

LUISS



DIPARTIMENTO DI SCIENZE POLITICHE
CORSO DI LAUREA TRIENNALE IN SCIENZE POLITICHE

Intelligenza Artificiale:
Lo Sviluppo di *National Security Policies* “Intelligenti” nella
Repubblica Popolare Cinese e negli Stati Uniti

Cattedra di Relazioni Internazionali

Prof. Raffaele Marchetti

Relatore

Federico Sergio (101352)

Candidato

A.A. 2023-2024

*A Mario, Quintina,
Biagio e Domenica,
nella speranza di avervi
reso fieri di me.*

Indice dei contenuti

<i>Abbreviazioni impiegate:</i>	3
<i>Introduzione</i>	4
<i>L'AI Governance nelle relazioni internazionali</i>	7
1.1 “Why Does AI Matter”	7
1.2 L'intelligenza artificiale e il rapporto con i fattori di potenza statale.....	10
1.2.1 <i>Politiche e strategie di sicurezza nazionale: definizioni, sviluppo e attuazione</i>	10
1.2.2 <i>Military AI: “state of the art”</i>	12
1.2.3 <i>Intelligenza artificiale e la dimensione economica statale</i>	15
1.3 L'IA come variabile del <i>balance of power</i>	16
<i>La grande scommessa: l'intelligenza artificiale negli Stati Uniti e in Cina</i>	20
2.1 Il “leapfrog development” cinese	20
2.1.1 “Intelligentized” (智能化) warfare.....	22
2.1.2 L'integrazione civile-militare nel dominio dell'IA	25
2.1.3 Strumentalizzazione dell'IA nell'Asia centrale	26
2.2 “Think different”: gli Stati Uniti leader del settore?	29
2.2.1 <i>Deep Green Concept: un simulatore militare predittivo ante litteram</i>	29
2.2.2 <i>Third Offset Strategy</i>	31
2.2.3 <i>Lo sviluppo di una difesa “intelligente”</i>	32
2.2.3.1 L'era del Project Maven (2017-2018).....	34
2.2.3.2 L'era del Joint Artificial Intelligence Center (2018-2022)	35
2.2.3.3 L'era del Chief Digital and Artificial Intelligence Office (2022-presente).....	35
2.2.4 <i>Il framework NATO</i>	36
2.3 Metodologia e domanda di ricerca	36
<i>Politiche e strategie di sicurezza nazionale “intelligenti”</i>	38
3.1 Caso Studio I: la Repubblica Popolare Cinese.....	38
3.1.1 <i>Il Next Generation Artificial Intelligence Development Plan</i>	38
3.1.2 <i>The Science of Military Strategy</i>	41
3.2 Caso Studio II: gli Stati Uniti d'America.....	44
3.2.1 <i>National Security Strategies 2017-2022: Trump c. Biden</i>	45
3.2.2 <i>National Artificial Intelligence Research and Development Strategic Plan</i>	46
<i>Conclusione</i>	53
<i>Bibliografia e sitografia</i>	55
<i>Abstract</i>	61

Abbreviazioni impiegate:

AGI: Artificial General Intelligence
AIDP: New Generation Artificial Intelligence Development Plan
AIRC: Artificial Intelligence Research Centre
AMS: Academy of Military Science
ANI: Artificial Narrow Intelligence
BRI: Belt and Road Initiative
CAICT: China Academy of Information and Communications Technology
CDAO: Chief Digital Artificial Intelligence Office
CMC: Central Military Commission
CMC S&TC: Central Military Commission Science and the Technology Commission
DARPA: Defense Advanced Research Projects Agency
DII: Defense Innovation Initiative
DoD: United States Department of Defense
DRS: Digital Silk Road
IA: Intelligenza Artificiale o Intelligenze Artificiali
JAIC: Joint Artificial Intelligence Center
LAWS: Lethal Autonomous Weapons Systems
ML: Machine Learning
NAIRDSP: National Artificial Intelligence Research and Development Strategic Plan
NAIRR: National Artificial Intelligence Research Resource Pilot
NIIDT: National Innovation Institute of Defense Technology
NSCAI: National Security Commission on Artificial Intelligence
NSP: National Security Policy
NSS: National Security Strategy
OODA: Observe-Orient-Decide-Act
PLA: Esercito Popolare di Liberazione
RAI S&IPathway: Responsible Artificial Intelligence Strategy and Implementation Pathway
R&D: Research and Development
TOS: Third Offset Strategy
UAS: Uncrewed Aerial Systems
UAV: Unmanned Aerial Vehicle (se UAVs al plurale)
UGV: Unmanned Ground Vehicle (se UGVs al plurale)
USRC: Unmanned System Research Centre
UUV: Unmanned Underwater Vehicle (se UUVs al plurale)

Introduzione

Quando si pensa ai conflitti, nell'ambito delle relazioni internazionali, ci si ritrova a categorizzare la guerra convenzionale come unica declinazione di questi. Le crescenti tensioni economiche e tecnologiche hanno aperto un nuovo dibattito accademico. L'uso di armi non convenzionali, di attacchi cyber e di interferenze estere nelle questioni interne di uno Stato, stanno erodendo i confini nei quali si configurano i conflitti. *Hybrid warfare*, *asymmetric warfare* e *gray-zone warfare* sono i termini che meglio descrivono la labile demarcazione dei conflitti odierni.

Il vento rivoluzionario che soffia sulla diffusione di queste nuove frontiere di conflitto è alimentato, anche, dalla rapida diffusione di sistemi d'Intelligenza Artificiale all'interno del mercato globale. L'impatto dirompente di questa tecnologia e le sue potenzialità in ambito sociale, economico e militare hanno visto un grande coinvolgimento da parte dei principali attori statali. L'aumento dei budget R&D per l'IA è incrementato esponenzialmente negli ultimi dieci anni, sia nel settore privato che in quello pubblico, favorendo una moderna corsa all'innovazione. La prospettiva di un avanzamento tecnologico e di una superiorità strategico-tecnologica hanno indotto Stati Uniti, Cina, Russia e molti altri paesi a contemplare la possibilità che questa tecnologia possa rappresentare l'inizio di una nuova era all'interno dello scacchiere internazionale. La sempre più attuale interconnessione tra i fattori economici, tecnologici e militari alimenta l'ambizione statale e detta la necessità di integrare, all'interno del quadro strategico-normativo, iniziative e progetti al fine di assicurarsi il titolo *AI great power*. Nella cornice appena definita, questa tesi si propone di rispondere alla domanda "*How is AI implemented in national security policies?*", analizzando le attuali strategie in ambito IA, qui rinominate "intelligenti", degli Stati Uniti d'America e della Repubblica Popolare Cinese al fine di constatare in che modo stia avvenendo l'implementazione dell'Intelligenza Artificiale all'interno delle *policies* nazionali. Per ciò che concerne la metodologia di ricerca l'elaborato indaga, in prima istanza, i contesti nazionali nei quali si inseriscono le *policies* sopra menzionate. Una prima panoramica è data

dall'individuazione del pensiero predominante cinese e americano in materia di IA, attraverso l'analisi delle principali posizioni governative di entrambi i paesi, dei documenti ufficiali, dei discorsi istituzionali e delle interviste disponibili in rete. A seguire, viene presa in esame la documentazione relativa all'IA dei due paesi, in particolar modo per la Repubblica Popolare Cinese, il *Next Generation Artificial Intelligence Development Plan* e la sino-dottrina militare elaborata nel *The Science of Military Strategy*, mentre nel caso statunitense vengono esaminati, *in primis*, i riferimenti all'IA all'interno delle più recenti *National Security Strategies*, del 2017 e del 2022, e successivamente l'ultima versione, pubblicata nel 2023, del *National Artificial Intelligence Research and Development Strategic Plan*. La tesi segue, quindi, una struttura conoidale inversa, partendo dal generale per arrivare al particolare, che si sviluppa in tre capitoli principali, a loro volta suddivisi in sottosezioni.

Il Capitolo I mira a fornire al lettore una differenziazione di ciò che si intende quando si parla di IA, fornendo definizioni generalmente accettate. Il capitolo prosegue poi con la differenziazione dei termini di *national security policy* e *national security strategy*, utile per la discussione del tema nelle sezioni successive. L'ultima sezione, invece, fornisce il quadro teorico nel quale si inserisce l'analisi e l'attuale implementazione delle tecnologie intelligenti all'interno dell'ambito economico e militare relativamente al potenziale e alle sfide che queste presentano nell'intricato sistema internazionale. Il capitolo si conclude con un inciso relativo all'impatto che l'IA, secondo la dottrina, potrebbe avere nell'ambito della teoria realista del *balance of power*.

Il Capitolo II introduce l'analisi dei *frameworks* nazionali di Stati Uniti e Cina. Attraverso l'analisi cronologica dei più recenti sviluppi in ambito IA dei due paesi viene anticipato il contesto nel quale si innesta il capitolo successivo. In questa sezione l'approccio cinese e quello americano sembrano molto simili, entrambi orientati all'implementazione dei sistemi intelligenti all'interno dei propri apparati militari. Quest'integrazione è constatabile dalla strategia cinese basata sul concetto di "*Intelligentized*" (智能化) *warfare*", ovvero lo sviluppo e l'operatività dell'intelligenza artificiale e l'abilitazione di tecnologie interconnesse necessarie per la sua realizzazione con fini militari. Altro campanello d'allarme risulta essere il potenziamento

dell'integrazione militare civile, programma che ha lo scopo di implementare, nel settore militare, le più sofisticate innovazioni in ambito IA sviluppate da privati o per fini civili. Sul fronte statunitense, invece, troviamo un continuo miglioramento delle strategie militari con il perseguimento della *Third Offset Strategy* che prevede di sviluppare tecnologie avanzate per compensare i progressi tecnologici della Cina e della Russia. A questo segue anche la messa in atto di programmi sempre più avanzati per delineare una difesa "intelligente".

Nel Capitolo III vengono analizzati i principali documenti in materia IA pubblicati da Cina e Stati Uniti. In questa sezione vengono alla luce le prime discrepanze tra il sino-approccio e l'approccio statunitense. Mentre la Repubblica Popolare Cinese si focalizza su una visione *dual-use* dell'IA, gli Stati Uniti sviluppano una strategia trasversale e multidisciplinare. La Cina, infatti, pone molta enfasi sulla possibilità di utilizzare tecnologie IA commerciali o civili per fini strategico-militari, soprattutto nell'ambito di uno cambio di paradigma strategico passando, quindi, da paese "*inseguitore*" a paese "*inseguito*". Questa constatazione è la risultante dei principali obiettivi enunciati nell'AIDP e nel documento ufficiale della sino-dottrina militare. La Repubblica Popolare ambisce al superamento, economico e strategico, attraverso l'elaborazione di tre diverse fasi temporali, degli Stati Uniti in ambito IA. Tramite l'esame dei dati attualmente disponibili, la Cina risulta ancora indietro rispetto al programma prefissato, rimanendo ancora al secondo posto in termini di industria IA. Ciò è dovuto anche all'assenza di un programma di sviluppo delle Intelligenze Artificiali a livello internazionale, variabile invece presente nello scenario statunitense. Al contrario gli Stati Uniti, nonostante adottino una filosofia simile per ciò che concerne il *dual-use* dei sistemi intelligenti, inseriscono, all'interno della propria strategia, una serie di obiettivi legati agli aspetti sociali, etici e produttivi tutelati da nuovi standard tecnici per l'amministrazione e lo sviluppo di sistemi IA. In ultimo, i progetti di cooperazione internazionale, tra cui scambi di esperti con i paesi alleati, garantiscono agli Stati Uniti, non solo di consolidare le alleanze politiche, ma anche di assicurarsi il maggior numero di specialisti del settore con l'obiettivo di sviluppare progetti governativi al fine di mantenere il titolo di potenza innovatrice globale.

Capitolo I

L'AI Governance nelle relazioni internazionali

Il recente e rapido sviluppo delle nuove tecnologie e, in particolar modo dell'Intelligenza Artificiale (IA) e del *Machine Learning* (ML), rappresenta uno dei fulcri su cui girano le politiche di avanzamento tecnologico dei principali attori statali globali. L'abilità, tra le altre, dell'IA di analizzare e riassumere informazioni e di velocizzare i processi di *decision-making* ha spinto le potenze mondiali, inclusi Stati Uniti, Cina, Regno Unito, Israele, Canada e Russia a investire pesantemente in queste nuove tecnologie. Il Presidente russo Vladimir Putin, nel 2017, ha asserito che chiunque guiderà l'innovazione in ambito di Intelligenza Artificiale diventerà “*il sovrano del mondo*”¹ e la Cina si è prefissata di divenire la potenza leader entro il 2030.²

1.1 “Why Does AI Matter”

Winston Churchill definì la potenza aerea come “*un'energia che può porre fine alla guerra o alla civiltà*”.³ Questo paragone con lo sviluppo della forza aerea, tra la Prima e la Seconda guerra mondiale, può aiutare i più a comprendere il ruolo e l'impatto che l'IA sta avendo e avrà nel prossimo futuro in ambito strategico-militare. Definire cosa si intende per intelligenza artificiale è funzionale per capire quali effetti sta avendo, e quali potrebbe avere, l'IA nelle politiche di sicurezza nazionale. Generalmente l'intelligenza artificiale è definita come “un sistema computerizzato in grado di svolgere compiti che richiedono normalmente l'intelligenza umana”.⁴ In ambito accademico, al momento, non esiste una definizione generalmente accettata di “sistemi intelligenti” ma si tende a

¹ James Vincent, «Putin Says the Nation That Leads in AI 'Will Be the Ruler of the World'», The Verge, 4 settembre 2017, consultato 9 febbraio 2024, <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world>.

² «A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf», consultato 9 febbraio 2024, <https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf>.

³ Winston S. Churchill, *Churchill Speaks: Winston S. Churchill in Peace and War: Collected Speeches, 1897-1963* (Windward, 1982).

⁴ «Artificial Intelligence», in *Oxford Reference*, s.d., consultato 9 febbraio 2024.

differenziare tra *Artificial Narrow Intelligence* (ANI o *weak AI*) e *Artificial General Intelligence* (AGI). La prima (ANI) è definita come un'intelligenza automatica addestrata a svolgere, nel miglior modo possibile, un compito cognitivo strettamente definito. Questo implica una competenza limitata ad un settore particolare che, però, le consente di migliorare le proprie prestazioni nel tempo attraverso l'apprendimento pratico (es. Alpha Go⁵ e Chat GPT).⁶ Per quanto concerne la AGI è definita dalla NSCAI come un'intelligenza artificiale in grado di svolgere compiti basati su parametri che non sono stati esplicitamente programmati in anticipo, alla ricerca non solo di una serie di soluzioni per i compiti assegnatigli (come nel caso delle ANI), ma anche di soluzioni per nuovi compiti.⁷ È però generalmente accettato il fatto che lo sviluppo dell'AGI, se realmente possibile, richiederà ancora molti anni. A queste due tipologie di IA si aggiunge una terza variante l'*Artificial Super Intelligence* (ASI), spesso tralasciata dalla letteratura accademica in quanto, come per l'AGI, si tratta di un'altra categoria teorica di intelligenza artificiale che va al di là di qualsiasi livello d'intelligenza umana. La crescita esponenziale delle performance computerizzate,⁸ l'aumento di disponibilità di enormi dataset con cui allenare i sistemi di *machine learning*, l'implementazione delle tecniche di *machine learning* in sistemi computerizzati e i rapidi e significativi aumenti degli investimenti commerciali⁹ hanno, però, contribuito alla rapida ascesa della *Artificial Narrow Intelligence*. Sulla base di questi fattori possiamo concludere che è la sotto branca del

⁵ AlphaGo è un algoritmo di gioco creato dalla società AI DeepMind. Nel marzo 2016, ha sconfitto il campione del mondo di Go, Lee Sedol, quattro partite a uno, ridefinendo le credenze sul gioco del Go, gioco da tavolo cinese simile alla nostra dama, si veda Cade Metz, «In Two Moves, AlphaGo and Lee Sedol Redefined the Future», *Wired*, consultato 9 febbraio 2024, <https://www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future/>.

⁶ Michael Horowitz, Shira Pindyck, e Casey Mahoney, «AI, the International Balance of Power, and National Security Strategy», in *The Oxford Handbook of AI Governance*, a c. di Justin B. Bullock et al., 1ª ed. (Oxford University Press, 2022), <https://doi.org/10.1093/oxfordhb/9780197579329.013.55>; si veda anche Alexander Babuta, Marion Oswald, e Ardi Janjeva, «Artificial Intelligence and UK National Security», RUSI Occasional Paper, 27 aprile 2020.

⁷ Eric Schmidt et al., «Final Report» (National Security Commission on Artificial Intelligence, 2021), <https://cybercemetery.unt.edu/nscai/20211005220330/https://www.nscai.gov/>.

⁸ Si veda «Moore's Law | Microprocessors, Transistors & Technology | Britannica», 5 gennaio 2024, <https://www.britannica.com/technology/Moores-law>.

⁹ Gregory C. Allen e Taniel Chan, «Artificial Intelligence and National Security», *National Security*, Belfer Center Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School (luglio 2017), <https://www.belfercenter.org/publication/artificial-intelligence-and-national-security>.

machine learning, definita come “la capacità di una macchina di imitare il comportamento umano intelligente”,¹⁰ a guidare l’avanzamento tecnologico dell’IA. Russell e Norvig identificano quattro principali meccanismi di apprendimento utilizzati nei sistemi di ML. (1) Il meccanismo di apprendimento supervisionato consiste nel far osservare alla macchina, o agente, alcuni esempi di coppie input-output con lo scopo di sviluppare una mappa di input e output. Un’applicazione pratica di questo meccanismo è identificabile nei robot sentinella sudcoreani SGR-A1.¹¹ (2) Il meccanismo di apprendimento non supervisionato, al contrario, presuppone che l’agente impari modelli input anche se non ne viene fornito nessun feedback esplicito sull’output. (3) L’apprendimento di rinforzo è, invece, una forma di apprendimento orientata agli obiettivi, in cui la macchina migliora nel completamento di un compito, in un determinato lasso di tempo, basandosi solo sull’esposizione a feedback positivi e negativi. Infine, (4) l’apprendimento semi-supervisionato coinvolge set di dati in cui alcune coppie input-output sono etichettate mentre gran parte non lo sono.¹²

L’intelligenza artificiale pervade già le nostre vite. Sistemi di questo tipo sono già presenti nei dispositivi che usiamo tutti giorni. Algoritmi di IA e ML sono stati adottati anche in ambito medico, ad esempio per l’individuazione di tumori della pelle e in ambito sociale, per l’identificazione di famiglie bisognose di sussidi governativi. Ai fini di questa ricerca è utile fornire, innanzitutto, una definizione di politica, e conseguentemente di strategia, di sicurezza nazionale per poi passare ad analizzare quale impatto l’IA e il ML stanno avendo in termini di aumento del potere militare ed economico dei principali attori statali e se questo incremento può intaccare la polarità del sistema internazionale.

¹⁰ Brown, Sara, «Machine Learning, Explained | MIT Sloan», 21 aprile 2021, <https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained>.

¹¹ Si veda Patrick Lin, George Bekey, e Keith Abney, «Autonomous Military Robotics: Risk, Ethics, and Design»: (Fort Belvoir, VA: Defense Technical Information Center, 20 dicembre 2008), p. 19, <https://doi.org/10.21236/ADA534697>.

¹² Stuart J. Russell e Peter Norvig, *Artificial intelligence: a modern approach*, 4^a ed., Pearson series in artificial intelligence (Hoboken: Pearson, 2021).pp. 706–08

1.2 L'intelligenza artificiale e il rapporto con i fattori di potenza statale

All'interno del mondo accademico delle relazioni internazionali e, sempre più, anche in quello del *policy-making* la domanda a cui si cerca di dare una risposta è come gli Stati acquisiscano potere. Kenneth N. Waltz, esponente e ideatore della teoria neorealista delle relazioni internazionali, nella sua più celebre opera *Theory of International Politics*, afferma che la politica internazionale è basata sulla concorrenza:

*Il destino di ogni Stato dipende dalle sue risposte a ciò che fanno gli altri Stati. La possibilità che il conflitto sia condotto con la forza porta alla competizione nelle arti e negli strumenti di forza. La concorrenza produce una tendenza verso l'identità dei concorrenti.*¹³

1.2.1 Politiche e strategie di sicurezza nazionale: definizioni, sviluppo e attuazione

Al fine di accrescere il proprio potere all'interno del contesto internazionale, gli Stati hanno la necessità di individuare i propri punti di forza ma, soprattutto, le proprie debolezze. In parte quest'analisi è fornita dalla c.d. dottrina di sicurezza nazionale, o politica (*National security policy*, in acronimo NSP), definita dal DCAF Geneva Centre for Security Sector Governance, la rappresentazione ufficiale di come uno Stato fornisce sicurezza a sé stesso e ai suoi cittadini. La politica di sicurezza nazionale è, quindi, una descrizione formale dei principi guida, valori, interessi, obiettivi, ambiente strategico, minacce, rischi e sfide di un paese, al fine di proteggere e promuovere la sicurezza nazionale. Tipicamente, la NSP si basa sulla costituzione di uno Stato, sui suoi documenti fondativi e sulla legislazione vigente. La NSP, quindi, chiarisce i comportamenti e le responsabilità delle istituzioni statali nel fornire sicurezza e sostenere lo stato di diritto. È interessante notare che non tutti i paesi possiedono un unico documento al cui interno è racchiusa l'intera dottrina di sicurezza nazionale ma riflettono la propria NSP in una serie di documenti che insieme compongono una politica integrata coerente. La politica di

¹³ Kenneth N. Waltz, *Theory of international politics*, Addison-Wesley series in political science (Reading, Mass: Addison-Wesley Pub. Co, 1979), p. 127.

sicurezza nazionale di uno Stato si compone, essenzialmente di cinque elementi. (1) Il primo si articola intorno alla *vision* e agli obiettivi del documento, ovvero una descrizione chiara e realistica delle condizioni della propria sicurezza nazionale e sulla scelta degli obiettivi e dei risultati da conseguire in futuro. (2) Il secondo punto sono, invece, i già citati principi e valori statali che definiscono entro quali limiti giuridici, nazionali ed internazionali, può muoversi la NSP. (3) Di seguito troviamo gli interessi nazionali e l'ambiente strategico, una descrizione delle priorità di sicurezza dello Stato sulla base del contesto, le priorità e gli obblighi nazionali. (4) Il quarto punto è rappresentato dagli obblighi internazionali che delineano una prospettiva nazionale in materia di sicurezza e cooperazione internazionale, tenendo conto degli obblighi multilaterali e degli impegni giuridici internazionali ratificati dai singoli Stati. (5) Il quinto punto, invece, individua le sfide, le minacce, i rischi e le opportunità correnti e future. Lo scopo della NSP è, dunque, quello di individuare e, mettere in atto, le c.d. *National Security and Defence Strategies*.

Talvolta però i termini “politica” e “strategia”, rimanendo nell’ambito della sicurezza nazionale, sono usati in modo intercambiabile. Come sopra riportato, una politica di sicurezza nazionale è una descrizione generale che stabilisce le priorità e gli obiettivi per la garanzia della sicurezza statale; una strategia di sicurezza nazionale (*National security strategy*, NSS), invece, descrive come gli obiettivi fissati in una politica di sicurezza nazionale possono essere raggiunti. La NSS è, dunque, un documento pratico (o un insieme di documenti) che specifica gli strumenti necessari per attuare una politica di sicurezza nazionale, il modo in cui tali strumenti dovrebbero essere impiegati per un periodo di tempo più lungo e il modo in cui dovrebbero essere utilizzati insieme al fine di utilizzare al meglio le risorse. In sintesi, possiamo definire la strategia di sicurezza nazionale come l’insieme dei metodi formali che verranno impiegati per raggiungere gli obiettivi di sicurezza e difesa descritti dalla politica di sicurezza nazionale (fig. 1).¹⁴

¹⁴ Si vedano: DCAF – Geneva Centre for Security Sector Governance, «NATIONAL SECURITY POLICIES Formulating National Security Policies for Good Security Sector Governance», SSR Backgrounder Series Geneva, consultato 13 marzo 2024, https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_09_NationalSecurityPolicies_Nov2022.pdf; «National Security Policy», Security Sector integrity, consultato 13 marzo 2024, <https://securitysectorintegrity.com/defence-management/policy/>.



Fig. 1. Fonte: «National Security Policy», Security Sector integrity.

1.2.2 Military AI: “state of the art”

L’intelligenza artificiale rappresenta un terreno di scontro per le grandi potenze. Il lancio di progetti come il *Coordinated Plan on Artificial Intelligence* da parte dell’Unione Europea, dell’*American AI Initiative* del governo americano e del *Next Generation Artificial Intelligence Development Plan*¹⁵ cinese sono un chiaro segnale che l’IA è entrata a far parte delle priorità statali, non solo da un punto di vista prettamente industriale, con l’attuazione di politiche mirate allo sviluppo tecnologico, ma anche a livello economico e militare. Gran parte della dottrina ritiene che l’IA stia già pervadendo gli ambiti militari ed economici statali. Tra questi i maggiori contributi sono forniti da Michael C. Horowitz e Gregory C. Allen, entrambi *Adjunct Fellow* al Center for a New American Security (CNAS). Nell’analizzare l’impatto dell’IA in ambito politico, entrambi, forniscono, *in primis*, un’analisi sistemica della sicurezza globale. L’assunto di base risulta essere che l’IA è uno strumento (in inglese “*tool*”) per l’incremento della

¹⁵ Si vedano in ordine: «Coordinated Plan on Artificial Intelligence | Shaping Europe’s Digital Future», 27 febbraio 2024, <https://digital-strategy.ec.europa.eu/en/policies/plan-ai>; «The American AI Initiative: The U.S. Strategy for Leadership in Artificial Intelligence», consultato 1 marzo 2024, <https://oecd.ai/en/wonk/the-american-ai-initiative-the-u-s-strategy-for-leadership-in-artificial-intelligence>; «A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf».

potenza statale. Horowitz, Pindyck e Mahoney sostengono che il potere statale si basi su due sfere interconnesse: la sfera economica e la sfera militare, intensa come cinetica e non cinetica (in inglese “*kinetic and non-kinetic*”). L’intelligenza artificiale in ambito militare è vista come un “*miglioramento delle abilità militari*”. L’utilizzo di sistemi di riconoscimento di *data patterns* complessi velocizza, e rende più efficaci, le operazioni militari. Algoritmi di *deep learning*, studiando l’ambiente circostante, possono anticipare e predire futuri attacchi o azioni nemiche. A livello tattico, piattaforme automatizzate e collegate alla rete assistono l’acquisizione di posizioni nemiche attraverso il coordinamento rapido di manovre e di fuoco, come dimostrato dal prototipo *U.S. Marine ball drones*.¹⁶ L’IA può essere utilizzata anche per operazioni di intelligence e di sorveglianza attraverso le abilità di riconoscimento e completamento di problematiche con una velocità estremamente maggiore rispetto all’essere umano. Esempio ne è il Progetto Maven statunitense che, attraverso algoritmi a IA è in grado di analizzare i filmati dei droni ed individuare attività ostili da contrastare.¹⁷ Il potenziale dell’IA è utilizzato anche sui sistemi d’arma autonomi. L’attenzione nei confronti degli *unmanned vehicles* (veicoli senza pilota), comunemente chiamati droni, e delle nuove tecnologie dell’IA e del ML, è elevata. Infatti, secondo il Boston Consulting Group, la spesa globale in robotica militare, intesa solo come *unmanned vehicles*, nel periodo 2000-2015 è triplicata, passando da 2,4 miliardi di dollari a 7,5 miliardi e le aspettative sono che raddoppierà ancora fino ad arrivare a 16,5 miliardi di dollari entro il 2025 (fig. 2).¹⁸ Analizzando l’andamento della spesa mondiale in robotica militare e sistemi autonomi (UAVs, UGVs, UUVs), Gill Pratt, già *Program Manager* del DARPA¹⁹ come direttore della DARPA Robotics Challenge, afferma che le tendenze economiche e tecnologiche convergeranno in un’esplosione cambriana dei nuovi sistemi robotici.²⁰ La questione

¹⁶ Horowitz, Pindyck, e Mahoney, «AI, the International Balance of Power, and National Security Strategy».

¹⁷ Gregory C. Allen, «Project Maven Brings AI to the Fight against ISIS», *Bulletin of the Atomic Scientists* (blog), 21 dicembre 2017, <https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/>.

¹⁸ Alison Sander e Mel Wolfgang, «The Rise of Robotics», *bcg.perspectives* by The Boston Consulting Group, 27 agosto 2014, https://web-assets.bcg.com/img-src/The_Rise_of_Robotics_Aug_2014_tcm9-82495.pdf.

¹⁹ La DARPA è un’agenzia governativa di R&D del Dipartimento della Difesa degli Stati Uniti. Fu istituita nel 1957 in risposta al lancio del progetto Sputnik sovietico e rappresenta il principale centro di sviluppo di nuove tecnologie militari.

²⁰ Gill A. Pratt, «Is a Cambrian Explosion Coming for Robotics?», *Journal of Economic Perspectives* 29, fasc. 3 (1 agosto 2015): 51–60, <https://doi.org/10.1257/jep.29.3.51>.

risulta essere ancora più rilevante visto il recente inserimento degli *unmanned vehicles* e dell'intelligenza artificiale, come EDTs (*Emerging and Disruptive Technologies*), all'interno della lista delle tecnologie chiave NATO.²¹

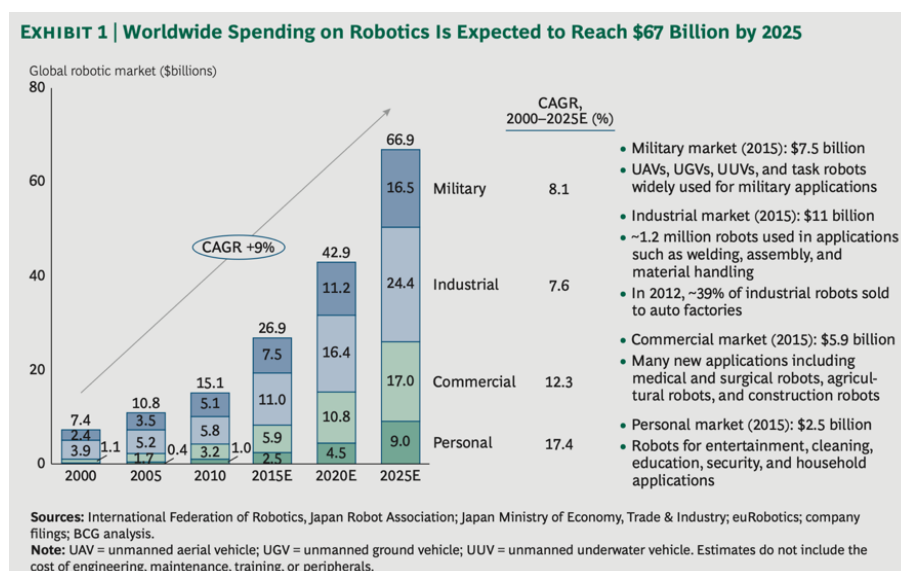


Fig. 2. Fonte: Alison Sander e Mel Wolfgang, «The Rise of Robotics», *bcg.perspectives*, 2017

Come ci si potrebbe aspettare, a tali opportunità si contrappongono alcune sfide. Alcune nuove situazioni, ad esempio, potrebbero non corrispondere pienamente o in parte a quelle precedentemente osservate dall'IA e questo errore di valutazione potrebbe aggravare la tensione e l'incertezza nella presa di decisioni cruciali per la sicurezza da parte dei *policy-maker*. Il tema era già stato introdotto da Graham T. Allison nell'articolo *Conceptual Models and the Cuban Missile Crisis* del 1969.²² L'estrema velocità dell'IA di analizzare delle situazioni deve fare i conti con diversi gradi di imprevedibilità, fattore caratteristico della natura dei conflitti armati. Un errore di calcolo delle azioni di un avversario potrebbe innescare un'escalation involontaria.²³

²¹ «NATO - Topic: Emerging and disruptive technologies», consultato 1 marzo 2024, https://www.nato.int/cps/en/natohq/topics_184303.htm.

²² Graham T. Allison, «Conceptual Models and the Cuban Missile Crisis», *American Political Science Review* 63, fasc. 3 (novembre 1969): 689–718, <https://doi.org/10.2307/1954423>.

²³ Jürgen Altmann e Frank Sauer, «Autonomous Weapon Systems and Strategic Stability», *Survival* 59, fasc. 5 (3 settembre 2017): p. 128, <https://doi.org/10.1080/00396338.2017.1375263>.

Per quanto concerne invece l'ambito tattico, i c.d. *bias* riguardanti la razza, la religione e il genere possono anche essere inseriti come parametri nei sistemi di IA. Sotto questo aspetto, *big data* e algoritmi possono rafforzare e amplificare le disuguaglianze esistenti, come già dimostrato nel caso Amazon del 2018 in cui, l'algoritmo di assunzione forniva punteggi più alti ai candidati di sesso maschile perché basato su *dataset* delle prestazioni lavorative in periodi storici in cui la maggior parte dei dipendenti erano uomini bianchi.²⁴ Questo aspetto si ripercuote anche nella sfera militare in cui le ipotesi relative all'età e al sesso dei civili possono influenzare non solo le decisioni del personale militare, ma anche i calcoli per il *targeting*. Le vittime civili a seguito di attacchi con droni sono spesso il risultato di errori di calcolo provenienti dal presupposto che tutti i maschi in età militare, nella zona dell'esplosione, siano combattenti.²⁵ Questi risvolti dell'IA potrebbero alterarne lo sviluppo: vista la "giovane età" dei sistemi di IA, l'industria responsabile della sua creazione rischia pregiudizi interessanti che possono influenzare le decisioni politiche per molti anni.

1.2.3 Intelligenza artificiale e la dimensione economica statale

Come anticipato, l'intelligenza artificiale potrebbe avere anche un impatto sistemico indiretto attraverso spostamenti di potere economico, in grado di mutare il potere di uno Stato a livello globale. *The Economist* ha infatti stimato che, nel 2017, le fusioni e le acquisizioni legate all'IA sono state 26 volte superiori rispetto a due anni prima, con una spesa di 22 miliardi di dollari.²⁶ Lo sviluppo di robot, sensori e la loro conseguente interconnessione, attraverso i processi di digitalizzazione, potrebbero plasmare le priorità perseguite da un'economia. I supermercati senza casse di Amazon, la creazione di assistenti virtuali come Alexa e Siri hanno evidenziato non solo la capacità della tecnologia di stimolare la crescita economica, ma anche la capacità di svolgere molte

²⁴ «Amazon Killed an AI Recruitment System Because It Couldn't Stop the Tool from Discriminating Against Women», *Fortune*, consultato 19 marzo 2024, <https://fortune.com/2018/10/10/amazon-ai-recruitment-bias-women-sexist/>.

²⁵ R. Charli Carpenter, «“Women, Children and Other Vulnerable Groups”: Gender, Strategic Frames and the Protection of Civilians as a Transnational Issue», *International Studies Quarterly* 49, fasc. 2 (giugno 2005): p. 302-305, <https://doi.org/10.1111/j.0020-8833.2005.00346.x>.

²⁶ «The workplace of the future», *The Economist*, consultato 19 marzo 2024, <https://www.economist.com/leaders/2018/03/28/the-workplace-of-the-future#>.

delle funzioni che in precedenza richiedevano capitale umano. I sempre crescenti investimenti, e i conseguenti progressi, hanno condotto gli economisti a porsi le seguenti domande: (1) L'IA aumenta la produttività riducendo la quantità di lavoro necessaria per produrre beni? (2) L'IA toglie produce o riduce la disoccupazione? (3) L'IA porta ad un aumento della disuguaglianza? Alcune ricerche recenti suggeriscono che l'IA ha il potenziale per aumentare la crescita della produttività, ma può avere effetti ambigui sulla domanda di lavoro, in particolare nel breve periodo. Alcune occupazioni e settori industriali possono beneficiarne mentre altri sperimentano sconvolgimenti del mercato del lavoro.²⁷ Tutti i fattori appena menzionati producono implicazioni importanti all'interno delle analisi legate all'impatto che i sistemi intelligenti possono avere sul potere economico. Il mutamento dell'assetto economico globale in ambito di IA, influenzerebbe inevitabilmente, vista la stretta inter-correlazione tra le due sfere, il potere militare statale e, conseguentemente, potrebbe condurre ad una ridefinizione del c.d. bilanciamento di potere.

1.3 L'IA come variabile del *balance of power*

Il dibattito accademico relativo al rapporto tra intelligenza artificiale e relazioni internazionali è prettamente focalizzato sull'impatto che l'IA, così come i sistemi intelligenti economici e militari, stanno avendo o potrebbero avere sulla polarità del sistema internazionale. I casi studio selezionati, Cina e Stati Uniti, che verranno analizzati nei Capitoli II e III, sono strettamente collegati al dibattito incentrato sulla c.d. *great power competition*. La caduta dell'Unione sovietica nel 1991 segna, come poche altre date, un taglio netto nel tessuto storico delle relazioni internazionali. Utilizzando, forse impropriamente, la metafora dantesca, in quell'anno il mondo ha visto tramontare uno dei suoi "due Soli". Dal 1990, si è dunque affermata la teoria dell'unipolarismo che vedeva negli Stati Uniti l'egemone globale. Questa tendenza si è mantenuta stabile per circa venti

²⁷ Jason Furman e Robert Seamans, «AI and the Economy», *Innovation Policy and the Economy* 19 (gennaio 2019): 161–91, <https://doi.org/10.1086/699936>.

anni, fin quando, citando, il documento del 2012 *Global Trends 2030: Alternate Worlds* del National Intelligence Council, “*il movimento unipolare si è esaurito*”.²⁸

Waltz, in *Theory of International Politics*, identifica cinque parametri di analisi per la misurazione della potenza di uno Stato: (1) spesa militare; (2) dimensione economica; (3) estensione geografica; (4) risorse statali ed infine (5) la sua popolazione. L'esponentiale crescita economica e demografica della Repubblica Popolare Cinese e la crisi dei mercati finanziari del 2008, infatti, sono state recepite da *policy-maker*, analisti ed accademici, come due campanelli d'allarme per una possibile inversione, o alterazione, di polarità sistemica. Su questo filone si basano opere come *The Post-America World* di F. Zakaria, la cui idea di base non è tanto l'imminente declino degli Stati Uniti, quanto più l'ascesa di nuovi attori statali a livello internazionale. A Zakaria si aggiungono altri studiosi che sostengono, invece, il lento declino dell'unipolarità statunitense. La Repubblica Popolare Cinese, a seguito dell'apertura effettuata da Deng Xiaoping nel 1978, ha quadruplicato il proprio tasso di crescita economico attestandosi come seconda potenza economica globale e, nel 2008, come secondo paese per spesa militare. Secondo G. Geeraerts gli scenari globali possibili sono due: nel primo troviamo gli Stati Uniti e una sempre più potente Cina; nel secondo, invece, l'autore si concentra sui principali attori regionali e, in particolar modo, sui BRICS (Brasile, Russia, India, Cina, Sud Africa), il Giappone e sui paesi dell'Unione europea.²⁹

La corrente di un nuovo bipolarismo, o multipolarismo, è contestata da autori come Wohlforth e Brooks i quali sostengono che il concetto di “polarità” genera tre principali insidie nelle valutazioni dei cambiamenti di capacità in ambito statale-internazionale: (1) l'uso del concetto di polarità incoraggia il pensiero dicotomico (il mondo è unipolare o multipolare/bipolare?) alimentando un dibattito artificiale sul fatto che tutto stia cambiando o che nulla stia cambiando; (2) richiede misurazioni ampie e trans-storiche della distribuzione delle capacità che non riescono a cogliere cambiamenti

²⁸ National Intelligence Council (U.S.), a c. di, *Global Trends 2030: Alternative Worlds: A Publication of the National Intelligence Council* (December 2012: National Intelligence Council, 2012).

²⁹ Gustaaf Geeraerts, «China, the EU, and the New Multipolarity», *European Review* 19, fasc. 1 (febbraio 2011): 57–67, <https://doi.org/10.1017/S1062798710000335>.

cruciali nelle sorgenti del potere statale nel corso del tempo; (3) il concetto non è in grado di cogliere la relazione tra struttura e agenzia, ovvero, quanto è probabile che l'azione di uno Stato possa alterare il sistema.³⁰ Brooks e Wohlforth, nel rispondere alla domanda su quali capacità fanno di uno stato una superpotenza e, più in generale, come si dovrebbe misurare oggi la distribuzione del potere nel sistema, hanno individuato solo tre elementi, contro i cinque di Waltz, per la misurazione di potere statale “materiale”: la capacità militare, la capacità economica e quella tecnologica. L’interconnessione tra questi tre fattori è essenziale per l’incremento di potenza. La capacità economica, infatti, è condizione necessaria, ma non sufficiente, per la potenza militare di uno Stato. Al fattore economico va aggiunto il progresso tecnologico, specialmente visti i recenti sviluppi in ambito strategico.³¹

Sulla base della teoria dell’interconnessione dei fattori utilizzata da Brooks e Wohlforth è possibile analizzare le sfide che l’IA presenta al sistema internazionale. Se i progressi dell’IA possano avere un impatto sulla polarità del sistema dipende, fondamentalmente, dal contributo che l’IA apporta al potere militare ed economico relativo dei membri costitutivi di un dato sistema. Per poter raggiungere il rango di *AI great power*, traducibile come superpotenza intelligente, uno Stato deve saper sia sfruttare l’IA grezza (in inglese “*raw*”), intesa come grandi quantità di dati grezzi, sia possedere, in partenza, fattori politici e istituzionali adatti intesi come, ad esempio, le capacità economiche di sviluppo di software intelligenti o una partnership tra settore privato e pubblico per il raggiungimento di tale fine. Al momento, come anticipato prima, i principali attori nel panorama dell’IA sono gli Stati Uniti e la Cina, seguiti da Russia, Gran Bretagna, Francia e Israele.

All’interno delle sue analisi, Horowitz si interroga sull’impatto che l’IA potrebbe avere nel rafforzamento della distribuzione multipolare del potere di oggi.³² L’adozione

³⁰ Stephen G. Brooks e William C. Wohlforth, «The Rise and Fall of the Great Powers in the Twenty-first Century: China’s Rise and the Fate of America’s Global Position», *International Security* 40, fasc. 3 (2015): 8–9.

³¹ *Ivi*, p. 16.

³² Per questa sezione si vedano: Horowitz, Pindyck, e Mahoney, «AI, the International Balance of Power, and National Security Strategy»; Michael C. Horowitz, «Artificial Intelligence, International Competition, and the Balance of Power», *Texas National Security Review: Volume 1, Issue 3, The Scholar* (maggio 2018).

dell'IA nelle relazioni internazionali, in particolare nelle applicazioni militari, potrebbe incidere su due fattori chiave della teoria del bilanciamento del potere. *In primis*, l'intelligenza artificiale potrebbe cambiare la velocità e "l'orizzonte temporale" del ricambio di potere nel sistema internazionale. La teoria della trappola di Tucidide, elaborata da Graham T. Allison, analizza 16 casi di transizione egemonica degli ultimi 500 anni, appurando che, in 12 casi su 16, la rivalità tra l'egemone e la potenza *challenger* ha dato adito ad una guerra.³³ Le transizioni egemoniche conducono, tendenzialmente, a due scenari: il mantenimento dello *status quo* da parte dell'egemone o il cambiamento di polarità del sistema. Horowitz argomenta che l'adozione delle tecnologie dell'intelligenza artificiale potrebbe accelerare i tempi dei conflitti e aumentare gli incentivi di un c.d. *first-strike* in una situazione di crisi. Questo è dovuto agli effetti multipli, alcuni dei quali precedentemente esaminati, che tali applicazioni potrebbero produrre. L'incertezza riguardante gli impatti dell'IA sul potere militare ed economico solleva ulteriori questioni informative, complicando gli sforzi degli Stati nel valutare la propria posizione rispetto agli altri e nel reagire in modo razionale.

Il secondo punto sul quale si focalizza la ricerca di Horowitz riguarda l'impatto che l'IA, come qualsiasi altra innovazione tecnologica e della dottrina militare, può avere nella selezione e classificazione degli obiettivi statali da parte dei *policy-maker* nell'adozione delle strategie di sicurezza. Si prendano in considerazione i due approcci realisti di protezione dalle minacce. Gli Stati, infatti, possono bilanciare internamente, attraverso lo sviluppo e la costruzione di armi, o, secondo Waltz, esternamente, attraverso la formazione di nuove alleanze per contrastare gli attori minacciosi. L'IA, in relazione al bilanciamento esterno potrebbe, invece, determinare la continuità o i cambiamenti nelle alleanze mutando completamente la composizione delle coalizioni internazionali che competono a livello globale.³⁴

³³ Graham T. Allison, *Destined for war: can America and China escape Thucydides's trap?* (Boston: Houghton Mifflin Harcourt, 2017).

³⁴ Horowitz, Pindyck, e Mahoney, «AI, the International Balance of Power, and National Security Strategy».

Capitolo II

La grande scommessa: l'intelligenza artificiale negli Stati Uniti e in Cina

Come anticipato nel capitolo precedente, l'intelligenza artificiale rappresenta uno strumento alquanto importante per il futuro. Le sue applicazioni in ambito medico, sociale, economico e, più generalmente, quotidiano forniscono una piccola panoramica dell'effettivo potenziale che l'IA rappresenta per noi, e, ai fini di questa ricerca, per i principali attori dello scacchiere geopolitico. Il capitolo qui presentato sarà suddiviso in tre sezioni: (1) analisi del contesto cinese in materia di intelligenza artificiale; (2) relativa analisi per lo scenario statunitense; infine, (3) definizione dei metodi e della domanda di ricerca della tesi qui proposta.

2.1 Il “*leapfrog development*” cinese

Il paese del dragone rappresenta al momento il primo paese al mondo per brevetti IA e per investimento in capitale di rischio in ambito IA, mentre è al secondo posto per numero di compagnie e come polo di talenti in ambito IA.³⁵ Il *New Generation Artificial Intelligence Development Plan* (AIDP - (新一代人工智能发展规划), del 2017, e il *Made in China 2025* (中国制造2025), rilasciato nel 2015, rappresentano il fulcro su cui gira la strategia “intelligente” cinese. L'AIDP, che si prefigge di affrontare i problemi principali nella ricerca e nello sviluppo, di perseguire la produzione di sistemi intelligenti e di coltivare ed espandere l'industria IA fino a 1 trilione di Yuan cinesi (circa 150 miliardi di dollari), si apre, infatti, con una dichiarazione del pensiero governativo cinese:

³⁵ Gregory C. Allen, «Understanding China's AI Strategy - Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security», Center for a New American Security (CNAS), 6 febbraio 2019, <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>.

*AI has become a new focus of the international competition. AI is a strategic technology that will lead in the future; the world's major developed countries are taking the development of AI as a major strategy to enhance national competitiveness and protect national security.*³⁶

Nel 2014, il Politburo del PCC dedicò una sessione di analisi dei nuovi trend in ambito di sviluppo militare globale promuovendo l'innovazione militare. Secondo i vertici del partito, infatti, è in corso una “*new RMA*” (*new Revolution in Military Affairs*).

Xi Jinping, sempre nel 2014, richiamò la Cina a perseguire gli avanzamenti in materia di innovazione militare al fine di “*narrow the gap and achieve a new leapfrogging as quickly as possible*”.³⁷ Il termine “*leapfrog development*” descrive una tecnologia per la quale i paesi più arretrati possono saltare una fase di sviluppo, o una per la quale, essere indietro sulla generazione attuale di tecnologia, offre concretamente un vantaggio nell'adozione della prossima generazione.³⁸ La sessione del Politburo, dell'ottobre 2018, presieduta da Xi Jinping, ha nuovamente evidenziato i principali obiettivi cinesi in ambito IA già presentati nell'AIDP e nel documento *Made in China 2025*, per i quali la Cina dovrebbe “*raggiungere il livello di leader mondiale*”³⁹ in ambito di tecnologie a IA e ridurre la sua vulnerabilità “*alla dipendenza esterna per le tecnologie chiave e i sistemi avanzati*”.⁴⁰ A questo il premier cinese ha aggiunto che la Cina deve “*garantire che il nostro paese marci in prima fila nella ricerca teorica nell'importante*

³⁶ «*新一代人工智能发展规划 -Next Generation Artificial Intelligence Development Plan*», Pub. L. No. 国发〔2017〕35号, § 科技、教育\科技, 000014349/2017-00142 27 (2017), p. 2, <https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>.

³⁷ «Xi Jinping: cogliere con precisione la nuova tendenza dello sviluppo militare mondiale e tenere il passo con i tempi per promuovere vigorosamente l'innovazione militare - Xinhuanet», consultato 5 aprile 2024, http://www.xinhuanet.com/politics/2014-08/30/c_1112294869.htm.

³⁸ Allen, «*Understanding China's AI Strategy*», p. 8.

³⁹ *新一代人工智能发展规划 -Next Generation Artificial Intelligence Development Plan*, p. 2.

⁴⁰ Consiglio di stato cinese, «*Made in China 2025*», 7 luglio 2015; traduzione in inglese disponibile su <http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf>.

settore dell'IA, e occupi l'high ground sulle tecnologie IA fondamentali e critiche".⁴¹ Al positivismo della leadership cinese bisogna contrapporre, però, lo scetticismo di alcuni esponenti del partito comunista cinese, tra cui Fu Ying, vicepresidente del Comitato affari internazionali del Congresso nazionale del popolo, che già nel 2018 aveva manifestato alcune remore, supportate da sviluppatori e *policy-makers* cinesi, nei confronti dell'IA definendola come una "*minaccia per l'umanità*" e consigliando una azione cooperativa per prevenire questa possibilità.⁴² La Fu, inoltre, ha affermato che la Cina sarebbe interessata ad assumere il ruolo di sherpa per la creazione di norme internazionali per mitigare questo rischio. La dichiarazione risulta supportata dalla pubblicazione, sempre del 2018, dell'*Artificial Intelligence Security White Paper*, da parte di uno dei più influenti think tank governativi cinesi, la China Academy of Information and Communications Technology (CAICT), che richiama il proprio governo ad evitare una corsa agli armamenti intelligenti internazionale.⁴³ Anche il fondatore di Alibaba, durante il Davos World Economic Forum del 2019, ha espresso le proprie preoccupazioni per un'imminente guerra:

*The First World War was because of the first technology revolution. [...] The second technology revolution caused the Second World War. [...] This is the third technology revolution - we're coming.*⁴⁴

2.1.1 "Intelligentized" (智能化) warfare

Nonostante le remore mosse da alcuni membri del partito, la maggioranza della leadership cinese sostiene che l'aumento dell'uso dell'IA in ambito militare verrà inevitabilmente perseguito in modo aggressivo. Le riforme militari dell'Esercito Popolare di Liberazione

⁴¹ «Xi Jinping Calls for 'Healthy Development' of AI (Translation)», New America, consultato 22 marzo 2024; traduzione in inglese disponibile su <http://newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-calls-for-healthy-development-of-ai-translation/>.

⁴² Allen, «Understanding China's AI Strategy» p. 5.

⁴³ «CAICT - WHITE PAPER», consultato 22 marzo 2024; traduzione in inglese disponibile su http://www.caict.ac.cn/english/research/whitepapers/202205/t20220510_401132.html.

⁴⁴ Ryan Browne, «Alibaba's Jack Ma Suggests Technology Could Result in a New World War», CNBC, 23 gennaio 2019, <https://www.cnbc.com/2019/01/23/alibaba-jack-ma-suggests-technology-could-result-in-a-new-world-war.html>.

(PLA) del 2015 hanno dato il via al processo di rinnovamento, e aumento, delle capacità militari cinesi. Attraverso queste riforme, il PLA Strategic Support Force (PLASSF) ha consolidato le capacità militari del paese nei domini cyber, spaziale, elettronico e psicologico. Tra le riforme troviamo la fondazione della Central Military Commission (CMC) Science and the Technology Commission (S&TC) il cui tenente generale Liu Guozhi asserisce che il mondo è “*alla vigilia di una nuova rivoluzione scientifica e tecnologica*”, e stiamo “*entrando nell'era dell'intelligentizzazione*”. Egli ritiene che l'IA comporterà cambiamenti fondamentali nella programmazione delle unità militari, degli stili operativi, dei sistemi di equipaggiamento e dei modelli di generazione di energia da combattimento, anche favorendo una profonda rivoluzione militare.⁴⁵ I più alti livelli del PLA intendono, infatti, trarre vantaggio dalla trasformazione delle odierne forme informatizzate di guerra per sviluppare future guerre “intelligentizzate” (in inglese *intelligentized*, in cinese 智能化). Il Maggior Generale Ding Xiangrong, *Deputy Director* dell'Ufficio generale della CMC cinese, ha affermato, durante il Beijing Xiangshan Forum del 2018, che gli obiettivi militari cinesi prevedono una chiusura della forbice tra gli assetti militari cinesi e le potenze globali più avanzate avvalendosi della “*nuova rivoluzione militare*” centrata sull'informazione tecnologica e sui sistemi intelligenti.⁴⁶ L'AIDP, infatti, prevede una promozione, da parte del governo cinese, di tutte le tipologie di sistemi intelligenti al fine di implementarle nell'ambito della difesa nazionale. Sistemi a IA sono già ampiamente utilizzati dal governo cinese per monitorare e sorvegliare alcune regioni del proprio paese, come nel caso dei prodotti sviluppati dall'azienda SenseTime utilizzati nella provincia autonoma dello Xinjiang, località in cui è presente la minoranza etnico-religiosa turco-musulmana degli Uiguri, soggetta a continue persecuzioni.⁴⁷ Il generale Ning del Chinese People's Armed Police Force ha

⁴⁵ «AlphaGo and Beyond: The Chinese Military Looks to Future “Intelligentized” Warfare», Default, consultato 3 aprile 2024, <https://www.lawfaremedia.org/article/alphago-and-beyond-chinese-military-looks-future-intelligentized-warfare.a>

⁴⁶ Allen, «Understanding China's AI Strategy».

⁴⁷ «Break Their Lineage, Break Their Roots», *Human Rights Watch*, 19 aprile 2021, <https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting>.

affermato che l'utilizzo dell'IA, attraverso sistemi di riconoscimento facciale, nella provincia, è necessario al fine di prevenire atti terroristici.⁴⁸

Altri dati a supporto dell'incremento dell'attenzione da parte della Cina all'IA è il cambiamento avvenuto nell'ambito dell'Academy of Military Science (AMS) del PLA. Tradizionalmente, l'AMS era responsabile della formulazione della strategia e della dottrina del PLA. Ad oggi, invece, sembra aver assunto un ruolo cruciale anche nell'ambito della teoria dell'innovazione militare cinese, istituendo il National Innovation Institute of Defence Technology (NIIDT) a cui si aggiungono due centri di ricerca focalizzati nello studio dell'uso militare dell'IA e tecnologie relative, l'Unmanned System Research Centre (USRC), l'Artificial Intelligence Research Centre (AIRC) e un polo scientifico, istituito della National University of Defence Technology (NUDT) del PLA, concentrato sullo studio dell'automazione di robot intelligenti, bionici e dello *swarm intelligence* (letteralmente, intelligenza di sciame).⁴⁹

Il concetto di “intelligentizzazione” (智能化), secondo la Dott.ssa E. Kania, comporta, quindi, lo sviluppo e l'operatività dell'intelligenza artificiale e l'abilitazione di tecnologie interconnesse necessarie per la sua realizzazione con fini militari. L'“intelligentizzazione” si basa sulle fasi precedenti della meccanizzazione e dell'informatizzazione, i processi attraverso i quali il PLA ha introdotto la tecnologia dell'informazione e ha intrapreso lo sviluppo delle sue capacità di C4ISR (comando, controllo, comunicazione, computer, intelligence, sorveglianza e ricognizione).⁵⁰ Questo determina che il concetto di “intelligentizzazione” militare non riguarda solo l'IA, ma, piuttosto, si riferisce alla descrizione operativa complessiva dei sistemi di forza costituiti da individui, armamenti, attrezzature, e modalità di combattimento. Il processo messo in atto dalla Cina non consiste solo in armamenti intelligenti ma anche in nuovo “sistema di

⁴⁸ Generale Wang Ning, *Global Terrorism: Threats and Countermeasures*, 8ª edizione del Beijing Xiangshan Forum, 5 ottobre 2018.

⁴⁹ Elsa B. Kania, «Artificial Intelligence in China's Revolution in Military Affairs», *Journal of Strategic Studies* 44, fasc. 4 (7 giugno 2021): 515–42, <https://doi.org/10.1080/01402390.2021.1894136>.

⁵⁰ *Ibidem*.

sistemi” militare che coinvolge l'integrazione uomo-macchina, con l'IA in una posizione dominante.

2.1.2 L'integrazione civile-militare nel dominio dell'IA

Tra i punti menzionati nell'AIDP e nel *The Science of Military Strategy* (战略学), principale documento della dottrina militare cinese nella versione rivisitata del 2020, ai fini di questa ricerca può essere utile analizzare il rafforzamento dell'integrazione militare-civile nel dominio dell'IA. L'AIDP discute, in particolar modo, l'attuazione di una strategia di fusione militare-civile (军民融合) integrando l'utilizzo delle più recenti scoperte in ambito IA, da parte di privati, in applicazioni militari che includono *command decision-making*, deduzioni militari (ad esempio, il *wargaming*), e attrezzature di difesa.⁵¹ Anche il *The Science of Military Strategy*, infatti, sostiene che l'interdipendenza tra i settori economico-sociale e militare sia di vitale importanza per lo sviluppo di una modernizzazione della sicurezza nazionale e degli apparati militari. A riprova del fatto che l'industria dell'IA si stia spostando a favore del settore privato, il PLA ritiene necessario sfruttare gli avanzamenti del settore privato in ambito IA per scopi militari.

A tal fine, la leadership cinese ha sviluppato una strategia nazionale di fusione militare-civile. L'AIDP sottolinea, inoltre, la necessità di continuare a stabilizzare e normalizzare i meccanismi di comunicazione e coordinamento tra gli istituti di ricerca scientifica, le università, le imprese e le unità dell'industria militare, cercando di garantire che le risorse di innovazione militari e civili siano “costruiti insieme e condivisi”.⁵² L'agenda strategica, data la direzione del Military-Civil Fusion Development Commission del Partito Comunista Cinese (中央军民融合发展委员会), risulta essere una questione ad alto livello di priorità nelle politiche del paese. La Commissione, fondata

⁵¹ 新一代人工智能发展规划 -Next Generation Artificial Intelligence Development Plan, p. 21.

⁵² Elsa B. Kania, «Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power», 28 novembre 2017, <https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>.

nel 2017, è, infatti, sotto la guida diretta di Xi Jinping. Analogamente al funzionamento del DARPA statunitense, la CMC del PLA, attraverso la CMC S&TC e il CMC Military and Scientific Research Guidance Committee (军委军事科学研究指导委员会), eserciterà i più alti compiti di coordinamento per l'R&D dell'agenda strategica della fusione militare-civile. In aggiunta, nel 2017, il Ministero della Scienza e della Tecnologia cinese, congiuntamente con la CMC S&TC, ha sviluppato il tredicesimo piano quinquennale speciale per la fusione militare-civile in ambito di scienze e tecnologie. La formazione di un organo di coordinamento, insieme alla redazione di un piano speciale per lo sviluppo tecnologico, fa intendere l'importanza strategica dell'attuazione di un sistema centrale integrato per il duplice utilizzo delle tecnologie IA.⁵³ Un esempio della collaborazione tra il settore privato e quello statale cinese è la licenza di partenariato fornita dal PLA alla iFlytek, start-up cinese focalizzata sul riconoscimento vocale intelligente.⁵⁴

2.1.3 Strumentalizzazione dell'IA nell'Asia centrale

L'Asia Centrale è caratterizzata da una forte presenza di materie prime quali petrolio, gas e minerali, che rappresentano circa il 50% delle esportazioni della regione.⁵⁵ In particolar modo, la regione detiene il 38,6% delle riserve mondiali di minerale di manganese, il 30,07% di cromo, il 20% di piombo, il 12,6% di zinco, l'8,7% di titanio.⁵⁶ Il Kazakistan, in particolar modo, rappresenta il principale competitor della Cina nella produzione di elementi di terre rare. Alle potenzialità geo-strategiche della regione si aggiunge una seconda variabile non indifferente per la Cina: l'istituzione della piattaforma diplomatica C5+1 nel 2015, infatti, ha garantito agli Stati Uniti una presenza sul territorio. L'approccio del governo degli Stati Uniti nell'Asia centrale, che coinvolge

⁵³ *Ibid*,

⁵⁴ Per un'analisi più dettagliata del fenomeno della fusione militare civile si veda: Kania, «Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power».

⁵⁵ Filippo Buranelli Costa, «Asia Centrale: tra grandi potenze e regionalismo», *ISPI* (blog), s.d., <https://www.ispionline.it/it/pubblicazione/asia-centrale-tra-grandi-potenze-e-regionalismo-131021>.

⁵⁶ «Central Asia's Critical Raw Materials: The Next Frontier in Global Power Rivalry?», *CABAR.Asia* (blog), 3 aprile 2024, <https://cabar.asia/en/central-asia-s-critical-raw-materials-the-next-frontier-in-global-power-rivalry>.

congiuntamente tutti e cinque i governi della regione (Kazakistan, Repubblica del Kirghizistan, Tagikistan, Turkmenistan e Uzbekistan) ha l'obiettivo di migliorare la cooperazione con e tra i paesi dell'Asia centrale (C5) per promuovere l'ideale di un'Asia centrale indipendente, prospera e sicura in partenariato con gli Stati Uniti. Le problematiche legate all'accesso alle risorse minerarie, divenute cruciali anche per le politiche di transizione energetiche, e all'instabilità regionale, causata dalle crescenti pressioni esercitate da Washington, sono entrambe questioni di rilevante importanza per la Repubblica Popolare nel quadro della realizzazione della Belt and Road Initiative (BRI). Bisogna inoltre ricordare che i minerali sopra citati sono divenuti essenziali per la realizzazione e fabbricazione di microchip e sistemi computerizzati. Come precedentemente analizzato, le politiche di sviluppo tecnologico sono un punto cardine nella strategia cinese. L'utilizzo di tecnologie che sfruttano algoritmi di intelligenza artificiale o di *machine learning*, infatti, rappresenta per la Cina un vantaggio a livello non solo a livello economico, ma anche politico e militare.

La massiccia presenza cinese in Asia Centrale, con esercitazioni congiunte, addestramenti di personale militare e con la costruzione di infrastrutture militari le ha permesso di aumentare il volume di scambi di armamenti nella regione. Se tra il 2010 e il 2014, l'1,5% delle importazioni militari dell'Asia centrale provenivano dalla Cina, tra il 2016 e il 2021 questa proporzione è cresciuta fino al 18%, garantendo alla Cina un mercato stabile per droni armati, apparecchiature di comunicazione e UAV.⁵⁷ Per quanto concerne, invece, l'aspetto economico, le tecnologie intelligenti costituiscono uno dei settori cruciali per l'economia domestica cinese, e per il progetto della BRI. Nel 2020, la misura dell'industria IA cinese ha raggiunto i 43.4 miliardi di dollari con una crescita del 15%. Con la pubblicazione dell'AIDP, compagnie come Baidu, Alibaba e ByteDance hanno incrementato in modo massiccio la ricerca in ambito IA.⁵⁸ Con l'aumento della competizione globale in ambito IA, le tecnologie intelligenti forniscono una grande opportunità per i giganti tecnologici cinesi, non solo in ottica di mercato domestico ma anche per la realizzazione della Digital Silk Road (DSR), componente digitale della BRI

⁵⁷ LTC Andrea Zanini, «China's New Military Posture in Central Asia», 2022.

⁵⁸ «China's AI industry scale exceeds 40 bln USD in 2020 - Xinhua | English.news.cn», consultato 29 marzo 2024, http://www.xinhuanet.com/english/2021-07/09/c_1310052462.htm.

che, attraverso la connettività digitale e l'applicazione di tecnologie smart, promuove lo sviluppo del progetto cinese delle *Safe/Smart City*⁵⁹ nell'Asia centrale. Partendo, nel 2003, da Pechino, Jinan, Hangzhou e Suzhou il *Safe Cities Project* aveva inizialmente lo scopo di favorire i bisogni dei consumatori e della forza lavoro, migrata nelle grandi città a seguito del progresso di urbanizzazione cinese. Il secondo step prevedeva la costruzione di città "sicure"/"intelligenti" nell'Asia centrale per diffondere le c.d. Chinese Information and Communication Technologies (ICT) nella regione. La massiccia esportazione di tecnologie smart, come il 5G, in Asia centrale ha creato le condizioni per l'incremento, strumentale, di progetti di cooperazione nell'ambito dell'economia digitale, dell'e-commerce e per espandere la presenza dell'IA in tutta la regione. Nel contesto del DSR, il lancio dello *Smart Cities Project* ha giocato un ruolo strategico nell'aggiungere maggiore valore alla leva della Cina sull'Asia centrale. In un'atmosfera di crescente sorveglianza, ci sono buone ragioni per affermare che l'investimento massiccio della Cina in questo progetto può servire a modificare le dinamiche geopolitiche della regione, sia attraverso la crescente dipendenza dalle tecnologie cinesi, sia per la sua crescente potenza intelligente nella regione. Alcuni esperti sostengono che la promozione di tecnologie IA, per la raccolta di dati all'interno delle città smart, può causare tre principali problemi: (1) l'abilità di un governo autoritario di monitorare costantemente la popolazione può sfociare in un "totalitarismo digitale"; (2) l'uso di tecnologie cinese accresce il rischio di accesso a dati sensibili da parte delle compagnie cinese e dello stesso governo; (3) l'uso di queste tecnologie crea una vulnerabilità per queste città, permettendo alle aziende cinesi di causare uno *shut down* ai principali servizi cittadini.⁶⁰ Il ruolo della Cina come principale fornitore di meccanismi digitali per la sorveglianza solleva soprattutto critiche sulla questione dell'esportazione dell'autoritarismo digitale. Attraverso politiche di *delinking* tra il commercio e i diritti umani, la politica di esportazione digitale della Cina,

⁵⁹ I termini "*Smart City*" e "*Safe City*" vengono usati in modo intercambiabile nella letteratura cinese. La distinzione tra città "sicure" e "intelligenti" non è chiara. Mentre le città sicure mirano principalmente a migliorare la sicurezza pubblica attraverso l'uso di telecamere e tecnologie digitali per monitorare e ispezionare comportamento sospetto, la tecnologia *Smart City* è per lo più attribuito ad automatizzare le funzioni comunali come il controllo del traffico, la raccolta dei rifiuti, la distribuzione di energia e i sistemi idrici, insieme alla videosorveglianza. Si veda anche: Helen Warrell et al., «Exporting Chinese surveillance: the security risks of 'smart cities'», *Financial Times*, 9 giugno 2021, sez. The Big Read, <https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab>.

⁶⁰ *Ibidem*.

non solo contribuisce a rafforzare il controllo dei regimi autoritari nella regione, ma rafforza anche la crescente dipendenza dalle tecnologie cinesi per la sopravvivenza di questi regimi. L'autoritarismo cinese sul controllo delle informazioni si manifesta anche nella corsa per le tecnologie future come i *chatbot AI*. Nel tentativo di sviluppare strumenti di AI simili a ChatGPT, Alibaba ha recentemente rilasciato la sua *chatbot* Tongyi Qianmen AI. A seguito del lancio di quest'ultimo, la Cyber Administration cinese ha rapidamente pubblicato alcune regole relative al funzionamento di queste tecnologie, tra cui il *range* di contenuti generabili permessi dal governo.⁶¹

2.2 “Think different”: gli Stati Uniti leader del settore?

Gli Stati Uniti rappresentano la principale potenza militare e tecnologica del mondo. Nell'ultimo decennio, l'attenzione della potenza egemone globale si è focalizzata sull'IA, considerata interesse vitale e meccanismo di assicurazione di potere militare ed economico. Con la pubblicazione, nel 2018, della *U.S. Department of Defence (DoD) Artificial Intelligence Strategy*, il governo statunitense ha ufficialmente formalizzato la definizione di IA nell'ambito della difesa americana. L'IA è quindi definita come “*the ability of machine to perform tasks that normally require human intelligence*”.⁶² L'investimento statunitense militare in Research & Development (R&D), in ambito di applicazioni di difesa IA, ha registrato un repentino e significativo aumento. Dei 773 miliardi di dollari richiesti dall'amministrazione Biden per il budget del Pentagono, per il *fiscal year* 2023, 130.1 miliardi sono stati designati al R&D di tecnologie emergenti, tra cui l'IA.

2.2.1 *Deep Green Concept: un simulatore militare predittivo ante litteram*

Il progetto Deep Green può essere quasi considerato un precursore dei più recenti algoritmi di ML e IA predittivi. Lanciato agli inizi degli anni 2000 dal DARPA,

⁶¹ Övgü Kalkan Küçüksolak e Tuba Firat, «The Geopolitics of Artificial Intelligence in Central Asia: Russian and Chinese Cases», *Güvenlik Bilimleri Dergisi* 12, fasc. 1 (31 maggio 2023): 25–44, <https://doi.org/10.28956/gbd.1249381>.

⁶² R Alan Blackburn, «Summary of the 2018 Department of Defense Artificial Intelligence Strategy», 2018.

rappresenta un approccio innovativo attraverso l'utilizzo di simulazioni a supporto di operazioni militari in corso, proponendosi di analizzare scenari operativi futuri. Partendo dal supercomputer IBM Deep Blue, il Deep Green è stato ideato dal DARPA per essere una tecnologia di direzione di comando. I tre obiettivi del progetto sono: (1) generare e analizzare le opzioni rapidamente, tra cui l'elaborazione di molteplici futuri possibili che possono derivare da una combinazione di "amichevole", "nemico", e altre linee di azione; (2) utilizzare le informazioni dell'operazione in corso per valutare quali scenari prossimi stanno diventando più probabili; infine, (3) prendere decisioni consapevoli degli effetti di secondo e terzo ordine di tali decisioni. L'utilizzo di questa piattaforma permette ai decisori di non rimanere a corto di opzioni, mantenendo il nemico all'interno del "ciclo decisionale". Il Deep Green, inoltre, fornisce un nuovo approccio nei confronti della precedente strategia statunitense dell'*Observe-Orient-Decide-Act* (OODA) (fig. 3).⁶³ Il programma si articola su due concetti principali: pianificazione anticipata ed esecuzione adattiva. Per quanto riguarda la pianificazione anticipata può essere descritta come il riadattamento preventivo ad una determinata situazione; l'esecuzione adattiva, invece, può essere ricondotta al concetto dell'associazione tardiva utilizzato dai sistemi IA, la quale permette ai software di prendere decisioni all'ultimo momento in modo da mantenere un ampio margine di flessibilità all'adattamento delle "traiettorie" operazionali.



Fig. 3. Fonte: John Surdu e Kevin Kittka, «The Deep Green concept», 2008.

⁶³ John Surdu e Kevin Kittka, «The Deep Green concept», 2008, 623–31.

2.2.2 *Third Offset Strategy*

La ricerca in campo IA è sempre stata finanziata, da prima della coniazione del termine nel 1956, da organizzazioni quali l'Office of Naval Research (ONR) e l'Advanced Research Projects Agency (ARPA), ora DARPA. Lo scopo di questi investimenti era, per la U.S. Navy, di sviluppare un software in grado di tradurre automaticamente dal russo all'inglese durante la Guerra fredda. I risultati sperati però non furono mai raggiunti. Alcuni si riferiscono a questo periodo come al "*first AI Winter*". Negli '80, però, il DARPA investì 1 miliardo di dollari in iniziative di strategie computerizzate con l'obiettivo di aiutare gli Stati Uniti ad eguagliare potenze informatiche come il Giappone.⁶⁴ Solo nel 2014, tuttavia, l'IA è divenuta una priorità per la sicurezza nazionale statunitense con la pubblicazione da parte del DoD della Third Offset Strategy, con lo scopo "*to draw U.S. advanced technologies to offset China's and Russia's technological advances*".⁶⁵ A seguito delle rivendicazioni territoriali da parte del PLA nel Mar cinese meridionale, e l'incremento della spesa in modernizzazione militare portata avanti dalla Cina, l'amministrazione Obama ammise pubblicamente i potenziali rischi di una rapida ascesa cinese. Nel novembre 2014, infatti, fu rilasciato un memorandum ufficiale per annunciare la creazione della Defence Innovation Initiative (DII), denominazione che verrà poi sostituita da quella ufficiale della Third Offset. La Third Offset Strategy (TOS) fa riferimento all'iniziativa statunitensi precedenti della c.d. First Offset, utilizzata dagli Stati Uniti durante la Guerra fredda per compensare, a livello tattico e strategico-nucleare, i vantaggi quantitativi del blocco sovietico, e della c.d. Second Offsett con cui gli US cercarono di eguagliare la superiorità numerica dei membri del Patto di Varsavia, soprattutto in vista di un'ipotetica "seconda invasione". La TOS, ancora una volta, si basa sulla compensazione delle capacità, questa volta tecnologiche, sviluppate da Cina e Russia, facendo menzione esplicita all'IA, al ML e ai veicoli autonomi. Tra gli obiettivi della TOS troviamo infatti: (1) il contenimento delle misure *anti-access/area denial* messe in atto dalla Cina e dalla Russia per le nuove tecnologie, in modo da proiettare le forze su minacce realistiche; (2) il riallineamento del rapporto tra il DoD e l'industria

⁶⁴ Lauren A Kahn, «Defense AI in the United States», DAIO Study, 23|07 (2023).

⁶⁵ Gian Gentile, Michael Shurkin, Alexandra T. Evans, Michelle Gris , Mark Hvizda, Rebecca Jensen, *A History of the Third Offset, 2014-2018* (RAND Corporation, 2021), <https://doi.org/10.7249/RRA454-1>.

statunitense con un focus, in ambito tecnologico, sulla Silicon Valley; (3) il cambiamento dell'approccio in termini di processi acquisitivi delle nuove tecnologie; (4) in ultimo, la diffusione della promozione dei valori della TOS attraverso due istituzioni, fondate dall'ex Deputy Secretary of Defense Robert O. Work, nonché ideatore della TOS, ovvero l'Advanced Capabilities and Deterrence Panel (ACDP) e il c.d. Breakfast Club. Il ruolo della TOS, e il lavoro di Work, hanno rappresentato un enorme passo avanti nella ridefinizione delle politiche di difesa statunitensi. La strategia ha rimodellato il pensiero del Pentagono in un'ottica più futuristica, ponendo le basi per i progetti futuri del DoD.⁶⁶

2.2.3 Lo sviluppo di una difesa “intelligente”

La pubblicazione, nel 2018, della prima strategia “intelligente” aveva l'obiettivo di assicurare al governo statunitense un vantaggio e una competitività militare maggiore rispetto a Cina e Russia, già avanti nell'investimento in sistemi IA. La strategia accompagnava la creazione del Joint Artificial Intelligence Center (JAIC), struttura con il compito di eseguire la visione del DoD e “*synchronize DoD AI activities to expand Joint Force advantages*”.⁶⁷ LA U.S. DoD AI Strategy si fonda su cinque pilastri: (1) consegnare capacità “intelligenti” in funzione delle missioni chiave; (2) ridimensionare l'impatto dell'IA sul DoD attraverso fondamenti comuni che possano garantire uno sviluppo e una sperimentazione decentralizzata; (3) coltivare una forza lavoro leader in ambito IA; (4) coinvolgere partner e alleati commerciali e accademici internazionali; (5) sviluppare un'etica militare e una sicurezza “intelligente” vincente.⁶⁸

Nel 2022, la strategia IA statunitense è stata aggiornata per far fronte ai progressi cinesi in materia di tecnologie avanzate, computer quantici e IA. Nell'ottica di uno scontro diretto con la Cina, il DoD ha modernizzato la propria strategia. Nel giugno 2022, l'ufficio del Chief Digital and AI Officer ha pubblicato la *Responsible Artificial Intelligence (RAI) Strategy and Implementation Pathway (RAI S&IPathway)*, documento che enfatizza la necessità per gli Stati Uniti di sviluppare una strategia di difesa in ambito

⁶⁶ Per un'analisi più dettagliata dell'argomento si rimanda a: G. Gentile et al., *A History of the Third Offset, 2014-2018*.

⁶⁷ *Ivi*, p. 9.

⁶⁸ *Ivi*, pp. 7-8.

IA responsabile. Il RAI S&IPathway descrive l'IA come efficace in quanto “*consistent with our national values, shared democratic ideals, and [...] military’s steadfast commitment to lawful and ethical behavior*”.⁶⁹ Il documento si basa su sei principi: (1) RAI *Governance*, il processo di modernizzazione delle strutture governative e dei processi burocratici; (2) *Warfighter Trust*, processo di standardizzazione della familiarità tecnologica e del profitto per operatori di sistemi IA; (3) ciclo vitale della produzione e dell’acquisizione di prodotti IA, in modo da garantire un equilibrio tra sicurezza e l’aumento di velocità dello sviluppo di capacità intelligenti; (4) validazione dei requisiti, per assicurare che le capacità IA incontrino i bisogni operativi; (5) ecosistema intelligente responsabile, per promuovere una comprensione condivisa, con partner domestici ed internazionali, per lo sviluppo di sistemi IA; (6) *AI workforce*, al fine di promuovere l’educazione e le capacità in ambito IA.⁷⁰

Come è possibile notare dal grafico sottostante (fig. 4), il report del Defense AI Observatory (DAIO) alla Helmut Schmidt University⁷¹ individua tre periodi distintivi, nell’ambito del progresso IA fatto dalle organizzazioni militari americane, principalmente suddivisi sulla base di come la difesa IA è stata organizzata dal DoD. Le tre “ere” sono: (1) la Project Maven Era, tra il 2017 e il 2018; (2) la JAIC Era, tra il 2018 e il 2022; (3) e, infine, la CDAO Era, che inizia nel 2022 ed è ancora in corso.

⁶⁹ DoD Responsible AI Working Council, «U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway» (2022), <https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF>.

⁷⁰ *Ivi*, p. 2.

⁷¹ Kahn, «Defense AI in the United States».

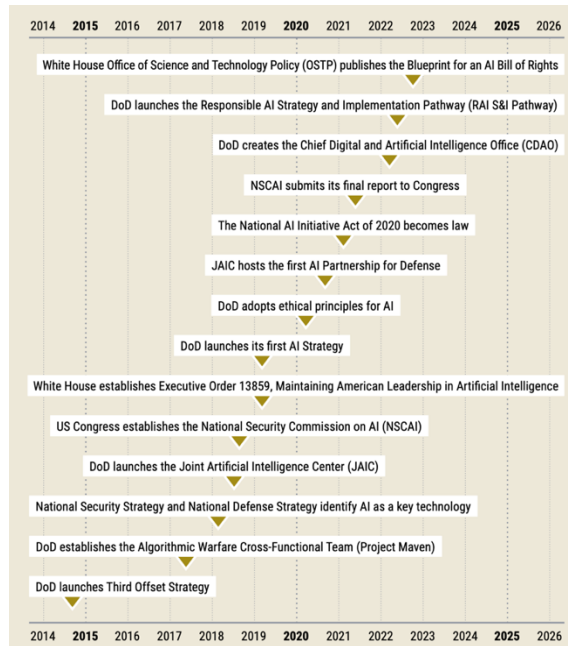


Fig. 4. Fonte: Lauren A Kahn, «Defense AI in the United States», DAIO Study, 23|07 (2023).

2.2.3.1 L'era del Project Maven (2017-2018)

Il Project Maven, fondato nel 2017 come *Algorithmic Warfare Cross-Functional Team*, è considerato il primo vero approccio dell'uso dell'IA per scopi difensivi negli Stati Uniti. Come detto precedentemente (Cap. I) l'algoritmo Maven si basa sull'automazione, totale o parziale, del processo di individuazione e classificazione di obiettivi nemici attraverso l'analisi dei video ottenuti dagli *uncrewed aerial systems* (UAS). G. C. Allen sostiene che il successo conseguito dal Project Maven si basa sulla struttura organizzativa di base utilizzata durante lo sviluppo:

*[...] a small, operationally focused, cross-functional team that was empowered to develop external partnerships, leverage existing infrastructure and platform, and engage with user communities iteratively during development.*⁷²

⁷² Allen, «Project Maven Brings AI to the Fight against ISIS».

2.2.3.2 L'era del Joint Artificial Intelligence Center (2018-2022)

Sulla scia del successo del Project Maven, nel 2018, il DoD ha istituito il JAIC, definito come il l'hub centrale del Dipartimento in materia di IA per *“seize upon the transformative potential of Artificial Intelligence technology for the benefit of America’s national security”*⁷³. Il lancio del JAIC ha provocato, negli Stati Uniti, un effetto a cascata favorendo la formazione della National Security Commission on Artificial Intelligence (NSCAI) da parte del Congresso, l’emanazione da parte della casa dell’*Executive Order 13589 on Maintaining American Leadership in AI*, la pubblicazione, come già accennato sopra, della prima strategia IA, e il rilascio da parte del DoD del primo set di principi etici guida per la difesa IA. Inoltre, Il JAIC ha fornito le basi per un riconoscimento universale sul territorio americano dell’importanza cruciale che l’IA potrebbe avere in futuro per la sicurezza nazionale americana; infatti, il JAIC *“made headway on AI adoption and data literacy, with initiatives like “AI 101”, and on the data integration issue, as part of the Artificial Intelligence and Data Initiative (AIDA)”*.⁷⁴

2.2.3.3 L'era del Chief Digital and Artificial Intelligence Office (2022-presente)

Il CDAO, fondato dal Pentagono, nasce con lo scopo di riorganizzare, a livello burocratico e infrastrutturale, tutta la dottrina di difesa intelligente. Il Chief Digital and Artificial Intelligence Office, infatti, ha comportato due principali cambiamenti: (1) il CDAO ha raggruppato il JAIC, il Defense Digital Service (DDS) e l’ufficio del Chief Data Officer (CDO) in un’ottica centralizzata o, utilizzando le parole dalla Deputy Defense Secretary Kathleen Hicks, *“make a drastic move from a hardware-centric to a software-centric enterprise”*; (2) il CDAO ha riassegnato il monitoraggio del Project Maven dal Office of the Under Secretary of Defense for Intelligence and Security al National Geospatial Intelligence Agency con l’obiettivo di supportare la spinta propulsiva

⁷³ Kahn, «Defense AI in the United States».

⁷⁴ Michael C. Horowitz e Lauren A. Kahn, «Why DoD’s New Approach to Data and Artificial Intelligence Should Enhance National Defense», Council on Foreign Relations, s.d., <https://www.cfr.org/blog/why-dods-new-approach-data-and-artificial-intelligence-should-enhance-national-defense>.

del Defense Department per studiare, testare e applicare al meglio IA sul campo di battaglia e “*behind the scenes*”.⁷⁵

2.2.4 Il framework NATO

Per quanto concerne la NATO, il report *2020-2040 S&T* del 2020, redatto dal NATO Science & Technology Organization (S&TO), l’Organizzazione del Trattato Nord-Atlantico adotta, per la prima volta, la definizione di IA, già utilizzata dalla U.S. DoD AI Strategy del 2019. Come constatato dal report, l’IA “*has the potential for revolutionary impact on NATO operations and capabilities*” descrivendo l’IA come “*a fulcrum around which big data will be turned into actionable knowledge, and, ultimately, a NATO decision advantage*”.⁷⁶

Nell’individuare le priorità per l’adozione di sistemi IA E. H. Christie identifica quattro aree di cui gli alleati dovrebbero tener conto: (1) sviluppo interattivo; (2) accesso al capitale umano; (3) accesso ai dati; (4) coinvolgimento con le istituzioni tecnologiche civili per un supporto innovativo dei meccanismi IA.⁷⁷

2.3 Metodologia e domanda di ricerca

Nel capitolo successivo verranno analizzati nel dettaglio i principali documenti in ambito IA dei casi studio proposti, in particolar modo l’AIDP e la *National Security Strategy* americana del 2022. L’obiettivo di questa ricerca è di analizzare il rapporto tra IA e ML, in ottica militare e difensiva, nell’ambito delle NSP e delle NSS. Il Capitolo III sarà quindi strutturato in questo modo: (1) analisi dettagliata dell’*Artificial Intelligence Development*

⁷⁵ Colin Demarest, «Pentagon’s Project Maven Transition Stymied by Congress, Official Says», C4ISRNet, 26 ottobre 2022, <https://www.c4isrnet.com/artificial-intelligence/2022/10/26/pentagons-project-maven-transition-stymied-by-congress-official-says/>.

⁷⁶ NATO Science & Technology Organization, «Science & technology trends 2020-2040: exploring the S&T edge», 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

⁷⁷ Edward H. Christie, «The NATO alliance and the challenges of Artificial intelligence adoption». In Sonia Lucarelli, Alessandro Marrone, e Francesco N Moro, «NATO Decision-Making in the Age of Big Data and Artificial Intelligence», s.d.

Plan cinese e documenti correlati alla definizione della NSP cinese in materia di sistemi intelligenti; (2) analisi delle *National Security Strategy* dell'amministrazione Biden del 2022, con un'analisi comparata focalizzata sulla rilevanza accordata all'IA all'interno della *National Security Strategy* di Trump del 2017 e, infine del *National Artificial Intelligence Research and Development Strategic Plan* aggiornato al 2023; (3) confronto qualitativo tra la *policy* cinese e quella americana.

Capitolo III

Politiche e strategie di sicurezza nazionale “intelligenti”

3.1 Caso Studio I: la Repubblica Popolare Cinese

Il primo paragrafo del Capitolo III, come precedentemente annunciato, è dedicato ai documenti in materia di *national security strategy* cinesi, tra cui il già citato *Next Generation Artificial Intelligence Development Plan* (新一代人工智能发展规划), documento pubblicato il 20 luglio 2017 dal Consiglio di Stato cinese, e la sezione dedicata all'IA nel testo di riferimento della dottrina militare cinese, *The Science of Military Strategy* (战略学).

3.1.1 *Il Next Generation Artificial Intelligence Development Plan*

Il *Next Generation Artificial Intelligence Development Plan*, documento pubblicato il 20 luglio 2017 dal Consiglio di Stato cinese, definisce l'approccio di alto livello del paese nello sviluppo delle tecnologie e delle applicazioni dell'intelligenza artificiale, si compone di sei sezioni: (1) situazione strategica; (2) requisiti generali; (3) *focus tasks*; (4) allocazione delle risorse; (5) misure di garanzia ed infine, (6) organizzazione e implementazione.

Come accennato nel Capitolo II, paragrafo 1, nell'analizzare la situazione strategica attuale il Consiglio di Stato cinese identifica l'IA come una variabile essenziale per il futuro del paese. Basandosi sull'esperienza pregressa dell'internet mobile, dei big data, di super computer e altri, il governo cinese sottolinea come le principali innovazioni tecnologiche degli ultimi 60 anni si sono basate sull'“*impulso congiunto di potenti*

esigenze di sviluppo economico e sociale".⁷⁸ Per il Consiglio di Stato cinese, lo sviluppo di una nuova generazione di IA e discipline correlate, la modellazione teorica, l'innovazione tecnologica e gli aggiornamenti hardware e software, in anticipo rispetto ai propri competitors, promuoveranno l'ascesa dei domini economici e sociali dalla digitalizzazione e dalla "networkizzazione" all'"intelligentizzazione".⁷⁹ Da come si evince dal capitolo, la situazione "complessa" della sicurezza nazionale e della competizione internazionale sta spingendo la Cina ad ampliare i propri orizzonti al fine di realizzare un piano di sviluppo dell'IA a livello strategico nazionale e cogliere con fermezza l'iniziativa strategica nella nuova fase della concorrenza internazionale nello sviluppo dell'IA, per creare un vantaggio competitivo e per proteggere efficacemente la sicurezza nazionale. Centrale è anche la visione dell'IA come un nuovo motore per lo sviluppo economico e il *main driver* della prossima rivoluzione industriale. La Cina, infatti, ambisce ad accelerare rapidamente l'applicazione dell'IA in ambito economico, coltivando ed espandendo l'industria intelligente con l'obiettivo di "iniettare" una nuova energia cinetica nello sviluppo economico del paese. Nel documento, oltre alle potenzialità di queste tecnologie, emergono anche le preoccupazioni del governo relative ai cambiamenti che l'IA potrebbe apportare ai meccanismi d'impiego, agli impatti legali, sociali ed internazionali che potrebbe avere. Pechino sottolinea l'importanza dei rischi potenziali e manifesta la propria volontà di prevenirli, minimizzando i rischi e sviluppando uno sviluppo sicuro, affidabile e controllabile dell'IA.⁸⁰

Per quanto riguarda i requisiti generali il primo risulta essere l'aderenza del piano di sviluppo al diciottesimo Congresso Partitico e alla terza, quarta, quinta e sesta seduta plenaria del diciottesimo Comitato Centrale. A questi si aggiunge l'implementazione dello spirito innovatore del Segretario Generale Xi Jinping nel quadro della strategia generale del "five in one", strategia che definisce le cinque aree di "costruzione" del paese: (1) l'economia (经济建设); (2) la politica (政治建设); (3) la cultura (文化建设);

⁷⁸ «*«*新一代人工智能发展规划 - A Next Generation Artificial Intelligence Development Plan*»*, Pub. L. No. 国发〔2017〕35号, § 科技、教育科技, 000014349/2017-00142 27 (2017), p. 2, <https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>.

⁷⁹ *Ibid.*

⁸⁰ *Ivi*, p. 3.

(4) la società (社会建设) e infine (5), la costruzione di una civiltà ecologica (生态文明建设) nell'ambito dello sviluppo sostenibile.⁸¹ Il documento procede con l'individuazione degli obiettivi strategici, punto rilevante ai fini di questa tesi. La suddivisione degli obiettivi è temporale e si focalizza su tre differenti anni, il 2020, il 2025 e il 2030. Entro il 2020, infatti, la Cina si era prefissa di raggiungere importanti progressi nelle nuove tecnologie IA, con un incremento delle abilità della *big-data intelligence*, della *cross-medium intelligence*, della *swarm intelligence* e altri. La competitività dell'industria dell'IA sarebbe dovuta entrare nel primo scaglione a livello internazionale e avrebbe stabilito gli standard iniziali delle tecnologie IA. La Cina avrebbe dovuto inoltre coltivare un certo numero di imprese leader del settore con una valutazione sul mercato di *AI core industry* superiore a 150 miliardi di RMB (renminbi cinese, circa 21 miliardi di dollari). Già nel 2019 la Cina, nelle statistiche globali, era #1 per il numero di documenti di ricerca sull'IA e per documenti altamente citati in tutto il mondo, #1 nei brevetti IA, #1 negli investimenti in capitale di rischio per l'intelligenza artificiale, #2 per numero di aziende IA e #2 nel più grande bacino di talenti IA.⁸² Si stima, invece, che nel 2024 il mercato dell'IA cinese potrebbe raggiungere i 34,2 miliardi di USD, circa 224,8 miliardi di RMB, rimanendo però al secondo posto subito dopo gli Stati Uniti, che si attestano su un valore stimato di 50,1 miliardi di USD.⁸³

Entro il 2025, invece, il paese del dragone ambisce a raggiungere importanti progressi nelle teorie di base per l'IA, in modo tale che alcune tecnologie e applicazioni raggiungano un livello leader mondiale e l'IA diventi la principale forza trainante per l'aggiornamento industriale e la trasformazione economica della Cina.⁸⁴ L'obiettivo è realizzare sistemi intelligenti con capacità di apprendimento autonome in grado di compiere progressi in molte aree al fine di divenire leader del settore. Secondo il governo,

⁸¹ «Five-in-One», *China Media Project* (blog), 12 aprile 2022, https://chinamediaproject.org/the_ccp_dictionary/five-in-one/.

⁸² Allen, «Understanding China's AI Strategy», p. 9.

⁸³ «Artificial Intelligence - China | Statista Market Forecast», Statista, consultato 12 maggio 2024, <https://www.statista.com/outlook/tmo/artificial-intelligence/china>.

⁸⁴ 新一代人工智能发展规划 -Next Generation Artificial Intelligence Development Plan, p. 6.

l'industria dell'IA entrerebbe, quindi, nella catena di valore globale di fascia alta. Questa IA di nuova generazione verrebbe ampiamente utilizzata nella produzione “intelligente”, nella medicina “intelligente”, nelle città “intelligenti”, nell'agricoltura “intelligente” e nella costruzione di una difesa nazionale più avanzata. Il documento si prefigge di raggiungere un valore di mercato superiore a 400 miliardi di RMB, e con un valore delle industrie correlate che supererebbe i 5 trilioni di RMB. Stando ai dati sopra riportati, al momento il valore dell'economia “intelligente” cinese è di poco superiore al 50% delle attese. La Cina, inoltre, ambisce a iniziare ad istituire leggi, regolamenti, norme etiche e sistemi politici in materia di IA, con una successiva formazione di capacità di valutazione e controllo della sicurezza dell'IA.⁸⁵

In ultima istanza, entro il 2030, il Consiglio di Stato cinese ambisce a rendere il proprio paese il principale centro di innovazione dell'IA al mondo, ottenendo risultati visibili nell'economia “intelligente” e nelle applicazioni della società “intelligente”. La Cina mira anche a formare la più matura teoria di nuova generazione IA e sistemi tecnologici, nonché a raggiungere un valore del mercato dell'IA cinese superiore a 1 trilione di RMB, e delle industrie correlate superiore a 10 trilioni di RMB. Entro il 2030, la Cina avrà, inoltre, creato una serie di centri di innovazione tecnologica e di formazione del personale leader a livello globale, e avrà istituito leggi e regolamenti sull'IA più completi, comprendenti un sistema di norme e politiche etiche.⁸⁶

3.1.2 The Science of Military Strategy

The Science of Military Strategy (战略学) rappresenta, per la Repubblica Popolare Cinese, il principale documento di dottrina militare. Più precisamente, ai fini di questa ricerca, si fa riferimento al testo pubblicato nel 2015 e successivamente aggiornato nel 2020. Tra i punti menzionati dalla dottrina, *in primis*, troviamo il potenziamento degli apparati militari attraverso la scienza e la tecnologia. Come già menzionato nella sezione dedicata al rafforzamento della fusione militare civile, il pensiero strategico cinese si basa

⁸⁵ *Ibid.*

⁸⁶ *Ivi*, p. 7.

sul miglioramento delle abilità e della qualità del proprio esercito attraverso il progresso scientifico e tecnologico, al fine di “migliorare l’efficacia combattiva dei militari, rafforzare la qualità dei militari, promuovere la trasformazione strategica della costruzione militare, e migliorare le capacità di combattimento dei militari e la qualità di preparazione di conflitti militari”.⁸⁷

L’intelligenza artificiale viene successivamente citata in merito all’evoluzione della *military intelligence*⁸⁸ del paese. L’assunto di base della dottrina cinese in materia viene così riassunto:

*The innovative application of artificial intelligence in the military field is setting off a wave of military intelligence. All aspects of the military field are being reshaped, and the form of warfare is gradually evolving to intelligent warfare.*⁸⁹

In prima istanza la sezione si apre con un’analisi della concorrenza in materia, in cui vengono citati esempi quali l’utilizzo di droni da parte di Israele nel conflitto con il Libano, l’utilizzo di *unmanned reconnaissance aircraft e combat robot* da parte della Russia nello scenario siriano, per poi concludere con un’analisi dello scenario statunitense.⁹⁰ Emerge la tendenza da parte della Cina ad avere un confronto costante con propri avversari strategici. In particolar modo, la dottrina cinese sottolinea l’importanza strategica della *Third Offset Strategy* americana nella corsa agli armamenti intelligenti, che rappresenta, per il paese, un potenziale rischio. Al fine di eguagliare l’avanzamento tecnologico di paesi come gli Stati Uniti, la Russia, la Francia e la Gran Bretagna, i più alti ranghi militari del paese del dragone hanno elaborato delle linee guida per i conflitti

⁸⁷ Xiao Tianliang et al., «战略学 - The Science of Military Strategy (Revised in 2020)» (National Defence University Press, 2015), p. 34, <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf>.

⁸⁸ Il termine è lasciato nella traduzione inglese di *military intelligence*. Dal documento emerge, però, che il significato attribuitogli non riguarda propriamente l’intelligence militare quanto più i cambiamenti in materia di sistemi intelligenti legati al settore militare. Di qui in avanti si farà riferimento ai sistemi intelligenti militari con i termini “intelligence militare” e “intelligenza militare”.

⁸⁹ Xiao Tianliang et al., «战略学 - The Science of Military Strategy (Revised in 2020)», p. 175.

⁹⁰ *Ivi*, pp. 175-176.

militari in ambito di intelligence. Il primo punto (1) si concentra sull'organizzazione scientifica del paese e l'avanzamento generale della costruzione e dello sviluppo di *military intelligence*. Nell'elaborare una strategia di sviluppo scientifico-tecnologica la Cina non ambisce solo a sviluppare vari sistemi *unmanned* nei domini militari convenzionali (terra, aria, acqua, spazio e cyber), ma anche all'esplorazione dei metodi e delle teorie di combattimento con armi intelligenti, influenzando profondamente l'istituzione attraverso modifiche e riforme del sistema militare. La strategia di sviluppo dovrebbe, quindi, chiarire "*the basic goals, guiding ideology, and basic path of the main ideas of the military's intelligent construction*".⁹¹ Il secondo punto (2) è dedicato alla conquista delle tecnologie chiave e alla padronanza dell'iniziativa nello sviluppo dell'intelligenza militare. La capacità di superare le tecnologie chiavi odierne, in ambito IA, potrebbe, stando alla dottrina del paese, influenzare direttamente il successo o il fallimento del paese nella competizione globale futura per lo sviluppo della *military intelligence*. A tal proposito, lo Stato promuove le ricerche in ambito scientifico, biologico e tecnologico per stimolare, in modo continuo, la capacità d'innovazione nel campo dell'IA.⁹² Il terzo punto (3) delle linee guida delineate dalla dottrina è rafforzare la ricerca "*lungimirante*" e approfondire continuamente l'innovazione della teoria militare intelligente. Il settore militare dovrebbe, quindi, prestare molta attenzione alle varie nuove tendenze e cambiamenti, chiarire il contesto dello sviluppo delle armi e degli equipaggiamenti intelligenti, riassumere le caratteristiche e le leggi per il loro sviluppo e applicazione e continuare ad approfondire la ricerca e l'innovazione della teoria militare.⁹³ Il penultimo punto (4), come anticipato nel Capitolo II, par. 2.1.2, è promuovere una profonda integrazione militare-civile e sfruttare le risorse sociali per sviluppare l'intelligence militare. Il piano prevede, quindi, di rafforzare la stretta cooperazione con il campo socioeconomico, assorbire tempestivamente i suoi risultati di ricerca e innovazione, integrare l'intelligenza militare nello sviluppo dell'intelligenza sociale.⁹⁴ Infine, (5) il Governo cinese mira a gestire correttamente le varie relazioni nello sviluppo dell'intelligenza militare. Queste relazioni sono: (I) il rapporto tra gli armamenti

⁹¹ *Ivi*, p. 178.

⁹² *Ibidem*.

⁹³ *Ivi*, p. 179.

⁹⁴ *Ibid*.

intelligenti e gli armamenti attuali; l'accelerazione dello sviluppo dei primi, infatti, non deve avvenire a discapito dei secondi. (II) Il rapporto tra l'apprendimento dalle forze militari straniere e l'innovazione indipendente. Il Governo sottolinea l'importanza di prestare attenzione agli sviluppi in ambito IA dei paesi stranieri mantenendo, però, il focus sull'innovazione nazionale. (III) Il rapporto tra lo sviluppo graduale e lo sviluppo "a balzi". Le indicazioni prevedono di preferire, in una situazione di stallo dello sviluppo graduale, una politica dirompente nell'ambito della ricerca e della realizzazione di nuovi sistemi militari intelligenti al fine di realizzare "the leap from following and running to leading in the field of military intelligence".⁹⁵

Le linee guida fornite dal Governo cinese, in sintesi, prevedono di definire in prima battuta una strategia congiunta che possa coordinare le varie attività del paese in questo settore. Nella *policy* cinese, inoltre, uno dei fulcri risulta essere lo sviluppo di armamenti intelligenti al fine di contrastare, o quanto meno eguagliare, gli avanzamenti di Stati Uniti, Russia, Francia, Gran Bretagna ed Israele. Ciò che più colpisce della sino-strategia è la volontà, più volte ribadita all'interno dell'AIDP e della *Science of Military Strategy*, di passare da paese "inseguitore" a paese "inseguito" per ciò che concerne l'innovazione intelligente. In conclusione, la strategia messa in atto dalla Repubblica Popolare Cinese per lo sviluppo dell'IA ed una sua applicazione per l'incremento della potenza militare, nonché il suo utilizzo per questioni di sicurezza nazionale, attraverso l'analisi dei documenti disponibili, risulta essere un quadro più generale che particolare, abbastanza vago ed incentrato principalmente sulla collaborazione dei vari sistemi nazionali, tra cui il *private sector*, il mondo accademico e la sfera militare.

3.2 Caso Studio II: gli Stati Uniti d'America

Nell'analizzare l'implementazione di tecnologie intelligenti come l'IA e il ML nel caso americano, è possibile confrontare la *National Security Strategy* del 2017 sotto la presidenza Trump con la più recente, emanata da Joe Biden nel 2022. Successivamente verrà preso in analisi il *National Artificial Intelligence Research and Development Strategic Plan* aggiornato al maggio 2023.

⁹⁵ *Ivi*, p. 180.

3.2.1 *National Security Strategies 2017-2022: Trump c. Biden*

Il primo documento a far menzione dell'impatto e dell'implementazione di strategie relative all'IA e al ML nelle *policies* americane è la *National Security Strategy* del dicembre 2017, emanata dal ex Presidente Donald Trump. L'IA compare in sole due sezioni del testo: la prima relativa alla strategia di ricerca tecnologica, innovazioni e invenzioni (*Lead in Research, Technology, Invention, and Innovation*) mentre la seconda volta in relazione all'*Information Statecraft*. È possibile assumere, già a priori, che l'importanza attribuita ai sistemi intelligenti nella politica americana del 2017 è estremamente labile. In particolar modo, nella sezione *Lead in Research, Technology, Invention, and Innovation*, il documento esorta il paese a dare priorità alle tecnologie emergenti “*critiche per la crescita economica e la sicurezza*”.⁹⁶ Tra queste tecnologie viene citata l'IA, “*from self-driving cars to autonomous weapons, the field of artificial intelligence, in particular, is progressing rapidly*”.⁹⁷ Nelle successive “*azioni prioritarie*”, sezione dedicata al delineamento della strategia, la Presidenza Trump fa cenno solo al mantenimento dello *status quo* di potenza innovatrice e incoraggia la collaborazione del governo con istituti scientifici, centri accademici e settore privato. Per quanto concerne, invece, la sezione dedicata all'*Information Statecraft*, l'IA è menzionata in merito ai potenziali rischi che il paese potrebbe trovarsi a contrastare. Stando al documento, i rischi per la sicurezza nazionale degli Stati Uniti in proporzione all'utilizzo, da parte di *competitors*, dei dati personali dei cittadini americani ricavati da fonti commerciali e analizzate e processate da algoritmi basati sull'IA e il *Machine Learning*, è elevato.⁹⁸ Il documento fa poi menzione dell'uso da parte della Repubblica Popolare Cinese di una combinazione di dati e IA per valutare la fedeltà dei suoi cittadini allo Stato, successivamente utilizzati per *rating* elaborati per determinare posti di lavoro e altro.⁹⁹

Cambiamenti evidenti non sono stati apportati neanche dalla *National Security Policy* dell'Ottobre 2022 emanata dal Presidente Biden. Infatti, anche in questo

⁹⁶ «National Security Strategy» (Seal of the President of the United States, dicembre 2017), p. 20, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

⁹⁷ *Ibid.*

⁹⁸ *Ivi*, p. 34.

⁹⁹ *Ivi*, p. 35.

documento l'IA risulta essere un elemento marginale. L'IA viene inizialmente menzionata, anche qui, per ciò che riguarda le tecnologie emergenti, ma questa volta con un chiaro riferimento alle trasformazioni che potrebbe apportare in scenari di guerra.

*We are investing in a range of advanced technologies, including applications in the cyber and space domains, missile defeat capabilities, trusted artificial intelligence, and quantum systems, while deploying new capabilities to the battlefield in a timely manner.*¹⁰⁰

Una leggera discrepanza con il documento precedentemente analizzato è la presenza di una sezione dedicata alla definizione delle regole della strada (in inglese *Shaping the Rules of the Road*) in ambito tecnologico. La Presidenza Biden esorta ad una cooperazione tra alleati e partner per sfruttare e “scalare” le nuove tecnologie e promuovere le tecnologie fondamentali del secolo corrente, in particolare modo le microtecnologie, l'informatica avanzata e le tecnologie quantistiche, l'intelligenza artificiale, le biotecnologie e le bioproduzione, le telecomunicazioni avanzate e le tecnologie energetiche pulite. Per raggiungere questi obiettivi, gli Stati Uniti delineano una strategia che coinvolge lo U.S.-EU Trade and Technology Council per promuovere il coordinamento transatlantico sulle catene di approvvigionamento di semiconduttori e minerali critici, l'intelligenza artificiale “affidabile”, la lotta alla disinformazione, agli abusi della tecnologia che minacciano la sicurezza e i diritti umani ed altro. Inoltre, attraverso l'Indo-Pacific Quad, gli Stati Uniti, mirano a coordinare l'avanzamento delle tecnologie critiche ed emergenti, delle infrastrutture digitali aperte di nuova generazione e degli scambi interpersonali.¹⁰¹

3.2.2 National Artificial Intelligence Research and Development Strategic Plan

L'aggiornamento del *National Artificial Intelligence Research and Development Strategic Plan* (NAIRDSP) del 2023 fa seguito ai precedenti *AI R&D Strategic Plan* del

¹⁰⁰ «National Security Strategy» (The White House Washington, ottobre 2022), p. 21, <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>.

¹⁰¹ *Ivi*, p. 33.

2016 e del 2019, riaffermando le otto strategie già presentate e aggiungendone una nona. Al fine di fornire un'analisi accurata della strategia generale statunitense è utile passare in rassegna i nove punti presenti nel documento: (1) investire a lungo termine nella ricerca “fondamentale” e “responsabile” in ambito IA; (2) sviluppare metodi efficaci per una collaborazione tra l'uomo e l'IA; (3) comprendere e affrontare le implicazioni etiche, legali e sociali dell'IA; (4) garantire la sicurezza dei sistemi IA; (5) sviluppare set di dati e ambienti pubblici condivisi per la formazione e il test dell'IA; (6) misurare e valutare i sistemi IA attraverso standard e *benchmarks*; (7) comprendere al meglio le esigenze nazionali della forza lavoro R&D dell'IA; (8) espandere le partnership tra settore privato e pubblico per accelerare gli avanzamenti nell'IA; infine, il nuovo punto apportato dal documento del 2023, (9) stabilire un approccio di principio e coordinato per la collaborazione internazionale nella ricerca sull'IA.¹⁰²

Partendo alla prima, la Strategia n. 1 si basa sul più volte citato “*mantenimento della leadership in ambito IA*”. Questo successo, a detta dello U.S. Selected Committee on Artificial Intelligence, è dovuto al continuo aumento dei programmi di sviluppo finanziati dal governo. Lo Stato deve, infatti, continuare a perseguire investimenti a lungo termine, fondamentali e responsabili per lo sviluppo di sistemi IA. L'obiettivo principale è spostare la concentrazione da sistemi IA per compiti individuali a sistemi più complessi, integrati e coordinati al fine di garantire una “*copertura*” multi-dominio, muovendosi verso la c.d. *general-purpose AI*. Le priorità riguardano l'utilizzo della quantità “*significativa*” di dati disponibili per l'apprendimento automatico (ML) e la scoperta della conoscenza, il miglioramento delle capacità dell'IA di percepire e agire e lo sviluppo di sistemi intelligenti per lavorare in ambienti reali e virtuali.¹⁰³

La Strategia n. 2 è denominata, invece, *Develop Effective Methods for Human-AI Collaboration*. Questa sezione sottolinea l'importanza e l'incremento dei sistemi autonomi che prevedono piccole interazioni con l'essere umano o addirittura nessuna. Per

¹⁰² «National Artificial Intelligence Research and Development Strategic Plan 2023 Update» (Executive Office of the President of the United States, maggio 2023), p. VII-VIII, <https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf>.

¹⁰³ *Ivi*, pp. 3-8.

gli Stati Uniti queste tecnologie sono di cruciale importanza nell'ambito industriale e nei domini "rischiosi" come lo spazio profondo e gli ambienti radioattivi. La critica mossa a questa completa automazione è relativa ad applicazioni dei sistemi IA in ambienti quali il *disaster recovery* o le scoperte scientifiche che richiedono un'interazione tra il fattore umano e la macchina al fine di bilanciare i rispettivi punti di forza e mitigare i rischi. In sintesi, questa strategia riconosce la crescente importanza dei fattori "socio-tecnici" e umani e affronta la necessità di sviluppare una ricerca multidisciplinare per consentire un'efficace collaborazione uomo-IA.¹⁰⁴

La terza sezione è dedicata alla Strategia n. 3, *Understand and Address the Ethical, Legal, and Societal Implications of AI*. Tra le minacce che l'IA può rappresentare per la società, gli Stati Uniti, a differenza della Cina, sottolineano il possibile impatto amplificatore di comportamenti ineguali e "effetti indesiderati per gli individui e le comunità". La Casa Bianca, infatti, ha sollevato la questione di redigere una bozza per una *AI Bill of Rights* al fine di proteggere le cinque garanzie di cui ogni cittadino americano dovrebbe godere nel momento in cui interagisce con sistemi intelligenti o autonomi. Queste comprendono la protezione da algoritmi discriminatori e la privacy dei dati. Nel Gennaio 2023, il National Institute of Standards and Technology (NIST) ha pubblicato un report per comprendere meglio i rischi associati all'IA in termini di tutela degli individui, delle comunità e delle diverse società. Questo report è utilizzato dal governo americano per sviluppare linee guida coerenti con la tutela delle classi menzionate. Il punto centrale è di assicurare "that AI broadly benefits the American people".¹⁰⁵ L'amministrazione americana delinea quindi una strategia che persegua obiettivi come l'equità, la correttezza, la privacy e l'autonomia.¹⁰⁶

La Strategia n. 4 è dedicata alla garanzia della sicurezza dei sistemi IA (in inglese *Ensure the Safety and Security of AI Systems*). L'avanzamento tecnologico e il rapido aumento dei dati utilizzati dall'IA potrebbero comportare alcuni rischi. I termini "safety" e "security" fanno esplicito riferimento alle definizioni contenute nella relazione

¹⁰⁴ *Ivi*, pp. 9-11.

¹⁰⁵ *Ivi*, p. 12.

¹⁰⁶ *Ivi*, pp. 12-15.

Assessing and Improving AI Trustworthiness: Current Context and Concerns, che definisce “*safety*” come “*attenuante contro un sistema che produce nuovi danni*”, e “*security*” “*come monitoraggio dell’integrità di un sistema*”.¹⁰⁷ Per gli Stati Uniti la garanzia di sicurezza deve essere perseguita in tutte le fasi di vita dello sviluppo dei sistemi IA, dall’ideazione fino alla messa in atto, con l’aggiunta di un monitoraggio costante. Il NAIRDSP individua due principali minacce. La prima, nel breve termine, consiste nella c.d. *data-poisoning*, pratiche attraverso cui vengono manipolati gli addestramenti o i dati di input dell’IA, e altre forme di attacchi nemici contro l’IA, come a sistemi di targeting collegati all’IA. Le modifiche ai dati audio o visivi, che non possono essere percepiti dagli esseri umani, possono modificare il modo in cui un sistema IA elabora i dati. La seconda minaccia è il rischio “*esistenziale*” di uno sviluppo di un’AGI in grado di modificarsi in modo autonomo. La prospettiva di sviluppare un sistema alla Hal 9000 o alla Skynet sembra uno scenario plausibile per il governo americano, rischio che invece non compare nei documenti cinesi.¹⁰⁸

La Strategia n. 5 delinea lo sviluppo di set di dati e ambienti pubblici condivisi per la formazione e il test dell’IA. L’obiettivo del quinto punto è di “*democratizzare l’accesso ai dati IA e alle risorse da essa elaborate*”. A tal fine, la National Artificial Intelligence Research Resource Pilot (NAIRR) Task Force ha pubblicato delle linee guida e un piano di attuazione per un’infrastruttura informatica di ricerca nazionale che faciliti l’accesso ai ricercatori ai dati, ai calcoli, ai banchi di prova, e alla formazione congiunta. Nel 2019 è inoltre stato emanato l’*OPEN Government Data Act* che ha dato il mandato al governo federale, attraverso la collaborazione e il coordinamento, di fornire dati aperti, impegnarsi in attività di costruzione delle prove, migliorare l’efficienza statistica, sostenere la protezione delle informazioni riservate e, laddove i dati riguardano gli esseri umani, rispettare la privacy.¹⁰⁹

La Strategia 6 riguarda, invece, le misure e la valutazione dei sistemi IA attraverso standard e *benchmarks*. Già l’*Executive Order on Maintaining American Leadership in*

¹⁰⁷ *Ivi*, p. 16.

¹⁰⁸ *Ivi*, pp. 16-17.

¹⁰⁹ *Ivi*, pp. 18-21.

Artificial Intelligence del 2019 e il *National Artificial Intelligence Initiative Act* del 2020 facevano espresso riferimento all'importanza di stabilire degli standard per la produzione di sistemi intelligenti.¹¹⁰

La settima strategia, *Better Understand the National AI R&D Workforce Needs*, vuole far fronte alla sempre più elevata richiesta di professionisti nel campo dei computer e delle scienze informatiche. Stando alle stime americane, infatti, la domanda di queste figure aumenterà del 22% nell'arco di questo decennio. A questo si aggiunge l'aspettativa, sempre per il periodo 2020-2030, che la ricerca sull'intelligenza artificiale dovrebbe contribuire fino a 11,5 trilioni di dollari nella crescita cumulativa nei soli paesi del G20. Tra i problemi maggiormente riscontrati dal Governo americano, troviamo la mancanza di personale per posizioni governative che richiedono un nullaosta di sicurezza. Questo fenomeno è dovuto all'esponenziale aumento di interesse, da parte soprattutto di studenti internazionali, di frequentare corsi *AI-based* negli atenei americani.¹¹¹

La Strategia n. 8 riprende il concetto di estensione della partnership tra settore privato e pubblico. Come sottolineato dall'American Academy of Arts and Science, la posizione degli Stati Uniti di leader nell'innovazione si basa su "*establishing a more robust national Government-University-Industry research partnership*". I punti portanti di questa Strategia sono: (1) trarre un maggior beneficio dalla sinergia della partnership pubblico-privato; (2) l'estensione delle partnership a un maggior numero di *stakeholders* diversi; (3) il miglioramento, l'allargamento e la creazione di meccanismi di partenariato in ambito R&D.¹¹²

In ultimo, la Strategia n. 9, implementata nell'aggiornamento del 2023, riguarda la definizione di un approccio di principio coordinato per la collaborazione internazionale nella ricerca IA. Al momento gli Stati Uniti primeggiano, a livello mondiale, come paese con la spesa in IA R&D. Stando al report *U.S. State of Science & Engineering 2022* nessuna nazione è considerabile leader in ogni campo della scienza e dell'ingegneria,

¹¹⁰ Per un'analisi più approfondita della Strategia: *ivi*, pp. 22-26.

¹¹¹ *Ivi*, pp. 27-30.

¹¹² *Ivi*, pp. 31-33.

nonostante le pubblicazioni in materia IA siano duplicate tra il 2010 e il 2020. Al fine di mantenere il primato di *hub AI*, gli Stati Uniti mirano a sviluppare programmi internazionali, infrastrutture, dataset congiunti e altro. Gli obiettivi del Governo americano sono principalmente tre: (1) coltivare una cultura globale per lo sviluppo e l'uso di IA affidabili. Questo punto si basa sugli aspetti affrontati nella Strategia n. 3, riguardanti la realizzazione di sistemi intelligenti conformi alla legge, ai valori etici e agli standard sociali. Alcuni esempi concreti di cooperazione internazionale sono il decimo *Memorandum of Understanding* (MOU10) con l'Australia's Commonwealth Scientific and Industrial Research Organization che ha avviato un programma di ricerca finanziato congiuntamente, che include lo sviluppo di un'IA equa e affidabile; altro esempio è l'accordo tra gli Stati Uniti e la Commissione europea per ulteriori ricerche sull'IA in settori di applicazione, tra cui le previsioni meteorologiche, gestione delle emergenze, miglioramento della salute e della medicina, ottimizzazione della rete elettrica e dell'agricoltura. Inoltre, il peso politico degli Stati Uniti nei fori di diplomazia multilaterale ha generato la pubblicazione da parte dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD), nel 2019, dell'*OECD Recommendation on AI* e il lancio da parte del G7 del *Global Partnership on AI*. (2) Supportare lo sviluppo di sistemi IA, standard e *framework* a livello globale. Per perseguire questo obiettivo gli Stati Uniti hanno avviato importanti progetti congiunti a livello internazionale tra cui la *Declaration of the U.S. and the United Kingdom on Cooperation in AI R&D* per sviluppare una visione collettiva e un ecosistema di ricerca complesso, e il recente impegno da parte del Quad (Stati Uniti, India, Australia e Giappone) con l'obiettivo di creare un gruppo per le comunicazioni avanzate IA, focalizzato su attività di sviluppo di standard condivisi. (3) Facilitare lo scambio internazionale di idee ed esperti. Le collaborazioni tra agenzie internazionali e i più ampi accordi di cooperazione bilaterali e multilaterali offrirebbero agli Stati Uniti l'opportunità di colmare le proprie lacune sfruttando competenze di ricerca IA provenienti da tutto il mondo.¹¹³

A differenza della Repubblica Popolare Cinese, che concentra i propri sforzi nella realizzazione di una strategia incentrata sull'implementazione dell'IA in ambiti militari, gli Stati Uniti mirano, piuttosto, a mantenere il proprio primato di potenza leader

¹¹³ *Ivi*, pp. 34-37.

nell'ambito dell'innovazione tech. Nel caso americano, quindi, la strategia messa in atto dal governo risulta essere più interdisciplinare e “multilaterale”, con strategie che concernono l'ampliamento della collaborazione internazionale e l'interesse nella tutela dei valori democratici fondamentali. Come visto in precedenza, però, non mancano programmi militari *AI-based*, che tuttavia non compaiono nei documenti ufficiali, come ad esempio la NSS del 2022.

Conclusioni

Il potenziale rappresentato dall'Intelligenza Artificiale, in termini di acquisizione di potere statale e terreno di sfida mondiale, sembra essere ancora un terreno fertile per il dibattito accademico. Nonostante le politiche messe in atto dai due principali competitor globali, Cina e Stati Uniti, gli impatti che l'IA potrebbe avere sulla sicurezza nazionale non sono ancora bene definiti. Gli sporadici accenni all'IA nelle *national security strategies* americane dimostrano come il potenziale dell'Intelligenza Artificiale, nella definizione delle strategie securitarie nazionali, sia ancora inesplorato. Questo aspetto è sopperito da documenti *ad hoc* che, però, utilizzando un approccio multidisciplinare e trasversale, tendono ad essere generali e vaghi. Al contrario, come già precedentemente sottolineato, la *vision* cinese risulta essere più concreta e focalizzata sull'implementazione di questi sistemi nell'ambito della sicurezza nazionale. Il programma di fusione militare-civile rappresenta solo la punta dell'iceberg nella definizione di una politica cinese improntata sulle *dual-use technology*, tecnologie ideate per scopi civili e successivamente, dato il loro potenziale strategico, integrate in sistemi militari. In particolare, questa *policy* potrebbe porre le basi per un sorpasso da parte della Cina con un conseguente distanziamento tecnologico-militare non indifferente. La definizione, però, della *Third Offset Strategy* americana, nel 2014, che inserisce l'IA e il ML come *main fields* per ciò che concerne l'avanzamento tecnologico del paese, evidenzia la tendenza statunitense nell'individuazione di nuove opportunità strategiche. Nonostante l'acume strategico degli Stati Uniti, l'implementazione di sistemi intelligenti da parte del DoD americano andrebbe interpretato come condizione necessaria ma non sufficiente per il mantenimento del primato di potenza innovatrice globale.

Il potenziale disruptivo dell'IA, le preoccupazioni mosse da alcuni esperti nel settore e l'apprensione mostrata dagli Stati relativamente alla realizzazione di Intelligenze Artificiali *self-evolving* o di una possibile perdita di controllo di queste tecnologie, non rende così remota la probabilità di un *third AI winter*. La volontà, questa volta comune, di Stati Uniti e Cina di individuare standard tecnici e di sviluppare leggi per la

regolamentazione di questi sistemi potrebbe concludersi con un accantonamento temporaneo di questa tecnologia.

Bibliografia e sitografia

- Allen, Gregory C. «Project Maven Brings AI to the Fight against ISIS». *Bulletin of the Atomic Scientists* (blog), 21 dicembre 2017. <https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/>.
- . «Understanding China's AI Strategy - Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security». Center for a New American Security (CNAS), 6 febbraio 2019. <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>.
- Allen, Gregory C., e Taniel Chan. «Artificial Intelligence and National Security». *National Security*, Belfer Center Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School (luglio 2017). <https://www.belfercenter.org/publication/artificial-intelligence-and-national-security>.
- Allison, Graham T. «Conceptual Models and the Cuban Missile Crisis». *American Political Science Review* 63, fasc. 3 (novembre 1969): 689–718. <https://doi.org/10.2307/1954423>.
- . *Destined for war: can America and China escape Thucydides's trap?* Boston: Houghton Mifflin Harcourt, 2017.
- Altmann, Jürgen, e Frank Sauer. «Autonomous Weapon Systems and Strategic Stability». *Survival* 59, fasc. 5 (3 settembre 2017): 117–42. <https://doi.org/10.1080/00396338.2017.1375263>.
- «A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf». Consultato 9 febbraio 2024. <https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf>.
- «Artificial Intelligence». In *Oxford Reference*, s.d. Consultato 9 febbraio 2024.
- Babuta, Alexander, Marion Oswald, e Ardi Janjeva. «Artificial Intelligence and UK National Security», RUSI Occasional Paper, 27 aprile 2020.
- Blackburn, R Alan. «Summary of the 2018 Department of Defense Artificial Intelligence Strategy», 2018.
- «“Break Their Lineage, Break Their Roots”». *Human Rights Watch*, 19 aprile 2021. <https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting>.

- Brooks, Stephen G., e William C. Wohlforth. «The Rise and Fall of the Great Powers in the Twenty-first Century: China's Rise and the Fate of America's Global Position». *International Security* 40, fasc. 3 (2015): 7–53.
- Brown, Sara. «Machine Learning, Explained | MIT Sloan», 21 aprile 2021. <https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained>.
- Browne, Ryan. «Alibaba's Jack Ma Suggests Technology Could Result in a New World War». CNBC, 23 gennaio 2019. <https://www.cnbc.com/2019/01/23/alibaba-jack-ma-suggests-technology-could-result-in-a-new-world-war.html>.
- Buranelli Costa, Filippo. «Asia Centrale: tra grandi potenze e regionalismo». *ISPI* (blog), s.d. <https://www.ispionline.it/it/pubblicazione/asia-centrale-tra-grandi-potenze-e-regionalismo-131021>.
- CABAR.asia. «Central Asia's Critical Raw Materials: The Next Frontier in Global Power Rivalry?», 3 aprile 2024. <https://cabar.asia/en/central-asia-s-critical-raw-materials-the-next-frontier-in-global-power-rivalry>.
- «CAICT - WHITE PAPER». Consultato 22 marzo 2024. http://www.caict.ac.cn/english/research/whitepapers/202205/t20220510_401132.html.
- Carpenter, Charli. «“Women, Children and Other Vulnerable Groups”: Gender, Strategic Frames and the Protection of Civilians as a Transnational Issue». *International Studies Quarterly* 49, fasc. 2 (giugno 2005): 295–334. <https://doi.org/10.1111/j.0020-8833.2005.00346.x>.
- China Media Project. «Five-in-One», 12 aprile 2022. https://chinamediaproject.org/the_ccp_dictionary/five-in-one/.
- «China's AI industry scale exceeds 40 bln USD in 2020 - Xinhua | English.news.cn». Consultato 29 marzo 2024. http://www.xinhuanet.com/english/2021-07/09/c_1310052462.htm.
- Consiglio di stato cinese. «Made in China 2025», 7 luglio 2015. <http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf>.
- «Coordinated Plan on Artificial Intelligence | Shaping Europe's Digital Future», 27 febbraio 2024. <https://digital-strategy.ec.europa.eu/en/policies/plan-ai>.
- DCAF – Geneva Centre for Security Sector Governance. «NATIONAL SECURITY POLICIES Formulating National Security Policies for Good Security Sector Governance», SSR Backgrounder Series Geneva. Consultato 13 marzo 2024. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_09_NationalSecurityPolicies_Nov2022.pdf.

- Default. «AlphaGo and Beyond: The Chinese Military Looks to Future “Intelligentized” Warfare». Consultato 3 aprile 2024. <https://www.lawfaremedia.org/article/alphago-and-beyond-chinese-military-looks-future-intelligentized-warfare>.
- Demarest, Colin. «Pentagon’s Project Maven Transition Stymied by Congress, Official Says». C4ISRNet, 26 ottobre 2022. <https://www.c4isrnet.com/artificial-intelligence/2022/10/26/pentagons-project-maven-transition-stymied-by-congress-official-says/>.
- DoD Responsible AI Working Council. U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway (2022). <https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF>.
- Fortune. «Amazon Killed an AI Recruitment System Because It Couldn’t Stop the Tool from Discriminating Against Women». Consultato 19 marzo 2024. <https://fortune.com/2018/10/10/amazon-ai-recruitment-bias-women-sexist/>.
- Furman, Jason, e Robert Seamans. «AI and the Economy». *Innovation Policy and the Economy* 19 (gennaio 2019): 161–91. <https://doi.org/10.1086/699936>.
- Geeraerts, Gustaaf. «China, the EU, and the New Multipolarity». *European Review* 19, fasc. 1 (febbraio 2011): 57–67. <https://doi.org/10.1017/S1062798710000335>.
- Generale Wang Ning. *Global Terrorism: Threats and Countermeasures*. 8ª edizione del Beijing Xiangshan Forum, 5 ottobre 2018.
- Gian Gentile, Michael Shurkin, Alexandra T. Evans, Michelle Gris , Mark Hvizda, Rebecca Jensen. *A History of the Third Offset, 2014-2018*. RAND Corporation, 2021. <https://doi.org/10.7249/RR454-1>.
- Horowitz, Michael C. «Artificial Intelligence, International Competition, and the Balance of Power», *Texas National Security Review: Volume 1, Issue 3, The Scholar* (maggio 2018).
- Horowitz, Michael C., e Lauren A. Kahn. «Why DoD’s New Approach to Data and Artificial Intelligence Should Enhance National Defense». Council on Foreign Relations, s.d. <https://www.cfr.org/blog/why-dods-new-approach-data-and-artificial-intelligence-should-enhance-national-defense>.
- Horowitz, Michael C., Shira Pindyck, e Casey Mahoney. «AI, the International Balance of Power, and National Security Strategy». In *The Oxford Handbook of AI Governance*, a cura di Justin B. Bullock, Yu-Che Chen, Johannes Himmelreich, Valerie M. Hudson, Anton Korinek, Matthew M. Young, e Baobao Zhang, 1ª ed. Oxford University Press, 2022. <https://doi.org/10.1093/oxfordhb/9780197579329.013.55>.

- Kahn, Lauren A. «Defense AI in the United States», DAIO Study, 23|07 (2023).
- Kalkan Küçüksoğak, Övgü, e Tuba Firat. «The Geopolitics of Artificial Intelligence in Central Asia: Russian and Chinese Cases». *Güvenlik Bilimleri Dergisi* 12, fasc. 1 (31 maggio 2023): 25–44. <https://doi.org/10.28956/gbd.1249381>.
- Kania, Elsa B. «Artificial Intelligence in China’s Revolution in Military Affairs». *Journal of Strategic Studies* 44, fasc. 4 (7 giugno 2021): 515–42. <https://doi.org/10.1080/01402390.2021.1894136>.
- . «Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power», 28 novembre 2017. <https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>.
- Lin, Patrick, George Bekey, e Keith Abney. «Autonomous Military Robotics: Risk, Ethics, and Design»: Fort Belvoir, VA: Defense Technical Information Center, 20 dicembre 2008. <https://doi.org/10.21236/ADA534697>.
- Lucarelli, Sonia, Alessandro Marrone, e Francesco N Moro. «NATO Decision-Making in the Age of Big Data and Artificial Intelligence», s.d.
- Metz, Cade. «In Two Moves, AlphaGo and Lee Sedol Redefined the Future». *Wired*. Consultato 9 febbraio 2024. <https://www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future/>.
- «Moore’s Law | Microprocessors, Transistors & Technology | Britannica», 5 gennaio 2024. <https://www.britannica.com/technology/Moores-law>.
- «National Artificial Intelligence Research and Development Strategic Plan 2023 Update». Executive Office of the President of the United States, maggio 2023. <https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf>.
- National Intelligence Council (U.S.), a c. di. *Global Trends 2030: Alternative Worlds: A Publication of the National Intelligence Council*. December 2012: National Intelligence Council, 2012.
- «National Security Strategy». Seal of the President of the United States, dicembre 2017. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- «National Security Strategy». The White House Washington, ottobre 2022. <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>.

- «NATO - Topic: Emerging and disruptive technologies». Consultato 1 marzo 2024.
https://www.nato.int/cps/en/natohq/topics_184303.htm.
- NATO Science & Technology Organization. «Science & technology trends 2020-2040: exploring the S&T edge», 2020.
https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.
- New America. «Xi Jinping Calls for ‘Healthy Development’ of AI (Translation)». Consultato 3 aprile 2024. <http://newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-calls-for-healthy-development-of-ai-translation/>.
- Pratt, Gill A. «Is a Cambrian Explosion Coming for Robotics?» *Journal of Economic Perspectives* 29, fasc. 3 (1 agosto 2015): 51–60.
<https://doi.org/10.1257/jep.29.3.51>.
- Russell, Stuart J., e Peter Norvig. *Artificial intelligence: a modern approach*. 4^a ed. Pearson series in artificial intelligence. Hoboken: Pearson, 2021.
- Sander, Alison, e Mel Wolfgang. «The Rise of Robotics», bcg.perspectives by The Boston Consulting Group, 27 agosto 2014. https://web-assets.bcg.com/img-src/The_Rise_of_Robotics_Aug_2014_tcm9-82495.pdf.
- Schmidt, Eric, Work, Robert, Catz, Safra, Horvitz, Eric, Chien, Steve, Jassy, Andrew, Clyburn, Mignon, et al. «Final Report». National Security Commission on Artificial Intelligence, 2021.
<https://cybercemetery.unt.edu/nscai/20211005220330/https://www.nscai.gov/>.
- Security Sector integrity. «National Security Policy». Consultato 13 marzo 2024.
<https://securitysectorintegrity.com/defence-management/policy/>.
- Statista. «Artificial Intelligence - China | Statista Market Forecast». Consultato 12 maggio 2024. <https://www.statista.com/outlook/tmo/artificial-intelligence/china>.
- Surdu, John, e Kevin Kittka. «The Deep Green concept», 623–31, 2008.
 «The American AI Initiative: The U.S. Strategy for Leadership in Artificial Intelligence». Consultato 1 marzo 2024. <https://oecd.ai/en/wonk/the-american-ai-initiative-the-u-s-strategy-for-leadership-in-artificial-intelligence>.
- The Economist*. «The workplace of the future». Consultato 19 marzo 2024.
<https://www.economist.com/leaders/2018/03/28/the-workplace-of-the-future#>.
- Vincent, James. «Putin Says the Nation That Leads in AI ‘Will Be the Ruler of the World’». *The Verge*, 4 settembre 2017.
<https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world>.

Warrell, Helen, James Kyng, Valerie Hopkins, e Kathrin Hille. «Exporting Chinese surveillance: the security risks of ‘smart cities’». *Financial Times*, 9 giugno 2021, sez. The Big Read. <https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab>.

Churchill Winston S. *Churchill Speaks: Winston S. Churchill in Peace and War: Collected Speeches, 1897-1963*. Windward, 1982.

«Xi Jinping: cogliere con precisione la nuova tendenza dello sviluppo militare mondiale e tenere il passo con i tempi per promuovere vigorosamente l’innovazione militare - Xinhuanet». Consultato 5 aprile 2024. http://www.xinhuanet.com/politics/2014-08/30/c_1112294869.htm.

Xiao Tianliang, Lou Yaoliang, Kang Wuchao, e Cai Renzhao. «战略学 - The Science of Military Strategy (Revised in 2020)». National Defence University Press, 2015. <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf>.

Zanini, LTC Andrea. «China’s New Military Posture in Central Asia», 2022.

新一代人工智能发展规划 -Next Generation Artificial Intelligence Development Plan, Pub. L. No. 国发〔2017〕35号, § 科技、教育\科技, 000014349/2017-00142 27 (2017). <https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>.

Abstract

Due to the recent switch of conflict combat techniques, the canonical warfare paradigm is changing. A new technological revolution is coming or already happening for someone else. Artificial Intelligence represents a new way to increase State power. The main actors of this new “race to innovation” are the People’s Republic of China and the United States, which are facing the challenge of implementing AI in their national security policy. On one side, China is trying to push military-civilian cooperation on AI, exploiting dual-use technology for military applications. On the other hand, the United States is approaching this gauntlet by defining a multidisciplinary strategy concerning social, ethical, and international cooperation issues related to AI.