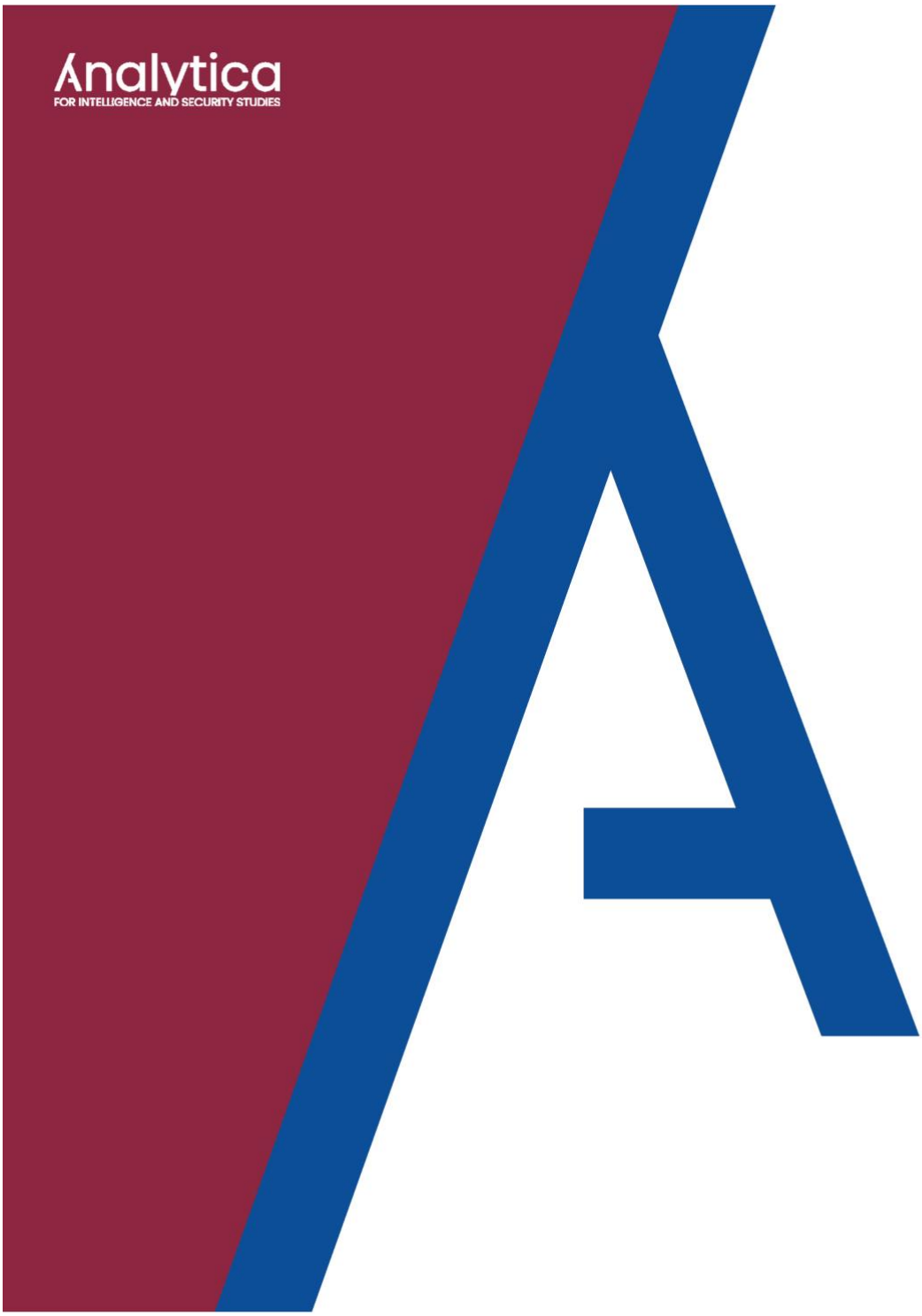

L’intelligenza artificiale nella Nuova Rivoluzione degli Affari Militari.

Arnold Koka

Analytica for intelligence and security studies

Paper Sicurezza&Difesa

L'intelligenza artificiale nella Nuova Rivoluzione degli Affari Militari.

Arnold Koka

Correzioni e revisioni a cura del Dottor PANEBIANCO Andrea

Torino, novembre 2020

Il futuro degli affari militari è nel network. Lo sviluppo delle ICT (Information&Communication Technologies) ha costituito la base tecnologica per la definizione delle teorie militari contemporanee, dove l'obiettivo fondamentale consiste nell'integrazione lineare e trasversale di tutti gli elementi di una forza in una stessa rete virtuale.[1] Una trasformazione finalizzata all'incremento della rapidità dell'azione militare, sempre più spesso affidata a sistemi autonomi come i mezzi a pilotaggio remoto, in cui l'elemento umano è fisicamente distinto – e distante – dalla piattaforma, spesso anche a migliaia di chilometri di distanza. In un mondo militare dominato dall'esigenza di rapidità e da sistemi autonomi, l'intelligenza artificiale (IA) costituisce una funzione rilevante per strategie di sicurezza nazionali che mirino ad identificare capacità tecnologiche in grado di definire il futuro quadro strategico della Difesa internazionale. Risulta dunque di particolare interesse esaminarne le opportunità dal punto di vista capacitivo così come le complessità e le incognite concettuali. L'IA dimostra essere di grande aiuto in attività specifiche, come l'analisi in tempo reale di minacce cyber, l'elaborazione di dati e immagini o nelle operazioni di guerra elettronica.[2] Tuttavia, la capacità di intervenire sul piano strategico e operativo, mediante l'introduzione di nuovi concetti e dottrine, risulta essere l'incognita maggiore. L'IA potrebbe avere implicazioni notevoli per concetti di deterrenza nucleare, proiezione del potere internazionale e delle stesse relazioni e partnership internazionali nei programmi di Difesa e procurement. Tutto ciò però non è scontato: i dubbi sul suo effettivo ruolo negli affari militari non mancano, tantomeno gli scetticismi più radicali, che contestano l'esistenza stessa di una vera e propria IA.[3] Ciononostante, alla luce dell'attuale scenario tecnologico e militare, la dimensione Difesa non può prescindere da considerare l'IA come una funzione di interesse strategico nel breve e lungo termine.

L'IA e la Terza Offset Strategy

Ogni attore nello scacchiere globale ricerca il conseguimento di un vantaggio competitivo netto per le proprie capacità militari rispetto ai suoi competitor. Ciò può essere ottenuto competendo in maniera simmetrica, ossia investendo in capacità simili a quelle con cui i quali i propri avversari conducono i propri affari militari; in maniera asimmetrica, introducendo degli '*offset*', elementi di discontinuità nella conduzione delle operazioni militari tali da modificare lo scenario militare per tutti gli attori coinvolti nel contesto globale. È questa la teoria della "Rivoluzione negli Affari Militari"[4], definibile come il cambiamento dell'intera struttura della conduzione degli Affari Militari rispetto al passato per tutti gli attori statali, risultante dall'introduzione di un nuovo elemento tecnologico nell'ambito militare. L'introduzione di un elemento di discontinuità è suscettibile di modificare tutti i livelli degli Affari Militari: la tattica, le operazioni, la strategia, le dottrine, le organizzazioni e le strutture stesse legate all'ambito della Difesa, determinando la necessità per gli Stati di acquisire strategie di sicurezza nazionali che si adattino all'evoluzione degli scenari militari

[1] Michele Nones, Alessandro Marrone, La trasformazione delle Forze Armate: il programma Forza NEC, IAI, 2011
[2] How AI Could Change The Art Of War, in Artificial Intelligence, the new frontline in defense, di BreakingDefense
[3] Intervista ad opera di ActuIA a Luc Julia, co-creatore di Siri ed ex-Chief Technology Officer (CTO) e Vice-Presidente per l'Innovazione di Samsung, https://www.youtube.com/watch?v=w4EIH7eiLpE
[4] Michael G. Vickers, Robert C. Martinage, A Revolution in War, Center for Strategic and Budgetary Assessments (CSBA), 2004

globali.

Gli Stati Uniti hanno ricercato la supremazia militare mediante l'adozione di tre *offset strategies* a partire dalla metà del XXI secolo.[5] La prima offset strategy fu introdotta nel 1953 nella "New Look Strategy" del Presidente Dwight D. Eisenhower, e mirava a sfruttare gli avanzamenti tecnologici statunitensi nell'ambito nucleare a discapito delle capacità convenzionali sovietiche.[6] La seconda fu introdotta nel 1977, dal Segretario della Difesa USA, Harold Brown, e mirava allo sviluppo di sistemi di munizionamento di precisione (PGMs) e alla loro integrazione in strutture di comando e controllo (C2) e di intelligence, sorveglianza e ricognizione (ISR).[7] Tuttavia, la supremazia statunitense negli ambiti di riferimento della Seconda Offset Strategy si sta logorando, con Cina e Russia più vicine al raggiungimento di una parità nelle capacità militari. Il Dipartimento della Difesa USA ha così riconosciuto la necessità di introdurre una Terza Offset Strategy, avviata nel 2014 dal Segretario della Difesa USA, Chuck Hagel, nella Defense Innovation Initiative.[8] Tale strategia è orientata alla deterrenza verso Cina e Russia, e orienta il proprio focus sulla ricerca e lo sviluppo (R&S) di capacità tecnologiche da utilizzare in specifici settori quali: sistemi autonomi avanzati; sistemi ad apprendimento autonomo; decision-making collaborativo uomo-macchina; operazioni umane assistite; sistemi d'arma autonomi, guerra elettronica, integrazione di forze in rete e cyber.[9] I settori di riferimento dell'R&S della Terza Offset Strategy sono dunque orientati all'utilizzo di sistemi in cui l'utilizzo dell'IA è imprescindibile per ottenere un vantaggio competitivo che vada oltre la dimensione tattica della singola piattaforma.

L'IA nei sistemi autonomi.

L'utilizzo di sistemi autonomi per attività di ISR e di combattimento non è una prerogativa esclusiva della Terza Offset Strategy. Già durante il conflitto in Vietnam, l'utilizzo di UAV (Unmanned Aerial Vehicles) era stato consistente, con 3,435 operazioni di ISR condotte tra il 1964 e il 1975 da sistemi unmanned appartenenti alla categoria dei *Ryan Firebee*[10], nonostante fossero poco affidabili a causa di una tecnologia ancora poco matura. Nel corso dei diversi conflitti, dall'Operazione Desert Storm nel 1990-91 ad Iraqi Freedom nel 2003-2011, l'incremento nell'utilizzo di sistemi autonomi è stato esponenziale, così come la loro relativa maturazione tecnologica.

---

[5] Adam J. Boyd, Michael Kimball, The Future Operating Environment and The Third Offset, in Closer Than You Think: The Implications of the Third Offset Strategy for the U.S. Army, 2017

[6] Ibidem

[7] Robert Martinage, Toward A New Offset Strategy - Exploiting U.S. Long-Term Advantages To Restore U.S. Global Power Projection Capability, Centre for Strategic and Budgetary Assessment (CSBA), 2014

[8] Discorso del Segretario della Difesa USA, Chuck Hagel, in occasione del lancio della Defense Innovation Initiative durante il Reagan National Defense Forum Keynote, 2014, https://www.defense.gov/Newsroom/Speeches/Speech/Article/606635/

[9] Vice-Segretario della Difesa USA, Robert Work, "Assessing the Third Offset Strategy: Progress and Prospects for Defense Innovation, Center for Strategic & International Studies Headquarters, https://www.csis.org/events/assessing-third-offset-strategy, 2016

[10] Richard Clark, Uninhabited Combat Aerial Vehicles: Airpower by the People, For the People, But Not With the People, Air University Press, Maxwell Air Force Base, https://apps.dtic.mil/dtic/tr/fulltext/u2/a382577.pdf, 2000

Il loro uso permette di ricavare vantaggi in una serie di dimensioni, quali la proiezione del potere a lunga distanza e la durabilità delle missioni: entrambi gli aspetti risultano estremamente prolungati grazie all'assenza dell'elemento umano all'interno del sistema, che può dunque muoversi su lunghe distanze e per periodi prolungati, senza necessità di interruzioni, con un incremento inoltre della manovrabilità e della possibilità di accedere a teatri operativi ostili con meno rischi per il personale. Integrare l'IA in sistemi autonomi di ISR e combat può incrementare ulteriormente la loro utilità. Il Project Maven USA è emblematico per quanto riguarda le potenzialità dell'IA nell'elaborazione di dati di intelligence: esso mira ad integrare nei sistemi autonomi algoritmi abilitati dall'IA, in grado di condurre analisi su migliaia di ore di video registrati durante operazioni ISR, attività altrimenti dispendiosamente effettuate da elementi umani.[11] In tal modo, la raccolta dati viene integrata con l'analisi, velocizzando il processo decisionale umano. L'integrazione in un singolo sistema delle attività di raccolta e analisi dei dati è inoltre la base per concepire un ulteriore potenzialità dell'AI nella fusione ed elaborazione dei dati. Estendere l'integrazione dei dati da un solo sistema ad un intera struttura unica di comando e controllo, infatti, permetterebbe di evitare duplicazioni e discrepanze dovute alla provenienza delle informazioni da una molteplicità di piattaforme.[12] Ulteriore vantaggio dell'utilizzo dell'AI nei sistemi autonomi sarebbe l'inserimento del modello del "deep machine learning" adottato dall'AI, ossia la simulazione virtuale dell'attività neurale umana ai fini dell'apprendimento, grazie al quale si escluderebbero i rischi derivanti da attacchi alle linee di comunicazione tra centro di comando e drone, rendendo quest'ultimo in grado di operare senza alcun intervento umano – tecnicamente definito come *human out-of-the-loop*.[13] Non manca inoltre lo sfruttamento dell'AI nel lato *combat*. La Defense Advanced Research Projects Agency (DARPA) USA ha dato avvio al programma OFFensive Swarm-Enabled Tactics (OFFSET). Il programma prevede che unità di fanteria siano in grado di utilizzare fino a 250 *unmanned vechicles* nel corso di missioni condotte in contesti urbani.[14] Grazie all'IA, lo "stormo" di droni sarebbe in grado di muoversi, raccogliere e trasmettere informazioni, e assumere decisioni coerentemente con la condotta delle unità di terra e dei centri di comando. Sulla scia dell'utilizzo di "stormi" di sistemi autonomi, la Royal Air Force britannica ha annunciato il "Project Mosquito"[15], il cui obiettivo è accompagnare ai jet F-35 in uso una serie di UAV Loyal Wingman, che sfrutterebbero l'IA per operare attività di ISR e guerra elettronica in coerenza con il velivolo di riferimento. L'implementazione dell'IA nei sistemi autonomi è suscettibile dunque di avere importanti risvolti sulla dimensione tattica che richiederanno l'introduzione di nuovi concetti operativi, in grado di fronteggiare la molteplicità degli scenari emergenti.

---

[11] Dipartimento della Difesa USA, Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges, 2017, https://www.defense.gov/Explore/News/Article/Article/1356172/project-maven-industry-day-pursues-artificial-intelligence-for-dod-challenges/

[12] Colin Clark, 'Rolling The Marble:' BG Saltzman On Air Force's Multi-Domain C2 System, https://breakingdefense.com/2017/08/rolling-the-marble-bg-saltzman-on-air-forces-multi-domain-c2-system/, 2017

[13] Cfr. Nota 7

[14] Defense Advanced Research Projects Agency (DARPA), OFFensive Swarm-Enabled Tactics (OFFSET), https://www.darpa.mil/program/offensive-swarm-enabled-tactics

[15] United Kingdom Government Website, Dstl to develop conceptual unmanned aircraft for RAF, https://www.gov.uk/government/news/dstl-to-develop-conceptual-unmanned-aircraft-for-raf

Difesa dinamica e deterrenza nello spazio cyber.

Le recenti dottrine e traiettorie strategiche militari, quali la Terza Offset e la Network Centric Warfare (NCW), si basano come detto sull'integrazione in rete di tutti gli elementi di una forza, con il fine di generare un vantaggio esponenziale mediante un processo informativo-decisionale-esecutivo sempre più rapido. Risulta evidente dunque che la difesa dello spazio cyber, ibrido e dinamico, rappresenta una priorità per una loro efficace realizzazione. La difesa cyber non rileva però solo ai fini militari: le strategie di sicurezza nazionali non mancano di porre l'accento sulla resistenza e resilienza delle proprie infrastrutture critiche. Queste ultime sono rappresentate da servizi, sistemi, processi o beni essenziali per il mantenimento vitale della società statale, e la crescente integrazione tra la dimensione fisica e quella virtuale ne rappresenta una minaccia considerevole. Un esempio tra tutti, il malware Stuxnet, di probabile origine statunitense-israeliana, che ha colpito una struttura nucleare a Natanz, Iran, diffondendosi poi in più di 10 paesi, tra cui Cina, India, Regno Unito, Austria e Germania e causando danni economici ingenti.[16] Stuxnet consisteva in un attacco software indirizzato ad un sistema fisico di controllo dell'infrastruttura (SCADA - Supervisory Control and Data Acquisition) e non rappresenta un unicum di proiezione della minaccia cyber allo spazio fisico – dunque, non più virtuale. Simili minacce sono in grado di diffondersi in una molteplicità di piattaforme e sistemi (più di 60,000 nel caso di Stuxnet)[17], spesso senza il volere degli "attaccanti", rendendo esponenziale il grado della propria minaccia. Minacce dinamiche, proliferanti ed in costante sviluppo richiedono una Difesa in grado di adattarsi costantemente in grado di rispondere rapidamente alle necessità. L'IA è in grado di rispondere efficacemente a questi requisiti, in quanto permette di elaborare grandi quantità di dati e di assumere decisioni flessibili in un contesto in rapida evoluzione; un approccio che un sistema di difesa automatizzato non è in grado di offrire: la quantità di dati da analizzare e la necessità di assumere decisioni rapide in base al contesto rimangono in questo caso subordinate ad interventi umani, più lente rispetto a quelle operate dall'IA. Un modello esemplificativo è l'utilizzo dei *deep neural networks* (reti neurali artificiali) nei sistemi di difesa cyber. Esse consistono in algoritmi che simulano l'attività di una rete neurale biologica ai fini dell'apprendimento e dell'esecuzione di specifiche attività, caratterizzandosi per la velocità operativa e la possibilità di essere utilizzato a livello hardware e software.[18] Tali network sono particolarmente utili per il rilevamento di intrusioni informatiche o di attacchi di tipo DoS (Denial of Service), ma non solo. Ci sono risultati promettenti per quanto riguarda l'utilizzo delle reti neurali artificiali per rilevare la provenienza di Advanced Persistence Threats (APT), minacce avanzate persistenti, attacchi altamente sofisticati principalmente condotti da entità statali per obiettivi politici, economici e militari.[19]

---

[16] James P. Farwell and Rafal Rohozinski, Stuxnet and the Future of Cyber War, in Survival, Global Politics and Strategy, gennaio 2011

[17] Ibidem

[18] Enn Tyugu, Artificial Intelligence in Cyber Defense , Cooperative Cyber Defense Center of Excellence (CCD COE) and Estonian Academy of Sciences, Tallinn, Estonia, in 3rd International Conference on Cyber Conflict, 2011

[19] Marc R. DeVore e Sangho Lee, APT(Advanced Persistent Threat)S And Influence: Cyber Weapons And The Changing Calculus Of Conflict, in The Journal of East Asian Affairs; Seoul Vol. 31, Fasc. 1, 2017

Una ricerca condotta dalla società di sicurezza informatica Deep Instinct Ltd ha utilizzato le reti neurali artificiali per attribuire la provenienza di APT operate da entità statali. Il risultato è stato l'individuazione corretta nel 94,6% dei casi.[20] Il problema dell'attribuzione certa degli attacchi cyber ha importanti risvolti politici e strategici. Gli attori nello spazio cyber operano in condizioni di *plausible-deniability*, ossia la possibilità di negare il proprio coinvolgimento in assenza di prove materiali, in quanto il tracciamento risulta fino ad ora difficoltoso se non impossibile. In tali condizioni, gli stati si trovano con poche o nessuna possibilità di rispondere agli attacchi, e questioni come l'attivazione dell'articolo 5 della Trattato NATO[21] – per cui ogni attacco nei confronti di un membro è da considerarsi come un attacco all'Alleanza – in caso di aggressione cyber, rimangono in un limbo concettuale. L'IA è suscettibile di cambiare radicalmente non solo la capacità degli Stati di difendersi in un ambiente dinamico ed incerto come quello cyber, ma anche i concetti stessi di deterrenza e difesa collettiva alla base delle strategie militari NATO.

La capacità decisionale: vulnerabilità tecnologiche e questioni morali.

La prerogativa che rende l'IA così rilevante è la capacità di apprendere e di assumere decisioni a seconda dell'evoluzione del contesto di riferimento. In questo l'IA rappresenta una funzione che permette ai sistemi autonomi di evolvere ulteriormente. Essi sono infatti in grado di svolgere mansioni a prescindere dall'intervento umano – in diversi gradi di presenza umana nel processo esecutivo – ma mancano di quella capacità di acquisire dati e di tradurli in un processo decisionale autonomo che escluderebbe *in toto* l'elemento umano. Ciò avviene per due ragioni: mancanza di maturità tecnologica e dubbi sull'eticità di un tale processo. Il livello di sviluppo tecnologico dell'IA si trova ancora in uno stadio embrionale. Le innovazioni tecnologiche principali si sono verificate in uno specifico ambito dell'IA, quello del *machine learning*, ossia della capacità dell'IA di apprendere in base ai dati raccolti o inseriti da un umano.[22] Ciò significa che l'IA rimane ancorata ad un input umano nella definizione del dominio di riferimento, per cui le regole in base alle quali essa simula il funzionamento della rete neurale umana rimangono dettate dai suoi programmatori, lo stesso vale per lo scenario in cui si vuole che essa funzioni. Il livello di sviluppo tecnologico dell'IA non è tale da permetterle di apprendere ed affrontare autonomamente questioni astratte, legate a valori o dilemmi etici.[23] Se l'IA nei droni del progetto OFFSET permetterà loro di coordinarsi in base alle attività dei soldati sul campo di battaglia, l'IA non ha idea di "cosa" sia una battaglia. Il suo impiego rimane legato al dominio di riferimento, e seppure sia in grado di apprendere estensivamente, essa non ha la capacità di comprendere la complessità di un contesto allo stesso modo in cui lo fa un umano.

---

[20] Ishai Rosenberg, Guillaume Sicard, and Eli (Omid) David, DeepAPT: Nation-State APT Attribution Using End-to-End Deep Neural Networks, in International Conference on Artificial Neural Networks, Alghero, Italy, September, 2017.
[21] Trattato Nord Atlantico, Washington, DC - 4 aprile 1949, https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=it
[22] Brian Bergstein, The Great AI Paradox, MIT Technology Review, 2017 https://www.technologyreview.com/2017/12/15/146836/the-great-ai-paradox/
[23] Kareem Ayoub & Kenneth Payne (2016) Strategy in the Age of Artificial Intelligence, Journal of Strategic Studies, 2016

Seppure il termine valga per entrambi, l'apprendimento dell'IA è ancora semplificato e limitato a specifici settori rispetto a quello umano, nel quale è inoltre presente la caratteristica della volontà personale. Una limitazione di questa natura ha risvolti importanti quando si tratta di effettuare autonomamente decisioni particolarmente delicate, come colpire un obiettivo con un missile rischiando di causare danni collaterali. Ciò vale anche nel caso di scenari di alta rilevanza strategica, compreso quello nucleare. Per quanto possa essere protetta, l'IA rimane vulnerabile ad una serie di fattori quali l'hacking, il bias degli algoritmi, o il data poisoning.[24] Il bias consiste in un pregiudizio dell'IA che sfocia in una decisione o un comportamento discriminante nei confronti di uno o più elementi. È l'elemento umano a programmare l'IA ed i bias della società civile, seppure latenti, si riflettono sui sistemi e sui set di dati (dataset) inseriti in questi ultimi. Tali discriminazioni possono alterare i processi di *target acquisition* e rendere problematica l'eventualità di delega del processo decisionale alla sola macchina. L'alterazione dei dataset può avvenire anche ad opera di attori malevoli tramite attacchi di data poisoning: essi consistono nella modifica dei dati alla base del processo di apprendimento dell'IA alterando l'algoritmo stesso o intervenendo sui dati raccolti dal sistema.[25] Un tale attacco potrebbe essere in grado di modificare la categorizzazione di un elemento da parte dell'IA da "malevolo" a "benevolo", o viceversa, rappresentando un rischio per le funzioni ad essa delegate. Attori ostili dunque potrebbero alterare la capacità di analisi dell'IA, ed in caso di una sua funzione in sistemi di offensivi o difensivi nucleari, essa rappresenterebbe un obiettivo critico da manipolare. Un attacco di data poisoning operato su in sistema di difesa missilistico sarebbe in grado di alterare la funzione di *threat detection*. . I rischi posti da una tale problematica non sono minori, e sono già visibili in sistemi autonomi privi di IA. Emblematico è il caso dei sistemi missilistici terra-aria MIM-104 Patriot, che nel 2003 durante il conflitto in Iraq non mancarono di colpire – tra gli altri – Black Hawk ed F-16 statunitensi a causa di errori di programmazione, causando diverse vittime.[26] È facile allora immaginare le conseguenze di un bias tecnologico in uno scenario nucleare. Tali rischi sono alla base delle politiche delle forze militari contemporanee di non affidare a sistemi autonomi, e dunque nemmeno a sistemi che implementano l'IA, capacità decisionale di tipo puramente offensivo. Non basta però escludere l'IA dal processo decisionale per eliminarne i rischi. Le stesse vulnerabilità relative all'hacking o al data poisoning possono essere sfruttate da attori ostili per alterare i risultati delle attività ISR operate da sistemi che implementano l'IA. Gli stessi dati elaborati dall'IA e forniti all'umano per effettuare una decisione scevra da rischi tecnologici potrebbero in realtà essere inficiati già alla base. Tali criticità rilevano in particolar modo per quanto riguarda il Global Surveillance and Strike (GSS) network teorizzato per la Terza Offset Strategy, un sistema di sorveglianza alimentato dalla capacità di raccogliere ed elaborare di sistemi autonomi.[27]

[24] How Might Artificial Intelligence Affect the Risk of Nuclear War?, RAND Corporation, 2018
[25] Battista Biggio, Fabio Roli, Wild patterns: Ten years after the rise of adversarial machine learning, Pattern Recognition, Volume 84, 2018,
[26] The Guardian, "Patriot in new 'friendly fire' incident", 2003, https://www.theguardian.com/world/2003/apr/04/iraq.rorymccarthy4
[27] Robert Martinage, Toward A New Offset Strategy - Exploiting U.S. Long-Term Advantages To Restore U.S. Global Power Projection Capability, Centre for Strategic and Budgetary Assessment, 2014

La corruzione della capacità di elaborare i dati dell'AI da parte di un attore ostile potrebbe avere conseguenze sull'intero sistema GSS USA, e allo stesso modo sui sistemi simili degli alleati NATO. Ulteriori criticità rilevate nell'impianto decisionale affidato all'AI sono relativa ad aspetti relativi ai valori etici alla base delle decisioni assunte e all'assunzione della responsabilità morale. Come detto, l'IA rimane una funzione tecnologica in grado di operare in specifici domini di riferimento, con attività indicate in un processo *top-down* dai suoi programmatori, e non è in grado di apprendere i valori astratti a cui gli esseri umani fanno riferimento nelle proprie decisioni. La risposta dell'IA in caso di decisioni in merito ad esecuzioni di attacchi sarebbe orientata unicamente al miglior risultato possibile nell'eliminazione dei target indicati dai suoi programmatori, senza tener conto di eventuali *trade-off* etici coinvolti nell'esecuzione, come vittime civili collaterali. Conseguentemente, l'attribuzione di responsabilità in caso di errore in un teatro operativo o di vere e proprie crisi internazionali scatenate da una decisione dell'IA, risulterebbe particolarmente difficili. Individuare il responsabile tra la molteplicità di attori coinvolti, dai programmatori agli organi militari coinvolti nell'utilizzo del sistema, fino allo stesso Stato, richiederebbe delle riflessioni ben oltre gli aspetti tecnico-informatici, ma che andrebbero ad includere i concetti stessi della responsabilità e della colpa.

Una nuova rivoluzione degli Affari Militari?

Alla luce dei cambiamenti nei concetti della difesa che potrebbero derivare dall'introduzione dell'IA a livello strutturale nel panorama militare, vale la pena chiedersi se essa non costituisca un elemento capace di porre in essere una vera e propria Rivoluzione degli Affari Militari. L'IA è una funzione tecnologica in grado di provocare cambiamenti a livello tattico, operativo e strategico. Un'introduzione dell'IA a livello strutturale nel panorama militare andrebbe a trasformare concetti della Difesa alla base delle strategie contemporanee come la deterrenza e la difesa collettiva. L'implementazione dell'AI in sistemi autonomi e nella robotica potrebbe mutare drasticamente le modalità di conduzione delle operazioni militari, con un crescente utilizzo di "stormi" di droni, come visto nel programma OFFSET statunitense, e con la crescente esclusione dell'elemento umano dal processo decisionale. Di certo l'IA è destinata a giocare un ruolo negli affari militari futuri, e non è un caso se il Presidente Russo Vladimir Putin ha affermato "chi avrà otterrà la supremazia nel campo dell'intelligenza artificiale, governerà il mondo". Tuttavia, la possibilità di inserire l'IA in una teoria della Rivoluzione militare trova dei limiti: l'IA è una tecnologia che deve ancora "maturare". È improbabile che la sola implementazione dell'IA possa mutare la conduzione degli affari militari in modo tale da generare una rivoluzione; quest'ultima sarebbe il risultato di uno sviluppo in concerto tra diversi elementi, quali la robotica ed i sistemi autonomi, di cui l'IA rappresenta attualmente una funzione. La limitazione delle attività e del *deep learning* ad attività legate a specifici domini di riferimento rappresenta allo stesso tempo dunque una limitazione pratica e concettuale per una trasformazione degli affari militari in senso rivoluzionario. Uno sviluppo verso una capacità "generale" dell'AI di operare a livello strategico, senza le limitazioni poste dall'uomo, appare quantomeno difficoltoso nel medio periodo.

Di certo, l'incremento di specifiche capacità tecnologiche nel mondo militare, come la robotica, i sistemi autonomi e lo spazio cyber, segnalano che è in atto un'evoluzione più ampia, dalle numerose opportunità ed incognite. Se della sua funzione tecnologica si intuisce la netta portata competitiva dunque, per essa manca una chiara sistemazione dottrinale negli affari militari. L'IA è infatti un elemento nebuloso dell'innovazione tecnologica. Essa lascia ancora spazio a dubbi sulla portata strategica dei suoi utilizzi futuri, tatticamente apprezzabili ma difficili da sistematizzare in concetti operativi e strategici trasversalmente validi. Inoltre, vanno messi in luce i rischi derivanti dall'utilizzo dell'IA, riguardanti il *conflict triggering*, la cui suscettibilità è stata rilevata soprattutto nell'ambito della deterrenza nucleare, e da vulnerabilità come bias degli algoritmi, hacking e data-poisoning. L'ambiguità e le opportunità offerte dall'IA necessitano dunque uno sguardo attento da parte del decisore al momento della strutturazione delle proprie capacità, nonché un'attenzione privilegiata nell'analisi della dimensione Difesa nazionale ed internazionale.

Bibliografia

Kareem Ayoub & Kenneth Payne (2016) Strategy in the Age of Artificial Intelligence, Journal of Strategic Studies, 39:5-6, 793-819

Battista Biggio, Fabio Roli, Wild patterns: Ten years after the rise of adversarial machine learning, Pattern Recognition, Volume 84, 2018, 317-331

Adam J. Boyd, Michael Kimball, (2017), *The Future Operating Environment and The Third Offset*, in *Closer Than You Think: The Implications of the Third Offset Strategy for the U.S. Army*, Army War College (U.S.). Strategic Studies Institute

Richard Clark, (2000), *Uninhabited Combat Aerial Vehicles: Airpower by the People, For the People, But Not With the People*, Air University Press, Maxwell Air Force Base

Colin Clark, (2017), '*Rolling The Marble:' BG Saltzman On Air Force's Multi-Domain C2 System*", BreakingDefense

Marc R. DeVore e Sangho Lee, (2017), *APT(Advanced Persistent Threat)S And Influence: Cyber Weapons And The Changing Calculus Of Conflict*, in The Journal of East Asian Affairs; Seoul Vol. 31, Fasc. 1

James P. Farwell and Rafal Rohozinski, (2011*), Stuxnet and the Future of Cyber War*, Survival, Global Politics and Strategy

Robert Martinage, (2014), *Toward A New Offset Strategy - Exploiting U.S. Long-Term Advantages To Restore U.S. Global Power Projection Capability*, Centre for Strategic and Budgetary Assessment (CSBA)

Michele Nones, Alessandro Marrone (2011), *La trasformazione delle Forze Armate: il programma Forza NEC*, Istituto Affari Internazionali (IAI)

RAND Corporation, (2018), *How Might Artificial Intelligence Affect the Risk of Nuclear War?*

Ishai Rosenberg, Guillaume Sicard, and Eli (Omid) David, (2017), *DeepAPT: Nation-State APT Attribution Using End-to-End Deep Neural Networks*, in International Conference on Artificial Neural Networks, Alghero, Italy, September, 2017.

Enn Tyugu, (2011), *Artificial Intelligence in Cyber Defense*, Cooperative Cyber Defense Center of Excellence (CCD COE) and Estonian Academy of Sciences, Tallinn, Estonia, in 3rd International Conference on Cyber Conflict

Michael G. Vickers, Robert C. Martinage (2004), *The Revolution in War*, Center for Strategic and Budgetary Assessments (CSBA)