in cui l'efficacia dello standard tecnico produce sia vantaggi comparativi sia vulnerabilità di dipendenza: l'insieme di questi processi– dalla compressione del ciclo sensore-tiratore alla traslazione dei medesimi grafi dati nella sfera giudiziaria, dall'armonizzazione di pratiche operative alle agende di ricostruzione–

[210] Kateryna Bondar, "Does Ukraine Already Have Functional CJADC2 Technology?," *Center for Strategic and International Studies*, 11 dicembre 2024.
[211] Max Hunder, "Ukraine Sees 'Priceless' Digital Battlefield Data Trove as Key to West's Support," *Reuters*, 27 agosto 2025.
[212] Margarita Konaev, "Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability," *CNA Analysis*, 2 ottobre 2023.

costituisce una traiettoria di integrazione che conferma, con linguaggio aggiornato all'era algoritmica, l'intuizione neofunzionalista secondo cui, quando gli interessi si ricalibrano intorno a infrastrutture condivise, l'integrazione tende a consolidarsi e a replicarsi oltre il dominio originario, fino a ridefinire istituzioni, responsabilità e confini della politica stessa.

3.9. Confronto tra i due casi studio e ultime note metodologiche

Capire cosa facciano davvero le tecnologie di guerra algoritmica, e soprattutto dove si collochino dentro la catena decisionale, diventa più facile quando mettiamo a confronto casi diversi per scopo, scala e linguaggio. In Ucraina, l'asse dell'innovazione si concentra sull'integrazione e sulla coerenza del quadro informativo: l'infrastruttura MetaConstellation, offerta da Palantir, ha la funzione dichiarata di raccogliere e combinare rapidamente fonti eterogenee – immagini satellitari ottiche, dati radar SAR, tracciamenti marittimi e aerei, flussi istituzionali – così da ridurre il tempo tra il segnale grezzo e l'informazione utile, senza sostituirsi formalmente all'ultima parola umana. In altre parole, agisce come un "orchestratore di dati" che accelera il ciclo di comando e controllo mantenendo la validazione finale al livello umano. Questa è una differenza strutturale rispetto a Gaza, dove i sistemi Lavender, Gospel (Habsora) e Where's Daddy? non si limitano a ricostruire il contesto, ma intervengono direttamente nella produzione di target: Gospel propone obiettivi infrastrutturali, Lavender assegna punteggi probabilistici a persone sospettate e alimenta liste semi-automatiche di bersagli, Where's Daddy? traccia gli spostamenti di chi è già stato marcato, per colpirlo in momenti prevedibili della vita privata. In questo schema, l'intervento umano scivola verso un controllo a posteriori o una verifica formale, mentre il cuore selettivo e predittivo della decisione si concentra nel sistema. La divergenza non è un dettaglio ingegneristico: corrisponde a due "epistemologie del conflitto" – un'automazione che aiuta a capire più in fretta in Ucraina, e un'automazione che stabilizza la messa in lista di vite a Gaza.

A questa differenza di funzione si sovrappone una differenza di scala e granularità. L'architettura ucraina è orientata al livello macro: comporre una mappa dinamica, incrociare fonti, creare un'immagine coerente del campo di battaglia. Il ritmo viene accelerato per favorire il coordinamento tra domini e ridurre la latenza decisionale, ma la finalità resta cognitiva e organizzativa. Nel contesto di Gaza, la scala si fa micro: l'attenzione scende sull'individuo, sulle routine, sui segnali deboli che permettono inferenze rapide; è qui che la velocità non è più solo condizione di efficacia, ma diventa vero e proprio dispositivo di produzione di target. Inchieste e testimonianze hanno descritto liste molto ampie di nominativi marcati, soglie di tolleranza del danno collaterale preimpostate e convalide estremamente rapide per le categorie più basse; le

repliche ufficiali hanno insistito sulla natura ausiliaria dell'AI e sulla presenza di un controllo umano. Al di là del dissenso, ciò che conta è l'effetto di standardizzazione: quando la lista nasce già "calda", l'umano tende a confermare più che a rimettere in discussione. Su entrambe le scene, la securitizzazione svolge un ruolo decisivo. In Ucraina, la sopravvivenza dello Stato sotto aggressione viene legata alla capacità di reagire in tempo quasi reale; la promessa di "vantaggio decisionale" eleva la gestione dei dati a priorità esistenziale e rende plausibile un'inedita integrazione tra attori pubblici e privati. Palantir non appare più soltanto come fornitore tecnologico: è costruita discorsivamente come "alleato" politico, un attore la cui presenza viene legittimata dalla promessa di protezione. È il discorso a convertire una piattaforma in garanzia di sicurezza, giustificando l'apertura di filiere dati civili e commerciali verso l'uso bellico. A Gaza, dopo gli attacchi del 7 ottobre 2023, il discorso securitizzante assume toni ancora più duri, e l'urgenza si traduce in una pressione costante ad aumentare il ritmo di produzione dei bersagli. Qui l'AI non è soltanto connessa alla sopravvivenza, ma alla necessità di sostenere campagne aeree in un contesto urbano densissimo, con l'effetto di spostare sul terreno operativo quella stessa idea di emergenza che nel discorso pubblico erode i confini tra civile e combattente. In entrambi i casi, il linguaggio dell'esistenza minacciata rende accettabili misure straordinarie: in Ucraina, la cooperazione strutturale con una corporation tecnologica; a Gaza, la normalizzazione di un targeting semi-automatizzato di soggetti umani. La lente neofunzionalista aiuta a cogliere un secondo meccanismo, più silenzioso ma non meno potente: lo spill-over, ovvero il travaso di standard, dati e prassi tra domini inizialmente separati, che tende a consolidarsi e a replicarsi quando "funziona". L'esperienza ucraina lo mostra dal lato della fusione informativa: tecnologie nate per la logistica commerciale o per la risposta ai disastri si saldano con flussi istituzionali e satelliti commerciali, stabilizzando un'infrastruttura di difesa "software-defined" difficilmente reversibile. L'efficacia operativa genera dipendenze, e le dipendenze generano regole e interfacce che, a loro volta, spingono verso ulteriore integrazione. A Gaza, il percorso è complementare: strumenti di sorveglianza e policing predittivo – riconoscimento facciale, raccolte biometriche, reti di checkpoint – vengono ricomposti dentro pipeline di targeting. Anche qui, una volta imboccata la strada, la dipendenza dagli standard e dai dataset si rafforza, e l'eccezione tende a diventare regola. La diagnosi neofunzionalista, però, va maneggiata con cautela: nasce per descrivere processi cooperativi a bassa conflittualità e rischia di naturalizzare come "integrazione funzionale" scelte che sono invece il prodotto di rapporti di forza, stati d'eccezione e conflitti asimmetrici. Nello scenario ucraino, molte decisioni sono la risposta a pressioni eccezionali; in quello di Gaza, l'uso duale di tecnologie di controllo riflette anche logiche coloniali e di occupazione. La prospettiva costruttivista illumina infine il piano simbolico e semantico, spesso

sottovalutato nei dibattiti tecnologici. In Ucraina, la trasformazione di Palantir in "alleato" segnala uno spostamento d'identità: l'azienda non è più soltanto un vendor, ma un componente della comunità politico-militare occidentale. Episodi pubblici e gesti ufficiali hanno "messo in scena" questa identità, rafforzando l'idea che la sovranità informativa ucraina passi per l'adozione di infrastrutture private. A Gaza, invece, i sistemi nominano le persone come punteggi, le case come coordinate, le routine come finestre d'ingaggio. La stessa scelta dei nomi – Lavender, Gospel, Where's Daddy? – banalizza il gesto di nominare e, così facendo, partecipa alla trasformazione delle persone in oggetti tecnici. Dire "punteggio 0,7" invece di dire "persona" sposta il baricentro etico e prepara culturalmente l'automatismo. Il costruttivismo non afferma che la tecnica sia mera retorica: mostra che il linguaggio è un dispositivo operativo, capace di ridisegnare identità e ruoli, e dunque di modellare responsabilità e aspettative.

Il confronto tra i due casi permette anche di ragionare più sobriamente sulla responsabilità. Dove l'AI funge da orchestratore, la domanda forte riguarda la provenienza dei dati, le regole di fusione, i protocolli di audit e la tracciabilità delle versioni. Se i decisori umani restano titolari dell'ultima autorizzazione, questa titolarità deve appoggiarsi a standard di trasparenza che rendano controllabili priorità e allarmi, e che evitino l'"overtrust" nell'interfaccia. Dove l'AI genera target, la responsabilità corre lungo tutta la pipeline: dalla qualità dei dataset alla scelta delle features, dalle soglie di rischio accettate alle pratiche di convalida, fino ai mezzi effettivamente impiegati nelle aree urbane. In questo secondo caso, il controllo umano "al clic finale" rischia di essere una finzione: il controllo significativo, come ricordano molte riflessioni contemporanee sul diritto umanitario, si esercita sulle soglie e sui passaggi della catena, non sull'ultimo gesto che spesso è già incanalato dalla lista proposta dal sistema. Anche il diritto umanitario in senso stretto risulta stressato in modo diverso nei due contesti. In Ucraina, la privatizzazione di funzioni critiche e la securitizzazione dell'infrastruttura digitale aprono problemi di trasparenza, accountability e controllo democratico di attori che non rispondono direttamente a mandati pubblici; qui la sfida è incastonare le piattaforme in cornici chiare di responsabilità, auditabilità e prova. A Gaza, l'automatizzazione della selezione e l'uso di soglie pre-autorizzate di danno collaterale toccano il cuore dei principi di distinzione, precauzione e proporzionalità: non è solo un tema di "rispetto formale", ma di trasformazione pratica di cosa conti come evidenza sufficiente, come errore accettabile, come tempo legittimo per decidere. È in questo slittamento che si consuma il passaggio dall'urgenza come argomento politico all'urgenza come norma tecnica. Se vogliamo tirare un filo, la differenza cruciale è nella collocazione dell'AI: in Ucraina accelera la comprensione e il coordinamento, a Gaza standardizza la selezione e la ritma; e tuttavia, al di sotto delle differenze,

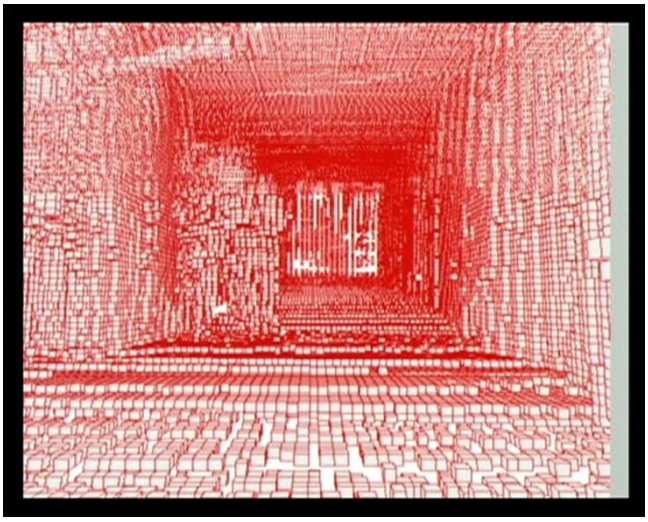
scorre una traiettoria comune fatta di normalizzazione dell'eccezione, militarizzazione dei dati e ridefinizione semantica dei soggetti. Per questo il dibattito non dovrebbe ridursi alla domanda "AI sì o no?", ma piuttosto alla domanda "AI dove e come?". Dove l'AI si colloca a monte e sostiene l'analisi, occorrono garanzie di trasparenza, tracciabilità e controllo pubblico; dove interviene a valle, nel momento selettivo, servono vincoli forti, revisione indipendente, poteri reali di blocco e criteri chiari per ripristinare la presunzione protettiva del diritto.

Sul piano metodologico, è importante essere chiari su ciò che questo confronto può e non può dimostrare. L'impostazione è descrittivo-esplorativa: mappiamo filiere informative, atti discorsivi e assetti organizzativi, senza promettere misurazioni tecniche delle performance algoritmiche o test ingegneristici dei modelli. Questa scelta nasce dal tipo di accesso possibile: i sistemi sono in larga parte opachi, coperti da segreto industriale o da classificazioni militari; i dati pubblicamente disponibili sono eterogenei e spesso confliggenti. Nel caso di Gaza, molte informazioni provengono da inchieste, leak e testimonianze, a cui si affiancano repliche ufficiali e rapporti di organizzazioni internazionali; nel caso ucraino, la base è più istituzionale e policy-oriented, fatta di documenti aziendali, resoconti di governi e alleanze, analisi di think tank e letteratura su tecnologie dual use. Questa asimmetria non è un vizio, ma un elemento costitutivo del campo: segnala che la "verità operativa" è essa stessa oggetto di lotta discorsiva. Per questo, invece di sciogliere il dissenso proclamando chi abbia ragione, lo assumiamo come materiale d'analisi: ciò che una parte presenta come supporto ausiliario, l'altra lo descrive come macchina di targeting; ciò che un'istituzione narra come alleanza, altri lo vedono come dipendenza da piattaforme private. Questa metodologia ha limiti chiari. Il primo riguarda l'opacità tecnica: non potendo aprire i modelli, non misuriamo drift, falsi positivi o la calibrazione delle soglie; non possiamo dunque fornire prove definitive su accuratezza e affidabilità. Per mitigare, spostiamo l'attenzione sulle condizioni di validità delle decisioni – provenienza dei dati, versionamento, auditing, criteri di fusione – e sulle interfacce che traducono calcolo in azione. Resta comunque un margine di indeterminazione non eliminabile con le fonti disponibili. Il secondo limite è la generalizzabilità: Ucraina e Gaza sono casi-limite, utili perché rendono visibili i meccanismi, ma non automaticamente estendibili a ogni contesto. Le culture strategiche, i regimi giuridici e le infrastrutture disponibili cambiano molto e con esse i modi in cui l'AI entra nelle procedure. Il terzo limite è il rischio di "ri-performare l'eccezione": raccontare l'urgenza può, se non sorvegliato, normalizzare ulteriormente la compressione dei tempi decisionali; denunciare la de-umanizzazione digitale può, se non articolato, appiattire la varietà d'usi della stessa tecnologia in contesti civili o forensi. Per ridurre questo rischio, il testo usa in modo intrecciato tre lenti –

securitizzazione, neofunzionalismo e costruttivismo – proprio per mantenere viva la tensione tra ciò che accelera, ciò che integra e ciò che ridefinisce i significati.

Anche la temporalità conta: l'analisi fotografa processi in corso, su finestre che vanno dall'ottobre 2023 all'aprile 2025 per Gaza e dal 2022 al 2025 per l'Ucraina. Le traiettorie tecnologiche e regolatorie sono mobili: ciò che oggi è supporto cognitivo potrebbe virare, domani, verso maggiore autonomia; ciò che oggi è targeting potrebbe subire restrizioni o essere incanalato in funzioni diverse, come la forensics investigativa. Per questo è utile trattare le conclusioni come ipotesi forti ma rivedibili, più che come verdetti. La qualità di un lavoro esplorativo si misura nella capacità di indicare dove andrebbero cercate le prove "dure" quando l'accesso sarà possibile: in che punti della catena si definiscono le soglie, quali audit indipendenti sarebbero sensati, quali garanzie probatorie servono per conciliare segreto industriale e responsabilità in caso di violazioni gravi. In Ucraina ciò significherebbe, per esempio, rendere più visibili i criteri con cui l'orchestratore pesa le fonti e decide le priorità; a Gaza significherebbe rendere tracciabili i dataset, le features e le versioni dei modelli che alimentano le liste e le raccomandazioni. Tenendo insieme questi fili, il confronto tra MetaConstellation e i sistemi di targeting israeliani non fornisce una tesi unica e chiusa, ma propone una cornice per leggere la guerra algoritmica senza farsi dettare le categorie dall'interfaccia. L'idea centrale è semplice: non esiste "l'AI" in astratto; esistono collocazioni istituzionali, soglie operative, regimi di responsabilità, semantiche che definiscono chi conta come civile o come combattente e chi è autorizzato a dire che cosa. La stessa tecnologia, incastonata in procedure diverse, può spingere nella direzione di un coordinamento più trasparente e verificabile, oppure nella direzione di una selezione opaca e industrializzata di bersagli. Se l'urgenza non è controllata da regole pubbliche chiare, tende a trasformarsi da argomento politico a automatismo tecnico. Ecco perché il punto non è scegliere tra ottimismo e pessimismo sulla tecnologia, ma chiarire dove mettiamo i freni, chi tiene i registri, come si rende discutibile ciò che oggi, troppo spesso, arriva già confezionato come "necessario".

CONCLUSIONE



Harun Farocki, Eye Machine III, © Harun Farocki, 2003.

Questo lavoro ha mostrato che la cosiddetta "guerra algoritmica" non coincide con un semplice aggiornamento tecnologico degli arsenali, ma implica una mutazione congiunta delle temporalità operative, delle infrastrutture istituzionali e delle categorie politiche e giuridiche con cui l'uso della forza viene legittimato. Nei due casi studio – l'ecosistema di orchestrazione dati di Palantir in Ucraina e la costellazione di sistemi di supporto al targeting impiegati da Israele a Gaza (Lavender, Gospel/Habsora, Where's Daddy?) – si osservano traiettorie diverse e tuttavia convergenti: da un lato la compressione del ciclo informativo-decisionale in funzione di "vantaggio decisionale", dall'altro la trasformazione del giudizio selettivo in un processo standardizzato e semi-automatizzato, in cui l'intervento umano rischia di ridursi a ratifica procedurale. La tesi ha seguito queste traiettorie con tre lenti teoriche – securitizzazione, neofunzionalismo, costruttivismo – per rendere visibile ciò che spesso resta nascosto dietro la retorica dell'efficienza e della precisione: che cosa diventa attaccabile, chi resta responsabile, come si costruisce discorsivamente l'urgenza che consente di sospendere garanzie e cautele. Il confronto comparato chiarisce innanzitutto la posizione funzionale occupata dall'automazione nei due teatri. In Ucraina, MetaConstellation agisce come infrastruttura di integrazione: fonde in una stessa interfaccia flussi eterogenei – telerilevamento ottico, radar SAR, tracciamenti commerciali (AIS/ADS-B), dati governativi – allo scopo di ridurre il sensor-to-shooter cycle e sincronizzare osservazione, orientamento, decisione, azione. L'automazione opera prevalentemente a livello cognitivo e organizzativo, accelerando la costruzione di un quadro situazionale coerente che resta, in linea di principio, subordinato a un ultimo vaglio umano. A Gaza, invece, l'automazione si insinua nel cuore della selezione: sistemi come Gospel/Habsora raccomandano "power targets" infrastrutturali, mentre Lavender attribuisce punteggi di affiliazione a individui sospettati e produce liste di possibili bersagli umani; Where's Daddy? ne traccia i movimenti per colpirli in ambito domestico, quando l'azione è più prevedibile anche al costo di un impatto civile più elevato. Non è soltanto un diverso uso dell'AI: è una mutazione della funzione della macchina dentro la catena di comando, che da ausilio cognitivo diventa motore selettivo.

Questa differenza funzionale si intreccia con una differenza di scala e di ritmo. Le inchieste giornalistiche e i report citati nella tesi hanno descritto un'accelerazione estrema della produzione di obiettivi a Gaza: decine di migliaia di nominativi in poche settimane, con procedure di validazione dell'ordine di pochi secondi per target e controlli di minima come la sola conferma del sesso maschile per figure di basso rango. In parallelo, sarebbero state adottate soglie predeterminate di "danno collaterale tollerato" – fino a 15–20 vittime civili per obiettivi minori, fino a 100 per figure apicali – e, per ragioni di costo, sarebbero state impiegate anche bombe a

caduta libera, meno precise in contesti urbani densissimi. L'insieme produce un triplice scarto rispetto al diritto internazionale umanitario: si incrina la distinzione tra civili e combattenti, si attenuano le precauzioni ex ante, si standardizza la proporzionalità trasformandola da giudizio contestuale a calcolo industrializzato. Le repliche ufficiali dell'IDF respingono la ricostruzione di una "kill-list automatica" e insistono sulla centralità umana nella valutazione finale; resta tuttavia l'evidenza, ricostruita nelle fonti, di un sistema operativo che tende a normalizzare la velocità come valore in sé, comprimendo i tempi della riflessione e della verifica. La lente della securitizzazione aiuta a comprendere perché questo scarto si presenti come inevitabile. A monte della macchina c'è un atto linguistico che costruisce la minaccia come esistenziale e la velocità come condizione di sopravvivenza. Nel caso ucraino, "decision advantage" ed "edge informazionale" diventano parole d'ordine che riorientano priorità, alleanze e procurement, rendendo accettabile l'apertura dei rubinetti dei dati commerciali e l'intreccio profondo con vendor privati, presentati come "alleati" della sicurezza nazionale. A Gaza, dopo il 7 ottobre, la narrativa dell'eccezione trasforma la popolazione in un indistinto orizzonte di sospetto e rende presentabili pratiche che in condizioni ordinarie apparirebbero giuridicamente e moralmente insostenibili. Securitizzare non significa solo chiedere poteri speciali; significa anche scolpire audience che accettino come "naturale" una rapidità che, di fatto, consuma le condizioni del controllo umano significativo. In questo senso, la velocità non è un dato tecnico: è un effetto discorsivo che autorizza la compressione dei tempi del diritto dentro i tempi della macchina.

Con il neofunzionalismo, si vede come questa accelerazione richieda e produca integrazione: per funzionare davvero, l'analisi rapida pretende standard condivisi, formati interoperabili, catene di custody dei dati, clausole contrattuali che vincolano pubblico e privato ben oltre l'emergenza. È la logica dello spill-over: tecnologie e infrastrutture nate in domini civili o amministrativi migrano stabilmente nella sfera bellica e, una volta incorporate, generano lock-in tecnici e istituzionali che rendono arduo tornare indietro. Project Nimbus – l'accordo cloud con provider globali per servizi a ministeri e apparato di sicurezza israeliani – è emblematico di questa torsione: la promessa di efficienza e sovranità dei dati si traduce in una presenza strutturale dell'industria digitale dentro la macchina della guerra, con l'effetto di normalizzare il dual use e di redistribuire potere verso chi controlla piattaforme, metriche e pipeline. Analogamente, l'adozione di piattaforme commerciali nel teatro ucraino esemplifica il modo in cui una necessità operativa, presentata come temporanea, precipita in un'infrastruttura di lungo periodo che ridefinisce ruoli, responsabilità e dipendenze. La chiave costruttivista consente infine di vedere la trasformazione più sottile, ma forse più radicale: la ridefinizione semantica delle identità coinvolte. Lavender non "scopre" terroristi;

produce categorie probabilistiche che recodificano comportamenti ordinari – cambiare SIM, frequentare certi gruppi WhatsApp, prossimità sociale – in segnali di affiliazione militante. Nei termini analitici ripresi dalla tesi, tecniche come il positive-unlabeled learning e l'uso di indicatori proxy instaurano una presunzione inversa rispetto al DIU: non più civili salvo prova contraria, ma sospetti fino a smentita, in un contesto in cui la smentita è materialmente improbabile. È qui che l'AI non automatizza (soltanto) armi; automatizza categorie: "junior militants", "power targets", "confidence score" smettono di essere etichette descrittive e diventano dispositivi performativi che organizzano la violenza. La digital dehumanization di cui parlano le ONG citate nella tesi non è un effetto collaterale estetico del linguaggio tecnico; è il dispositivo simbolico che rende governabile l'eccezione, trasformando persone in punteggi e responsabilità in correlazioni.

Questa tripla lettura – urgenza che comprime, integrazione che vincola, semantiche che ridefiniscono – riconduce l'intero problema alla questione del controllo. Il lessico dominante parla di *meaningful human control*, come se bastasse garantire un "clic umano" alla fine della catena per salvare il nucleo etico-giuridico del diritto di guerra. I casi esaminati mostrano il contrario: il controllo è significativo se è istituzionale e ciclico, non se è puntuale e terminale. Controllo istituzionale significa che ciò che conta non è l'ultimo gesto, ma l'intera architettura che rende possibile l'ultimo gesto: provenienza e qualità dei dati; criteri di feature engineering e di addestramento; soglie operative, modalità di audit, versionamento dei modelli; possibilità effettive di *override* quando il drift dei dati o l'emergere di bias erodono l'affidabilità. Senza questi presìdi, il clic è un feticcio, e l'umano non decide, timbra. E qui torna, non come reliquia retorica ma come bussola normativa, la clausola di Martens: anche quando il diritto positivo non anticipa il dettaglio tecnico, valgono i principi di umanità e i dettami della coscienza pubblica. La loro traduzione, nell'era degli AIDSS, non è un appello astratto alla prudenza; è la richiesta concreta che la pipeline che produce la violenza sia auditable, tracciabile, contestabile. L'analisi svolta su Gaza rende questo punto persino più netto. Se l'urgenza securitizzante trasforma la proporzionalità in algoritmica delle soglie e se l'integrazione infrastrutturale contamina senza soluzione di continuità sorveglianza civile e targeting letale, allora la difesa dello spazio di giudizio umano non può consistere nell'inserire una firma nel flusso; deve consistere nel ridisegnare il flusso. Questo comporta, sul piano giuridico, spostare la presunzione valida in guerra dal "probabile combattente" al "civile fino a prova contraria" quando la prova è fornita da correlazioni opache; e, sul piano organizzativo, significa rendere obbligatoria la ricostruibilità ex post delle condizioni in cui un modello ha "consigliato" l'ingaggio: quale versione, con quali pesi, con quali soglie, su quali dati, sotto quale supervisione legale. L'opacità proprietaria non può più fungere da barriera assoluta

contro l'indagine su violazioni gravi: il segreto industriale va contemperato con un regime di discovery probatoria e con audit indipendenti protetti da garanzie legali. Solo così i principi di distinzione, precauzione e proporzionalità – che il caso Gaza mostra messi a dura prova tra soglie pre-autorizzate e uso di munizionamento meno preciso – possono riprendere spessore operativo in un ambiente di alta automazione.

La traiettoria ucraina, dal canto suo, segnala una diversa forma di rischio: quello della dipendenza strategica da attori privati che diventano, di fatto, co-proprietari dell'infrastruttura bellica. La narrativa del "game-changer" tecnologico tende a confondere mezzi e fini, attribuendo alla piattaforma una funzione quasi salvifica. La lente costruttivista ha mostrato come questa investitura simbolica ridefinisca identità e ruoli – l'impresa privata come "alleato", l'infrastruttura commerciale come "sovranità informativa" – con conseguenze materiali sulla governance della guerra e del dopoguerra. La velocità e l'interoperabilità sono beni preziosi in conflitto ad alta intensità, ma, se non incanalate in un disegno istituzionale che preservi prerogative pubbliche, rischiano di cristallizzare lock-in tecnologici difficili da sciogliere, con spostamenti di potere che eccedono il campo strettamente militare. Come ogni indagine esplorativa, anche questa tesi ha incontrato limiti che sono, in parte, il rovescio della medaglia della scelta di campo: ricostruire filiere informative, atti discorsivi e assetti organizzativi, senza poter aprire realmente la "scatola nera" dei modelli proprietari. Le controversie sul grado di autonomia dei sistemi, sull'accuratezza degli output, sul ruolo residuo dell'umano sono state riportate come materiali di analisi più che come questioni da risolvere. E tuttavia proprio questa postura ha consentito di leggere i dissensi non come rumore, ma come sintomi: le divergenze tra inchieste, ONG e repliche ufficiali dicono che la posta in gioco non è soltanto tecnica; è semantica, politica, istituzionale. L'assenza di una misura unica di "verità" sugli algoritmi impiegati non annulla l'urgenza di fissare condizioni minime di verificabilità e di responsabilità. È qui che il diritto internazionale umanitario e le scienze politiche, con i loro strumenti distinti, possono convergere: non per inseguire la promessa impossibile della trasparenza totale, ma per imporre, anche alla macchina, il tempo minimo della prova e il luogo materiale della responsabilità.

Se dovessimo condensare, a conclusione, ciò che emerge con maggiore forza, potremmo dirlo così: l'AI militarizzata non autonomizza soltanto i mezzi, autonomizza le soglie. Soglie di attenzione, perché il flusso incessante di segnali spinge a fidarsi della macchina più che dell'umano; soglie di responsabilità, perché la decisione si dissolve in raccomandazioni probabilistiche distribuite lungo la pipeline; soglie di legittimità, perché categorie giuridiche storicamente "spesse" – civile/combattente, proporzionalità/necessità – sono consumate da metriche addestrate su dati

opachi. La risposta non è una ritirata antitecnologica; è un avanzamento istituzionale: riportare nel cuore della macchina il tempo della legge e la forma della prova, ricostruendo il controllo umano come controllo del ciclo e non del clic. In Ucraina questo significa governare l'infrastruttura, prevenendo la deriva della dipendenza privata; a Gaza significa ripristinare la presunzione protettiva del DIU contro l'algoritmica della soglia fissa e dell'eccezione normalizzata. Solo così la promessa di "efficienza" cessa di essere un eufemismo di deresponsabilizzazione e torna ad essere compatibile con la dignità delle persone su cui, in ultima istanza, la guerra algoritmica opera. In definitiva, i due casi studio, letti attraverso securitizzazione, neofunzionalismo e costruttivismo, mostrano che la partita non si gioca soltanto sui campi di battaglia o nei data center, ma nel modo in cui società e istituzioni decidono di significare la tecnologia, di integrarla nelle proprie architetture, di renderla responsabile. La sfida che si apre dopo questa tesi è duplice e simultanea: guardare dentro i sistemi per capire come producono "verità operative" e guardare oltre i sistemi per ribadire che ciò che è computabile non coincide con ciò che è lecito. Se questa consapevolezza verrà tradotta in procedure, regole e culture organizzative – e non solo in dichiarazioni di principio – allora l'innovazione potrà nutrire la sicurezza senza erodere il diritto; altrimenti, resterà un accelerante che consuma, nel medesimo gesto, il giudizio e la giustizia.

BIBLIOGRAFIA

Abraham, Yuval, “Lavender: The AI Machine Directing Israel’s Bombing Spree in Gaza,” +972 Magazine and Local Call, April 2024.

Abraham, Yuval, “The System Known as ‘Where’s Daddy?’ and the Targeting of Homes in Gaza,” +972 Magazine, April 2024.

Gordon Anna et al., “How Israel Uses AI in Gaza – And What It Might Mean for the Future of Warfare,” TIME, 18 dicembre 2024.

Amnesty International, *Automated Apartheid: How Israel’s Digital Surveillance of Palestinians Entrenches Oppression* (London: Amnesty International, 2023).

Amoore, Louise, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others* (Durham, NC: Duke University Press, 2020).

Amoore, Louise, Marijn Hoijtink e Daniel Lambach, “Innovating Algorithmic Warfare: Experimentation with Information Manoeuvre beyond the Boundaries of the Law,” Global Policy 15, *no. S1* (2024): 28–40.

Amoore, Louise, *The Politics of Possibility: Risk and Security Beyond Probability* (Durham: Duke University Press, 2013).

Amoore, Louise, “Algorithmic War: Everyday Geographies of the War on Terror,” Antipode 41, no. 1 (2009): 49–69.

Apprich, Clemens, Wendy Hui Kyong Chun, Florian Cramer, and Hito Steyerl, *Pattern Discrimination* (Lüneburg: meson press, 2018).

Azoulay, Ariella, *The Civil Contract of Photography* (New York: Zone Books, 2008).

Balzacq, Thierry, ed., *Securitization Theory: How Security Problems Emerge and Dissolve* (London: Routledge, 2011).

Bergengruen, Vera, “How Tech Giants Turned Ukraine Into an AI War Lab,” TIME, 8 febbraio 2024.

Bigo, Didier, “Security and Immigration: Toward a Critique of the Governmentality of Unease,” *Alternatives: Global, Local, Political* 27, no. 1 (2002): 63–65.

Bo, Jessica Dorsey e Marta, “AI-Enabled Decision-Support Systems in the Joint Targeting Cycle: Legal Challenges, Risks, and the Human(e) Dimension,” *International Law Studies* 106 (2025), preprint SSRN (27 giugno 2025).

Boghairy, Mohammad Nazer Shahir and Ali, *Constructivist Analysis of Russia’s Military Invasion of Ukraine* (2022).

Bondar, Kateryna, “Does Ukraine Already Have Functional CJADC2 Technology?,” *Center for Strategic and International Studies*, 11 dicembre 2024.

Bossong, Annegret Bendiek and Raphael, “The EU’s Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges,*” SWP Comment 47* (Berlin: Stiftung Wissenschaft und Politik, November 2017*).*

Boyd, John, *A Discourse on Winning and Losing* (Maxwell Air Force Base, AL: Air University, 1987).

Buzan, Barry, Ole Wæver e Jaap de Wilde, Sicurezza. *Una nuova struttura per l’analisi* (Roma: Luiss University Press, 2017).

Caldwell, Timothy Lenoir and Luke, “The Military-Entertainment Complex,” in Image Operations: Visual Media and Political Conflict, ed. Jens Eder and Charlotte Klonk (Manchester: Manchester University Press, 2017).

Chafkin, Max, “Palantir’s Karp Is First Western CEO to Visit Zelenskyy in Kyiv,” Bloomberg, *June 2022.*

Chamayou, Grégoire, *Teoria del drone*. *Principi filosofici del diritto di uccidere*. Trad. it. di Caterina Zanfi (Roma: DeriveApprodi, 2013).

Chouliaraki, Lilie, *The Ironic Spectator: Solidarity in the Age of Post-Humanitarianism* (Cambridge: Polity Press, 2013), 54–59.

Christensen, Christian, “Disciplining the Viewer: YouTube, Real-Time Evidence and the ‘War on Terror’,” in *Image Operations: Visual Media and Political Conflict*, ed. Jens Eder and Charlotte Klonk (Manchester: Manchester University Press, 2017), 201–217.

Clausewitz, Carl von, *Della guerra*, trad. it. di Piero Martinetti (Milano: Rizzoli, 2006).

Criddle, Cristina, “NATO Acquires AI Military System from Palantir,*”* Financial Times (aprile 2025).

Cristiano, Fabio, Emilio Iasiello, and Massimiliano Signoretti, eds. *Artificial Intelligence and Cybersecurity: Emerging Challenges and Opportunities* (Leiden: Brill, 2023).

Cristiano, Fabio, Emilio Iasiello, and Massimiliano Signoretti, eds. *Artificial Intelligence and Cybersecurity: Emerging Challenges and Opportunities* (Leiden: Brill, 2023). *Cybersecurity and Infrastructure Security Agency* (CISA), "United States and Ukraine Expand Cooperation on Cybersecurity," *CISA Press Release*, 27 luglio 2022.

Dastin, Jeffrey, "Ukraine Is Using Palantir's Software for 'Targeting,' CEO Says," Reuters, February 1, 2023.

Davies, Bethan McKernan e Harry, "'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets," The Guardian.

Stato Maggiore della Difesa, *La trasformazione net-centrica: Il futuro dell'interoperabilità multinazionale e interdisciplinare* (Roma: Stato Maggiore della Difesa, 2006).

Dorsey, Marta Bo e Jessica, "The 'Need' for Speed – The Cost of Unregulated AI Decision-Support Systems to Civilians," Opinio Juris, 4 aprile 2024.

Eder, Jens, "Affective Image Operations," in Image Operations: Visual Media and Political Conflict, ed. Jens Eder and Charlotte Klonk (Manchester: Manchester University Press, 2017), 89–107.

European Defence Agency, *Trustworthiness for AI in Defence* (White Paper), 9 maggio 2025.

Evron, Yoram, "China's Military-Civil Fusion: Origins, Drivers and Implications," Journal of Strategic Studies 43, *no. 3* (2020): 400–420.

Richard A. Bitzinger, "Civil–Military Integration and Chinese Military Modernization," Asian Security 15, no. 1 (2019): 45–61.

Farocki, Harun, "Cross Influence/Soft Montage," in Harun Farocki. Against What? Against Whom? *eds. Antje Ehmann and Kodwo Eshun* (London: Koenig Books, 2009), 285–289.

Farocki, Harun, "Operative Images," in Harun Farocki. Working on the Sightlines, *ed. Thomas Elsaesser* (Amsterdam: Amsterdam University Press, 2004), 17–21.

Farocki, Harun, "Phantom Images,*" Public 29* (2004).

Floyd, Rita, *The Morality of Security: A Theory of Just Securitization* (Cambridge: Cambridge University Press, 2019), e anche Mitja Sardoc, "The Ethics of Securitisation: An Interview with Rita Floyd," Critical Studies on Terrorism 14, *no. 1* (2021): 139–148.

Flusser, Vilém, *Into the Universe of Technical Images* (Minneapolis: University of Minnesota Press, 2011).

Flusser, Vilém, *Per una filosofia della fotografia*, (Torino: Bruno Mondadori, 2006).

GAIA-X Association, *"GAIA-X Strengthens European Digital Sovereignty at European Parliament Reception"* (21 marzo 2025).

Ginevra, Protocollo Addizionale I alle Convenzioni di, art. 1(2).

Ginevra, Protocollo Addizionale I alle Convenzioni di, art. 57.

International Committee of the Red Cross (ICRC), Customary International Humanitarian Law, Regola 14.

Ginevra, Protocollo Addizionale I alle Convenzioni di, artt. 48 e 57;

International Committee of the Red Cross, Customary International Humanitarian Law, Regole 7 e 15.

Ginsburg, Eyal Weizman and Ruthie, "Israel's AI Program, Lavender, Is Automating the Killing in Gaza," The Philadelphia Inquirer, *April 7*, 2024.

Gregory, Sam, "Cameras Everywhere: Ubiquitous Video Documentation of Human Rights, New Forms of Video Activism, and Human Rights 'Seeing,'" Journal of Human Rights Practice 2, *no. 2* (2010): 191–207.

Grylls, George, "Ukraine's Secret Weapon: The £40bn Tech Firm That Found Bin Laden," The Times, 2023.

Grylls, George, Palantir. Ukraine's Technological Edge. Reprint da The Times, 24 dicembre 2022.

Haas, Ernst B., *L'unificazione dell'Europa*. Forze politiche, sociali ed economiche, 1950-1957 (Bologna: Il Mulino, 1970).

Haas, Peter M., "Epistemic Communities and International Policy Coordination," International Organization 46, no. 1 (1992): 1–35.

Harel, Amos, “A Failure of All Systems, With Political Shock Waves Like ’73,” Haaretz, 8 ottobre 2023.

Harel, Amos, “Gospel and Lavender: Israel’s AI Targeting Systems in Gaza,” Haaretz, December 2023.

Holert, Tom, “Aerial Perspectives: The Drone Gaze,” in *Image Operations: Visual Media and Political Conflict*, ed. Jens Eder and Charlotte Klonk (Manchester: Manchester University Press, 2017), 151–165.

Human Rights Watch, “Questions and Answers on the Israeli Military’s Use of Digital Tools in Gaza,” 10 settembre 2024.

Human Rights Watch, “Gaza: Israeli Military’s Digital Tools Risk Civilian Harm,” 10 settembre 2024.

Hunder, Max, “Ukraine Sees ‘Priceless’ Digital Battlefield Data Trove as Key to West’s Support,” Reuters, 27 agosto 2025.

Huysmans, Jef, The Politics of Insecurity: Fear, *Migration and Asylum in the EU* (London: Routledge, 2006).

I, Protocollo Addizionale, art. 51(4)(b)(c).

I, Protocollo Addizionale, art. 57.

International Committee of the Red Cross (ICRC), Customary International Humanitarian Law, Regola 7.

ICRC, Customary International Humanitarian Law, Regola 14.

ICRC, “Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach,” 2021 (n.1).

Ignatius, David, “How the Algorithm Tipped the Balance in Ukraine,” The Washington Post, December 19, 2022.

International Committee of the Red Cross, “Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach,” International Review of the Red Cross 102, no. 913 (2021).

International Committee of the Red Cross, “Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach,” International Review of the Red Cross 103, no. 916–917 (2021).

International Institute for Strategic, *Software-Defined Defence* (London: IISS, 2023), 25.

Internazionale, Statuto di Roma della Corte Penale, art. 30, 17 luglio 1998.

Irrgang, Diedrich, “Projective Imagination: Vilém Flusser’s Concept of the Technical Image,” Theory, *Culture & Society 40*, no. 7–8 (2023).

Irvine, Martin, “Po-Mo SF: William Gibson’s Neuromancer and Post-Modern Science Fiction,”

Technoculture, Georgetown University, rev. 12 gennaio 1997, archiviato su Internet Archive Wayback Machine (19 ottobre 2006), consultato il 26 agosto 2025.

Jaura, Ramesh, Software on the Front Line: How Palantir Is Aiding Ukraine in Its War With Russia,” Eurasia Review, 6 settembre 2025.

Jensen, Eric, Christopher Whyte, and Carla Anne Robbins Cuomo, “Learning, Sensing, Moving: AI on the Battlefield,*”* in *Software-Defined Defence: Algorithms at War* (London: IISS, *2023).*

Jones, John Hewitt, “Palantir to Help Ukraine Process Data in War Crimes Investigations,” FedScoop, *25 aprile 2023* e vedi anche International Criminal Court, Situation in Ukraine, accessed august 2025.

Judson, Colin Demarest e Jen, “Palantir’s Karp Is First Western CEO to Visit Zelenskyy Amid Invasion,” Defense News, *2 giugno 2022.*

Jünger, Ernst, *La mobilitazione totale, in Saggi di politica e di letteratura*, trad. it. di Julius Evola (Roma: Edizioni di Ar, 1990).

Kierszenbaum, Bethan McKernan and Quique, “Israel Uses AI System to Generate Targets in Gaza Airstrikes,” The Guardian, 3 aprile 2024.

Klonk, Jens Eder and Charlotte, eds., *Image Operations: Visual Media and Political Conflict* (Manchester: Manchester University Press, 2017).

Klonowska, Klaudia, “AI-Based Targeting in Gaza: Surveying Expert Responses, Refining Debate,*” Articles of War* (Lieber Institute, *West Point)*, 7 giugno 2024.

Konaev, Margarita, “Tomorrow’s Technology in Today’s War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability,” CNA Analysis, 2 ottobre 2023.

Kumbaracibasi, Arda Can, “Understanding Israel’s Foreign Policy from the Perspective of Identity and Security,” Insight Turkey 24, no. 1 (2022).

Kydd, Andrew, *Trust and Mistrust in International Relations* (Princeton: Princeton University Press, 2005).

Lamport, Leslie, Robert Shostak, and Marshall Pease, “The Byzantine Generals Problem,” ACM Transactions on Programming Languages and Systems 4, no. 3 (1982).

Lappin, Yaakov, “How Israel’s AI Targeting System Changed Warfare in Gaza,” Jerusalem Post, July 7, 2024.

Lindsay, Avi Goldfarb and Jon R., “Prediction and Judgment in Military Applications of Artificial Intelligence,*”* in *Software-Defined Defence: Algorithms at War* (London: IISS, *2023)*, 12–15.

Longobardo, Federico, Il principio di precauzione nel diritto dei conflitti armati (Napoli: Editoriale Scientifica, 2020).

Loughlin, Ben O, Andrew Hoskins, and Akil Awan, *War and Media: The Emergence of Diffused War* (Cambridge: Polity Press, 2010).

Loughlin, Ben O, “Images as Weapons of War: Representation, Mediation, and Interpretation,” Review of International Studies 44, no. 3 (2018): 414–416.

Maçaes, Bruno, TIME, “How Palantir Is Shaping the Future of Warfare,” July 4, 2023.

Martens, Clausola, Protocollo I aggiuntivo alle Convenzioni di Ginevra, art. 1(2).

Martino, Luigi, “La quinta dimensione della conflittualità. L’ascesa del cyberspazio e i suoi effetti sulla politica internazionale,” Politica & Società 7, n. 1 (gennaio–aprile 2018): 61–76.

Maupas, Stéphanie, “À Gaza, l’armée israélienne utilise un logiciel d’intelligence artificielle pour désigner des cibles,” Le Monde, 5 April 2024.

Mazarr, Michael J., *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: U.S. Army War College Press, 2015).

McLuhan, Marshall, *Gli strumenti del comunicare* (Milano: Il Saggiatore, 1967).

Michel, Arthur Holland, "The Accountability Surface of Militaries Using Automated Technologies," *Centre for International Governance Innovation* (CIGI), 14 giugno 2021.

Ministry of Economy of Ukraine, "Automation of Demining Processes and the Use of AI: The Ministry of Economy Signs a Partnership Agreement with Palantir," Government Portal of Ukraine, 3 aprile 2023.

Mirzoeff, Nicholas, *How to See the World* (London: Pelican, 2015).

Morris, Shira Rubin and Loveday, "Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank," The Washington Post, 5 novembre 2021.

Mysyshyn, Anna, "Advanced Technologies in the War in Ukraine: Risks for Democracy and Human Rights," German Marshall Fund of the United States, 30 settembre 2024.

Nashif, Neta Alexander and Nadim, "Project Nimbus: Cloud Computing, Digital Occupation and Resistance," Journal of Palestine Studies 52, no. 4 (2023): 7–20.

National Institute of Standards and Technology (NIST), Zero Trust Architecture, Special Publication 800-207 (Gaithersburg, MD: U.S. Department of Commerce, 2020).

NATO Supreme Headquarters Allied Powers Europe, "NATO Acquires AI-Enabled Warfighting System (MSS NATO)," press release (14 aprile 2025).

Aradau, Claudia, "Security and the Democratic Scene: Desecuritization and Emancipation," Journal of International Relations and Development 7, no. 4 (2004): 393–94.

Nye, Joseph S., *The Future of Power* (New York: PublicAffairs, 2011).

Paglen, Trevor, *Invisible: Covert Operations and Classified Landscapes* (New York: Aperture, 2010).

Paglen, Trevor, *"Invisible Images* (Your Pictures Are Looking at You)," The New Inquiry, *December 8*, 2016.

Palantir Technologies, Foundry for Resilience Planning (London: Palantir Technologies UK).

Palantir Technologies, *Response to the Office of Science and Technology Policy: National Priorities on AI* (Washington, DC: Executive Office of the President, 2023).

Palantir Technologies, "AI Systems Governance through the Palantir Platform," *Palantir Blog* (20 dicembre 2024)

Palantir Technologies, “AI Systems Governance through the Palantir Platform,” Palantir Blog, December 20, 2024.

Palantir Technologies, “Data Lifecycles: Protecting Data with Privacy First Principles,” Palantir Blog, June 16, 2023.

Palantir Technologies, “MetaConstellation: Artificial Intelligence for Real-Time Space Operations,*”* Palantir (2022).

Palantir Technologies, “Palantir to Support Ukrainian Prosecutor General’s Investigation into War Crimes,” comunicato stampa, 22 aprile 2023.

Palantir Technologies, “Palantir to Support Ukrainian Prosecutor General’s Office in Investigating War Crimes,” BusinessWire, 24 aprile 2023.

Palantir Technologies, “Palantir’s Recommendations to the White House OSTP on Developing an AI Action Plan,” Palantir Blog, March 17, 2025.

Palantir Technologies, “Palantir’s Response to OMB on AI Governance, Innovation, and Risk Management,” Palantir Blog, December 14, 2023.

Palantir Technologies, “Security Auditing • Audit Logging Overview,*”* Foundry Docs (13 marzo 2023).

Palantir Technologies. Palantir Technologies Official Website. Accessed August 26, 2025.

Pantenburg, Volker, “Working Images: Harun Farocki and the Operational Image,” in Image Operations: Visual Media and Political Conflict, ed. Jens Eder and Charlotte Klonk (Manchester: Manchester University Press, 2017), 49–65.

Pasquale, Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

Payne, Kareem Ayoub and Kenneth, “Strategy in the Age of Artificial Intelligence,*” in Software-Defined Defence: Algorithms at War* (London: IISS, *2023)*, 26–28.

Perrigo, Billy, “How Palantir Is Shaping the Future of Warfare,” TIME, 10 luglio 2023.

President of Ukraine, “President of Ukraine and Palantir CEO Discussed Cooperation in the Defense and Security Sector,” Office of the President of Ukraine, 2 giugno 2022.

Price, Brian R., “Decision Advantage and Initiative: Completing Joint All-Domain Command and Control,” Air & Space Operations Review 3, no. 1 (2024).

Probasco, Emelia S., Helen Toner, Matthew Burtell, e Tim G. J. Rudner, *AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks* (Washington, DC: Center for Security and Emerging Technology, aprile 2025).

Protocollo Addizionale alle *Convenzioni di Ginevra del 12 agosto 1949 relativo alla protezione delle vittime dei conflitti armati internazionali* (Protocollo I), 8 giugno 1977, artt. 35–36, 48 e 51.

Rahman, Amber, "Explainer: The Role of AI in Israel's Genocidal Campaign Against Palestinians,*" Institute for Palestine Studies*, October 16, 2024.

Rancière, Jacques, *La partizione del sensibile. Estetica e politica* (Roma: DeriveApprodi, 2007).

Reuters, "AI, Ukraine War Shows Urgency of Military, Palantir CEO Says", February 15, 2023.

Reuters, "Data company Palantir to help Ukraine prosecute alleged Russian war crimes," 22 aprile 2023.

Robel, Md. Rabioul Aual, "US–Israel Relation: How Constructivism Works," International Journal of Social Science and Humanity 5, no. 7 (2015): 651–657.

RUSI, Royal United Services Institute, "Israel's Targeting AI: How Capable Is It?," RUSI Commentary, 8 febbraio 2024.

S. Department of Defense, Summary of the JADC2 Strategy; U.S. Government Accountability Office, DOD and Air Force Continue to Define Joint Command and Control (Washington, DC: GAO, 2023).

Shahir, Mohammad Nazer, and Ali Boghairy. *"Constructivist Analysis of Russia's Military Invasion of Ukraine* (2022); Investigating Putin's Identity Model and Cognitive Actions." Journal of World Sociopolitical Studies 8, *no. 4* (Autumn 2024): 846–850.

Sikkink, Martha Finnemore and Kathryn, "International Norm Dynamics and Political Change," International Organization 52, *no. 4* (1998): 887–917.

SIPRI, *Mapping the Development of Autonomy in Weapon Systems* (Stockholm: SIPRI, 2017).

Soare, Simona R., *Software-Defined Defence: Algorithms at War* (London: IISS, 2023).

Steyerl, Hito, *Duty-Free Art: Art in the Age of Planetary Civil War* (London: Verso, 2017), 145–150.

Steyerl, Hito, "In Defense of the Poor Image,*" e-flux journal 10* (2009).

Sweet, Wayne Sandholtz and Alec Stone, *European Integration and Supranational Governance* (Oxford: Oxford University Press, 1998).

Taqiya, Farah Muna Safa, "Can Constructivism Hold Israel Accountable?," Modern Diplomacy, *January 2024.*

Tawil-Souri, Helga, "Digital Occupation: Gaza's High-Tech Enclosure," Journal of Palestine Studies 41, *no. 2* (2012): 27–43.

Tharoor, Ishaan, "How the Algorithm Tipped the Balance in Ukraine," The Washington Post*, 19 dicembre 2022.*

The Guardian, "We are Google and Amazon workers. We condemn Project Nimbus," 12 ottobre 2021.

Verge, The, "Internal Google documents reveal concerns about its cloud contract with Israel," 3 dicembre 2024.

Tripodi, Francesco Simonetti e Laura, "Automation and the Future of Command and Control," Journal of Advanced Military Studies 11, no. 1 (Spring 2020): 145–164.

U.S. Congress, S.*5239 - Artificial Intelligence Weapons Accountability and Risk Evaluation* (AWARE) Act of 2024.

U.S. Department of Defense, *Summary of the Joint All-Domain Command and Control Strategy* (Washington, DC: Department of Defense, 2022).

U.S. Department of State, U.S. Security Cooperation with Ukraine, Bureau of Political-Military Affairs, aggiornato 2023.

United Nations, International Covenant on Civil and Political Rights, adottato dall'Assemblea Generale delle Nazioni Unite il 16 dicembre 1966.

United Nations, Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories, 20 settembre 2024.

United Nations Human Rights Office of the High Commissioner, "UN Expert Warns of New Instance of Mass Ethnic Cleansing of Palestinians, Calls for Immediate Ceasefire," Press Release, 14 ottobre 2023.

Vincent, Brandi, "Army Plans Big Shake-Up in Software Buying Practices with Palantir Deal,*"* *DefenseScoop* (31 luglio 2025).

Virilio, Paul, Guerra e cinema. Logistica della percezione, trad. it. *di Fabio Tarzia* (Milano: Raffaello Cortina, 1984).

Virilio, Paul, Velocità e politica. Saggio di dromologia, trad. it. *di Giancarlo Pavanello* (Milano: SugarCo, 1981).

Wendt, Alexander, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999).

Wired, "The Hidden Ties Between Google and Amazon's Project Nimbus and Israel's Military," 2024.

Woods, David L., "Algorithmic Warfare: Applying Artificial Intelligence to Warfighting," Military Review 98, no. 5 (2018): 81–89.

Zimmermann, Hubert, Alex Burkhardt, e Milena Elsinger, "The Israel/Palestinian Crisis and International Relations Theory," Social Science Space, 12 agosto 2024.

Zimmermann, Hubert, Andreas Dür, e Thomas Risse, eds., *International Relations Theories: Discipline and Diversity* (London: Sage, 2023).

Zureik, Elias, *Israel's Colonial Project in Palestine: Brutal Pursuit* (London: Routledge, 2016).