

Che il campo della guerra in tutte le sue articolazioni, tattiche e strategie, tecniche organizzative, raccolta e gestione delle informazioni -in tempo reale, localmente sul campo di battaglia, su tutto lo scenario del confronto bellico e strategico- sia un terreno privilegiato per l'applicazione delle tecnologie digitali sino all'ultima frontiera dell'Intelligenza Artificiale, non deve assolutamente stupire. Quando si parla dei dispositivi di comando, controllo e coordinamento, si rende conto sinteticamente della assoluta necessità di gestire l'informazione in tutte le sue articolazioni per condurre il confronto bellico e più in generale il confronto strategico, che comprende lo sviluppo della deterrenza, la preparazione del confronto diretto oltre che la sua esplicazione sul campo di battaglia.

È stato il termine 'guerra ibrida' e definisce l'associazione ai tradizionali terreni del confronto militare della capacità attraverso i dispositivi e le reti digitali di influire sul complesso delle relazioni, delle procedure, dei livelli organizzativi, sino alla coesione sociale, alla raccolta del consenso nella compagine sociale, politica, produttiva e militare dell'avversario/nemico.

I confini tra le varie forme di competizione e conflitto sfumano, salvo il superamento di soglie che definiscono traiettorie verso un conflitto aperto.

Il venir meno dell'utopia/distopia della globalizzazione neoliberista, la fine cioè di quella perfetta integrazione e gerarchizzazione dei sistemi produttivi nazionali e regionali, sotto la regia del capitale finanziario, proiettata verso un futuro radioso all'inarrestabile progresso tecnologico- è il prodotto dell'emergere della competizione, del conflitto tra i principali attori del sistema mondo, della formazione sociale globale, Cina e Stati Uniti in primo luogo, dell'emergere di nuovi protagonisti, di una configurazione variabile delle alleanze e degli schieramenti.

Da sempre l'organizzazione militare è associata a vari livelli di integrazione con tutti i dispositivi, i livelli e le procedure della cosiddetta sicurezza interna, tanto quanto - è bene ribadirlo- le pratiche miranti a minare la sicurezza e la coesione interna degli avversari.

Lo sviluppo tumultuoso delle tecnologie digitali da ultimo dell'ecosistema tecnologico dell'intelligenza Artificiale (I.A.) è coinvolto in questa dimensione complessiva del confronto strategico in tutte le sue articolazioni, dalla sicurezza interna al confronto militare diretto. In generale le società che sviluppano le tecnologie digitali sono impegnate in questo sviluppo, le Big Tech sono ovviamente protagoniste di questo mercato e sono cresciute a tutti i livelli le relazioni che le legano all'apparato di governo, ai centri decisionali dove si definiscono le strategie e si operano le scelte in merito alle tecnologie ai dispositivi, alle soluzioni in campo militare.

Nel seguito prenderemo in esame le informazioni in merito fornite in modo approfondito da

articoli, documenti e ricerche.

Al centro di tutte le considerazioni c'è il cosiddetto dual use delle tecnologie digitali, in particolare dell'I.A. di cui abbiamo reso conto in un precedente articolo 'A.I Dual Use: Doctor Jekyll and Mister Hyde'¹, vale a dire il continuo travaso tecnologico dal settore civile al militare e viceversa, con una crescente domanda da parte del settore militare.

Nel contesto di questa doppia faccia dello sviluppo tecnologico-digitale è legittimo, anzi necessario porsi la domanda di quali strade percorre la ricerca e lo sviluppo applicativo, quanto l'attrattività in termini di profitto delle applicazioni militari le determini. E' una domanda che la ricerca 'How Big Tech and Silicon Valley are Transforming the Military-Industrial Complex'² che analizza il rapporto tra le Big Tech ed in generale la rete delle società del digitale e l'apparato militare industriale negli USA, sfatando anche il mito che nella Silicon Valley si resista a questa collaborazione, forse una reminiscenza dell'originale ideologia hacker. Per ognuna delle soluzioni tecnologiche escogitate per soddisfare le esigenze delle pratiche militari e securitarie, ci si chiede quali altre esigenze in campi applicativi non connessi a quelle pratiche avrebbero potuto spingere alla creazione di quelle tecnologie orientandone lo sviluppo in direzioni diverse, con altri caratteri e funzioni. Questa è una considerazione fondamentale che riguarda quindi non solo la destinazione dei fondi, l'uso delle risorse, ma anche lo spettro alternativo delle soluzioni, dei prodotti e dei servizi che in alternativa si sarebbe potuto sviluppare; certo una contaminazione, dicevamo una quota di travaso c'è spesso, ma la possibilità di finanziamenti, di quote di profitto garantite e crescenti orientano in modo prevalente l'indirizzo delle ricerche.

L'oggetto e la conclusione della ricerca stanno nella seguente affermazione, "Sta emergendo una nuova economia politica, guidata dagli imperativi delle grandi aziende tecnologiche, del venture capital e delle società di private equity."

Che rende il complesso di soggetti che si mobilitano per trarre profitto dai sistemi e dai dispositivi militari abilitati dalle tecnologie digitali.

Inoltre. "Questo rapporto esamina come le priorità dell'industria tecnologica, le peculiarità delle strutture di finanziamento del capitale di rischio (VC) e il modello di startup della Silicon Valley possano portare a prodotti costosi e high-tech che sono inefficaci, imprevedibili e non sicuri se implementati in condizioni reali. (...)

Negli ultimi due anni, gli eventi globali hanno ulteriormente alimentato la domanda del Pentagono di tecnologie della Silicon Valley, tra cui il dispiegamento di droni e sistemi d'arma abilitati all'IA in Ucraina e a Gaza, e i timori di una corsa globale agli armamenti dell'IA contro la Cina.

(...)

I nuovi flussi di spesa del Pentagono sono destinati a una diversa tipologia di appaltatori della difesa: una combinazione di gigantesche aziende tecnologiche (ad esempio, Microsoft, Amazon, Google, Oracle, Hewlett Packard, Dell, Motorola e IBM) e centinaia di piccole start-up supportate da società di venture capital. Quasi tutte le startup sono nella fase di finanziamento pre-IPO.

(...)

Questo documento confuta anche l'errata percezione popolare secondo cui la Cina è pronta a superare gli Stati Uniti in una "corsa agli armamenti dell'IA" globale che determinerà il futuro della geopolitica e del dominio economico globale. Lo fa mostrando come la narrativa della corsa agli armamenti sia stata propagata dai funzionari del Pentagono e dai leader tecnologici che trarranno vantaggio dall'aumento delle vendite di armi ad alta tecnologia, sorveglianza e sistemi logistici abilitati dall'intelligenza artificiale. Questi miti e percezioni errate rischiano di dirottare i fondi dei contribuenti verso progetti di ricerca e sviluppo (R&S) che soddisfino le esigenze militari, piuttosto che quelle civili.

(...)

In un periodo di tempo relativamente breve, i funzionari del Dipartimento della Difesa hanno creato una vasta infrastruttura progettata per fornire supporto finanziario alle aziende tecnologiche della difesa. Ad esempio, nel 2015, il Pentagono ha istituito una società di venture capital finanziata dai contribuenti statunitensi, DIUx (Defense Innovation Unit-Experimental, ora chiamata DIU) per finanziare piccole startup che sviluppano prodotti per applicazioni militari. Nello stesso anno, ha anche creato MD5 (ribattezzato National Security Innovation Network) - pubblicizzato come un "acceleratore tecnologico per la sicurezza nazionale" - per accelerare lo sviluppo di tecnologie utili al Pentagono. Più di recente, il Dipartimento della Difesa ha lanciato l'Office of Strategic Capital, un'entità per collegare l'intelligenza artificiale, la biotecnologia e altre startup con fonti di capitale privato. Tutti i principali rami armati delle forze armate statunitensi hanno ora una serie di organizzazioni progettate per semplificare "l'ecosistema dell'innovazione" del DoD.

(...)

Più recentemente, il Dipartimento della Difesa ha compiuto uno sforzo concertato per rinnovare i suoi legami con l'industria tecnologica. Sotto la guida di Ash Carter, che ha ricoperto il ruolo di Segretario alla Difesa dal 2015 al 2017, i funzionari del Pentagono hanno lanciato una serie di organizzazioni progettate per rinnovare e consolidare i legami del Dipartimento della Difesa con la Silicon Valley. Questi includevano il fondo di venture

capital DIUx del Pentagono (vedi sopra) e il Defense Innovation Board (DIB), un trust di cervelli civili d'élite composto da dirigenti di Google, Facebook e altre aziende tecnologiche. Nel 2018, il Congresso degli Stati Uniti ha creato la National Security Commission on Artificial Intelligence (NSCAI) e l'ex CEO di Google Eric Schmidt è stato nominato presidente sia del DIB che dell'NSCAI.

Il Pentagono ha anche lanciato silenziosamente il Project Maven nel 2017, uno sforzo per utilizzare l'apprendimento automatico (una forma di intelligenza artificiale) per analizzare enormi set di dati costituiti da immagini di sorveglianza scattate da droni in Medio Oriente e in altri luoghi."

Trasparenza.

"Secondo l'organizzazione di ricerca senza scopo di lucro Tech Inquiry³, tre delle più grandi società tecnologiche del mondo hanno ricevuto circa 28 miliardi di dollari dal 2018 al 2022, tra cui Microsoft (13,5 miliardi di dollari), Amazon (10,2 miliardi di dollari) e Alphabet, la società madre di Google (4,3 miliardi di dollari).

Un'altra complicazione che rende difficile l'analisi dei contratti di appalto del Dipartimento della Difesa è il fatto che le principali aziende tecnologiche si aggiudicano spesso grandi subappalti da intermediari relativamente oscuri o società "passthrough" a cui vengono concessi contratti primari dal Pentagono. Tali accordi rendono difficile, ma non impossibile, determinare la misura in cui l'industria tecnologica è coinvolta nel lavoro militare"

Contratti.

Dopo una serie infinita di vertici, forum e incontri privati che hanno riunito funzionari del Dipartimento della Difesa, accademici, dirigenti della Silicon Valley e investitori influenti, nonché anni di messaggi persistenti da parte dei leader del Pentagono e dei think tank di politica pubblica falchi su una "corsa agli armamenti dell'IA" con la Cina e le imminenti minacce alla sicurezza nazionale degli Stati Uniti poste da Russia e Iran, il Dipartimento della Difesa e la CIA ora assegnano regolarmente contratti pluriennali alle principali aziende

tecnologiche.

Da un punto di vista aziendale, l'espansione di tali attività presenta dei vantaggi. In primo luogo, in un periodo di crescenti preoccupazioni per i conflitti globali (in Ucraina e in Medio Oriente) e per la "competizione tra grandi potenze", alcuni dirigenti tecnologici possono posizionarsi – e le loro aziende – come guardiani della sicurezza nazionale americana.

(...)

Alla fine del 2022, molti osservatori hanno preso nota quando il Pentagono ha annunciato che un contratto da 9 miliardi di dollari per la sua iniziativa Joint Warfighting Cloud Capability (JWCC) era stato assegnato congiuntamente a Microsoft, Google, Oracle e Amazon. L'obiettivo dichiarato del programma è quello di fornire servizi di cloud computing "alla velocità della missione, a tutti i livelli di classificazione, dal quartier generale alla dimensione tattica".

(...)

Ad esempio, all'inizio del 2019, il Pentagono ha assegnato a Microsoft un contratto quinquennale da 1,76 miliardi di dollari per lo sviluppo di software e servizi (vedi Tabella 1).³⁵ Nello stesso anno, i fornitori dell'azienda (General Dynamics, Dell e Minburn Technology Group) si sono assicurati un accordo decennale da 7,6 miliardi di dollari per il contratto Defense Enterprise Office Solutions, che fornisce strumenti di Office 365 come fogli di calcolo, e-mail e software di elaborazione testi al Pentagono

(...)

Amazon è un altro vincitore del JWCC che ha ricevuto importanti contratti dal Dipartimento della Difesa. Molti di questi sono per i servizi di cloud computing, che vengono utilizzati per l'archiviazione e la comunicazione dei dati all'interno e tra le agenzie militari e di intelligence. Più di un decennio fa, l'azienda ha ottenuto un accordo da 600 milioni di dollari con la CIA per tali servizi. Nel 2021, l'NSA ha concesso all'azienda un contratto decennale da 10 miliardi di dollari chiamato "Wild and Stormy".

Uno degli obiettivi principali del progetto è quello di spostare i dati di intelligence e sorveglianza globale dell'Agenzia dai server interni al cloud di Amazon. Un anno dopo, la Marina degli Stati Uniti ha assegnato all'azienda un contratto del valore di 724 milioni di dollari per servizi simili. Questi sono solo alcuni dei molti contratti ottenuti dall'azienda negli ultimi anni. Per anni, l'amministratore delegato dell'azienda, Jeff Bezos, ha sostenuto con entusiasmo legami più stretti tra l'industria tecnologica e le agenzie di sicurezza nazionale e ha respinto le critiche dei dipendenti di Amazon."ù

Storicamente le grandi corporation hanno dominato il mercato delle forniture militari, tra queste le BigTech del digitale, quando è esploso il mercato dei prodotti e dei servizi digitali.

“L’immensa dimensione delle grandi aziende tecnologiche ha reso relativamente facile per loro fare offerte per contratti di agenzie di difesa e intelligence, e alcune lo fanno da decenni. Lo stesso non si può dire per le piccole start-up che sono spesso affamate di liquidità e hanno bisogno di flussi di entrate per sopravvivere. Secondo alcuni analisti, i progetti pilota lanciati dalle startup tecnologiche della difesa possono riuscire a creare prototipi, ma spesso non riescono ad attraversare la cosiddetta “valle della morte” che si trova tra la produzione dei primi prototipi e i contratti pluriennali del Pentagono. Storicamente, i costi generali associati ai processi di approvvigionamento del governo degli Stati Uniti hanno reso difficile la concorrenza per le imprese più piccole.

Questo ha iniziato a cambiare nel 2015, quando l’allora segretario alla Difesa Ash Carter ha fondato DIUx. Aveva sede nella Silicon Valley ed era stato progettato come un fondo di venture capital: l’obiettivo era quello di identificare e investire rapidamente in startup che sviluppavano tecnologie all’avanguardia che potessero avere applicazioni militari.⁴⁸ Con DIUx, il Pentagono ha costruito il proprio acceleratore di startup per finanziare aziende specializzate in intelligenza artificiale, robotica, analisi dei dati, sicurezza informatica e biotecnologia. DIUx è stato intenzionalmente situato nel cuore della Silicon Valley, vicino al Lab126 di Amazon, al campus della Silicon Valley di Microsoft e agli uffici aziendali di Apple.

Carter, che aveva trascorso diversi anni alla Stanford University prima della sua nomina a Segretario alla Difesa, era rimasto impressionato dallo spirito imprenditoriale innovativo della Bay Area.⁴⁹ Nel 2018, DIUx è stato rinominato Defense Innovation Unit (DIU), indicando che non era più sperimentale. Tra giugno 2016 e settembre 2022, DIU ha assegnato contratti per un valore totale di 1,2 miliardi di dollari a più di 320 aziende.”

A questo punto la ricerca, dopo aver elencato un certo numero di strat up di successo, osserva che se i fondi fossero arrivati da istituzioni civili avrebbero potuto sviluppare le medesime tecnologie destinandone appunto ad usi civili, di utilità sociale, dall’agricoltura alla sanità.

“Invece, tutte queste startup sono state in parte supportate da agenzie militari che

presumibilmente hanno avuto un ruolo vitale nell'influenzare lo sviluppo delle nuove tecnologie. Come ha osservato Hugh Gusterson⁴: "Quando la ricerca che potrebbe essere finanziata da agenzie civili neutrali è invece finanziata dall'esercito, la conoscenza è sottilmente militarizzata e piegata nel modo in cui un albero viene piegato da un vento dominante".

"DIU e In-Q-Tel fanno parte di un'infrastruttura di investimento che si è espansa rapidamente nel tempo. Come notato sopra, il Dipartimento della Difesa ha creato MD5, ora chiamato National Security Innovation Network, poco dopo la fondazione di DIUx e l'anno scorso ha istituito l'*Office of Strategic Capital* come mezzo per collegare le startup tecnologiche della difesa a fonti di capitale di rischio e private equity. Inoltre, il Dipartimento della Difesa ha rapidamente sviluppato una serie di "acceleratori", "incubatori" e "hub" per coltivare "ecosistemi di innovazione" che mettono in contatto piccoli imprenditori e startup con potenziali clienti delle agenzie di difesa e intelligence statunitensi."

Il processo messo in atto, con la prospettiva di implementare tecnologie innovative in nuovi prodotti, dispositivi o servizi, è quello di attivare una massa crescente di tecnici, ricercatori, forza lavoro altamente qualificata che creano start up alla ricerca di finanziamenti da parte di venture capitalist, per le loro ricerche, progetti o prototipi. Il risultato poi è una selezione darwiniana.

"Le startup in genere seguono uno dei tre percorsi. Di gran lunga, il più comune è il fallimento. Secondo stime prudenti, il 75% delle startup non riesce a portare sul mercato un prodotto commercialmente valido, o i suoi primi investitori non riescono a realizzare un profitto.⁵⁷ Altre stime collocano il tasso di fallimento a circa il 90%. Le poche startup che riescono a sopravvivere o "diventano pubbliche", cioè emergono come società quotate in borsa, oppure vengono acquistate e fuse con (o acquisite da) un'azienda più grande. Man mano che si sviluppano e sostengono spese, le startup di successo generalmente organizzano diverse fasi di raccolta fondi o "round di finanziamento" (Seed, Serie A, Serie B, Serie C, Serie D, ecc.) per rimanere a galla."

"Per illustrare come le agenzie militari e di intelligence statunitensi abbiano sostenuto le startup tecnologiche, si consideri il caso di Keyhole, una piccola azienda con sede a San Francisco che ha sviluppato software per la creazione di modelli tridimensionali della superficie terrestre. Mettendo insieme immagini satellitari e foto aeree, il programma potrebbe essenzialmente produrre una mappa ad alta risoluzione dell'intero pianeta. Nel 2003 In-Q-Tel ha fornito finanziamenti iniziali e, nel giro di due settimane, le agenzie militari e di intelligence hanno riferito di aver utilizzato il software di Keyhole per sostenere la

guerra degli Stati Uniti in Iraq. L'anno successivo, Google ha acquisito Keyhole per una somma non rivelata. È stata ribattezzata Google Earth e oggi vale circa 4 miliardi di dollari.

In questo caso, l'investimento di In-Q-Tel ha dato i suoi frutti in termini monetari, ma il più grande Il jackpot era il programma Keyhole stesso, che la CIA e il Pentagono hanno immediatamente schierato a sostegno delle operazioni militari."

Quello di Google Earth è un caso più evidente di dual use di una tecnologia, associato allo sviluppo finanziato da fondi pubblici, destinati ad una start up che viene infine acquisita da una delle Big Tech, ma non è sempre ciò che succede.

"Non tutte le startup finanziate da DIU e In-Q-Tel vengono acquisite da aziende più grandi. Molte di esse falliscono e alcune diventano società quotate in borsa. Forse l'esempio più noto di quest'ultimo è Palantir, fondato nel 2003 da Peter Thiel, Alex Karp e altri.

La missione dell'azienda era quella di sviluppare un software che aiutasse a contrastare la minaccia del terrorismo. Secondo quanto riferito, Palantir ha faticato a raccogliere finanziamenti nella fase iniziale, fino a quando In-Q-Tel ha investito circa 2 milioni di dollari.⁶⁶ Nel 2013, i clienti dell'azienda includevano la CIA, la NSA, l'FBI, il Corpo dei Marines, l'Air Force e il Comando delle Operazioni Speciali.⁶⁷ Negli anni successivi, Palantir ha ampliato la sua lista di clienti per includere i dipartimenti di polizia degli Stati Uniti e le forze dell'ordine regionali, l'Immigration and Customs Enforcement degli Stati Uniti, e il servizio sanitario nazionale del Regno Unito, tra gli altri. Secondo quanto riferito, ha anche rilevato Project Maven del Dipartimento della Difesa dopo che i dirigenti di Google hanno scelto di non rinnovare il suo contratto⁵.

Per anni, Palantir ha avuto più contratti con le forze di difesa israeliane e ha esteso il suo sostegno a Israele dopo l'inizio della sua guerra contro Hamas nell'ottobre 2023. L'azienda ha anche svolto un ruolo nel sostenere le forze ucraine contro l'esercito russo."

In questo articolato processo di allargamento della rete di imprese che forniscono prodotti e servizi fondati sulle tecnologie digitali, stante l'esistenza di grandi imprese fornitrici del Pentagono, è naturale porsi il seguente interrogativo.

"Le aziende tecnologiche finiranno per sostituire gli appaltatori della difesa come principali destinatari della spesa militare degli Stati Uniti? Dato lo schiacciante potere finanziario di Big Tech, uno scenario più probabile è che aziende come Microsoft e Amazon inizieranno ad acquisire pezzi del complesso militare-industriale "tradizionale" e che aziende "tradizionali" come Northrop Grumman e RTX inizieranno ad acquistare promettenti startup tecnologiche per la difesa."

(...)

“Come notato in precedenza, il Dipartimento della Difesa e la CIA hanno i propri bracci VC (DIU e In-Q-Tel), ma le startup tecnologiche della difesa ricevono molti più finanziamenti da fonti private. A differenza delle società di investimento statunitensi più vecchie e consolidate, le società di venture capital tendono a concentrarsi sul finanziamento di startup che si trovano nelle prime fasi di sviluppo. Si tratta di iniziative notoriamente rischiose, ma investire in una startup di successo può portare a enormi profitti. In termini geografici, gli investimenti in VC sono fortemente concentrati nella Silicon Valley: più di un terzo di tutti i finanziamenti VC in America proviene da investitori nella grande San Francisco Bay Area.”

Ciò che la ricerca mette in evidenza è una trasformazione progressiva del complesso militare industriale, fornendolo di una nuova base ideologica, di un complesso di giustificazioni che ne rafforzino il potere, la presa sulle strategie della amministrazione.

“Le trasformazioni politiche ed economiche stanno rimodellando il complesso militare-industriale, e una sovrastruttura ideologica sta rafforzando questi processi di cambiamento. È composto da diversi elementi: una macchina dell’hype dell’intelligenza artificiale che fa affermazioni grandiose sull’efficacia dell’intelligenza artificiale; la sopravvalutazione delle capacità militari e tecnologiche della Cina; l’idea che solo l’America abbia la capacità (e il dovere) di proteggere le società democratiche del mondo; e la ferma convinzione che il modo migliore per preservare il dominio degli Stati Uniti sia attraverso un libero mercato in gran parte non regolamentato che dia priorità alle esigenze delle imprese. Queste prospettive, che svolgono un ruolo nell’aumentare la domanda di IA militare, sono promulgate da una rete interconnessa di dirigenti tecnologici, venture capitalist, analisti di think tank, ricercatori accademici, giornalisti e leader del Pentagono.

Nel corso di pochi anni, questo gruppo ha saturato il panorama dei media con uno scenario spaventoso: *affermano che l’America è sul punto di perdere un’epica lotta per la supremazia geopolitica ed economica globale, a meno che non riesca a superare la Cina nella “corsa agli armamenti dell’IA”. Questa idea convincente ricorda le narrazioni della Guerra Fredda e serve a giustificare e accelerare la spesa militare degli Stati Uniti nel settore tecnologico.*”

La figura più eminente di questo gruppo è Eric Schmidt un tempo Ceo di Google, che presiedette sia Defense Innovation Board (DIB) che il National Security Commission on Artificial Intelligence (NSCAI), secondo lui per gli Usa si stava avvicinando uno ‘Sputnik moment’, che richiede massicci investimenti nelle tecnologie digitali, I.A. in primo luogo,

per mantenere un vantaggio sulla Cina⁶.

Nella azione di Schmidt si saldano interessi personali ed azione di lobbying ad ampio raggio.

"Schmidt è tra i maggiori azionisti di Alphabet, possedendo azioni della società madre di Google per un valore di oltre 5 miliardi di dollari. E negli ultimi anni, ha investito milioni di dollari dalla sua società di venture capital in startup tecnologiche per la difesa, tra cui Rebellion Defense. Nel 2022, Schmidt, insieme a Peter Thiel (dirigente tecnologico, venture capitalist e co-fondatore di Palantir) e altri, *ha fondato l'America's Frontier Fund (AFF)*, un'organizzazione di venture capital senza scopo di lucro "che investe per l'interesse nazionale" sostenendo le aziende tecnologiche, in particolare le società di semiconduttori.⁹⁶ Sebbene i co-fondatori del gruppo abbiano un patrimonio netto di decine di miliardi di dollari, gli investitori di AFF hanno incontrato i legislatori del Congresso poco dopo la sua istituzione, alla ricerca di 1 miliardo di dollari di finanziamenti. Dopo che il Congresso non ha stanziato alcun denaro per l'AFF, il gruppo è riuscito a convincere il New Mexico State Investment Council a impegnare 100 milioni di dollari nel suo fondo."

La minaccia cinese è l'argomento fondamentale per incrementare i finanziamenti federali verso sempre nuove tecnologie e progetti in campo militare, i portatori di questa azione di propaganda sono sia nel Dipartimento della Difesa che nelle grandi imprese fornitrici, d'altra parte i due gruppi sono interconnessi dalla pratica delle porte girevoli, che vede gli stessi soggetti protagonisti in ambedue i campi.

"Anche think tank bipartisan -falchi- dell'establishment – *in particolare il Center for a New American Security (CNAS) e il Center for Strategic and International Studies (CSIS)* – stanno propagando l'idea di una corsa agli armamenti dell'IA contro la Cina. Ad esempio, il personale del CNAS ha scritto numerosi rapporti sull'argomento e ha testimoniato in audizioni del Congresso relative alle capacità di IA della Cina.¹⁰⁷ Il CSIS ha ospitato eventi simili e i suoi colleghi spesso producono rapporti a sostegno di politiche statunitensi più severe contro la Cina, come controlli più severi sulle esportazioni di microchip e semiconduttori avanzati.

Come molti think tank americani, CNAS e CSIS fanno molto affidamento sui finanziamenti aziendali. I maggiori donatori delle due organizzazioni includono le aziende della difesa Lockheed Martin, Northrop Grumman e RTX e, significativamente, giganti della tecnologia come Alphabet-Google, Microsoft, Amazon, Meta-Facebook e Apple. *Ciò solleva seri interrogativi su come tali collegamenti finanziari stiano plasmando le prospettive e le proposte politiche offerte dagli analisti di CNAS e CSIS.*"

Non tutti gli esperti e dirigenti del Pentagono concordano sulla retorica che la Cina sia in

grado di superare gli USA nello sviluppo tecnologico.

“Almeno un ex leader del Pentagono ha espresso dubbi sulla retorica di una corsa agli armamenti dell'IA. Il tenente generale in pensione dell'aeronautica statunitense Jack Shanahan, *che è stato direttore della Commissione congiunta per l'intelligenza artificiale del Dipartimento della Difesa*, ha recentemente osservato: “A volte sembra che siamo pericolosamente vicini a fare lo stesso tipo di valutazione errata del ‘bomber/missile gap’ con l'IA che abbiamo fatto con l'Unione Sovietica nei primi anni '60. Non sono esattamente esente da colpe qui.)” L'osservazione tra parentesi di Shanahan è un riferimento al fatto che, in qualità di direttore del Joint Artificial Intelligence Center del DoD e di direttore del Project Maven, egli ha promosso la rapida adozione dell'IA nelle applicazioni militari.”

Di sicuro la competizione tecnologica, in particolare sul piano militare, tra Cina e USA è in pieno sviluppo, la spesa militare degli USA è di gran lunga superiore a quella cinese, tuttavia opportune strategie possono concentrare in modo opportuno le risorse, un dato non differente è la crescita del numero dei ricercatori, degli ingegneri dei tecnici che possono essere dedicati allo sviluppo tecnologico, come già è avvenuto in diversi campi; vedremo nei prossimi anni come la competizione si svilupperà, al di là della propaganda.

Per quanto riguarda gli USA, le cui spese militari unite a quelle per la sicurezza ammontano ad un trilione di dollari, una quota crescente degli investimenti dedicata ad un ulteriore, continuo e crescente sviluppo tecnologico non farà che incrementarla.

Le Big Tech in buona sostanza si autoregolano e di fatto hanno il controllo dello sviluppo tecnologico nel campo della difesa. Il costo crescente è quindi di tipo politico a fronte della mancanza di un reale controllo pubblico su tutto il settore, ciò che rimanda all'allarme lanciato dal presidente Eisenhower negli anni '50. Tutto cambia affinché nulla cambi. Uno delle conseguenze è il tentativo di ridurre al minimo ogni regolazione nel campo delle tecnologie dell'I.A. e nell'accesso ai dati -stante la fame di dati delle applicazioni di I.A. - nella difesa della privacy, stante le 'esigenze' di controllo e sicurezza all'interno e nella competizione geostrategica, non stante che il presidente Biden abbia emesso un ordine esecutivo sul controllo delle tecnologie di IA.

Il quadro che emerge è di una sostanziale instabilità, in rapida evoluzione in termini tecnologici, economici, sociali, politici ed istituzionali; un quadro interno agli Stati Uniti strettamente correlato al quadro globale, alla competizione geostrategica.

In questa instabilità ha un ruolo anche la fame di profitti dei venture capitalist che spingono verso l'adozione di prodotti e tecnologie prima che ne sia testate in modo adeguato le caratteristiche.

“Per loro stessa natura, le società di venture capital cercano rapidi ritorni sull’investimento portando rapidamente un prodotto sul mercato e quindi “incassando” vendendo la startup o quotandosi in borsa. Ciò significa che le aziende tecnologiche della difesa finanziate da VC sono sotto pressione per produrre rapidamente prototipi e poi passare alla produzione prima che siano stati effettuati test adeguati. Le società di venture capital sono interessate a *“vendere nuove modalità di guerra ai funzionari del Pentagono non perché questo approccio si adatti a un quadro strategico, ma perché si allinea con il loro modello di business.”*

Infine. “Oltre alle grandi aziende tecnologiche, anche le startup stanno ricevendo più dollari che mai per la difesa, e queste tendenze stanno indirizzando il percorso di nuova ricerca e sviluppo verso esigenze militari, piuttosto che civili. Poiché i contratti del Dipartimento della Difesa sono spesso classificati e sono caratterizzati da una generale mancanza di trasparenza, *è impossibile determinare esattamente quanto sta andando nelle mani dell’industria tecnologica.”*

Ciò che emerge da questa ricerca è la sostanziale autonomia, autodeterminazione dell’apparato militare industriale, la sua capacità di piegare le strategie pubbliche ai propri interessi. Il carattere duale delle tecnologie viene piegato all’uso militare a scapito di processi di innovazione di utilità sociale, aggiungendo danno a danno. La struttura complessiva della società ne viene fortemente determinata. La conseguenza che possiamo trarne è che qualsiasi progetto di trasformazione della società deve impattare il ruolo che l’apparato militare-industriale ha nell’indirizzarne lo sviluppo, combattendo il prevalere del carattere militare nel dual use potenziale di qualsiasi tecnologia.

Roberto Rosso

1. <https://transform-italia.it/a-i-dual-use-doctor-jekyll-and-mister-hyde/> [↔]
2. <https://watson.brown.edu/costsofwar/papers/2024/SiliconValley> [↔]
3. *Tech Inquiry è un’organizzazione di ricerca senza scopo di lucro che utilizza il FOIA (il Freedom of Information Act degli Stati Uniti), tra gli altri metodi, per raccogliere, confrontare e analizzare i documenti del governo pubblico, in particolare i contratti di approvvigionamento con aziende che forniscono sistemi d’arma, tecnologie di sorveglianza e servizi di cloud computing alle agenzie governative degli Stati Uniti. L’organizzazione è stata fondata dal matematico Jack Poulson, a suo tempo ricercatore a Google, techinquiry.org* [↔]
4. Gusterson, H. (2008, June 10). *The U.S. Military’s Quest to Weaponize Culture*. Bulletin of the Atomic Scientists. <https://thebulletin.org/2008/06/the-u-s-militarys-quest-to-weaponize-culture/> [↔]
5. https://www.washingtonpost.com/world/national-security/palantir-wins-competition-to-build-army-intelligence-system/2019/03/26/c6d62bf0-3927-11e9-aaae-69364b2ed137_story.html
<https://jackpoulson.substack.com/p/pentagon-certified-palantir-as-only-supplier> Pentagon certified Palantir as only supplier

for artificial intelligence targeting tool known as “Maven Smart System”

Palantir was named yesterday as the only suitable supplier for the “Maven Smart System”. The \$13 million contract is follow-on to Palantir’s previous work on Pentagon AI surveillance, Project Maven. [↔]

6. Schmidt, E. (2020, February 27). *I Used to Run Google. Silicon Valley Could Lose to China*. The New York Times. <https://www.nytimes.com/2020/02/27/opinion/eric-schmidt-ai-china.html> ; 2023 February 28). *Innovation Power—Why Technology Will Define the Future of Geopolitics*. Foreign Policy. <https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics>; Allison, G., & Schmidt, E. (2021, December 7). *China Will Soon Lead the U.S. in Tech*. Wall Street Journal. <https://www.wsj.com/articles/china-will-soon-lead-the-us-in-tech-global-leader-semiconductors-5g-wireless-green-energy-11638915759> [↔]