OSSERVATORIO SUGLI AFFARI STRATEGICI ED INTERNAZIONALI

ISTITUTO ITALIANO DI STUDI STRATEGICI

ITALIAN INSTITUTE OF STRATEGIC STUDIES

Niccolò Machiavelli

INTELLIGENCE HYPER-LOOP:

COME LA CONSIDERAZIONE DEL CONCETTO "HUMAN-IN-THE-LOOP" È VITALE PER LA RIVOLUZIONE DIGITALE DELLO SPIONAGGIO

FABIO VANORIO

FRANCESCO D'ARRIGO

EDIZIONI MACHIAVELLI

www.strategicstudies.it

DICEMBRE 2020

***G**lobal **E**ducation and*
O**ccident **S**tatecraft **Enterprise

Global Education and Occident Statecraft Enterprise (acronimo GEOS Enterprise) é una società italiana che realizza le proprie strategie di business in sinergia con altre imprese, università, centri di ricerca, *think-tank*, organizzazioni nazionali ed estere, in tutti gli ambiti aventi ad oggetto la diffusione della conoscenza, l'alta formazione, lo sviluppo delle tecnologie nei campi degli affari strategici, della sicurezza internazionale, della difesa, dell'intelligence, dell'economia, delle relazioni politiche internazionali, dell'organizzazione delle imprese, della comunicazione, degli affari legali, dei trasporti, dell'energia, dell'ambiente, dell'aerospazio, della cibernetica, dello sport e di ogni altra disciplina di tipo socio-economico di interesse strategico.

www.geosenterprise.com

ISTITUTO ITALIANO DI STUDI STRATEGICI

ITALIAN INSTITUTE OF STRATEGIC STUDIES

Niccolò Machiavelli

L'***Osservatorio sugli affari strategici ed internazionali*** costituisce, all'interno dell'Istituto Machiavelli, il principale centro di analisi delle dinamiche e delle tendenze strategiche nel campo degli affari internazionali.

L'Osservatorio elabora con continuità, autonomamente e su commissione, analisi, scenari e studi previsionali su temi politici, militari ed economico-finanziari di rilevanza strategica per l'interesse nazionale italiano e per il decisore pubblico e privato.

AUTORI

Fabio Vanorio è cultore della materia intelligence da circa trent'anni. La sua attività di studio e ricerca è svolta in maniera indipendente. Ogni opinione e valutazione espressa nel presente documento è da riferire esclusivamente all'autore e alle fonti bibliografiche citate, senza alcun coinvolgimento di terze parti.

Francesco D'Arrigo è socio fondatore e Direttore dell'Istituto Italiano di Studi Strategici "Niccolò Machiavelli". Già Ufficiale di Stato Maggiore nella Marina Militare Italiana (Naval Aviator, Comandante di aerei ed elicotteri), ha maturato esperienza ultradecennale nel settore dell'Aviazione militare e civile. Ha curato, per università e think tank, la progettazione e realizzazione di programmi di ricerca finanziati dalla Commissione Europea, master, corsi di alta formazione, seminari, congressi di livello internazionale e pubblicazioni in ambito *strategic intelligence*, *statecraft* e *security*.

Copyright © 2020
Istituto Italiano di Studi Strategici "Niccolò Machiavelli" – Roma

È vietata la riproduzione non autorizzata, anche parziale, realizzata con qualsiasi mezzo, compresa la fotocopia, anche ad uso interno o didattico.

I pareri espressi in questo documento sono personali dell'autore e non rappresentano necessariamente le opinioni dell'Istituto.

Indice

Introduzione V

Intelligenza Artificiale e Policy Planning. Definizione di Hyper-Loop. VII

Il progresso dell'Intelligenza Artificiale nella "National Security Enterprise" X

Potenziali risposte alla domanda di ricerca XI

1. La politicizzazione dell'Intelligence XI
2. La resistenza culturale alla tecnologia all'interno della Comunità Intelligence XIV
3. Restrizioni all'accesso ai dati XVI
4. "Outsourcing" delle funzioni vitali del ciclo dell'Intelligence XVII

Conclusioni XVIII

Lavori citati XX

Introduzione

Lo scopo di questa ricerca è di indagare scientificamente sul ruolo che gli esseri umani possono svolgere nel promuovere o ostacolare il progresso tecnologico della Comunità *Intelligence*.

Più che di Comunità Intelligence, il paper utilizza la definizione di "*National Security Enterprise*" (NSE) tratta da George (2020), ovvero, "*a complex web of agencies and processes that work together in a whole-of-government fashion to achieve a common vision or purpose*". L'utilità di questa definizione è nella sua applicabilità a realtà del settore di qualunque paese.

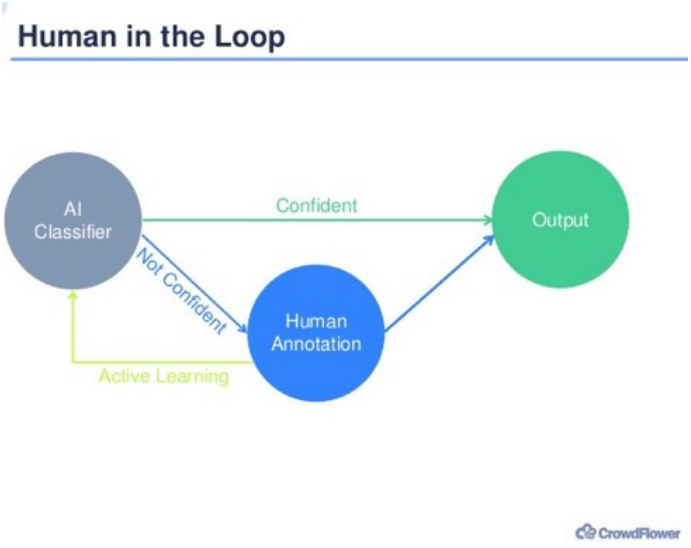
Un secondo concetto che viene introdotto è quello di "*Human-In-The-Loop*". Questa nozione è riconducibile al rapporto tra Uomo e Macchina, intese come le due componenti principali alla base dell'avanzamento tecnologico di un sistema. Il ruolo dell'Uomo è cruciale nell'agevolare l'accrescimento tecnologico di ogni struttura, e nel nostro specifico settore di interesse in ciascuna delle sei fasi dell'*Intelligence Loop* (o Ciclo *Intelligence*, costituito da indirizzi di ricerca, pianificazione e direzione, raccolta, trattamento ed elaborazione, analisi e produzione, e disseminazione[1]). Gli esseri umani sono coinvolti, in particolare nel crescente rapporto

con l'evoluzione dell'Intelligenza Artificiale e del *Machine Learning*, in circoli virtuosi dove sviluppano e testano algoritmi per addestrare le macchine.

Gli esseri umani rappresentano, però, anche l'"anello debole" dell'*Intelligence Loop* (Soni, Kosal 2018). Nel corso degli anni, infatti, gli sforzi dell'*Intelligence nel catching-up* tecnologico hanno dimostrato come i pregiudizi degli esseri umani influenzino -positivamente o negativamente - la diffusione delle nuove tecnologie, incidendo sull'efficienza del sistema organizzativo.

1. Immagine da https://www.fbi.gov/image-repository/intelligence-cycle-graphic.jpg

Anche la tecnologia più innovativa e dirompente non può essere efficace in un processo organizzativo che non funziona. Il *catching-up* tecnologico può migliorare il ciclo *Intelligence* solo se la struttura organizzativa sottostante è la più efficiente possibile. In primis, se la fase di reporting colma adeguatamente il *gap* di conoscenza decisionale a qualsiasi livello politico grazie alla migliore comunicazione possibile tra il produttore di *intelligence* (la "*National Security Enterprise*") e il consumatore (i *decision-maker*). In caso contrario, i collassi organizzativi, dovuti principalmente a *bias* comportamentali, possono portare a fallimenti decisionali anche in presenza di tecnologie intelligenti.



Nei più recenti progressi coinvolgenti, ad esempio, *Big Data*, operazioni *Cyber* o a Realtà Aumentata, gli esperti si sono domandati se (e come) il ruolo degli esseri umani nell'*Intelligence Loop* debba essere modificato (Check 2018.) Il miglioramento delle interazioni tra l'Uomo, le risorse tecniche, e la struttura organizzativa della "*National Security Enterprise*" giocano, infatti, un ruolo cruciale nella diffusione delle tecnologie emergenti nell'*Intelligence Loop*. Rallentamenti nell'applicazione possono avere costi eccessivamente elevati in termini finanziari e nella competizione (non solo tecnologica) tra paesi, oltreché umani, laddove le attività operative restino obsolete rispetto alle innovazioni tecnologiche.

La domanda di ricerca alla base del documento è, dunque, relativa a quali circostanze possono rendere il concetto di "*Human-In-The-Loop*" un ostacolo alla diffusione dell'alta tecnologia, in particolare dell'Intelligenza Artificiale, nella "*National Security Enterprise*".

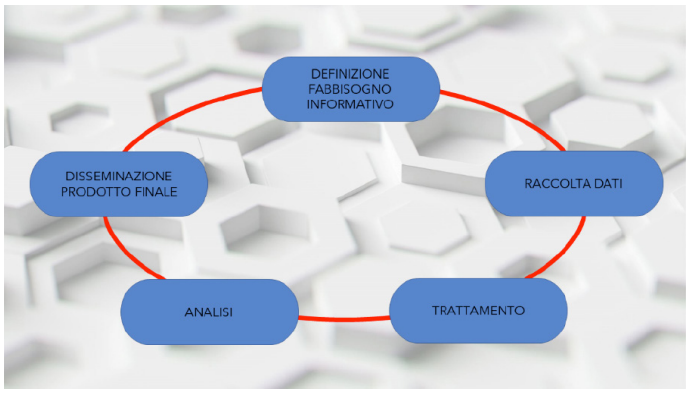
Intelligenza Artificiale e *Policy Planning*. Definizione di *Hyper-Loop*.

Con l'introduzione dell'Intelligenza Artificiale nel processo decisionale politico, la ricerca di sinergie tra Uomo e Macchina genera una triplice sfida:

1. Come possono i prodotti informativi ottenuti con l'introduzione dell'Intelligenza Artificiale migliorare le procedure decisionali umane? In che misura tali prodotti dovrebbero essere ritenuti affidabili - per riflettere un'appropriata valutazione del contesto situazionale e strategico - nell'informare le decisioni umane?
2. In che misura il processo decisionale assistito dall'Intelligenza Artificiale dovrebbe sostituire o integrare il processo decisionale umano?
3. Quali sono le interazioni tra le forze in competizione in un determinato scenario, se non in stato di conflitto, palese o ibrido?

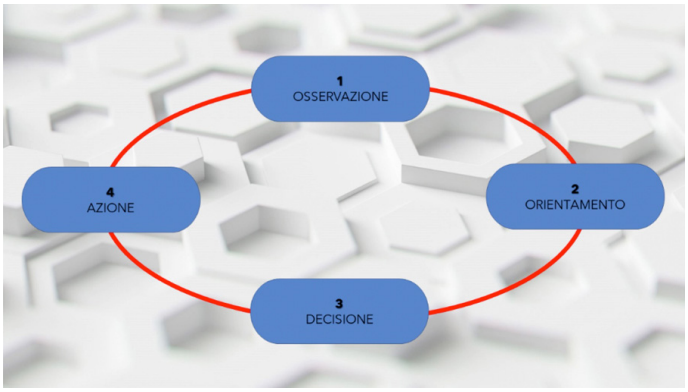
La complessità raggiunta dai sistemi decisionali ampliati dall'Intelligenza Artificiale determina la necessità di ridefinire la portata delle informazioni disponibili e del loro significato. Le tecnologie basate sull'Intelligenza Artificiale creano nuove opportunità e problematiche, sia all'interno delle burocrazie militari che tra gli istituti di ricerca in materia di sicurezza, con il processo [dati → informazioni → Intelligenza Artificiale → decisioni] come nuovo paradigma tecnologico.

I sistemi di Intelligenza Artificiale, e le conseguenti elaborazioni avanzate dei dati, consentono di analizzare ex ante ogni specifica decisione di politica governativa (in termini di azioni, conseguenza e reazioni) e di registrarne gli effetti in tempo reale. Come punto di partenza nell'analisi di come l'Intelligenza Artificiale possa potenziare la *policy*, generando una "*Hyper-policy*", possiamo considerare due cicli tradizionali di decision-making.



Il loop evidenziato nel grafico è l'Intelligence Loop tradizionale a supporto di qualunque azione di governo (Dickow, Jacob 2018).

Analogamente, può essere anche considerato il ciclo OODA (Osservazione, Orientamento, Decisione, Azione) di riferimento per l'ambiente militare. Il ciclo decisionale OODA, prevalentemente tattico (non contemplando la fase di indirizzo governativo) ma comunque scalabile a livello strategico, è più diretto di quello tradizionale e più "aumentabile" tramite Intelligenza Artificiale.



Date queste premesse, è lecito chiedersi quanto un ciclo di *policy planning* del tipo di quello qui rappresentato possa giovarsi dell'introduzione di strumenti tecnologicamente avanzati di Intelligenza Artificiale. In altre parole, se un "salto tecnologico" possa produrre una maggiore efficienza nell'*output* finale.

Possiamo aspettarci due potenziali risposte alternative: (1) una interna al ciclo informativo, (2) l'altra interna alle modalità di lavoro alla base del prodotto finale.

1. Per quanto riguarda la risposta interna al ciclo informativo, come già anticipato, un recupero del divario tecnologico può migliorare l'*Intelligence Loop* solo in presenza della più efficiente struttura organizzativa, con i prodotti di Analisi Intelligence (basati sulle risultanze *HUMINT -Human Intelligence-*, *TECHINT -Technical Intelligence-* e *SIGINT -Signal Intelligence-*) che soddisfano adeguatamente il gap informativo dichiarato dall'autorità di governo a qualsiasi livello. Anche in un contesto operativo tecnologicamente "intelligente", strutture organizzative carenti e pregiudizi umani nel processo decisionale possono portare a fallimenti nel *policy planning*.

2. Per quanto riguarda la risposta interna alle modalità di lavoro, l'adattamento e l'integrazione degli strumenti tradizionali di *Intelligence* ai cambiamenti prodotti dall'Intelligenza Artificiale sarebbero sufficienti per veicolare i progressi necessari al conseguimento di posizioni di superiorità tecnologica. Nell'ultimo decennio, l'uso di Internet come "vettore di trasformazione" nell'*Intelligence* è sempre stato frenato dall'incapacità da parte delle strutture di gestire la minaccia *cyber* in un contesto di integrazione tra *web* e lavoro quotidiano (utilizzando forme arcaiche di protezione, tipo lo sdoppiamento delle postazioni di lavoro).

Alcune nuove iniziative hanno cercato di mostrare "interfacce di adeguatezza", come la comunicazione sui *social media*, ma nessuna di queste ha rappresentato un reale cambiamento radicale rispetto alle tradizionali modalità di lavoro.

Come il concetto di *Hyper-Loop* (ossia il ciclo di policy potenziato con l'Intelligenza Artificiale) può migliorare l'efficienza nell'*Intelligence*? La chiave è nell'adattamento efficace, ossia nel progressivo, pragmatico e metodico assorbimento e integrazione dei nuovi processi organizzativi basati sulla Intelligenza Artificiale nelle strutture consolidate[2].

L'*Hyper-Loop* è un ciclo di analisi continuo, dove il fabbisogno informativo è soddisfatto da un supporto decisionale permanente. Nasce dall'associazione tra Intelligenza Artificiale ed il tradizionale ciclo di *policy* laddove in ogni fase vi è un'integrazione tecnologica in base all'utilità specifica per ogni fase del processo.

Nel "ciclo assistito" di *policy*, l'Intelligenza Artificiale svolge l'intero "feedback loop," automaticamente ed iterativamente, basandosi su continue immissioni di *Big Data* (che, nel caso dell'*Intelligence*, sono rappresentate dalle evidenze della ricerca operativa), addestrando algoritmi di raccolta ed analisi (che, nel caso dell'*Intelligence*, devono essere rappresentati da programmi costruiti *in-house* non potendo impiegare prodotti in commercio per evidenti vulnerabilità conseguenti), migliorando ad ogni *round* ciò che funziona e aggiustando ciò che non funziona, e fornendo al destinatario finale l'output di cui ha bisogno, nella forma grafica a lui necessaria

2. Per la realizzazione del grafico "Hypercicle", ringraziamo il Col. Francesco Marradi per le considerazioni innovative suggerite.

Il progresso dell'Intelligenza Artificiale nella "*National Security Enterprise*"

I rapidi avanzamenti tecnologici stanno rendendo tali scenari sempre più possibili e vicini alla perfezione. Oggi, l'Intelligenza Artificiale sta subentrando ad Internet come "tecnologia trasformativa" attraverso nuove applicazioni basate su processi di *Machine Learning* condizionate alla disponibilità di enormi patrimoni di dati strutturati e non (i più preziosi in quanto grezzi) per "addestrare" gli algoritmi in termini di classificazione ed interpretazione delle informazioni (Dickow, Jacob 2018). La quantità, la qualità e la rappresentatività dei dati di addestramento sono fattori decisivi per un corretto apprendimento da parte della Macchina e il suo successivo utilizzo ottimale nella previsione.

Paul Scharre (2019) ha riassunto come l'Intelligenza Artificiale cambi radicalmente il panorama della sicurezza nazionale, migliorando il conflitto ad alta e bassa intensità, lo spionaggio e l'*Intelligence*. Le implicazioni dell'Intelligenza Artificiale per la sicurezza nazionale e per l'*Intelligence* vanno dalla produzione di contenuti mediatici contraffatti ("*deepfake*"), agli armamenti autonomi, come, ad esempio, sciami di droni armati (Allen and Chan 2017).

Nel secolo scorso, il matematico John von Neumann ritenne che il progresso tecnologico ci avrebbe guidati verso una "singolarità" essenziale nella storia della razza umana, oltre la quale le attività, così come a noi note, non avrebbero più potuto essere considerate tali. Egli fu il primo a chiamare questo evento una "singolarità'." (Oxtoby, Pettis, Price 1958).

Murray Shanahan, professore all'*Imperial College* di Londra, ha sottolineato come l'Intelligenza Artificiale possa produrre un imprevedibile "*feedback loop*" ("Quando ciò che viene ingegnerizzato è l'intelligenza cerebrale umana, cioè la base dell'ingegneria, l'Intelligenza Artificiale può migliorare sé stessa autonomamente. In breve tempo, secondo l'ipotesi della singolarità, l'essere umano può essere rimosso dal ciclo decisionale", Shanahan 2015).

Per la casualità di questo "ciclo di *feedback*", nell'Occidente tecnologicamente avanzato, la necessità etica di preservare il concetto di *Human-In-The-Loop* nel processo decisionale sta assumendo priorità. Tuttavia, altri attori globali meno sensibili dal punto di vista etico stanno sfruttando le preoccupazioni occidentali per aumentare la loro superiorità tecnologica. Ciò sfruttando le titubanze etiche nell'avanzamento della ricerca, ma anche le inefficienze prodotte dall'Uomo nell'applicazione del progresso tecnologico (meno diffuse, se non addirittura assenti, in Stati autoritari).

L'analisi costi/benefici del concetto di *Human-In-The-Loop* è diventata, dunque, il riferimento teorico precedente ad ogni cambiamento di paradigmi tecnologici inerenti l'Intelligenza Artificiale.

Potenziali risposte alla domanda di ricerca

Nelle decisioni politiche, l'*Intelligence* non è mai il fattore decisivo. Le influenze che contano sono quelle che un leader politico porta con sé: il suo senso strategico, le lezioni che ha tratto dalla Storia o dall'esperienza personale, gli imperativi della politica interna, le proprie emozioni e paure. Un promemoria o un *briefing* preparato da qualche analista sconosciuto difficilmente ha la possibilità di influenzare la decisione finale.

Una buona *Intelligence* può, però, essere fondamentale nell'aiutare a gestire l'incertezza, definendo, tramite la costruzione di scenari credibili e fondati, la portata di tale indeterminatezza ed evidenziando ciò che all'occhio profano rimarrebbe nascosto. Può distinguere la "vera incertezza" dalla "semplice ignoranza", anche se non può evitare le sorprese che Donald Rumsfeld chiamava "incognite sconosciute".

Quattro sono le potenziali risposte alla domanda di ricerca offerte in questa sede.

1. La politicizzazione dell'*Intelligence*

Il concetto di Human-In-The-Loop può ostacolare la diffusione della tecnologia all'interno della "National Security Enterprise" in una condizione di intensa politicizzazione dell'Intelligence.

Nella "Rivoluzione Digitale", il contributo della politica al miglioramento tecnologico della "*National Security Enterprise*" è scadente soprattutto a causa della limitata conoscenza sia dei meccanismi e delle priorità dell'*Intelligence Loop*, sia dei concetti base dell'Intelligenza Artificiale (*Machine Learning, Big Data, e 5G*).

Successivamente al ricevimento di macro-indirizzi informativi da parte dell'autorità di governo, spesso generici ed incompleti, nella seconda fase dell'*Intelligence Loop* (Pianificazione e Direzione), la Comunità *Intelligence* deve dettagliare i propri piani

di ricerca informativa in modo indipendente per poter operare al massimo delle sue potenzialità, proponendo priorità ai decisori politici da perseguire in una prospettiva globale. Queste proposte, pur finalizzate al conseguimento dei macro-indirizzi ricevuti, spesso si scontrano con l'agenda dei decisori, a sua volta frequentemente non nota alla "*National Security Enterprise*".

Le micro-esigenze informative dei decisori politici, talvolta, non vengono condivise con la Comunità Intelligence per mancanza di fiducia, per timori di compromissioni (in presenza di fughe di notizie), o semplicemente perché è la politica a non conoscere cosa l'*Intelligence* le può fornire di utile.

Per ottenere la fiducia del decisore politico, spesso la "*National Security Enterprise*" sposta l'intera sua attività di ricerca informativa verso i micro-obiettivi individuali di membri del governo, del parlamento, o di altre *élite* politiche dando vita alla c.d. "politicizzazione dell'*Intelligence*". Poiché la somma delle micro-esigenze dei singoli politici non è uguale ai macro-indirizzi informativi per la realizzazione del bene pubblico-*Intelligence*, detta politicizzazione va a danno dell'indipendenza che dovrebbe essere alla base di una delle funzioni vitali dello Stato, ossia la tutela della sicurezza nazionale.

Problemi nel rapporto tra "*National Security Enterprise*" (il produttore di nuova conoscenza) e i decisori politici (i consumatori di nuova conoscenza) possono sorgere in ogni fase dell'*Intelligence Loop* (Johnson, Lock K. 1986). In primo luogo, bias cognitivi e comportamentali dovuti alla presenza dell'Uomo nel ciclo possono porsi ad ostacolo nell'offrire prodotti di analisi competitivi scevri da considerazioni soggettive (spesso camuffate dietro l'appellativo di "esperienza").

Peggio ancora, quando l'*Intelligence* raccolta viene veicolata - ancora grezza e non contestualizzata - negli edifici governativi, questa subisce un processo di appesantimento causato da errori individuali nell'interpretazione, da pressioni burocratiche nel dover (o voler) necessariamente "leggere" determinate evidenze (che in realtà una accurata analisi avrebbe evitato). La differenza tra questa realtà distorta e una situazione ideale di valutazioni affidabili è una "zona grigia" composta da ipotesi sbagliate, valutazioni manipolate, analisi imprecise e parzialità.

Consapevole dell'esistenza di pregiudizi e disinformazioni mescolate a fatti veritieri, la *leadership* della "*National Security Enterprise*", alla fine, spesso decide di optare per dati che possono essere misurati - ad esempio, dai dispositivi di sorveglianza -, cercando di rendere accurati e coerenti i propri rapporti e le proprie valutazioni (Brewer, Bracken 1984). Un aereo spia di ricognizione è qualcosa di tangibile rispetto ad una fonte umana clandestina: scatta fotografie, e la sua esistenza può essere dimostrata (in contesti democratici) davanti a Commissioni parlamentari in caso di richieste di stanziamenti o di inchieste (Burrows 1986).

In secondo luogo, la politicizzazione dell'*Intelligence* ha conseguenze negative sulle scelte operative, orientando le preferenze verso fonti tecniche (*TECHINT* e *SIGINT*, in primis) rispetto alle fonti umane (*HUMINT*). L'Intelligence, infatti, non può mai parlare esplicitamente di "*covert action*" davanti alle Commissioni parlamentari (George 2020). Per i politici, le "azioni clandestine" sono qualcosa di astratto, quindi inutili (e pericolose) per il loro consenso elettorale. Inoltre, le gigantesche corporazioni aerospaziali fanno pressione per contratti di sorveglianza e hardware con i Ministeri della Difesa. La *HUMINT*, invece, non ha sostenitori così influenti e ha in più costi enormi in termini di potenziale compromissione di identità e documenti, e perdita di vite umane.

Date le pressioni di cui sopra, si comprende perché i politici siano poco incentivati a stanziare ingenti stanziamenti di bilancio per investimenti ad alta tecnologia, quando non siano funzionali al miglioramento del consenso politico. Solo un'azione congiunta tra la *leadership* dell'*Intelligence* e il complesso militare-industriale può esercitare adeguate azioni di *lobbying* per creare maggiore attenzione verso detti investimenti.

2. La resistenza culturale alla tecnologia all'interno della Comunità *Intelligence*

Il concetto di Human-In-The-Loop può rappresentare un ostacolo alla diffusione della tecnologia all'interno della National Security Enterprise in presenza di "resistenza culturale".

La *leadership* della "*National Security Enterprise*" è sempre più incline a guardare all'Intelligenza Artificiale e ai lavori basati sull'automazione per soddisfare la crescente domanda di nuova conoscenza con una forza lavoro minore. La tecnologia moderna, inoltre, richiede l'aggiornamento (e talvolta la sostituzione) delle infrastrutture e delle attrezzature esistenti. Entrambi gli argomenti rafforzano una "resistenza culturale" da parte degli addetti ai lavori.

Esiste una fisiologica avversione degli esseri umani verso il progresso tecnologico dovuta alla modifica delle gerarchie esistenti nei posti di lavoro, ed alla necessità di aggiornare le loro competenze e di cambiare i loro metodi di lavoro. Il rischio maggiore di questa "resistenza culturale" è quello di

creare nuova disoccupazione in presenza di casi di sabotaggio (cioè minacce endogene all'organizzazione) contro le politiche di innovazione.

Una recente indagine sull'adozione della *Robotic Process Automation* (RPA) in Europa ha rilevato che uno degli ostacoli più critici alla crescita della RPA è "l'ostruzionismo", con il 33% degli intervistati che definisce la "resistenza organizzativa al cambiamento" come il principale ostacolo (Jones, Bakker 2018).

La "resistenza culturale" è decisamente un ostacolo significativo alla competitività digitale della Comunità *Intelligence*. Le spie umane, come tradizionalmente considerate, sono in via di estinzione non potendo contrastare (nonostante i tentativi dei "tradizionalisti") la forza devastante della tecnologia sul terreno. Le spie di oggi hanno lo stesso problema di ieri: la necessità di essere invisibili. Ciò che è cambiato è il nemico. Oltre ad ingannare altri esseri umani, gli agenti devono oggi anche raggirare le macchine.

Nel 2018, al *GEOINT Symposium* di *Tampa* (Florida), ospitato dalla *U.S. Geospatial Intelligence Foundation*, Dawn Meyerriecks, vicedirettore della CIA (Central Intelligence Agency) responsabile dell'innovazione digitale, ha affermato[3] che nell'era dei *social media* le difficoltà per gli agenti operativi a lavorare sotto una falsa identità sono crescenti. Nel 2005, le identità segrete della CIA avevano specifiche caratteristiche digitali: una casella postale in Virginia e un Social Security Number.

Oggi, inserendo questi indicatori in un *database open-source*, è possibile ottenere una lista di identità degne di un'ulteriore sorveglianza per ogni controspionaggio straniero (Lord (2015).

Secondo Meyerriecks, con alcuni progressi nella localizzazione satellitare e nell'*Intelligence* geospaziale, le spie umane non avranno alcuna possibilità di affermarsi contro la prossima generazione di Intelligenza Artificiale. Per questo l'Agenzia sta cambiando il target passando dall'agente straniero alla Macchina.

Amazon e Google hanno perfezionato strumenti e infrastrutture per l'analisi di grandi insiemi di dati per identificare e persino prevedere modelli di *business* fraudolenti. Gli stessi strumenti possono identificare attività clandestine, morfologicamente simili alle frodi. Cercando in vaste aree di informazioni digitali alla ricerca di indicatori specifici che potrebbero indicare un'identità di copertura, i computer valutano istantaneamente se l'identità di un individuo è probabile che sia reale o falsa, in base alla quantità e alle caratteristiche dei dati disponibili relativi a tale identità.

Con simili scenari così ostili agli esseri umani, comportamenti di ostruzionismo nel lavorare fianco a fianco con le Macchine possono creare inefficienze tali nella diffusione dell'alta tecnologia da giustificare, nel prossimo futuro, l'avvio di un progressivo processo di sostituzione tra Uomo e Macchina.

3. Video disponibile su vimeo.com/266022328.

3. Restrizioni all'accesso ai dati

Il concetto di Human-In-The-Loop può ostacolare la diffusione della tecnologia all'interno della "National Security Enterprise" in presenza di limitazioni alla disponibilità dei dati.

Nell'attuale configurazione della Comunità Intelligence, la gerarchia governa l'accesso ai dati. Generalmente, l'accesso ai dati sensibili è limitato, in particolare *HUMINT* e *SIGINT*. Dato l'elevato costo (umano e tecnico) del loro trattamento, gli analisti spesso non possono accedervi a causa delle minacce di compromissione. Ciò accade ancora di più con la politicizzazione dell'*Intelligence* quando è la politica a favorire le carriere.

L'accesso limitato ai dati sensibili frustra le comunità di analisti e rende l'Intelligenza Artificiale inutile.

Come ogni materia prima, i dati devono essere raccolti, affinati e resi disponibili per l'analisi. I dati sono rinnovabili, autogeneranti e virtualmente senza limiti. Entro il 2025, la sfera globale dei dati supererà i 175 zettabyte rispetto ai 33 zettabyte del 2018 (Reinsel, Gantz, Rydning, 2018). Entro il 2020, l'Internet degli oggetti (IoT) sarà composta da oltre 50 miliardi di dispositivi connessi, che producono e consumano dati in modo silenzioso e inesorabile (Davis 2018).

Negli ultimi anni, l'analisi *Intelligence* è diventata sempre più impegnativa a causa di un aumento senza precedenti del volume e della velocità dei dati sia grezzi che strutturati (principalmente dati testuali, audio e video, che rappresentano il 95% di tutti i *Big Data* in circolazione, Gandomi, Haider 2015), raccolti attraverso piattaforme classificate e *open-source*. Interrogare i *Big Data* strutturati è relativamente semplice. I dati non strutturati, invece, sono allo stato grezzo e ancora da trattare e interpretare, ma - per questi motivi – anche molto preziosi. Ne sono un esempio i *social media*, le *e-mail*, i *blog* e i contenuti multimediali (Sivarajah, Kamal, Irani, Weerakkody, 2017).

L'abnorme volume di informazioni, ancora da elaborare prima di diventare "*actionable Intelligence*", sta sovraccaricando le capacità cognitive di ogni singolo analista e di ogni team. Dal 1995 al 2016, la quantità di lettura richiesta a un analista di *Intelligence* americano medio dedicato ad un paese a bassa priorità è aumentata da 20.000 a 200.000 parole al giorno. La previsione per il 2025 è circa un volume di dati digitali dieci volte superiore a quello attuale (Regens 2019).

Una volta che i dati siano stati contestualizzati e trasformati in informazioni potenzialmente rilevanti per l'*Intelligence*, la cognizione umana diventa vitale per la sua interpretazione. La capacità di astrazione umana conserva, infatti, un notevole vantaggio rispetto alla macchina. Per ricordare un'immagine, un testo, un numero, un essere umano necessita di vederlo un numero di volte notevolmente inferiore a quello di una macchina (Turing 1950).

La potenza della tecnologia può essere efficacemente impiegata per aumentare le prestazioni umane nell'*Intelligence Loop* "alimentando" le capacità umane (cognitive e fisiche) con l'apporto che le macchine possono fornire, traslando in avanti la "frontiera delle possibilità di produzione" della Comunità *Intelligence* ed aumentando il volume di dati che l'uomo può elaborare senza ridurre la sua capacità di concentrazione, apprendimento e identificazione degli elementi chiave incorporati in quei flussi di dati.

4. "*Outsourcing*" delle funzioni vitali del ciclo dell'Intelligence

Il concetto di Human-In-The-Loop può ostacolare la diffusione della tecnologia all'interno della National Security Enterprise in presenza di "outsourcing" dei compiti tecnologici dell'Intelligence Loop.

Ragioni etiche potrebbero indurre i contractor, non appartenenti alla "*National Security Enterprise*" (condizionati da accordi di non divulgazione, ma disinteressati emotivamente al concetto intrinseco di tutela della sicurezza nazionale), a rifiutare di sviluppare tecnologie per i teatri di guerra.

La *partnership* tra Google e il Dipartimento della Difesa statunitense relativa al "Project Maven" fornisce un caso di studio. Nell'aprile 2017, il Pentagono ha istituito il "*Algorithmic Warfare Cross-Functional Team*" (*AWCFT*) noto come "*Project Maven*", per integrare *Machine Learning* e *Big Data* a livello operativo militare (Work 2017).

Google ha collaborato al "*Project Maven*", applicando le proprie soluzioni di Intelligenza Artificiale all'attività di velivoli senza equipaggio (*Unmanned Aerial Vehicles*, *UAV*) sia nel *targeting* dei droni (Fang 2018) che nell'analisi delle riprese effettuate (Conger, Cameron 2018). Per aiutare gli analisti ad esaminare gli oggetti nelle immagini, Google ha fornito al Pentagono il suo "*TensorFlow*", una *API* (*Application Programming Interface*, Pettey 2017) *open-source* utilizzata nelle applicazioni di *Machine Learning* di Google per riconoscere gli oggetti sui dati (Conger, Cameron 2018). Il primo obiettivo della *partnership* è stato quello di sviluppare la capacità di rilevare automaticamente circa 38 classi di oggetti regolarmente presenti nei filmati dei droni militari.

Nell'aprile 2018, circa 3.100 dipendenti di Google hanno firmato una lettera che invitava l'allora CEO Pichai Sundararajan ad abbandonare il "*Project Maven*". Nonostante le assicurazioni fornite dal management di Google di essersi limitato al solo rendere disponibile il software *open-source* per il riconoscimento degli oggetti (fruibile da qualsiasi *client* di Google Cloud) per aiutare l'aviazione militare statunitense ad alleggerire il carico di lavoro dei suoi analisti, sulla spinta interna Google ha dovuto abbandonare il progetto all'inizio del 2019.

Conclusioni

Nell'attuale, profondo cambiamento tecnologico delle Comunità *Intelligence*, l'Intelligenza Artificiale può aumentare l'efficienza delle fasi di *reporting* e la reattività della *National Security Enterprise* alle esigenze dei responsabili politici.

La questione etica riguarda il grado di inclusione dell'essere umano nell'*Intelligence Loop* man mano che l'automazione dei processi decisionali aumenta. La politicizzazione dell'*Intelligence*, la resistenza degli addetti ai lavori, l'accesso limitato ai dati per gli analisti

e l'"*outsourcing*" delle funzioni tecnologiche del ciclo dell'*intelligence* rendono difficile per i "sostenitori" dell'essere umano prevalere sui sostenitori della macchina. Inoltre, le azioni di *lobbying* del complesso militare-industriale orientano la scelta verso tecnologie intelligenti e autonome del ciclo.

Nell'attuale fase storica, nelle Comunità *Intelligence* le capacità analitiche sono inutili se non sono accompagnate da forti relazioni interpersonali con la politica. Il primato delle relazioni personali sulle capacità intellettuali rende l'efficienza dell'Intelligenza Artificiale quasi ingombrante, se rapportata alle decisioni assunte da gruppi d'interesse nell'influenzare il processo decisionale governativo e parlamentare.

Nonostante il riconoscimento pubblico dei profondi cambiamenti tecnologici, le odierne istituzioni di *Intelligence* continuano ad operare con lo spirito della Guerra Fredda. Tali organizzazioni non hanno ancora incorporato la complessità dell'attuale era tecnologica, che richiede di abbandonare l'idea che la "*National Security Enterprise*" abbia il monopolio della conoscenza.

La progressiva riduzione delle capacità di tutela della segretezza a causa dell'avanzare dei *social media* e dell'estensione della sorveglianza "intelligente" aumenterà sempre di più la capacità delle macchine di ricercare "impronte" nel mondo digitale.

Questi temi devono rappresentare un richiamo all'azione e non una capitolazione al determinismo tecnologico. Nell'era digitale, le "*covert action*" hanno bisogno di nuove metodologie, e l'*Intelligence* deve sfruttare al meglio la tecnologia per ottenerle. Allorquando il riconoscimento facciale vanificherà un'operazione clandestina, sarà perché l'*Intelligence* e i responsabili politici non avranno riconosciuto adeguatamente la minaccia e avranno rinunciato ad agire deliberatamente per mitigarne gli effetti.

In un mondo anarchico come quello dell'*Intelligence*, in cui non esistono regole né autorità che garantiscono l'ordine, solo la creazione di massicci patrimoni di dati e la velocità e l'automazione nel trattarli garantiranno alle Comunità *Intelligence* statali di sopravvivere come funzione rilevante del processo decisionale in materia di sicurezza nazionale, evitando di lasciare il posto ad analoghe componenti private.

Lavori citati

Allen, Greg, and Taniel Chan. 2017. *Artificial Intelligence and National Security*. Belfer Center for Science and International Affairs, Harvard Kennedy School.

Brewer, Gary D., and Paul Bracken. 1984. "Some Missing Pieces of the C3 Puzzle". *Journal of Conflict Resolution* 28: 453.

Burrows, William E. 1986. *Deep Black: Space Espionage and National Security.* p.116. Random House, New York

Check, Meghan A. 2018. *Augmenting Intelligence: What Augmented Reality Technology Means for the Intelligence Community*, in Kosal, Margaret E., "Technology, and the Intelligence Community. Challenges and Advances for the 21st Century." Springer International Publishing AG.

Conger, Kate, and Dell Cameron. 2018. *Google Is Helping the Pentagon Build AI for Drones*, Gizmodo.

Davis, Gary. 2018. "2020: Life with 50 billion connected devices." *2018 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, USA.

Dickow, Marcel, and Daniel Jacob. 2018. "The Global Debate on the Future of Artificial Intelligence. The Need for International Regulation and Opportunities for German Foreign Policy." *SWP (Stiftung Wissenschaft und Politik)* Comments, no. 23.

Fang, Lee. 2018. *Google is quietly providing AI technology for drone strike targeting project*, The Intercept.

Gandomi, Amir, and Murtaza Haider. 2015. "Beyond the Hype: Big Data Concepts, Methods, and Analytics." *International Journal of Information Management*. 35: 137–144.

George, Roger Z. 2020. *Intelligence in the National Security Enterprise*, Georgetown University Press.

Johnson, Lock K. 1986. "Making the Intelligence "Cycle" Work." *International Journal of Intelligence and Counterintelligence*, 1(4): 1-23.

Jones, Stanton, and Alex Bakker. 2018. "RPA in Europe: Enterprise Plans, Budgets & Organizational Impact." *ISG Insights*.

Lord, Jonathan. 2015. "Undercover Under Threat: Cover Identity, Clandestine Activity, and Covert Action in the Digital Age". *International Journal of Intelligence and CounterIntelligence*. 28(4): 666-691,

Oxtoby, John C., Pettis, Billy J., and Griffith B. Price. 1958. "John von Neumann, 1903-1957". *Bulletin of American Mathematical Society* 64(3, Part II.)

Pettey, Christy. 2017. *Put APIs at the Center of Your Digital Business Platform*, https://www.gartner.com/smarterwithgartner/put-apis-at-the-center-of-your-digital-business-platform/.

Regens, James L. 2019. "Augmenting human cognition to enhance strategic, operational, and tactical intelligence." *Intelligence and National Security* 34: 1-15.

Reinsel, David, Gantz, John, and John Rydning. 2018. "Data Age 2025. The Digitization of the World. From Edge to Core." *IDC White Paper*, Seagate.

Scharre, Paul. 2019. *Army of None: Autonomous Weapons and the Future of War*, W.W. Norton & Co Inc.

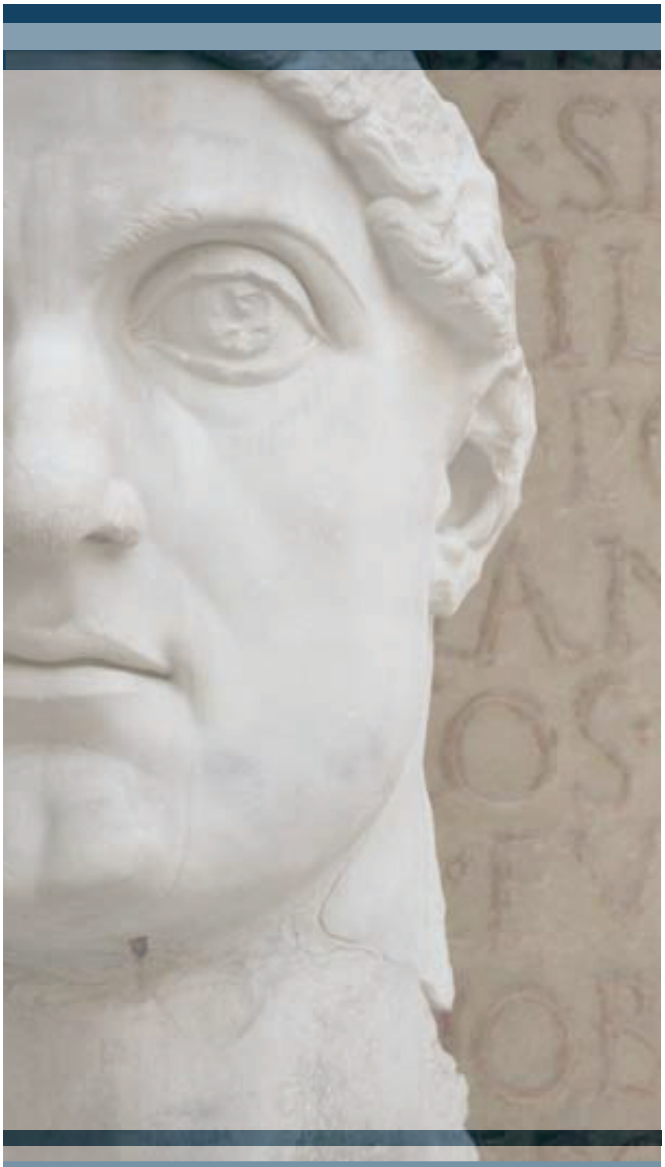
Shanahan, Murray. 2015. "The Technological Singularity." *MIT Press Essential Knowledge*.

Sivarajah, Uthayasankar, Kamal, Muhammad Mustafa, Irani, Zahir, and Vishanth Weerakkody. 2017. "Critical Analysis of Big Data Challenges and Analytical Methods." *Journal of Business Research* 70: 263–286.

Soni, Anmol, and Margaret E. Kosal. 2018. *Conclusions*, in Kosal, Margaret E., "Technology, and the Intelligence Community. Challenges and Advances for the 21st Century." Springer International Publishing AG.

Turing, Alan M. 1950. "Computing Machinery and Intelligence." *Mind* 49: 433–460.

Work, Robert. 2017. *Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)*. Deputy Secretary of Defense Memorandum. US Department of Defense.



ISTITUTO ITALIANO
DI STUDI STRATEGICI
ITALIAN INSTITUTE
OF STRATEGIC STUDIES
Niccolò Machiavelli

L'Istituto Italiano di Studi Strategici *"Niccolò Machiavelli"* è un'associazione culturale senza scopo di lucro costituita a Roma nel 2010.

L'Istituto, think tank indipendente, nasce dall'iniziativa di un gruppo internazionale di personalità del mondo economico, accademico ed istituzionale civile e militare, con l'obiettivo di contribuire alla rinascita del pensiero strategico italiano.

La complessità e l'ampiezza delle sfide che attendono il Paese nel XXI secolo richiede conoscenza, consapevolezza e capacità prospettiche. L'Istituto Machiavelli, anche grazie al proprio network globale, promuove l'interscambio culturale tra il decisore italiano ed internazionale, pubblico e privato, e svolge attività di ricerca finalizzate ad elevare il livello di competitività globale del "Sistema Paese".

L'Istituto Machiavelli, autonomamente o in collaborazione con istituzioni, organizzazioni ed aziende nazionali ed estere, realizza studi ed analisi strategiche *policy-oriented*, organizza briefing, seminari e workshop, cura corsi di alta formazione per i *leader*.

Per ulteriori informazioni:

Istituto Italiano di Studi Strategici "Niccolò Machiavelli"
Circonvallazione Clodia N. 163/167
00195 – Roma
Tel.: (+39) 06 45422952
Fax: (+39) 06 97259168
email: info@strategicstudies.it
www.strategicstudies.it