CENTRO ALTI STUDI
PER LA DIFESA

ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

Stefania Rutigliano

Big Data emergenti dalla gestione finanziaria delle Forze Armate e relativa analisi alla luce delle nuove tecnologie di *machine learning*. Profili di impiegabilità dell'Intelligenza Artificiale applicata al controllo operativo delle risorse finanziarie assegnate alle Forze Armate in ottica di scelte sempre più informate a rigore logico, efficacia, efficienza, pienezza del risultato atteso nonché supportate dalla valorizzazione di dati storici di gestione, di *trend*, di simulazioni sulla *performance* dell'organizzazione

AS-SMA-04

ISTITUTO DI RICERCA E ANALISI DELLA DIFESA

L'Istituto di Ricerca e Analisi della Difesa (di seguito IRAD), per le esigenze del Ministero della Difesa, è responsabile di svolgere e coordinare attività di ricerca, alta formazione e analisi a carattere strategico sui fenomeni di natura politica, economica, sociale, culturale, militare e sull'effetto dell'introduzione di nuove tecnologie che determinano apprezzabili cambiamenti dello scenario di difesa e sicurezza, contribuendo allo sviluppo della cultura e della conoscenza a favore della collettività e dell'interesse nazionale.

L'IRAD, su indicazioni del Ministro della difesa, svolge attività di ricerca in accordo con la disciplina di Valutazione della Qualità della Ricerca e sulla base della Programma nazionale per la ricerca, sviluppandone le tematiche in coordinamento con la Direzione di Alta Formazione e Ricerca del CASD.

L'Istituto provvede all'attivazione e al supporto di dottorati di ricerca e contribuisce alle attività di Alta Formazione del CASD nelle materie d'interesse relative alle aree: Sviluppo Organizzativo; Strategia globale e sicurezza/Scienze Strategiche; Innovazione, dimensione digitale, tecnologie e cyber security; Giuridica.

L'Istituto opera in coordinamento con altri organismi della Difesa e in consorzio con Università, imprese e industria del settore difesa e sicurezza; inoltre, agisce in sinergia con le realtà pubbliche e private, in Italia e all'estero, che operano nel campo della ricerca scientifica, dell'analisi e dello studio.

L'Istituto, avvalendosi del supporto consultivo del Comitato scientifico, è responsabile della programmazione, consulenza e supervisione scientifica delle attività accademiche, di ricerca e pubblicistiche.

L'IRAD si avvale altresì per le attività d'istituto di personale qualificato "ricercatore della Difesa, oltre a ricercatori a contratto e assistenti di ricerca, dottorandi e ricercatori post-dottorato.

L'IRAD, situato presso Palazzo Salviati a Roma, è posto alle dipendenze del Presidente del CASD ed è retto da un Ufficiale Generale di Brigata o grado equivalente che svolge il ruolo di Direttore.

Il Ministro della Difesa, sentiti il Capo di Stato Maggiore dalla Difesa, d'intesa con il Segretario Generale della Difesa/Direttore Nazionale degli Armamenti, per gli argomenti di rispettivo interesse, emana le direttive in merito alle attività di ricerca strategica, stabilendo le linee guida per l'attività di analisi e di collaborazione con le istituzioni omologhe e definendo i temi di studio da assegnare all'IRAD.

I ricercatori sono lasciati liberi di esprimere il proprio pensiero sugli argomenti trattati: il contenuto degli studi pubblicati riflette quindi esclusivamente il pensiero dei singoli autori e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali i Ricercatori stessi appartengono.

Stefania Rutigliano

"*Big Data* emergenti dalla gestione finanziaria delle Forze Armate e relativa analisi alla luce delle nuove tecnologie di *machine learning*. Profili di impiegabilità dell'Intelligenza Artificiale applicata al controllo operativo delle risorse finanziarie assegnate alle Forze Armate in ottica di scelte sempre più informate a rigore logico, efficacia, efficienza, pienezza del risultato atteso nonché supportate dalla valorizzazione di dati storici di gestione, di *trend*, di simulazioni sulla *performance* dell'organizzazione"

AS-SMA-04

"*Big Data* emergenti dalla gestione finanziaria delle Forze Armate e relativa analisi alla luce delle nuove tecnologie di *machine learning*. Profili di impiegabilità dell'Intelligenza Artificiale applicata al controllo operativo delle risorse finanziarie assegnate alle Forze Armate in ottica di scelte sempre più informate a rigore logico, efficacia, efficienza, pienezza del risultato atteso nonché supportate dalla valorizzazione di dati storici di gestione, di *trend*, di simulazioni sulla *performance* dell'organizzazione"

NOTA DI SALVAGUARDIA

Quanto contenuto in questo volume riflette esclusivamente il pensiero dell'autore, e non quello del Ministero della Difesa né delle eventuali Istituzioni militari e/o civili alle quali l'autore stesso appartiene.

NOTE

Le analisi sono sviluppate utilizzando informazioni disponibili su fonti aperte.

Questo volume è stato curato dall'**Ufficio Studi, Analisi e Innovazione dell'IRAD**.

Direttore
Gen. B. Gualtiero Iacono

Capo dell'Ufficio Studi, Analisi e Innovazione
Col. AArnn Pil. Loris Tabacchi

Progetto grafico
1° Mar. Massimo Lanfranco – C° 2ª cl. Gianluca Bisanti – Serg. Manuel Santaniello

Revisione e coordinamento
C.V. Massimo GARDINI – S.Ten. Elena PICCHI – Funz. Amm. Aurora Buttinelli – Ass. Amm. Anna Rita Marra

Autore
Stefania Rutigliano

Stampato dalla Tipografia del **Centro Alti Studi per la Difesa**

Istituto di Ricerca e Analisi della Difesa
Ufficio Studi, Analisi e Innovazione
Palazzo Salviati
Piazza della Rovere, 83 - 00165 – Roma
tel. 06 4691 3205
e-mail: irad.usai.capo@casd.difesa.it

chiusa a settembre 2024

ISBN 979-12-5515-083-1

INDICE

Sommario

Lo sviluppo tecnologico ha da sempre sospinto il progresso umano, adattandosi prontamente alle esigenze della società che, nel corso degli anni, sono emerse.

Ad oggi, la piena espressione del progresso tecnologico è testimoniata dai sistemi impieganti Intelligenza Artificiale (IA) in grado di emulare – e, in taluni casi addirittura superare – il *modus cogitandi et operandi* dell'essere umano, appropriandosi di talune caratteristiche proprie della logica, dell'analisi e delle decisioni umane.

Il tema della ricerca, muovendo dall'analisi dell'Intelligenza Artificiale nel suo complesso, si è focalizzata, specificatamente, sugli algoritmi e sui sistemi per l'analisi avanzata dei *Big Data* (*Big Data Advanced Analytics,* BDAA).

Il presente elaborato affronta, dunque, il tema dello sviluppo scientifico e tecnologico, con un'enfasi sull'importanza della gestione dei dati, in particolare dei *Big Data*, nell'attuale scenario: si sottolinea l'importanza dell'Intelligenza Artificiale, in particolare del *Machine Learning e del Deep Learning*, nel contesto dell'analisi dei dati. Nel corso dell'elaborato, infatti, analizzeremo come l'IA possa rivoluzionare il modo in cui le Forze Armate raccolgono, analizzano ed utilizzano i *Big Data* militari per prendere decisioni informate.

Nondimeno, da un canto, tali sistemi rappresentano una opportunità ed uno strumento al servizio del genere umano, in grado di migliorare, rendere più rapide, efficienti ed informate le decisioni, dall'altro canto nascondono, al momento in cui si scrive, insidie applicative che andrebbero cautamente contemperate coi benefici. Nell'elaborato si analizzano, dunque, in dettaglio i vantaggi e le sfide dell'utilizzo dell'IA nella *Big Data Advanced Analytics* (BDAA).

Invero, nella loro capacità applicativa, i sistemi adoperanti l'IA potrebbero prescindere dal rispetto di talune regole afferenti alla sicurezza, come, a titolo di esempio, il rischio di diffusione dei dati processati dai sistemi o di violazione della *privacy*. Difatti, inserire in un sistema automatizzato dei dati, a maggior ragione se sensibili o classificati, appare ancora oggi non scevro da rischi: si analizzano, nel corso dell'opera, i rischi connessi al modo di raccogliere i dati e processarli. Entrambi tali aspetti paiono risentire di taluni *vulnera*: nella prima fase, di approvvigionamento dei dati, i sistemi mostrano una opacità di funzionamento dei sistemi algoritmici, non essendo in grado di produrre nel dettaglio quali sono i processi decisionali sottesi e le rispettive motivazioni. Inoltre, potrebbero sorgere problemi *a capite* riguardo la qualità dei dati raccolti, che potrebbero essere viziati o integrati da dati non veritieri (si parla, in tal caso, di "*hallucination*" dell'IA). Durante il secondo segmento del processo, quello volto ad analizzare e processare i dati raccolti, potrebbero parimenti

esservi rischi insistenti sulla privacy e sulla sicurezza delle informazioni raccolte, che potrebbero essere adoperate dal sistema in altri contesti e diffuse inavvertitamente ad altri utenti.

Per tali ragioni, si auspicherebbe l'applicazione di una IA che sia responsabile (*Responsible Artificial Intelligence*, RAI) ed esplicabile (*eXplicable Artificial Intelligence*, XAI) unitamente ad una supervisione umana dell'apprendimento dei sistemi IA.

Ciononostante, a fronte delle interviste condotte con svariati esperti, considerando l'importanza di bilanciare l'efficacia nell'analisi dei dati con la sicurezza delle informazioni, e considerando le attuali esigenze che le Forze Armate italiane potrebbero considerare per la gestione dei dati finanziari, si è trascurata, al momento in cui si scrive, la possibilità di adoperare sistemi impieganti IA e ci si è concentrati, piuttosto, sulla possibilità di dotare le Forze Armate di un sistema intelligente per condurre la BDAA *ad hoc*, ovvero l'adozione di strumenti esistenti, già implementati ed in uso a livello sovranazionale.

In conclusione, il testo suggerisce che ulteriori studi dovrebbero essere condotti per valutare le opzioni in modo più dettagliato, compresa un'analisi SWOT per valutare i punti di forza (*Strengths*), le debolezze (*Weaknesses*), le opportunità (*Opportunities*) e le minacce (*Threats*) delle opzioni presentate nel corso dell'elaborato, per determinare l'approccio migliore per condurre analisi di gestione dei dati finanziari ed, eventualmente, l'implementazione dell'IA nelle Forze Armate italiane.

Il percorso del lavoro ha richiesto di affacciarsi anche in ambiti multidisciplinari per poter identificare aree propositive nell'attuale scenario. Ciò ha permesso di comprendere la tecnologia dell'intelligenza artificiale e le opportunità che offre, nonché le applicazioni presenti e future, e quindi esaminarne l'impatto sullo scenario attuativo.

È stato altresì necessario guardare ai benefici, alle potenzialità, agli aspetti critici fino agli abusi dell'impiego dell'analisi condotta tramite IA, non solo in ambito nazionale ma europea, utile per una valutazione compiuta, rapportare quanto rilevato nei diversi scenari normativi all'ambito europeo attuale e alla sua possibile evoluzione.

L'elaborato è organizzato in cinque capitoli, che possono essere racchiusi in tre parti che concernono, rispettivamente, l'inquadramento della intelligenza artificiale, con cenni storici e applicativi (Premessa e Metodologia e Capitolo I), l'applicazione degli strumenti adoperanti intelligenza artificiale per processare i *Big Data*, con particolare riferimento all'applicazione in ambito militare (Capitolo II) e i rischi e benefici connessi (Capitolo III) nonché, infine, gli aspetti applicativi, mutuati sullo scenario attuale delle Forze Armate (Capitolo IV) e, sulla scorta di analisi comparatistiche, le proposte e le prospettive dell'applicazione delle nuove tecnologie declinate nell'attuale stato dell'arte (Conclusioni). Il

fine è quello di creare una visione sistemica ed un quadro completo dell'uso futuro della tecnologia in base alle esigenze e all'uso delle Forze Armate. Il capitolo V e le conclusioni forniranno una serie di suggerimenti pratici per l'uso appropriato di queste nuove tecnologie, sviluppati dall'analisi condotta nei capitoli precedenti.

Abstract

Technological development has always driven human progress, readily adapting to the needs of society that have emerged over the years.

Today, the full expression of technological progress is witnessed by systems employing Artificial Intelligence (AI) capable of emulating – and in some cases even surpassing – the *modus cogitandi et operandi* of the human being, appropriating certain characteristics of human logic, analysis and decision-making.

Starting from the analysis of Artificial Intelligence as a whole, the theme of the research focused, specifically, on algorithms and systems for the advanced analysis of Big Data (Big Data Advanced Analytics, BDAA).

This paper, therefore, deals with scientific and technological development, with an emphasis on the importance of data management, especially Big Data, in the current scenario: the importance of Artificial Intelligence, especially Machine Learning and Deep Learning, in the context of data analysis is emphasised. In the course of the paper, we will analyse how AI can revolutionise the way the Armed Forces collect, analyse and use military Big Data to make informed decisions.

Nonetheless, on the one hand, such systems represent an opportunity and a tool at the service of mankind, capable of improving, making faster, more efficient and informed decisions; on the other hand, they conceal, at the time of writing, application pitfalls that should be cautiously balanced against the benefits. In the paper, therefore, the benefits and challenges of using AI in Big Data Advanced Analytics (BDAA) are analysed in detail.

Indeed, in their applicative capacity, systems using AI could disregard certain rules pertaining to security, such as, for example, the risk of leakage of data processed by the systems or violation of privacy. Indeed, entering data into an automated system, all the more so if it is sensitive or classified, still appears to be not risk-free: the risks connected to the way data is collected and processed are analysed in the course of the work. Both of these aspects seem to suffer from certain vulnerabilities: in the first phase of data procurement, the systems show an opacity in the functioning of algorithmic systems, not being able to produce in detail what the underlying decision-making processes and their respective motivations are (so-called ‘black box’).

Furthermore, there could be problems in understanding the quality of the data collected, which could be flawed or supplemented by untrue data (in this case, we speak of AI ‘hallucination’). During the second segment of the process, that of analysing and processing the collected data, there could likewise be persistent risks to the privacy and security of the collected information, which could be used by the system in other contexts and inadvertently disseminated to other users.

For these reasons, the application of responsible (Responsible Artificial Intelligence, RAI) and explicable (eXplicable Artificial Intelligence, XAI) AI together with human supervision of the learning of AI systems would be desirable.

Nevertheless, considering the interviews conducted with various experts, the importance of balancing effectiveness in data analysis with information security, and the current requirements that the Italian Armed Forces might consider for the management of financial data, it has been disregarded, at the time of writing, the possibility of using systems employing AI and we have focused, rather, on the possibility of equipping the Armed Forces with an intelligent system to conduct ad hoc BDAA, i.e. the adoption of existing tools already implemented and in use at supranational level.

In conclusion, the paper suggests that further studies should be conducted to evaluate the options in more detail, including a SWOT analysis to assess the Strengths, Weaknesses, Opportunities and Threats of the options presented in the paper, to determine the best approach to conducting financial data management analysis and, possibly, the implementation of AI in the Italian Armed Forces.

The course of the work also required looking into multidisciplinary areas in order to identify proactive areas in the current scenario. This made it possible to understand artificial intelligence technology and the opportunities it offers, as well as present and future applications, and thus examine its impact on the implementation scenario.

It was also necessary to look at the benefits, potentials, critical aspects as well as abuses of the use of AI, not only in a national but also in a European context, which is useful for a comprehensive assessment, comparing the findings of the different regulatory scenarios to the current European context and its possible evolution.

The paper is organised into five chapters, which can be grouped into three parts concerning, respectively, the framework of artificial intelligence, with historical and applicative hints (Foreword and Methodology and Chapter I), the application of artificial intelligence tools to process Big Data, with particular reference to its application in the military sphere (Chapter II) and the related risks and benefits (Chapter III), as well as, lastly, the application aspects, borrowed from the current scenario of the Armed Forces (Chapter IV) and, on the basis of comparative analyses, the proposals and prospects of the application of the new technologies as they are currently applied (Conclusions). The aim is to create a systemic vision and a comprehensive picture of the future use of technology according to the needs and use of the Armed Forces. Chapter V and the Conclusions will provide a series of practical suggestions for the appropriate use of these new technologies, developed from the analysis conducted in the previous chapters.

1. Premessa e Metodologia

Nel corso della storia, lo sviluppo scientifico e tecnologico si è assunto il compito di soddisfare, adattandosi prontamente, alle esigenze della società. Nell'odierno contesto, la gestione efficiente ed efficace e l'analisi dei dati hanno assunto un ruolo cruciale.

Le Forze Armate, non solo a livello nazionale, ma anche a livello europeo e globale, si trovano ad oggi dinanzi ad una enorme mole di dati ed informazioni da processare, provenienti da numerose fonti, tra cui reti di *intelligence* e comunicazioni.

Questi dati, che assumono il nome di *Big Data*, se processati nel modo corretto, grazie alle nuove tecnologie emergenti, rappresentano una inestimabile risorsa per l'acquisizione di vantaggi strategici, potendo garantire una efficiente gestione finanziaria delle risorse e risultati accurati e molto più rapidi.

In tale contesto, in cui vi è l'aumento della potenza di calcolo degli elaboratori elettronici, ma anche la disponibilità di una grande quantità di *data*, si è diffusa l'applicazione dell'Intelligenza Artificiale (IA), e in particolare quella fondata su tecniche di *Machine Learning*, tra cui va annoverato anche il *Deep Learning,* che appare un vero e proprio catalizzatore, rappresentazione di un cambiamento rivoluzionario che il mondo digitale sta vivendo.

Sebbene sia complesso rendere una definizione unitaria di IA, potremmo intenderla come la disciplina che studia quelle modalità di addestramento degli algoritmi che siano in grado, con diversi gradi di autonomia, di raggiungere un dato obiettivo tramite la gestione ed elaborazione di dati, indipendentemente dall'implementazione dell'algoritmo in una macchina[1].

Invero, le diverse tecniche applicanti l'IA sono accomunate da questa capacità di elaborazione dei dati inseriti in modo evidentemente rapido ed autonomo: l'IA potrebbe potenzialmente trasformare il modo in cui le Forze Armate raccolgono, analizzano ed usano i *Big Data* per prendere decisioni informate a rigore logico ed efficacia e migliorare, di tal guisa, la loro capacità operativa.

Questo elaborato, nella sua prima parte presenta una breve storia dello sviluppo dell'IA, esaminando i progressi e lo stato dell'arte della disciplina dell'IA, in particolare come

---

[1] Giusti E. (2020). Intelligenza artificiale e sistema sanitario. In Dorigo S., a cura di, *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa: PaciniEditore, 310; Romano G. (2020), Diritto, robotica e teoria dei giochi: riflessioni su una sinergia. In Alpa G., a cura di, *Diritto e Intelligenza Artificiale*, Pisa: PaciniEditore,108. Sul punto è stato osservato come non sia il *corpus mechanicum* a definire e qualificare l'AI bensì un processo totalmente automatizzato basato sull'acquisizione e l'elaborazione di informazioni in grado di fornire un risultato, di correggerlo e implementarlo. Trevisi C. (2018). La regolamentazione in materia di intelligenza artificiale, robot, automazione: a che punto siamo, *Medialaws – Rivista di diritto dei media*, 2: 447; Peluso M. G. (2022). Intelligenza Artificiale e dati di qualità: la tecnologia come valido alleato*. Medialaws – Rivista di diritto dei media*, 2.

applicata nel contesto dell'analisi dei dati, anche in ambito militare e, nella seconda parte, esplora l'incidenza dell'IA nell'elaborazione dei *Big Data* militari, interrogandosi se e come questa tecnologia possa affrontare le sfide attuali e aprire nuove opportunità per l'innovazione militare. In ultimo, come capitolo conclusivo della parte seconda, si tenta di offrire una prospettiva sul futuro di tale applicazione, considerando le attuali esigenze delle Forze Armate.

Nella prima parte, di natura descrittiva, si procederà dunque a definire cosa sia l'IA e come, nel corso degli anni, si sia adattata alle numerose e diverse esigenze, sino ad arrivare ai più moderni sistemi e, nello specifico quale sia il suo funzionamento.

In particolare, l'oggetto dell'analisi concerne la *Big Data Advanced Analytics* (BDAA), vertendo principalmente sulle capacità dell'IA di gestire una enorme mole di dati in tempo reale, rassegnare delle analisi predittive, potendo anticipare modelli e minacce potenziali, grazie all'utilizzo di algoritmi e supportare la decisione degli operatori (*decision-making support*).

D'altro canto, l'elaborato esamina anche le sfide ed i rischi connessi all'utilizzo dell'IA, come, ad esempio, l'intrinseca opacità di funzionamento dei sistemi adoperanti IA e la *ratio* a fondamento delle decisioni prese, altresì definita "*black box*", i rischi connessi alla diffusione di dati e la mancata tracciabilità degli stessi.

Pertanto, sebbene l'IA fungerà di certo da spina dorsale delle nuove rivoluzioni tecnologiche e, come vedremo, dovrà di certo essere tenuta in debita considerazione per i futuri sviluppi dell'applicazione delle nuove tecnologie, anche nel contesto militare, la sua applicazione va adeguatamente contemperata con i rischi sottesi.

Al fine di produrre questo elaborato, oltre allo studio della principale dottrina disponibile sul tema, ci si è avvalsi dell'opinione di taluni esperti di diverse discipline, tramite delle *interviews*, inserite come annessi.

2. L'Intelligenza Artificiale: cenni storici e applicativi

2.1 Definizione ed excursus storico

L'Intelligenza Artificiale (IA), in quanto innovazione tecnologica di spicco, assume un ruolo centrale nel plasmare la società contemporanea e ridefinire il panorama delle applicazioni tecnologiche.

Invero, tale tecnologia pervade, in maniera sempre più pregnante, ogni aspetto della vita, a seconda delle diverse applicazioni concrete: coinvolge la necessità di sviluppare competenze digitali sempre maggiori per sviluppare solide competenze applicative per talune professioni[2] e consente di comprendere le implicazioni sociali, etiche ed economiche, determinate dalla tecnologia[3].

L'IA è applicabile per risolvere molti problemi complessi in vari settori come la sicurezza, la finanza, l'assistenza sanitaria, i trasporti, grazie alla sua capacità di gestire numerosi dati, di affrontare problemi non lineari e di essere adatta all'uso nella predizione e nella generalizzazione più rapida una volta addestrata[4].

Pertanto, appare evidente come la richiesta di competenze in tale dominio sia, ad oggi, indispensabile, in quanto utile allo svolgimento di ruoli critici in molte discipline e settori e sottenda elevate competenze tecnologiche, legali, applicative e pedagogiche[5]. Infatti, al fine di sfruttare le potenzialità dell'IA al meglio non ci si dovrebbe limitare ad "insegnare con l'aiuto della macchina", bensì ad insegnare a comunicare con la macchina, abilitarne l'uso, ma anche comprendere perché e su quali meccanismi tecnologici la macchina comunica[6].

Sebbene siano disponibili numerose definizioni di IA, la comunità scientifica non sembra unanime nella scelta di una definizione che sia in grado di abbracciare le diverse

---

2 La richiesta di competenze nel dominio dell'IA è diventata ormai stringente in quanto funzionale allo svolgimento di ruoli critici in varie discipline e settori. Bawden, D. (2008). Origins and concepts of digital literacy. Digital Literacies: Concepts, Policies and Practices. Bern: Peter Lang Publishing, 17–32.

3 Si pensi, ad esempio, all'enorme quantità di dati personali che in ogni momento, ed in maniera principalmente inconsapevole, rilasciamo nel cyberspazio. Per un commento si veda Panciroli, C., Rivoltella, P. C., Gabbrielli, M., Zawacki Richter, O. (2020). Artificial Intelligence and education: new research perspectives. *Form@re - Open Journal Per La Formazione in Rete*, 20(3): 1-12.

4 Bello, O.; Holzmann, J.; Yaqoob, T.; Teodoriu, C. (2015). Application of artificial intelligence methods in drilling system design and operations: A review of the state of the art. *Journal of Artificial Intelligence and Soft Computing Research.* 5: 121–139.

5 Ng, D. T. K., Leung, J. K. L., Chu, S. K. W., & Qiao, M. S. (2021). Conceptualizing AI literacy: An exploratory review. *Computers and Education: Artificial Intelligence*, 2; Touretzky, D., Gardner-McCune, C., Martin, F., & Seehorn, D. (2019). "Envisioning AI for K-12: What Should Every Child Know about AI?" paper for the Thirty-Third AAAI Conference on Artificial Intelligence (AAAI-19), 33, 9795–9799. Steinbauer, G., Kandlhofer, M., Chklovski, T., Heintz, F., & Koenig, S. (2021). A Differentiated Discussion About AI Education K-12. *KI - Künstliche Intelligenz*, 35(2): 131–137.

6 Secondo gli autori si tratta di conoscere "sia le basi teoriche e tecnologiche, sia il volto culturale e sociale dei nuovi media". Ciotti, F. Roncaglia, G. (2008). *Il mondo digitale. Introduzione ai nuovi media*. Roma-Bari: Laterza, p. VII. Si veda, per un commento esteso, Cuomo S., Biagini G., Ranieri M. (2022) Artificial Intelligence Literacy, che cos'è e come promuoverla. Dall'analisi della letteratura ad una proposta di Framework. *Media Education* 13(2): 161-172.

branche di studio che interessano la materia[7]. Secondo la definizione rassegnata dalla *Army Science Board* una macchina programmabile mostra intelligenza artificiale "se è in grado di incorporare l'astrazione e l'interpretazione nell'elaborazione delle informazioni e di prendere decisioni a un livello di sofisticazione tale da essere considerato intelligente negli esseri umani"[8].

L'IA è il campo di studi che analizza il comportamento intelligente, comprende le tecniche computazionali per l'esecuzione di compiti che presuppongono intelligenza se eseguiti dagli esseri umani e punta, quale obiettivo finale, a sviluppare una teoria dell'intelligenza che, studiando il comportamento delle entità intelligenti presenti in natura, guidi la creazione di entità artificiali dotate e capaci di comportamenti intelligenti. [9]

L'IA rappresenta una particolare modalità di risoluzione dei problemi, diversa dagli approcci tradizionali orientati agli algoritmi, che si concentra su problemi dimostrabili dall'uomo ma per i quali non esiste una metodologia praticabile che gli esseri umani affrontano continuamente nel rapporto con il mondo[10].

---

7 Diverse definizioni sono state coniate nel corso degli anni: secondo Russell e Norvig «l'IA è la ricerca del miglior programma agente per una specifica architettura» (Russell S., Norvig P. (2005) *Intelligenza Artificiale un approccio moderno*, Milano: Pearson, vol. 1, 588 ss.). La Commissione europea ha fornito una definizione di Intelligenza Artificiale come attenente a «*systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)*». Comunicazione della Commissione, *Un'intelligenza artificiale per l'Europa*, COM (2018) 237 final. L'High-Level Expert Group on AI ha elaborato una definizione, precisando che per AI debbano intendersi: «*software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)*». High Level Expert Group, *Definition of AI. Main capabilities and disciplines*, in *ec.europa.eu*, 8 aprile 2019. Si veda, per alter definizioni, Barr A., Feigenbaum E. (1981) *The Handbook of Artificial Intelligence*, vol. 1, Stanford: Butterworth-Heinemann, p. 3; Romano G. (2020), op. cit., Pisa: PaciniEditore, 108. Winston P. H. (1977) *Artificial Intellifence*. Reading: Addison Wesley Publishing Co., 1977, p. 1; Clifton P. O. (1985), *Artificial Intellifence A "User Friendly" Introduction*. Alabama: Air University Press, p. 2. Si legga Akgül A. (1990). *Artificial Intelligence: Military Applications*. Ankara Üniversitesi SBF Dergisi 45.
Lesmo riprende la definizione fornita dall'Associazione Italiana di Intelligenza Artificiale, che nel suo statuto definisce l'IA come «quella disciplina che studia i fondamenti teorici, le metodologie e le tecniche che permettono di concepire, progettare, realizzare, sperimentare ed utilizzare sistemi artificiali (hardware e software) sia con l'obiettivo di ottenere prestazioni ritenute caratteristiche dell'intelligenza (umana) sia con l'obiettivo di fornire modelli computazionali di processi cognitivi» Lesmo L. (1991). *ad vocem IA. Grande Dizionario, Appendice V*. Torino:UTET.

8 "*A programmable machine exhibits artificial intelligence if it can incorporate abstraction and interpretation into information processing and make decisions at a level of sophistication that would be considered intelligent in humans*". Brownstein B. J. et al., "Technological assessment of future battlefield robotic applications", in Procesedings of the army Conference on Application of AI to Battlefield Information Management, US Navy Surface Weapons Center, White Oak, 1983, p. 169.

9 Genesereth M. R., Nilsson N. J. (1987). *Logical Foundations of Artificial Intelligence*. Burlington: Morgan Kaufmann Publishers, p. 1.

10 Schutzer D. (1987) *Artificial Intelligence An Application-Oriented Approach*. New York: Van Nostrand Reinhold, p. 2.. Gevarter W. B. (1983) *An Overview of Artificial Intelligence and Robotics*. NASA Scientific and Technical Braanch, Washington, vol. 1, p. 1. Akgül A. (1990) op. cit., Ankara Üniversitesi SBF Dergisi 45.

Il lavoro preparatorio e prodromico alla nascita effettiva dell'Intelligenza Artificiale, definito "periodo di incubazione dell'IA", può farsi risalire al periodo precedente agli anni Cinquanta[11]. Tuttavia, il vero momento decisivo si è osservato nel 1952, quando lo scienziato Arthur Samuel ha sviluppato un programma di dama che poteva apprendere modelli impliciti dalla posizione corrente e istruire le mosse successive, applicazione embrionale di apprendimento automatico e vicina al processo di cognizione umana[12].

Poco dopo, il termine "Intelligenza Artificiale" fu formalmente coniato, varando una ricerca successiva dai notevoli risultati, tra cui apprendimento automatico, dimostrazione di teoremi, risoluzione dei problemi e riconoscimento di modelli[13].

Solo negli anni Settanta le ricerche condotte sin dagli anni Cinquanta hanno iniziato a produrre risultati concreti: l'approccio emerso consisteva nella creazione di sistemi più ristretti, altamente specializzati, caratterizzati da estese basi di conoscenza specifiche del campo d'azione e una vasta comprensione delle procedure specifiche relative al problema in questione[14].

Durante quel periodo apparvero nuove tecniche di rappresentazione della conoscenza, iniziarono a maturare le tecniche di ricerca, si verificarono interazioni con altri campi, e furono dimostrati approcci fattibili per l'elaborazione del linguaggio, la comprensione del parlato, la *computer vision* e programmi informatici in grado di eseguire esportazioni[15].

La dottrina della fine degli anni Settanta delineò una vera e propria dicotomia tra una Intelligenza Artificiale dal paradigma "forte" (laddove la macchina abbia capacità ed abilità cognitive e, teoricamente, potrebbe evolversi senza un ulteriore intervento umano) e "debole" (se le funzioni della macchina appaiono del tutto sovrapponibili a quelle dell'uomo,

---

[11] Nel 1936, il matematico Alan Turing propose un modello matematico di un computer ideale, che pose le basi teoriche per i successivi computer elettronici. I neurofisiologi W. McCulloch e W. Pitts costruirono il primo modello di rete neurale (modello M-P) nel 1943. Si veda Zhang L., Zhang B. (1990) A geometrical representation of McCulloch-Pitts neural model and its applications. *IEEE Transact Neural Networks*,10(4): 925–9.
Il modello M-P è il primo modello matematico costruito per imitare la struttura e il principio di funzionamento dei neuroni biologici. Può essere considerata come la prima rete neurale artificiale. Nel 1949, Hebb propose il meccanismo di apprendimento basato sulla neuropsicologia. Kuriscak E., Marsalek P., Stroffek J., Toth PG. (2015) Biological context of Hebb learning in artificial neural networks, a review. *Neurocomputing*. 152:27–35.

[12] "*Hebb learning rule*" è una regola di apprendimento non supervisionato, che può estrarre le caratteristiche statistiche dei set di addestramento e classificare i dati in base alla somiglianza dei dati. Samuel A.L. (2000) Some studies in machine learning using the game of checkers. *IBM Journal*, 44(1.2):206–26. Si veda, per un commento esteso Jiang Y., Li X., Luo H., Yin S., Kaynak O. (2022) Quo vadis artifcial intelligence?. *Discover Artifcial Intelligence,* 2:4.

[13] Fu John McCarthy a coniare originariamente il termine AI al Dartmouth Summer Research Project on Artifcial Intelligence del 1956, pertanto costui è considerato il padre dell'intelligenza artificiale. McCarthy J., Minsky M.L., Rochester N., Shannon C.E. (1995) *A proposal for the Dartmouth summer research project on artifcial intelligence*. Stanford: AI Magazine.

[14] Schutzer D. (1987) op. cit., New York: Van Nostrand Reinhold, p. 8. Akgül A. (1990) op. cit., Ankara Üniversitesi SBF Dergisi 45.

[15] Gevarter W. B. (1983) op. cit., *NASA Scientific and Technical Braanch*, Washington, vol. 1, 1983, p. 8.

ma basate su una programmazione algoritmica)[16]. Ciò che caratterizza tali sistemi è la flessibilità dei modelli che lo realizzano, che tengano conto di fattori probabilistici e consentano di gestire adeguatamente le incertezze[17].

In sintesi, se da un lato l'IA "debole" mira a simulare il comportamento umano, replicando artificialmente i suoi processi di ragionamento e rispondendo rapidamente in modo autonomo, dall'altro, invece, con l'IA "forte" l'informatica assume un ruolo predominante, con l'intento di sviluppare meccanismi di ragionamento analoghi a quelli umani e creare capacità coscienti e senzienti[18].

Sebbene l'IA "forte" abbia avuto una diffusione più limitata, in quanto più difficilmente valutabile in termini di risposta, percentuali di successo e generale accettabilità pratica[19], essa ha potenzialità intrinseche indubbiamente maggiori e con una maggiore attrattività, in quanto slegate alla mera soluzione algoritmica.

In tale ottica, il tradizionale processo di programmazione è stato sostituito dall'introduzione dell'apprendimento automatico (*Machine Learning*) il quale prevede che il computer apprenda autonomamente anziché richiedere una specifica dettagliata da parte dell'essere umano su come reagire in varie situazioni ed ha dimostrato di eccellere soprattutto nell'analisi del linguaggio naturale umano[20]. L'apprendimento automatico mostra la superiorità e la capacità di adattarsi con un apprendimento incrementale e permanente anzitutto nel poter imparare da enormi quantità di dati strutturati, nella buona capacità di generalizzazione e nella capacità di aggiornare le proiezioni *input-output* con l'inserimento di ogni nuovo dato disponibile[21].

---

16 La maggior parte dei sistemi di intelligenza artificiale esistenti sono progettati in modo dedicato per una gamma limitata di attività predefinite. In questo contesto, sono chiamati intelligenza ristretta artifcial (ANI) o IA debole. Searle J. R. (1980) Minds, brains, and programs. *Behavioral and Brain Sciences* 3 (3). Jiang Y., Li X., Luo H., Yin S., Kaynak O. (2022) op. cit. *Discover Artifcial Intelligence*,2:4.

17 Questo è stato oggetto di diversi studi in ambito internazionale: si veda*, inter alia*, De Landa M. (1991). *War in the Age of Intelligent Machines*. New York: Zone Books, p. 10. De Spiegeleire S., Maas M., Sweijs, T. (2017). Artificial Intelligence and the Future of Defense – Strategic Implications for Small- and Medium-Sized Force Providers. *The Hague Centre for Strategic Studies* (HCSS). Flammini F. (2018) Artificial Intelligence (Ai) Applicata Agli Autonomous Systems, Report per il Centro Militare di Studi Strategici, CASD Roma, p. 15.

18 Searle J. R. (1980) op. cit., *Behavioral and Brain Sciences* 3 (3).

19 Cuomo S., Biagini G., Ranieri M. (2022) op. cit. *Media Education* 13(2): 161-172.

20 Piuttosto che specificare gli *input* e gli algoritmi definiti dall'uomo per ottenere gli *output*, un mezzo alternativo per risolvere problemi complessi è selezionare gli *input* e gli *output* attesi e usare le macchine per trovare automaticamente i modelli tra loro e quindi "imparare" gli algoritmi. Javed K., Gouriveau R., Zerhouni N. (2015) A new multivariate approach for prognostics based on extreme learning machine and fuzzy clustering. *IEEE Transactions on Cybernetics*, 45(12):2626–39. Aizpurua J.I., McArthur S.D.J., Stewart B.G., et al. (2019) Adaptive power transformer lifetime predictions through machine learning and uncertainty modeling in nuclear power plants. *IEEE Transactions on Industrial Electronics*, 66(6):4726–37. Lee H., Kim Y., Kim C.O. (2017) A deep learning model for robust wafer fault monitoring with sensor measurement noise. *IEEE Transactions on Semiconductor Manufacturing*, 30(1):23–31.

21 Szegedy C., Zaremba W., Sutskever I. et al (2013) *Intriguing properties of neural networks*. Cornell: Cornell University; Zhang T., Su G., Qing C., et al (2021) Hierarchical lifelong learning by sharing representations and integrating hypothesis. *IEEE Transactions on Semiconductor Manufacturing,* 51(2):1004–14.

2.2 Tecniche dell'Intelligenza Artificiale

Un sistema di controllo si definisce come dotato di "intelligenza artificiale" laddove consenta di correlare le azioni del sistema di attuazione alle percezioni provenienti dal sistema sensoriale.

Invero, il sistema di controllo si dota, anzitutto, di sensori, elementi di *input* in grado di misurare fattori ambientali (ad esempio temperatura, umidità, luminosità etc.) ed attuatori, elementi in grado di operare modifiche sull'ambiente circostante, imprimendo dei semplici ordini di *output*, quali accensione, spegnimento, regolazione velocità e movimento.[22]

In seguito, il sistema di controllo riceve le informazioni raccolte dal sistema sensoriale, le interpreta e opera una decisione, poi inviata al sistema di attuazione, applicando un algoritmo che può avere differente complessità. Se le informazioni che transitano dal sistema sensoriale a quello di controllo sono "dati grezzi" (*raw data*), allora il sistema di controllo dovrà effettuare tutta una serie di operazioni preliminari per la codifica ed interpretazione dei dati[23].

Catalogando e classificando le diverse tecniche di IA adoperate principalmente dalle reti di sensori *wireless* (*Wireless Sensor Network*, WSN), esse possono sinteticamente essere riportate come:

a. la ricerca euristica o metaeuristica;
b. metodi di apprendimento;
c. il senso comune e la logica o "logica *fuzzy*";
d. i linguaggi e gli strumenti dell'IA**[24]**.

Di seguito viene presentata una breve panoramica di queste tecniche.

2.2.a) Ricerca euristica o Metaeuristica

Il principale lavoro dell'IA si concentra sull'indagine di problemi e sulla creazione di relativi programmi che ne forniscano soluzione. Tuttavia, la realtà fattuale e situazionale di tali problematiche può essere sempre diversa e comportare la diramazione di numerose opportunità e decisioni diverse: la tecnica della ricerca euristica, o metaeuristica rappresenta il più comune algoritmo, che adopera un certo grado di casualità per ottenere soluzioni ottimali a problematiche complesse[25].

---

22 Flammini F. (2018) op. cit., Roma, p. 16 e ss.
23 Flammini F. (2018) op. cit., Roma, p. 18 e ss.
24 Nilsson N. J. (1982) Artificial Intelligence: engineering, science or slogan. *AI Magazine*, vol. 3, n. 1, p. 2-9.
25 Luke S. (2013) *Essentials of Metaheuristics*, Wuhan: Lulu Enterprises.

L’applicazione degli algoritmi meta-euristici abbraccia un ampio spettro di domini, con vari schemi di classificazione utilizzati per classificarli: tra questi, uno schema distingue tra approcci basati sulla traiettoria e approcci basati sulla popolazione[26].

Le strategie basate sulle traiettorie sono progettate principalmente per individuare una singola soluzione ottimale navigando nello spazio di ricerca in modo frammentario, attraverso il movimento nello spazio di ricerca e progettazione.

Al contrario, le metodologie basate sulla popolazione esplorano più soluzioni potenziali nello spazio di ricerca e si basano su interazioni cooperative per convergere verso una soluzione finale. Esempi di approcci basati sulla popolazione sono la computazione evolutiva, la computazione ispirata alla fisica[27] e la computazione ispirata alla natura[28].

Più agenti intelligenti possono affrontare collettivamente problemi complessi che un singolo agente o un sistema monolitico non sarebbe in grado di risolvere autonomamente e, a tal fine, esplorano attivamente il loro ambiente, interagiscono con gli agenti vicini e adattano i loro comportamenti in base alla conoscenza condivisa e alle intuizioni apprese per portare a termine le loro missioni designate[29].

2.2.b) Metodi di apprendimento

Il comportamento intelligente dei sistemi che applicano IA dipende principalmente dalle conoscenze e dal metodo di apprendimento sotteso: al fine di risolvere una problematica, il sistema necessita di una conoscenza sostanziale e di metodi per conformare efficientemente tale conoscenza, al fine di renderla facilmente accessibile.

Pertanto, la rappresentazione della conoscenza è, ad oggi, uno dei fulcri delle aree di ricerca e l’apprendimento è parte integrante dell’IA sotto forma di *Artificial Neural Network* (ANN), *Reinforcement Learning* (RL) e *Deep Learning* (DL)[30].

---

[26] Yang X.S. (2010) *Nature-Inspired Metaheuristic Algorithms*. Bristol: Luniver Press.

[27] La computazione ispirata alla fisica trae ispirazione dai principi della meccanica classica e quantistica, della termodinamica, dell'elettromagnetismo, della relatività e dell'ottica. Gli algoritmi di questo settore comprendono l'ottimizzazione della forza centrale, l'algoritmo di ricerca gravitazionale, le gocce d'acqua intelligenti e altri ancora. Osamy W., Khedr A. M., Salim A., et al (2022), op. cit., *Electronics*, 11(3):313.

[28] Il calcolo evolutivo si ispira all'evoluzione biologica e alla selezione naturale, con operatori come il *crossover* o la ricombinazione e la mutazione. Gli algoritmi più noti di questa categoria sono gli algoritmi genetici, l'evoluzione differenziale e gli algoritmi memetici. Osamy, W., Khedr A. M., Salim A., et al (2022) Recent Studies Utilizing Artificial Intelligence Techniques for Solving Data Collection, Aggregation and Dissemination Challenges in Wireless Sensor Networks: A Review. *Electronics*, 11(3): 313. Le computazioni ispirate alla natura emulano i comportamenti di varie entità naturali come colonie, uccelli, stormi e insetti, considerando i loro metodi di interazione e comunicazione. Un esempio significativo è il comportamento collettivo esibito dagli insetti sociali all'interno di un gruppo, definito *Swarm Intelligence* (SI), che si concentra sugli sforzi collaborativi di numerosi individui simili all'interno di un ambiente. Brownlee J. (2011) *Clever Algorithms: Nature-Inspired Programming Recipes.* Wuhuan: Lulu.

[29] Dorri A., Kanhere S.S., Jurdak R. (2018) Multi-agent systems: A survey. *IEEE Access*, 6: 28573–28593.

[30] Bengio Y. (2009) Learning Deep Architectures for AI*. Foundations and Trends in Machine Learning*, 2(1): 10 ss.; Lexcellent C. (2019) *Artificial intelligence versus human intelligence: are humans going to be hacked?*. Berlino: Springer, 10 ss.

In particolare, le ANN appaiono in grado di risolvere problemi impegnativi, grazie alla loro capacità di imitare la rete neurale biologica e le caratteristiche umane: strutturalmente, esse sono formate da molteplici dispositivi interconnessi, anche noti come nodi, ispirati ai neuroni biologici di un cervello, da cui passano le informazioni attraverso collegamenti rappresentati da una freccia[31]. Il vantaggio principale dell'utilizzo delle ANN rispetto ad altri metodi risiede nella sua capacità di modellare processi non lineari e complessi senza troppe interruzioni tra variabili di *input* e *output*[32].

Il *Reinforcement Learning* (RL), invece, attiene alle modalità con cui gli agenti intelligenti interagiscono in un ambiente, con l'obiettivo di massimizzare il concetto di ricompensa cumulativa. In tal caso, l'apprendimento si ottiene grazie all'interazione tra le entità di apprendimento e l'ambiente che le circonda, anche attraverso tentativi e primi errori, poiché sussistono numerose azioni praticabili per ciascuna condizione, in uno specifico momento[33].

Per contro, l'architettura che caratterizza il *Deep Learning* (DL) include differenti livelli tra *input* e *output* e unità di elaborazione delle informazioni non lineari ed è considerato come uno schema di apprendimento universale, essendo applicato per la soluzione di svariati problemi in diverse aree di applicazione[34].

Il DL, essendo un sistema autonomo dotato della capacità di apprendere imitando il cervello umano nell'elaborazione di dati e creazione di modelli per il processo decisionale, ed attingendo da dati non strutturati e non etichettati, è una funzione sofisticata dell'IA basata sull'apprendimento della rappresentazione[35].

Pertanto, il DL viene altresì adoperato per risolvere problemi di analisi di *Big Data,* inclusi quelli che presuppongono la determinazione del volume di informazione di *input* necessarie per rappresentare gli algoritmi DL e ottenere buone astrazioni e rappresentazioni dei dati[36].

Attualmente, DL è praticamente utilizzato in quasi tutti i campi, pertanto è spesso definita come tecnica di apprendimento universale[37].

---

31 Osamy W., Khedr A. M., Salim A., et al (2022), op. cit., *Electronics*, 11(3):313. Per un approfondimento tecnico in merito al funzionamento delle diverse tipologie di reti neurali si rimanda a Russell S., Norvig P. (2005) op. cit. Milano: Pearson, vol. 1, 423 ss. e a Goodfellow-Y. I. Courville Bengio-A. (2016) *Deep Learning*, Cambridge: Cambridge Press, 489 ss. È possibile vedere le modalità di funzionamento di una rete neurale all'indirizzo *playground.tensorflow.org*.

32 Bello, O.; Holzmann, J.; Yaqoob, T.; Teodoriu, C. (2015). op. cit. *Journal of Artificial Intelligence and Soft Computing Research.* 5: 121–139. Osamy W., Khedr A. M., Salim A., et al (2022), op. cit., *Electronics*, 11(3):313.

33 Chen S.H.; Jakeman A.J.; Norton J.P. (2008) Artificial intelligence techniques: An introduction to their use for modelling environmental systems. *Mathematics and Computers in Simulation.* 2(78): 379–400.

34 Alom M. Z.; Taha T. M.; Yakopcic C.,et al (2019) A state-of-the-art survey on deep learning theory and architectures. *Electronics*, 8: 292.

35 Osamy W., Khedr A. M., Salim A., et al (2022), op. cit., *Electronics*, 11(3):313.

36 Chang C. W., Lee H. W.; Liu C.H. (2018) A review of artificial intelligence algorithms used for smart machine tools. *Inventions*, 3: 41.

37 Alom M. Z.; Taha T. M.; Yakopcic C.,et al. (2019) op. cit. *Electronics*, 8: 292. Osamy W., Khedr A. M., Salim A., et al (2022), op. cit., *Electronics*, 11(3):313.

2.2.c) Il senso comune e la logica o "logica fuzzy"

Nei sistemi che applicano IA, le caratteristiche più complesse da sviluppare sono di certo ciò che intendiamo come senso comune o buon senso, in quanto esso si fonda sulle esperienze che il sistema necessariamente deve immagazzinare e processare nel tempo e la logica, ovverosia la capacità della macchina di dedurre qualcosa basandosi sulla realtà fattuale presentata, dimostrando che la conclusione a cui il sistema perviene segue un insieme logico di premesse. In effetti, la logica computazionale è stata la speranza che, sin dagli albori delle ricerche, ha tenacemente spinto lo sviluppo dell'IA, con l'idea di fornire un metodo universale di risoluzione dei problemi.

Tuttavia, dopo prime fallaci applicazioni sui problemi complessi[38], la logica dei sistemi di IA, basata su nuove formulazioni e sull'uso di ricerche euristiche per raggiungere le soluzioni sembra adesso tornata a rappresentare le priorità delle ricerche e della letteratura.

Difatti, la logica "*fuzzy"* (LF) è una tecnica dell'IA che imita il modo di prendere le decisioni umane ed è adoperata per ragionamenti incerti o per processare e gestire informazioni incomplete[39]: quando il sistema di descrizione è un modello incerto o l'oggetto di controllo ha una forte non linearità e un grande ritardo, gli insiemi e le regole *fuzzy* simulano la modalità di lavoro del cervello umano per esprimere limiti transitori o esperienza di conoscenza qualitativa e formulare giudizi[40].

2.2.d) Linguaggi e strumenti dell'IA

Nell'ambito informatico e nell'IA, sono stati sviluppati linguaggi specifici di alto livello, adattati ai diversi domini applicativi: al momento i principali linguaggi di programmazione dell'IA sono LIPS[41] e PROLO[42] con caratteristiche distintive e importanti applicazioni non solo nel campo dell'IA ma anche nella programmazione logica.

---

38 Per un commento sul punto, si veda Akgül A. (1990) op. cit., Ankara Üniversitesi SBF Dergisi 45.

39 Bello, O.; Holzmann, J.; Yaqoob, T.; Teodoriu, C. (2015). op. cit. *Journal of Artificial Intelligence and Soft Computing Research.* 5: 121–139. Leung Y. (2009) Fuzzy set and fuzzy logic. *International Encyclopedia Human Geography*, 32(4): 283-287.

40 Boucher P. (2019) *How Artificial Intelligence Works; Scientific Foresight Unit*; EPRS | European Parliamentary Research Service, European Union. Osamy W., Khedr A. M., Salim A., et al (2022), op. cit., *Electronics*, 11(3):313.

41 LISP, acronimo di "LISt *Processing*," è un linguaggio di programmazione funzionale, originariamente concepito per progetti di ricerca informatica, come IA, robotica, elaborazione del linguaggio naturale e la dimostrazione di teoremi. Una delle caratteristiche del LISP è la completa equivalenza tra i programmi e i dati: le strutture dati possono essere eseguite come programmi e i programmi possono essere trattati come dati. Inoltre, il LISP crea un ambiente interattivo in cui i programmi possono cambiare forma dinamicamente, consentendo agli utenti di inserire sequenze di espressioni da valutare direttamente al terminale.

42 Il Prolog, d'altra parte, è un linguaggio di programmazione logica che fa ampio uso del calcolo dei predicati per risolvere problemi, il cui obiettivo principale è fornire una descrizione dettagliata della soluzione, consentendo al sistema di derivare l'esecuzione della sequenza anziché richiedere la definizione di algoritmi specifici per risolvere il problema. L'interprete Prolog riceve input dall'utente sotto forma di *query*, restituendo *output* come vero o falso a seconda delle assegnazioni alle variabili nella *query.* Colmeraue A. (1985), Prolog in 10 figures. *Communications of the ACM*, 28(12).

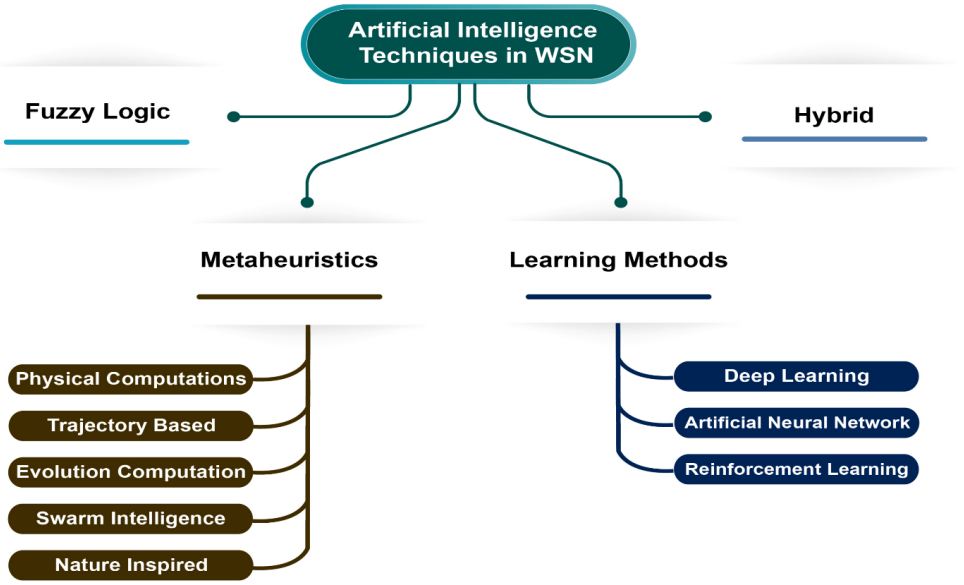

Fig. 1 - Metodi di intelligenza artificiale applicati per affrontare le sfide di raccolta, aggregazione e diffusione dei dati WSN.

Fonte: Electronics | Free Full-Text | Recent Studies

2.3 Aree di Applicazione dell'Intelligenza Artificiale

2.3.1 Applicazioni generali

Al fine di fornire un quadro completo delle soluzioni proposte dall'Intelligenza Artificiale, la dottrina ha individuato diverse aree di applicazione dell'IA, distinte in base alle finalità di utilizzo, tra le quali vi è l'elaborazione di linguaggio, *recommendation systems*, la visione artificiale, i sistemi esperti e le soluzioni fisiche[43].

L'elaborazione del linguaggio naturale, o *Natural Language Processing* (NLP) è una branca dell'IA che attiene all'informazione espressa nel linguaggio naturale finalizzata all'elaborazione di un linguaggio che appaia naturale, riguardando il linguaggio come *front-end* per i programmi informatici, la comprensione del testo, la traduzione, fino alla produzione di testo in modo autonomo a partire da dati o documenti forniti in *input*.

Per quanto concerne i *recommendation systems*, talune applicazioni dell'IA sono predisposte per influenzare le scelte degli utenti sulla scorta di informazioni da essi fornite in modo esplicito o implicito. Un esempio lampante di applicazione di sistema di raccomandazione, grazie all'IA, è rappresentato dai sistemi che suggeriscono taluni acquisti, in base a scelte già espresse dall'*end user*, largamente impattando l'esperienza di acquisto del consumatore e, più in generale, lo stesso processo decisionale dell'utente.

---

[43] Nilsson N. J. (1982) op. cit. *AI Magazine*, 3(1): 6. Si veda altresì la ricerca condotta dall'Osservatorio di Artificial Intelligence, reperibile online al sito La Ricerca dell'Osservatorio Artificial Intelligence.

La visione artificiale, o *computer vision*, è un campo scientifico responsabile di condurre studi su algoritmi e tecniche che siano in grado di fornire ai computer una elevata comprensione dei contenuti di immagini o video. Ciò comporta anche la possibilità non solo di analizzare immagini, singole o in sequenza al fine di riconoscere soggetti o cose presenti nell'immagine stessa, ma anche di effettuare un riconoscimento biometrico e di estrarre dati ed informazioni dall'immagine.

A mero titolo di esempio, basti considerare che l'accuratezza della classificazione di immagini del *software* ImageNet ha superato quella umana[44] e, in generale il tasso di riconoscimento facciale condotto dai sistemi di IA ha raggiunto la percentuale di 99,8% di successo, largamente adoperati nell'ambito della videosorveglianza e della pubblica sicurezza[45].

In ultimo, per quanto attiene ai sistemi esperti, valga considerare come il fine ultimo a cui i sistemi di IA tendono è di riuscire autonomamente a emulare i comportamenti umani e, tra questi, quelli più sofisticati, che presupponendo una certa *expertise* negli argomenti, possa portare i sistemi a fornire analisi, progettazioni o diagnosi[46].

In tale ambito possiamo ricomprendere sistemi di programmi informatici intelligenti che utilizzano la tecnologia di IA e la tecnologia informatica per svolgere ragionamenti e giudizi secondo le conoscenze e l'esperienza fornite da uno o più esperti e simulano il processo decisionale di esperti umani per risolvere i complessi problemi.

Tra questi sistemi vi sono l'*Intelligent Data Processing* e i *Virtual Assistants*, come i *Chatbot:* i primi menzionati sono algoritmi che conducono analisi su dati specifici, al fine di estrapolarne le informazioni più importanti e, sulla scorta di essi, compiere azioni conseguenti. In tale categoria troviamo, ad esempio, i sistemi di analisi predittiva, i quali analizzano i dati per fornire previsioni sulle tendenze future di taluni fenomeni.

La seconda categoria, forse la più diffusa e nota, è quella degli assistenti virtuali o *chatbot*, agenti *software* in grado di eseguire azioni o erogare determinati servizi per un utente o un gruppo di essi, seguendo comandi precedentemente ricevuti. Tali sistemi sono fortemente comuni nei servizi di assistenza clienti di aziende, in quanto i bot sono in grado di cogliere gli aspetti cruciali dei dialoghi, memorizzare le informazioni raccolte e fornire soluzioni.

---

[44] Markowitz J., Schmidt A. C., Burlina P. M. et al (2017) "Combining deep universal features semantic attributes and hierarchical classification for zero-shot learning" in Conference proceedings of 2017 IAPR MVA Conference pp. 1-17.

[45] W.-Y. Yang, H. Zhang, D.-Z. Song and F.-N. Lai (2018) "Review of face recognition methods" in Conference Modeling Simulation Optim. Technol. Appl. 560-564.

[46] Per un commento sui sistemi esperti, si veda Mohiuddin A. K. M. (2003) "Expert system for the thermal design of mechanical devices" in Conference proceedings Intell. Eng. Syst. (INES), 212-214.

Tra la classe di applicazioni delle soluzioni fisiche, invece, rientrano i mezzi di trasporto autoguidati, ossia gli *Autonomous Vehicle*, veicoli adoperati per il trasporto di persone, animali o oggetti non solo via terra, ma anche via mare o per via aeree.

Inoltre, gli oggetti smart, o *intelligent objects*, capaci di compiere azioni autonomamente, senza l'intervento o il supporto umano, e di prendere decisioni sulla scorta dell'analisi dell'ambiente circostante.

2.3.2) Applicazioni militari

Nell'ambito militare, l'impatto che l'IA potrebbe ottenere sulla tecnologia e le tattiche militare sarebbe potenzialmente enorme, potendo migliorare sistemi d'arma e personale, dotandoli di una sempre maggiore autonomia e sofisticazione[47].

A ben vedere, le attività legate alla tecnologia dell'IA e le sue applicazioni in ambito militare sono cresciute esponenzialmente: il rinnovato interesse del settore militare per l'utilizzo di strumenti che utilizzano l'IA appare speculare ed osserva la sempre crescente complessità delle operazioni militari odierne, le quali stanno sperimentando significativi progressi nella velocità e precisione di sensori ed armi[48].

Non solo, il settore militare ha anche assistito ad una rapidissima crescita delle quantità di informazioni da processare, analizzare e produrre (*Big Data*), in condizioni di grave limitazione di personale e tempistiche.

Pertanto, l'IA parrebbe poter essere uno strumento efficace per poter sormontare tali problematiche, grazie anche ai numerosi e concreti progressi che tali tecnologie stanno compiendo nel settore civile, in particolare in centri di ricerca e nelle applicazioni commerciali[49].

---

47 Martin E. W. (1983) "Artificial Intelligence and Robotics for Military Systems" in proceeding of the army conference on application or artificial intelligence to Battlefield Information Management, US Navy Surface Weapons Centre, p. 3.

48 Gli Stati di ogni continente stanno forgiando i propri percorsi verso la raccolta delle loro capacità nazionali per realizzare un'IA pronta per il campo di battaglia. Un esempio fondamentale è il Project Maven del Dipartimento della Difesa degli Stati Uniti: il progetto tenta di fornire informazioni migliori e più fruibili creando algoritmi di "visione artificiale" che riconoscono e identificano le classi di oggetti dalle riprese video dei droni per supportare il processo decisionale mirato. Allo stesso tempo, la Repubblica popolare cinese ha lavorato per realizzare un piano in tre fasi per diventare il leader mondiale nell'IA entro il 2030. Facendo eco alla Cina, dal 2017 anche la Federazione Russa ha investito nell'IA, anche se a un livello molto più basso rispetto agli Stati Uniti o alla Cina. Inoltre, l'israeliana Rafael Advanced Defense Systems ha presentato una nuova munizione guidata di precisione Spice-250, che pretende di utilizzare l'intelligenza artificiale e l'apprendimento profondo per consentire il "riconoscimento automatico del bersaglio". Singapore sta usando l'intelligenza artificiale per "condurre la manutenzione predittiva sulle navi della marina". La Repubblica di Corea ha in corso due progetti di elaborazione e risposta alle informazioni AI denominati Exobrain e ADAMs, nonché un Gyun-Ma, un progetto di veicolo da combattimento senza equipaggio. Si veda Horowitz M. C., Kahn L., Mahoney C. (2020) The Future of Military Applications of Artificial Intelligence: A Role for Confidence-Building Measures?. *Foreign Policy Research Institute*, 532.

49 Encyclopedia of Artificial Intelligence, Wiley, 1987, 604.

Sebbene non originariamente progettate pensando alle applicazioni militari, molte di queste capacità sono "duali o multiuso in contesti civili e militari"[50] e le forze armate appaiono adattarsi, seppur lentamente, all'idea che la proliferazione dell'IA potrebbe essere indispensabile, sebbene valutando eventuali ricadute o rischi applicativi.

Se in passato il settore militare pareva essere il pioniere nell'elaborazione di tecnologie e sistemi, che successivamente venivano impiegati anche nel settore civile, divenendo di uso comune[51], ad oggi, molte tecnologie impiegate nell'ambito civile sono trasposte nel settore militare, decretando come la *leadership* dell'innovazione tecnologica sia ad oggi sospinta dalle ricerche in ambito civile, con le nuove necessità, priorità e paradigmi della società odierna[52].

Pertanto, è necessario che vi sia un trasferimento delle tecnologie abilitanti dal dominio civile a quello militare e viceversa (c.d. *cross-fertilisation*) e la possibilità di attingere utilmente dall'esterno (*open innovation*).

Al momento, vi sono già numerose specifiche applicazioni militari dell'IA in settori cruciali quali il C4ISR (Comando, controllo, comunicazioni, computer, intelligence, sorveglianza e ricognizione), dove i sistemi autonomi abilitati all'IA offrono supporto decisionale con conseguenti analisi di *intelligence* più affidabili e nell'area delle operazioni critiche di Comando, Controllo, Comunicazione e Intelligenza (C^3I), ove vi è la necessità di una risposta appropriata e in tempo reale a situazioni dinamiche.

L'IA, inoltre, supporta la pianificazione delle capacità a lungo termine mediante lo sviluppo di soluzioni analitiche, incluso il supporto di processi decisionali complessi mediante valutazioni di fattori complessi, come la penuria di tempo disponibile per prendere decisioni tattiche, cercando di trovare la prima soluzione che soddisfi un determinato insieme di condizioni o che superi una determinata soglia[53].

Generalmente, le aree specifiche di applicazione dell'IA nell'ambito militare si riconducono a tre: i veicoli terrestri autonomi (*autonomous land vehicle*), i piloti associati

---

[50] Morgan F. E., Boudreaux B., Lohn A.J. et al. (2020) *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. Santa Monica: RAND Corporation.

[51] A mero titolo di esempio, si ricorda l'ARPANET, precursore dell'attuale Internet, sviluppato nel dipartimento di difesa degli Stati Uniti d'America, così come algoritmi di cifratura dei dati e telecamere termiche. Si veda Flammini F. (2018) op. cit., Roma.

[52] Basti pensare Smart-City e Industry 4.0. Si pensi ad esempio ai veicoli a guida autonoma, nati in ambito militare ma che si stanno sviluppando rapidamente - probabilmente più rapidamente - in ambito civile con le cosiddette *self-driving cars*. Flammini F. (2018) op. cit., Roma,

[53] Szabadföldi I. (2021) Artificial Intelligence In Military Application – Opportunities And Challenges. *Revista Academiei Forţelor Terestre*. 2 (102), 162.

intelligenti (*pilot's associate*) e la gestione della battaglia navale (*naval battle management*)[54].

Per quanto riguarda le aspettative riguardanti l'IA nell'applicazione militare nel prossimo decennio, alcune delle sue tecniche definiranno o ridefiniranno le principali tecnologie militari avanzate: le soluzioni di IA saranno interconnesse per utilizzare la rete di domini virtuali e fisici, inclusi sensori, organizzazioni, individui e agenti autonomi, sfruttando anche il vantaggio della tecnologia *blockchain* per l'integrità dei dati[55].

Inoltre, potrebbe esservi la possibilità di concepire, grazie all'applicazione dell'IA, nuove metodologie per gestire problemi di acquisizione ed elaborazione delle informazioni, con meno risorse computazionali e di comunicazione delle attuali, agevolando la trasmissione di informazioni in tempi rapidi.

Tale possibilità risulta essere non troppo remota, considerando l'enorme potenzialità dell'IA di trasformare dati numerici grezzi in domini di entità simboliche e semantiche in molti livelli di elaborazione delle informazioni e dei dati[56].

---

[54] Lo sviluppo di un veicolo terrestre autonomo si concentra su tecnologie di visione computerizzata e di comprensione delle immagini: il veicolo è in grado di determinare in modo automatico il percorso di una strada, seguirlo, rilevare un ostacolo sul suo percorso, determinarne la natura e di reagire di conseguenza. L'aggiunta di tecniche avanzate di ragionamento AI potrebbe consentire al veicolo non solo di percepire e reagire, ma anche di interpretare l'ambiente circostante e di adattare di conseguenza la strategia della missione. Tra questi sistemi autonomi, vi sono gli UxV (*Unmanned Vehicles*, veicoli senza pilota) che possono operare su un livello di efficienza e sicurezza molto più elevato con il supporto AI e di sistemi di deep learning che estende significativamente le capacità robotiche per la navigazione. Il progetto *Pilot's Associate* mira a fornire al pilota di un aereo da combattimento il supporto e le competenze logiche in aree specifiche attraverso il concetto di cabina di pilotaggio integrata. L'interfaccia pilota-veicolo include tecniche avanzate di controllo, visualizzazione e automazione che utilizzano il riconoscimento vocale, la comprensione del linguaggio naturale e la sintesi vocale. Il sistema è costituito da quattro principali sottosistemi esperti interattivi: un gestore della valutazione della situazione, un gestore della pianificazione tattica, un gestore della pianificazione della missione e un gestore dello stato del sistema. Uno degli obiettivi del programma di gestione delle battaglie è contribuire allo sviluppo di aiuti decisionali automatizzati per il complesso ambiente di combattimento attraverso funzioni di gestione della battaglia che comprendono i requisiti delle forze, la valutazione delle capacità, la simulazione della campagna, la pianificazione delle operazioni e la valutazione della strategia. I sistemi esperti sviluppati per queste applicazioni dovranno interagire e cooperare tra loro. Encyclopedia of Artificial Intelligence, Wiley, 1987, p. 604. Morgan F. E., Boudreaux B., Lohn A.J. et al. (2020) op. cit. Santa Monica: RAND Corporation.14 e ss.

[55] NATO Science & Technology Organization. (2020). Science & Technology Trends 2020-2040. Brussels, Belgium, available at: https://www.nato.int/nato_static_fl2014/ assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

[56] Salisbury A. B. (1983) "Opening remarks on artificial intelligence", in Proceedings of the Arm Conference on Application of Artificial Intelligence to Battlefield Information US Navy Surface Weapons Center, White Oak, p. 7.

3. L'applicazione di strumenti di Intelligenza Artificiale e *Machine Learning* per processare i *Big Data.*

L'odierna indagine riguarda la possibilità di adoperare strumenti quali l'IA e ML al fine di processare dati, estrarne tendenze ed informare futuri investimenti ed acquisti delle Forze Armate.

Ebbene, al fine di poter condurre questa indagine appare opportuno partire dalla definizione di *Big Data*, i quali sono risorse informative ad alto volume, alta velocità, alta varietà e alta veridicità (4V) che richiedono forme economiche e innovative di elaborazione delle informazioni per una migliore comprensione e processo decisionale[57]. Inoltre, negli ultimi anni, l'applicazione di *Big Data*, la sua acquisizione e l'analisi adoperante sistemi e algoritmi di IA e ML sono stati applicati per identificare informazioni critiche per i processi decisionali[58].

Un dato è un'informazione di cui non si conosce la chiave di decodifica ed interpretazione: al fine di rendere un insieme di dati un'informazione effettivamente utilizzabile, è necessario conoscere il modello che associa l'informazione alla sua rappresentazione, ovverosia il dato.

Il termine "*Big Data*" è stato recentemente applicato agli insiemi di dati che crescono così tanto da rendere difficile il lavoro con i tradizionali sistemi di gestione dei *database*. Si tratta di insiemi di dati le cui dimensioni superano la capacità degli strumenti *software* e dei sistemi di archiviazione comunemente utilizzati di acquisire, archiviare, gestire ed elaborare i dati entro un tempo tollerabile[59].

Il fulcro di un sistema di intelligenza artificiale è rappresentato dagli algoritmi dell'applicazione e dalle sue capacità e prestazioni. Come vedremo più avanti, questi algoritmi hanno caratteristiche vantaggiose ma anche a volte contraddittorie, che potrebbero portare a problemi nel loro funzionamento in una varietà di domini applicativi[60].

---

[57] In questa definizione, il volume si riferisce alla grandezza o alla dimensione dei dati, la varietà si riferisce all'eterogeneità strutturale nel *set* di dati, la velocità si riferisce alla velocità con cui i dati sono generati e la veridicità si riferisce alla veridicità o affidabilità dei dati. Rajšp A., Fister I. (2020) A systematic literature review of intelligent data analysis methods for smart sport training. *Applied Science* 10:3013. Roy R., Paul A., Bhimjyani P., et al. (2020) A short review on applications of *Big Data* analytics. In: Mandal J.K., Bhattacharya D. et al., a cura di, *Emerging technology model graph*. Singapore:Springer, 265–78. Claudino J.G., Cardoso F. C.A., Boullosa D., et al. (2021) The role of veracity on the load monitoring of professional soccer players: a systematic review in the face of the big data era. *Applied Science* 11:6479.

[58] Cottle M., Hoover W., Kanwal S., et al (2013) Transforming health care through *Big Data*: strategies for leveraging big data in the health care industry. *Institute Health Technology Transformation - iHT*.

[59] Kubick W.R. (2012) Big Data, Information and Meaning. *Clinical Trial Insights*, pp. 26–28.

[60] Lovergine S. (2022) Breve disamina degli algoritmi di intelligenza artificiale. Aspetti tecnologici e metodologici, Rapporto dell'Istituto Nazionale per Analisi Politiche Pubbliche (INAPP), 7, 8.

Pertanto, nei sistemi di monitoraggio distribuito è indispensabile connettere i *Big Data* alla sintesi che permetta di estrarre le informazioni rilevanti, solo dopo aver condotto una opportuna analisi, ossia il *Big Data Analytics*. A seguito di tale analisi dei dati, vengono estratte delle informazioni rilevanti, definite "*features*", che influenzano il livello successivo, ossia la *decision fusion*, volta a prendere la decisione complessiva sull'evento analizzato, sulla scorta delle decisioni prese dai singoli componenti distribuiti su una certa area[61].

Per questo motivo, l'analisi dei *Big Data* è l'applicazione di tecniche analitiche avanzate a grandi insiemi di dati che rivela e sfrutta i cambiamenti e le tendenze di un'organizzazione.

Ci sembra come l'elaborazione di ingenti quantità di dati costituisca la chiave di volta dell'*investment management*, principalmente nel settore privato, rappresentato da operazioni quali gestione del portafoglio, dei rischi e il *trading*, consentendo ai gestori patrimoniali di avere una più chiara panoramica dei dati, adoperando l'IA e le operazioni di *data-crunching*[62] che, tuttavia, potrebbe essere declinato alle esigenze delle Forze Armate.

3.1 *Big Data Advanced Analytics* (BDAA) e rapporto con l'Intelligenza Artificiale

Uno strumento che si potrebbe adoperare al fine di processare *Big Data* è, come già accennato, l'Analisi Avanzata dei *Big Data* (*Big Data Advanced Analytics*, BDAA).

I sistemi *software* basati su tecniche di intelligenza artificiale disponibili ai centri di controllo devono prevedere meccanismi di consapevolezza situazionale (*situation awareness*), allerta precoce (*early warning*) e supporto alle decisioni (DSS, *Decision Support Systems*) realizzati tramite analisi e correlazione dei dati (*Big Data Analytics*), fusione delle informazioni (*information fusion*), riconoscimento di eventi/sequenze (*event/pattern recognition*), approcci di *soft-computing* ed euristiche che consentano di gestire incertezze, attacchi imprevisti e minacce sconosciute.

La BDAA si basa dunque su tecnologie avanzate non solo necessariamente sull'IA e l'apprendimento automatico, ma anche l'analisi dei dati in tempo reale e l'elaborazione distribuita, che consentono di gestire grandi quantità di dati provenienti da diverse fonti, come sensori, dispositivi IoT, social media, transazioni commerciali etc. Secondo l'Organizzazione NATO per la Scienza e la Tecnologia, l'analisi avanzata dei *Big Data* comprende quattro componenti fondamentali: la raccolta dei dati attraverso sensori, la

---

61 Flammini F. (2018) op. cit., Roma,

62 Il *data crunching* è il processo di automatizzazione del filtraggio e della traduzione dei dati da un formato all'altro. Spesso si occupa di dati testuali, ma può anche trattare XML, dati binari e database relazionali. Joyce J. (2005). Data crunching. *Scientific Computing and Instrumentation* 22(8):47.

comunicazione dei dati, l'analisi dei dati e il processo decisionale[63]. Questa tecnologia consente di comprendere e visualizzare grandi quantità di informazioni, offrendo una maggiore consapevolezza situazionale (*Situational Awareness*)[64] e una migliore pianificazione e preparazione dei piani. Inoltre, l'analisi avanzata dei *Big Data* può migliorare la gestione delle organizzazioni, ottimizzando i processi e monitorando in tempo reale i risultati delle decisioni prese[65].

Come vedremo più nello specifico, l'analisi avanzata dei *Big Data*, combinata con l'intelligenza artificiale, potrebbe fornire valutazioni prescrittive attraverso modellazione e simulazione avanzate e garantire un approccio completo alla pianificazione operativa, all'analisi dei corsi di azione e al *targeting*[66].

Anzitutto, come rilevato durante l'intervista con l'esperto di IA, possiamo individuare tre diverse tipologie di analisi che possano essere condotte grazie alla BDAA: descrittiva, predittiva e prescrittiva.

La prima, analisi di tipo descrittivo, appare essere la più elementare, in quanto consente di analizzare le tendenze storiche e individua modelli rilevanti per ottenere informazioni sui *trend.* Tale tipologia di analisi implica la formulazione di domande non complesse e dirette quali "cosa è successo?", "in quale quantità?" ed adopera tecniche statistiche e matematiche di base per ottenere indicatori chiave di prestazione che mettano in luce le tendenze dei dati storici di gestione. Pertanto, lo scopo principale di tale analisi non è stimare un valore, ma ottenere informazioni sul comportamento che lo genera. A tal fine, strumenti come Microsoft Excel (o, in alternativa PowerBi o Tableu), attualmente in uso alle Forze Armate, possono essere largamente adoperati ed eseguirebbero una prima indagine descrittiva.

La seconda tipologia di analisi, quella predittiva, appare più complessa in quanto adopera la modellazione statistica per determinare la probabilità che si verifichi un

---

63 NATO Science & Technology Organization. (2020). Big Data Advanced Analytics (BDAA) for Defence. Department of Defense Independent Technical Risk Assessment Execution Guidance: 2.1

64 La consapevolezza della situazione (SA) è la percezione e la comprensione degli elementi ambientali nelle profondità del tempo e dello spazio, la comprensione delle intenzioni di altri agenti e l'inferenza della tendenza dello stato da sviluppare. Con lo sviluppo della tecnologia dell'informazione, la modalità di guerra è cambiata da combattimento singolo a combattimento congiunto integrato, il che significa l'unificazione e il coordinamento di tutte le unità di combattimento. A causa delle caratteristiche del combattimento congiunto, come uno spazio di combattimento multidimensionale, più forze di combattimento e un comando di battaglia unificato dell'operazione complessiva, i comandanti devono avere il comando in tempo reale del campo di battaglia. La capacità di acquisire conoscenza della situazione del campo di battaglia dipende fortemente da una varietà di sistemi di consapevolezza del campo di battaglia.
È fondamentale elaborare le informazioni fuse per formare conoscenze e comprensione situazionali che riflettano la situazione attuale e quindi trasmetterle al conducente e ad altri sistemi. L'intero processo operativo, come la gestione dei sensori, il processo decisionale degli assistenti e la gestione dell'interfaccia uomo-macchina (MMI), si basa sulla qualità di SA .Endsley M. R., Praphrcul G. (1999) 'Supporting situation awareness in aviation systems,' *Brit. J. Occupational Therapy*, 5(62), 131–135.

65 NATO Science & Technology, ibidem.

66 NATO Science & Technology, ibidem.

determinato risultato nel futuro. Le domande che, in tal caso, il sistema si pone sono del tipo "Cosa potrebbe avvenire?". Tale modello prende comunque in considerazione il modello descrittivo e tuttavia, al contrario di questo, non appare ancorato ai dati storici, ma il processo decisionale di dati strutturati. Questa tipologia di analisi consentirebbe alle Forze Armate di prendere decisioni informate, non solo basandosi e fornendo un resoconto onnicomprensivo degli storici, ma analizzando tramite indagine probabilistica la fattibilità di taluni investimenti eventuali e l'utilità di talaltri investimenti già effettuati. I modelli comunemente adoperati sono: RapidMiner, R, Python, SAS, Matlab, Dataiku DSS, e molti altri.

In ultimo, l'analisi prescrittiva rappresenta il tipo più sofisticato di analisi, che adopera l'ottimizzazione e la simulazione stocasistica per valutare le opzioni possibili e consigliare la migliore azione possibile, data la situazione fattuale. In tal caso, le domande poste sono del tipo: "Cosa dovrei fare in tale data situazione?". Grazie a questa analisi, si ottiene un vero e proprio supporto decisionale su quale scelta ed azione intraprendere sulla scorta di una quantificazione dell'impatto delle azioni future sulla metrica dell'organizzazione. Tali modelli sintetizzano dunque i *Big Data* e le regole dell'organizzazione nella quale operano usando algoritmi complessi per valutare quale, tra tutti i probabili risultati di un'azione, sia quella ottimale.

Tali modelli possono arrivare ad essere estremamente sofisticati e performanti, tanto da essere in grado di apprendere costantemente ed automaticamente dai dati inseriti per migliorarsi. Gli strumenti utilizzati per eseguire i modelli prescrittivi sono per lo più gli stessi dei modelli predittivi, tuttavia richiedono capacità avanzate di infrastruttura dei dati e, solo in questa ultima analisi, l'utilizzo dell'IA appare indispensabile, potendosi, nelle tipologie meno avanzate come quelle descrittive e predittive usarsi *software* non impieganti sistemi IA.

In tale sede, appare opportuno altresì menzionare un sistema alternativo, sempre finalizzato a rendere il processo decisionale più efficace e informato a rigore logico, efficacia ed efficienza è l'approccio, introdotto da Boyd, dell'OODA (*Observation, Orientation, Decision and Action*)[67].

Tale *framework* si è dimostrato utile per affrontare le sfide del processo decisionale in ambienti complessi e l'OODA *loop* è composto da quattro fasi interconnesse – osservazione (*observation*), orientamento (*orientation*), decisione (*decision*), e azione (*action*) ed offre una struttura per la raccolta di informazioni, l'analisi, la decisione e l'implementazione delle azioni.

---

[67] Il colonnello John Boyd, uno stratega militare, ha sviluppato il framework OODA (*Observation, Orientation, Decision, and Action*)

Il framework OODA, tuttavia, si differenzia dalla categoria di nostro interesse della *Big Data Advanced Analytics* (BDAA), in quanto è un modello concettuale sviluppato per guidare il processo decisionale in situazioni ad alta velocità e ad alta incertezza, come ad esempio le operazioni militari[68].

D'altra parte, la BDAA si riferisce all'applicazione di tecniche e strumenti avanzati per analizzare *Big Data* al fine di estrarre informazioni significative, identificare modelli e tendenze, e prendere decisioni informate[69], coinvolgendo l'uso di algoritmi di *machine learning*, intelligenza artificiale e altre tecniche analitiche per estrarre valore dai dati.

Sebbene il framework OODA possa essere utilizzato in combinazione con l'analisi dei dati, non è specificamente legato all'ambito della BDAA. Nondimeno, entrambi i *framework* adoperano dei processi comuni, che possiamo analizzare congiuntamente. Valga tuttavia rimarcare come il modello di riferimento che riteniamo più confacente alle necessità delle forze armate rimanga quello della BDAA, non invece quello di OOD, che potrebbe essere adoperato, piuttosto, nelle applicazioni operative militari.

3.1.1) Fusione delle Informazioni (Information Fusion)

La fusione delle informazioni o dati è un ambito di ricerca con forti sovrapposizioni con l'IA, in grado di integrare ed elaborare in modo completo informazioni e conoscenze derivanti da fonti diverse, anche sorgenti non affidabili ed eterogenee, al fine di ottenere una descrizione e comprensione il più accurate e affidabili possibili.

L'IF generalmente adotta una struttura di fusione a tre strati: fusione del livello dati (anche partendo da dati grezzi di sensori non tradizionali), sino ad arrivare a fusione del livello di funzionalità e, nei casi più alti, raffinamento cognitivo e fusione del livello decisionale, includendo il ragionamento classico e i sistemi esperti[70].

La tecnologia di IF fornisce un campo di applicazione e spazio di ricerca molto ampio, le cui applicazioni sono le già menzionate teoria fuzzy e l'ANN[71].

---

[68] Boyd J. R. (1996). A Discourse on Winning and Losing. Alabama: Air University Press Maxwell AFB. 2018.

[69] Provost F., Fawcett, T. (2013). Data science and its relationship to big data and data-driven decision making. *Big data*, 1(1), 51-59.

[70] Joshi R., Sanderson A. C. (1990) *Multisensor data fusion*. Singapore: World Scientific, 25–42. Wang W., Liu H., Lin W., et al (2020) Investigation on Works and Military Applications of Artificial Intelligence. *IEEE Access*. 8. Flammini F., Setola R., Franceschetti G. (2013). *Effective surveillance for homeland security*. Boca Raton: CRC Press.

[71] Abiyev R. H., Kaynak O. (2008) Fuzzy wavelet neural networks for identification and control of dynamic plants—A novel structure and a comparative study. *IEEE Transactions on Industrial Electronics*, 55(8): 3133–3140.

3.1.2) Situational Awareness (SA)

La consapevolezza della situazione o *Situational Awareness* (SA) è quella percezione, nonché comprensione degli elementi circostanti, tenendo in considerazione tempo, spazio, le intenzioni di altri agenti e l'inferenza della tendenza dello stato da sviluppare[72].

Tale concetto fa riferimento alla capacità di comprendere ed interpretare correttamente la situazione attuale, considerando fattori ambientali, condizioni operative e informazioni rilevante ed è cruciale in un contesto complesso e ad alta intensità di informazioni come il campo militare.

Nel contesto della BDAA, il SA basa la sua analisi su diverse sorgenti come sensori, dispositivi di *Internet of Things*, social media e altro per avere una diapositiva completa e in tempo reale dello scenario, potendo poi identificare *pattern*, anomalie, rilevazione di eventi critici, previsione di situazioni future e rischi potenziali e relazioni tra i dati[73].

3.1.3) Decision Support System (DSS)

Il sistema di supporto alle decisioni (*Decision Support System*, DSS) usa diversi modelli quantitativi per risolvere problemi decisionali sia semi-strutturati che non strutturati[74], adoperando l'impulso fornito dai decisori, il dialogo tra uomo e computer e processando i dati è in grado di supportare le parti strutturate e chiare del processo decisionale.

Nel processo di realizzazione delle attività, laddove l'ambiente risulti cambiare repentinamente, gli oggetti ed i problemi del processo decisionale diventano più incerti e molto confusi.

In tal caso, laddove vi siano problemi decisionali complessi da affrontare attraverso il ragionamento logico, si può sfruttare il DSS Intelligente (IDSS), che risulta essere una combinazione tecnologica tra IA e DSS, aggiungendo un motore di inferenza e una base di regole al sistema, che dota il DSS di facoltà quali la conoscenza descrittiva dei problemi decisionali, la conoscenza dei processi nel processo decisionale, la conoscenza del ragionamento necessaria per risolvere i problemi e un sistema decisionale ausiliario[75].

---

[72] Endsley M. R., Praphrcul G. (1999) op. cit. *Brit. J. Occupational Therapy*, 5(62), 131–135.

[73] Chen H., Chiang R. H., Storey V. C. (2012) Business intelligence and analytics: From big data to big impact. *MIS quarterly*, 36(4): 1165-1188

[74] Angehrn A. A., Dutta S. (1998) Case-based decision support, *Communications of the ACM*, 41(5), 157–165.

[75] Il concetto di IDSS è stato proposto per la prima volta da Bonczek et al. nel 1980. Bonczek R. H., Holsapple C. W., Whinston A. B. (1980) The evolving roles of models in decision support systems, *Decision Sciences*, 11(2), 337–356.

3.1.4) Pianificazione del percorso

La Pianificazione di un percorso è adoperato per aiutare l'utente a scegliere il percorso appropriato, secondo i suggerimenti forniti da un IDSS tattico, che aiuti ad aggirare ostacoli o minacce[76].

A tal fine, la capacità di Pianificazione del percorso deve dotarsi di una capacità di rispondere rapidamente e ragionevolmente, per raggiungere gli obiettivi prefissati con un percorso ottimizzato. La ricerca comune sulla Pianificazione del percorso include la pianificazione basata su V graph[77], su algoritmi genetici[78], la pianificazione dinamica e la pianificazione basata su algoritmi A∗.

[76] Yao M., Zhao M. (2015) Unmanned aerial vehicle dynamic path planning in an uncertain environment. *Robotica* 33(3) 611–621.

[77] Harel J., Koch C., Perona P. (2007) Graph-based visual saliency. *Advances in Neural Information Processing Systems* 19, 545.

[78] Wang Y., Chen Z. (1999) Genetic algorithm (GA) based flight path planning with constraints, Beijing University of Aeronautics and Astronautics 25(3), 355–358, 1999.

4. Benefici e rischi connessi all'utilizzo dell'IA nel processare dati della difesa

4.1 I benefici dell'impiego di IA

L'utilizzo di strumenti adoperanti l'IA nel settore militare comporterebbe di certo numerosi benefici in relazione all'analisi dei *Big Data*, che analizzeremo in questa sezione dell'elaborato, anche sulla scorta dell'analisi già condotta nel precedente capitolo, a riguardo del funzionamento di tali sistemi.

Anzitutto, il beneficio principale derivante dall'impiego di sistemi adoperanti IA riguarda i documenti o i dati di dimensioni considerevoli, che avrebbero difficoltà ad essere memorizzati nella memoria di un computer e che, con difficoltà, potrebbero essere gestiti da un singolo computer dato che sono generati molto rapidamente. In tal caso, le macchine e l'IA hanno un funzionamento molto performante laddove vi siano numerosi dati resi disponibili: l'enorme volume di informazioni raccolte da vari sensori è più di quanto un essere umano o un team di esseri umani possa analizzare[79]. Con tutti i dati generati, c'è una chiara necessità e motivazione per l'automazione nel processo di analisi di tali dati, al fine di trarne le informazioni rilevanti.

Inoltre, e non meno importante, vi è la fase di raccolta dei dati da parte dei sistemi adoperanti IA, che riescono ad effettuare uno *screening* molto rapido di dati, principalmente da sorgenti aperte (o *Open Sources*, OS) e a classificare secondo una data tassonomia, taggare e processare gli stessi, fornendo poi all'utente una risposta. In particolare, per analizzare e creare contenuti, i sistemi più comuni utilizzano una rete neurale di tipo *Transformer* che è in grado di processare e comprendere i dati in maniera più efficiente rispetto ai metodi preesistenti[80].

L'analisi dei dati raccolti, attraverso l'utilizzo dell'IA, potrebbe fornire all'utente l'analisi prescrittiva di cui abbiamo già parlato, consentendo di raccomandare opzioni ai responsabili delle decisioni più rapidamente, fornendo numerose opzioni superiori tra cui scegliere e, in generale, potendo informare anche futuri acquisti, la pianificazione e la pianificazione strategica.

Peraltro, generalmente, salvo nei casi che vedremo nel prossimo paragrafo, l'IA può garantire una maggiore accuratezza e precisione nel processare i dati rispetto all'uomo. Ciò

---

[79] Levine S., Pastor P., Krizhevsky A., Quillen D. (2017) Learning Hand-Eye Coordination for Robotic Grasping with Deep Learning and Large-Scale Data Collection. *International Journal of Robotics Research*, 37(4–5): 421–436.

[80] Tra I sistemi più diffusi di IA, vi è il noto ChatGPT. Il suo processo di addestramento utilizza una tecnologia di apprendimento automatico nota come apprendimento profondo (*deep learning*), in cui una rete neurale viene alimentata con grandi quantità di dati e si "allena" a riconoscere e generare il linguaggio.

deriva da talune proprietà intrinseche, proprie di tali sistemi, come, ad esempio, l'uniformità tra i sistemi e del tempo, che non risentono di fattori esterni o da condizionamenti.

Inoltre, un aspetto rilevante dell'IA, di cui non possiamo occuparci nel dettaglio data la poca attinenza all'indagine condotta, riguarda la *cybersicurezza*: ad oggi, si sta diffondendo la prassi di osservare i *dataset* di comportamento dei *malware* per creare una IA *ad hoc* in grado di osservare il *software* su un sistema e contrassegnare le azioni definite sospette[81]. Come illustrato dalla *Cyber Grand Challenge* della DARPA, c'è anche un crescente interesse per il potenziale delle macchine in grado di trovare e correggere le vulnerabilità nei sistemi amici o trovare e attaccare le vulnerabilità nei sistemi nemici, ma queste applicazioni non sono ancora in grado di eseguire questi compiti a livello di esseri umani esperti[82].

In maniera più trasversale, poi, senza uno specifico *focus* sulla trattazione dei dati, è chiaro che sistemi impieganti IA possano sopperire alla mancanza di personale disponibile nelle Forze Armate, potendo agevolmente occuparsi di compiti – non senza supervisione e posteriore controllo umano – quali analisi dei testi, traduzioni e realizzazione di presentazioni.

In generale, dunque, l'IA ha dimostrato la capacità di migliorare o ottimizzare processi di molti tipi diversi, il che, a sua volta, porta a riduzioni dei costi.

4.2 I rischi connessi all'utilizzo dell'IA

Come abbiamo analizzato, l'IA potrebbe avere un impatto potenzialmente dirompente e trasformativo, per cui risulta necessario analizzare i rischi connessi e le conseguenze negative.

Difatti, risulta necessario garantire un uso etico, trasparente e responsabile dell'IA, che ha portato alla creazione della metodologia dell'intelligenza artificiale responsabile (*Responsible Artificial Intelligence*, RAI): gli approcci AI non devono solo essere ben performanti, ma anche affidabili, trasparenti, interpretabili e spiegabili[83].

---

81 Storicamente, uno dei modi in cui i sistemi antivirus hanno identificato il *malware* è stato quello di controllare i tag statici rivelatori, immagini invisibili fisse che indicano 19 il codice è illegittimo. Gérard W., Alexandre D. (2009) Torinji: Automated Exploitation Malware Targeting Tor Users. Radu State University of Luxembourg. Tuttavia, non è più sufficiente utilizzare semplicemente tag statici per identificare il *malware*, perché gli aggressori hanno scoperto modi per generare *malware* con meno di questi tag.

82 La DARPA Cyber Grand Challenge 2016 è stata una competizione per creare sistemi difensivi automatici in grado di ragionare sulle falle, formulare patch e distribuirle su una rete in tempo reale. Vedi Coldeway D. (2016) "Carnegie Mellon's Mayhem AI Takes Home $2 Million from DARPA's Cyber Grand Challenge," TechCrunch Conference, August 5, 2016.

83 Holzinger A., Biemann C., Pattichis C.S., Kell D.B. (2017) What do we need to build explainable AI systems for the medical domain?. *Computer Science*. Dignum V. (2017) Responsible Artificial Intelligence: Designing AI for human values.
ITU Journal 1.

4.2.1 I rischi connessi all'approvvigionamento di dati: qualità ed autenticità

I sistemi applicanti IA stanno ottenendo risultati con *output* dalla elevata affidabilità e correttezza, purtuttavia, una delle maggiori preoccupazioni riguarda la cosiddetta opacità di funzionamento dei sistemi algoritmici.

Difatti, se da un canto sarebbe astrattamente possibile conoscere i dati di addestramento e gli *output* della macchina, d'altro canto, risulta più complesso comprendere la *ratio* che sottende la decisione presa nel singolo caso concreto. Ciò è dovuto alla complessità del sistema, caratterizzato da una elevata mole di interazioni tra i nodi che compongono i livelli intermedi e "nascosti" in queste reti. Ne discende, dunque, come sia difficile risalire a quale delle possibili variabili, in una fitta rete di connessioni e interazioni, abbia avuto un peso prevalente nella determinazione della scelta della macchina[84].

Questa caratteristica è conosciuta con il nome di "*black box*", ossia scatola nera, proprio in virtù dell'opacità del funzionamento e della sua complessità[85].

Pertanto, uno dei principali rischi connessi all'utilizzo dei sistemi adoperanti IA risiede nella qualità dei dati che sono raccolti: la criticità sta nel verificare che, a discapito del volume e dell'eterogeneità di tali dati, essi siano esatti, precisi ed autentici.

Ciò risulta tanto più vero se si considera che i dati raccolti vengono poi adoperati dal sistema per impostare il funzionamento degli algoritmi combinazione e ricerca di ricorrenze statistiche, su cui, a sua volta, si fondano gli *output* del sistema: anche le modalità di analisi probabilistiche usate per trarre nuovi dati da quelli raccolti originariamente devono essere affidabili[86].

A tal riguardo, si fa riferimento al principio cosiddetto di esattezza dei dati, così come definito dal GDPR[87] volto a evitare qualsiasi distorsione nella rappresentazione dei dati, necessario per rendere effettivo il diritto all'autodeterminazione informativa.

Il principio, dunque, si attesta come fondamentale in quanto legato alla necessità di affidabilità dei dati, ma anche della modalità di raccolta e analisi degli stessi.

Le applicazioni *data driven*, infatti, sono in grado di identificare collegamenti, estrarre *trend* e mettere in luce ricorrenze statistiche e tuttavia, la qualità di tali operazioni segue ed

---

84 Peluso M. G. (2022) op. cit. *Rivista diritto dei media - Medialaws*, 2.

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

86 Pizzetti F. (2016) *Privacy e il diritto europeo alla protezione dei dati personali*, *Dalla direttiva 95/46 al nuovo Regolamento europeo*. Torino:Giappichelli 260-261. L'Autore richiama inoltre la necessità che il concetto di esattezza venga parametrato anche alla dimensione "tempo", ciò in quanto la realtà è in continua evoluzione, comportando così l'inevitabile "invecchiamento" dei dati e la loro perdita di esattezza, intesa come "corrispondenza alla porzione di realtà".

87 «[I dati personali devono essere, ndr] esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati», art. 5, lett. *d*), GDPR.

è fortemente condizionata dalla qualità e bontà dei dati processati, che, laddove siano alterati o falsati, condurrebbero a risultati di uguale siffatta natura.

Inoltre, è altrettanto importante che i dati ed i processi di analisi di essi, compiuti da sistemi adoperanti IA, siano tracciabili ed interpretabili correttamente[88]. Per questa ragione, si rende necessario l'utilizzo di una IA che fornisca dettagli, ragioni sottese, che renda il suo funzionamento chiaro e facile da capire: a tal proposito si parla di XAI (*eXplainable Artificial Intelligence*)[89].

La XAI mira a colmare il divario tra complessità del modello da spiegare e abilità cognitive degli utenti, soprattutto nei sistemi di ML, mirando a fornire una utile spiegazione della loro logica, delineando i punti di forza e debolezza e trasmettendo una comprensione dei comportamenti futuri[90].

La RAI estende poi ulteriormente la XAI, assicurando che aspetti critici della modellazione siano considerati se si implementano sistemi basati sull'IA nella pratica. Ciò non attiene solo alle proposte di algoritmi, ma anche nuove procedure che garantiscano la responsabilità nell'applicazione e nell'utilizzo di modelli di IA, come strumenti per la responsabilità e la *governance* dei dati, metodi per spiegare l'impatto delle decisioni prese o tecniche per rilevare e mitigare l'effetto della distorsione sull'*output*[91].

Per poter attenuare gli effetti negativi derivanti dalla cattiva qualità dei dati, si renderebbe necessaria una verifica alla fonte, effettuata dai programmatori o dai *Data Scientists*, volta ad assicurare la bontà dei dati raccolti[92].

In particolare, il GDPR prevede un obbligo, da parte del titolare, di verificare esattezza e aggiornamento dei dati rispetto alle finalità per le quali gli stessi saranno trattati[93], secondo un onere di "fedeltà contenutistica"[94]. Non solo, anche la proposta di regolamento "Data Act" emanata dalla Commissione il 23 febbraio 2022 fa espresso riferimento alla qualità dei dati

---

88 Zhu J., Liapis A., Risi S., Bidarra R., Youngblood G., (2018) "Explainable ai for designers–A human-centered perspective on mixed- initiative co-creation" in IEEE Conference on Computational Intelligence and Games (CIG), p. 1-8.

89 Barredo Arrieta A., Díaz-Rodríguez N., Del Ser J. et al. (2020) Explainable Artificial Intelligence (xai)–Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58:82-115

90 Turek M. (2016). Explainable Artificial Intelligence (XAI). *Defence Advanced Research Project Agency* 16(53).

91 Barredo Arrieta A., Díaz-Rodríguez N., Del Ser J. et al. (2020) op. cit. *Information Fusion*, 58:82-115

92 Moretti A. (2018) Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679. *Diritto dell'informazione e dell'informatica*, 4-5, 815 ss.

93 Il titolare è chiamato a comunicare a tutti coloro a cui egli abbia trasmesso i dati le eventuali rettifiche, cancellazioni o richieste di limitazione di trattamento. È tuttavia previsto un limite a questo obbligo, che altrimenti avrebbe potuto comportare un eccessivo aggravio degli oneri del titolare, prevedendo che questo non sussista nel caso in cui si riveli impossibile, a fronte della natura del trattamento, o implichi uno sforzo sproporzionato. Si v. art. 34, par. 3, GDPR.

94 Dell'Utri M. (2019) Principi generali e condizioni di liceità del trattamento dei dati personali. In Cuffaro V., D'Orazio R., Ricciuto V., a cura di, *I dati personali nel diritto europeo*, Torino: Giappichelli, 210. Sul punto Di Resta, facendo uno specifico richiamo all'ambito giornalistico, parla di introduzione di uno "standard di diligenza" che verrebbe così a gravare sul titolare del trattamento nella gestione dei dati raccolti. La DARPA Cyber Grand Challenge 2016 è stata una competizione per creare sistemi difensivi automatici in grado di ragionare sulle falle, formulare patch e distribuirle su una rete in tempo reale. Vedi Di Resta F. (2018) *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Torino: Giappichelli, 46 citato da Peluso M. G. (2022). op. cit. *Medialaws – Rivista di diritto dei media*, 2.

quale requisito in grado di incrementare la competitività e l'innovazione, assicurando al contempo una crescita sostenibile[95].

Concetti di tal fatta, come correttezza e adeguatezza, devono essere utilmente parametrati agli scopi perseguiti e con una verifica della loro utilità e correttezza: i dati dovrebbero rispondere agli scopi del trattamento in modo adeguato ed utile, ponendo attenzione sulla loro attualità e l'aggiornamento, la loro non contraddittorietà e, infine, la completezza, cioè la presenza di un numero di attributi sufficiente a rappresentare correttamente il fenomeno analizzato[96].

Pertanto, considerata l'elevatissima quantità di dati che i sistemi di IA e ML devono processare, grazie alle tecniche di *data mining*, che consentono di estrarre informazioni da un numero indefinito e imprecisato di fonti, la priorità posta in luce dal GDPR sembra, piuttosto, guardare alla qualità dei dati, richiedendo che si presti una concreta attenzione alla bontà del dato.

Dunque, i sistemi adoperanti IA dovrebbero comunque essere combinati con il ragionamento, la conoscenza, e l'expertise umana, chiamati ad operare un controllo preventivo ed ulteriore, per evitare che i *dataset* siano compromessi.

Un altro rischio, connesso all'utilizzo dell'IA, è la c.d. "*hallucination*"[97], ossia la formulazione di una risposta, da parte del sistema, che non appare corroborata o giustificata dai dati e dai riferimenti addotti i quali, talvolta, sono inventati. In sostanza, talvolta, il sistema estrae contenuti da articoli scientifici che non sono rintracciabili poiché mai pubblicati[98].

I sistemi, difatti, sono organizzati per fornire all'utente dei risultati che siano "verosimili", ma non necessariamente veri o veritieri.

Anche a tal proposito, è necessaria una supervisione umana*a posteriori*, che garantisca la qualità e l'accuratezza dei dati estratti e forniti e che verifichi che non vi siano stati errori di comprensione del senso del testo o del contesto in cui lo stesso è stato pubblicato.

In conclusione, una maggiore qualità dei dati, maggiore trasparenza del funzionamento, tracciabilità dei processi favorirebbe non solamente un miglior governo

---

95 Si rimanda al testo della Commissione, *Proposal for a Regulation of the European parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, 23.2.2022, COM(2022) 68 final

96 Pizzetti F. (2018) *Intelligenza Artificiale, protezione dei dati personali e regolazione.* Torino: Giappichelli, 44-60-61; Resta F. (2018), *Sub* art. 5. In: Riccio G.M, Scorza G., Belisario E., a cura di, *Commentario GDPR e normativa privacy*, Milano: Wolters Kluwers, 58-59.

97 Alkaissi H., McFarlane S.I. (2023) Artificial Hallucinations in ChatGPT: Implications in Scientific Writing. *Cureus* 19, 15(2).

98 L'esempio più comune e lampante è ChatGPT, su cui vi sono numerosi articoli che hanno denunciato la cosiddetta "AI Hallucination". Castelvecchi D. (2022) Are ChatGPT and AlphaCode going to replace programmers? *Nature*, Stokel-Walker C. (2022) AI bot ChatGPT writes smart essays – should professors worry? *Nature*, Stokel-Walker C (2023) ChatGPT listed as author on research papers: many scientists disapprove. *Nature*. 613(7945):620-621, Gordijn B. (2023) Have HT. ChatGPT: evolution or revolution? *Medical Health Care Philosophy*.

dei *Big Data*, ma anche il miglioramento dei processi che causano dati errati e conseguenti analisi distorte.

4.2.2 I rischi connessi al trattamento di dati: sicurezza e privacy

Un ulteriore rischio intrinseco che l'IA nasconde riguarda il modo in cui i dati vengono processati nella fase immediatamente successiva a quella di raccolta.

Difatti, i dati, durante la fase di analisi da parte di sistemi impieganti IA, potrebbero essere non solo integrati ed affiancati da altri dati non affidabili, ma anche essere diffusi in rete, minando non solo la sicurezza ma anche la privacy.

Proprio per questo, è auspicabile l'utilizzo di mezzi adoperanti IA che però siano esplicabili (XAI) e responsabili (RAI), di modo da consentire all'utente di avere possibilità, su richiesta, di comprendere e ripercorrere il processo decisionale del sistema per raggiungere risultati responsabili, trasparenti e tracciabili.

A tal proposito, al fine di sovvertire tali rischi incombenti sul modo di processare i dati, sono stati introdotti *privacy* e sicurezza *by design*, ossia sin dalla progettazione.

Per quanto riguarda il primo, la privacy e la protezione dei dati dovrebbero essere considerati in ogni fase del processo decisionale, e, in particolar modo dalla progettazione.

Tuttavia, la *privacy by design* (PbD), *framework* per incorporare proattivamente la *privacy* direttamente nella tecnologia dell'informazione, nelle pratiche commerciali, nella progettazione fisica e nelle infrastrutture di rete, rendendola l'impostazione predefinita, è stato per primo introdotto nel 1990, laddove la complessità e interconnessione delle tecnologie dell'informazione risultava sempre crescente[99].

L'UE ha integrato la direttiva sulla protezione dei dati nelle norme del regolamento generale sulla protezione dei dati (GDPR): i titolari e i responsabili del trattamento sono tenuti ad attuare "la protezione dei dati fin dalla progettazione e per impostazione predefinita"[100].

L'obiettivo principale del requisito consiste nel fornire «le garanzie necessarie per il trattamento al fine di soddisfare i requisiti del suo regolamento e proteggere i diritti degli interessati». Per fare ciò, i titolari o i responsabili del trattamento devono attuare una serie di procedimenti che, in base alle capacità dell'organizzazione e allo stato dell'arte, saranno

---

[99] Cavoukian A. (2012). Privacy by design origin and evolution. *IEEE Explore*.

[100] European Parliament, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation). In particolare, art. 25. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

in grado di correlare la natura del trattamento (finalità, tipo di dati, ecc.) con i rischi inerenti ad esso e progettare adeguate condizioni di conformità normativa.

Inoltre, il GDPR ha anche applicato un nuovo principio di *privacy by default*, "protezione dei dati per impostazione predefinita", che prevede il principio di minimizzazione dei dati. Ciò che il legislatore prevede è determinare il volume, la natura e la qualità dei dati richiesti per una particolare attività di trattamento.

Privacy by design e *by default* tengono conto della *privacy* e della protezione dei dati nell'intero processo di sviluppo dall'inizio del suo sviluppo e durante l'intero ciclo di vita a tutti i tipi di informazioni sensibili come le informazioni sanitarie[101].

Un altro rischio sotteso all'utilizzo di strumenti di IA è il "*leakage risk*", ossia la possibilità che i dati inseriti nel sistema di IA vengano divulgate, che vengano condivise con terze parti[102] o che siano usate dal sistema come base per fornire risposte su *queries* simili.

Difatti, taluni autori hanno rilevato come una modifica ai dati di addestramento del sistema, prima che vengano elaborati, possa causare la memorizzazione e potenzialmente la perdita dell'informazione da parte del modello di apprendimento automatico[103].

Per quanto concerne la sicurezza *by design*, valga considerare che, generalmente, si tenta di trovare soluzioni che consentano ai sistemi informativi di contenere le informazioni processate in un certo perimetro, protetto da minacce provenienti dal mondo esterno[104].

Il concetto di protezione delle informazioni si basa sulla nozione di contenimento, creazione di confini fisici attorno al bene che necessita protezione[105] e richiede che la percezione del rischio prenda in considerazione ed analizzi un contesto più ampio[106].

---

[101] Iachello G., Hong J. (2007) End-user privacy in human-computer interaction Found. *Foundations and Trends® in Human–Computer Interaction*, 1:1-137, Dang L., Piran M., Moon D.H.K.M.H. (2019) A survey on internet of things and cloud computing for healthcare. *Electronics*, 7:768, Semantha F.H., Azam S., Yeo K.C., Shanmugam B. (2020) A systematic literature review on privacy by design in the healthcare sector. *Electronics,* 3:452.

[102] Considerato che alcuni sistemi di IA sono integrati in una varietà di plug-in di terze parti, i rischi relativi ai dati trapelati sono alti.

[103] Song C., Ristenpart T., Shmatikov V. (2017) "Machine Learning Models that Remember Too Much" Conference CS '17, Dallas, TX, USA.

[104] Van Deursen N., Buchanan W.J., Duff A. (2013) Monitoring information security risks within health care, *Computer Security*, 37:31-45

[105] Van den Hoven J., Blaauw M., Pieters W., Warnier M., (2020) Privacy and information technology. In: E.N. Zalta, a cura di, *The Stanford Encyclopedia of Philosophy, Metaphysics Research Lab*, Stanford:Stanford University.

[106] Gerber M., von Solms R. (2005) Management of risk in the information age. *Computer Security*, 24:16-30, Dourish P., Anderson K., Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human Computer Interaction* 319-342. Dhillon G., Backhouse J. (2001) Current directions in is security research– Towards socio-organizational perspectives. *Information System Journal*, 11:127-153

5. Il caso militare italiano: stato dell'arte e possibili applicazioni di nuove tecnologie per analizzare i Big Data

L'obiettivo principale della presente indagine, come più volte rimarcato, attiene a fornire una analisi della impiegabilità di sistemi di IA al controllo operativo di risorse finanziarie assegnate alle Forze Armate italiane.

A tal proposito, lo scenario corrente risulta non particolarmente all'avanguardia in termini di utilizzo delle nuove tecnologie a disposizione come, *inter alia*, quelle più volte citate, che sfruttano sistemi di IA e ML.

Nella situazione odierna, le forze armate ed i ministeri sono chiamati a processare e memorizzare una quantità di dati particolarmente corposi, come ad esempio quelli attenenti agli storici di contratti di acquisizione di beni e servizi, come possono essere risorse comuni quali carburanti, bollette, investimenti.

Peraltro, l'ambito finanziario prima atteneva unicamente alla rendicontazione degli stipendi, laddove dal 2016 in poi, si sono aggiunte numerose voci di bilancio e spesa addizionali, da quando il *benchmark* di spesa superiore al 2% è stato richiesto dalla NATO[107], che si è riflesso in una maggiore pletora di investimenti di cui tenere traccia.

Idealmente, attraverso le nuove tecnologie, si dovrebbe, dopo aver condotto appropriate e necessarie analisi, agevolmente raggiungere un *output* che delinei quali sistemi, estratti dallo storico, sono stati acquistati, in che numero e che funzione essi svolgono nonché che sia in grado di confrontare tali dati ed estrarne *trend* e *pattern*.

Difatti, laddove i dati afferenti alle spese venissero analiticamente listati, confrontati ed analizzati, ciò condurrebbe anche ad una più elevata efficienza della spesa stessa, che sarebbe più informata e rivolta ad uno scopo più preciso ed individuato.

In tal caso, si potrebbe confrontare se talune scelte di investimenti e voci di spesa in una determinata capacità o sviluppo di essa possano essere invece allocati e destinati ad altro impiego.

---

[107] Al vertice del Galles del 2014, in risposta all'annessione illegale della Crimea da parte della Russia e alle turbolenze in Medio Oriente, i leader della NATO hanno deciso di invertire la tendenza al calo dei bilanci della difesa.
Gli alleati che attualmente rispettano la linea guida del 2% per la spesa per la difesa continueranno a farlo, gli alleati la cui attuale percentuale di PIL speso per la difesa è inferiore a questo livello: arresteranno qualsiasi declino, punteranno ad aumentare la spesa per la difesa in termini reali con la crescita del PIL e ad avvicinarsi alla linea guida del 2% entro un decennio con l'obiettivo di raggiungere i loro obiettivi di capacità della NATO e colmare le carenze di capacità della NATO.
Sebbene la linea guida del 2% del PIL da sola non garantisca che il denaro venga speso nel modo più efficace ed efficiente per acquisire e dispiegare capacità moderne, rimane un importante indicatore della volontà politica dei singoli alleati di destinare alla difesa un livello di risorse relativamente ridotto ma comunque significativo. Nel 2014, tre alleati hanno speso il 2% o più del PIL per la difesa; nel 2022 la cifra salirà a sette alleati. Inoltre, il 2022 è stato l'ottavo anno consecutivo di aumento della spesa per la difesa tra gli alleati europei e il Canada, con un incremento del 2,2% in termini reali rispetto al 2021. Si veda NATO - Topic: Funding NATO

Al momento in cui si scrive ed alla luce dell'intervista con il Generale in annesso, i dati di cui sopra parrebbero venire raccolti ed inseriti in taluni documenti, con limitate possibilità di automatizzare i processi di addizione, confronto e estrazione di *trend*, in quanto rimesse principalmente all'intervento manuale dei dipendenti.

Nell'ambito di questo capitolo, continueremo ad esplorare quali possano essere le modalità di fronteggiare tale necessità di rendere il processo decisionale più efficace in un ambiente dinamico come quello della difesa.

Invero, analizzeremo quali siano i profili di impiegabilità di sistemi adoperanti IA e ML al fine di automatizzare tali processi, rendendoli più rapidi, precisi, efficaci ed efficienti, valorizzando i dati storici di gestione, e se, a fronte di tali necessità possano essere sufficienti *tool* diversi che, seppur performanti, non adoperino l'IA.

In tale scenario, poi, confronteremo come tali sistemi possano raccogliere i dati, effettuare le operazioni di analisi avanzate degli stessi, senza compromettere sicurezza e confidenzialità degli stessi.

5.1 Impiegabilità dei sistemi adoperanti IA

Come emerge dalle *interviews* tenute con gli esperti, implementare sistemi adoperanti IA nello scenario attuale, potrebbe di certo comportare dei benefici notevoli, come, a mero titolo di esempio, il supporto alle decisioni nell'ambito della gestione finanziaria, che risulti informata a rigore logico, efficienza e completezza dei dati.

Difatti, adoperare un sistema con IA consentirebbe agevolmente di effettuare uno *screening* delle risorse aperte per verificare anche le scelte di gestione finanziaria di altri scenari nazionali ed internazionali, comparando le scelte più opportune e proficue e influenzando la scelta nazionale.

Inoltre, tali strumenti consentirebbero una lettura agevole della grande mole di dati inserita manualmente e permetterebbero l'estrazione di *trend*, la raccolta di dati storici di gestione e potrebbero condurre simulazione sulla *performance* dell'organizzazione.

Tuttavia, come rilevato nel precedente capitolo, l'applicazione di tecnologie quali l'IA appare come un Giano bifronte, la cui altra faccia della medaglia è l'opacità di funzionamento, la poca tracciabilità dei sistemi algoritmici che sottendono il processo decisionale e, talvolta, la bassa qualità dei dati raccolti *a capite* da fonti aperte, che potrebbe generare informazioni a loro volta poco affidabili.

Inoltre, laddove non si accerti un utilizzo di IA esplicabile ed anche responsabile, i sistemi hanno dei *glitchs* o malfunzionamenti, che portano risultati viziati, in quanto la finalità ultima dei sistemi è quella di fornire risultati all'utente, talvolta compromettendo la qualità

degli stessi: non sono pochi i casi di "*hallucinations*" dei sistemi di IA, che corroborano le proprie tesi con fonti inesistenti o travisate.

Peraltro, vale la pena notare come anche laddove si accerti la genuinità dei dati inseriti, essi potrebbero essere processati, se non si adottano delle fondamentali precauzioni[108], senza aver rispetto di sicurezza informatica e trattamento dei dati, comportando dei *leakage* di tali informazioni che potrebbero essere confidenziali ovvero segrete.

Ciò detto, si è indagata la possibilità di estrarre dati, *trend* ed avere suggerimenti sui dati inseriti adoperando dei *tool* già esistenti non necessariamente adoperanti l'IA, per soddisfare le richieste delle Forze Armate, come ad esempio taluni già implementati nel settore civile ed attualmente in uso in molte società[109].

Difatti, come già analizzato, al fine di soddisfare le attuali richieste delle Forze Armate, sarebbe sufficiente uno strumento in grado di fornire un'analisi descrittiva, che attraverso le KPI (*Key Performance Indicator*) consenta di analizzare e comparare dati storici e attuali per estrarne delle tendenze ed un'analisi predittiva, che possa prevedere i mutamenti futuri ed informare i futuri investimenti sulla base dei dati attuali.

Non risulta, invece, a nostro parere, indispensabile condurre anche un'analisi prescrittiva, ovverosia in grado di formulare una vera e propria prescrizione basata sulla capacità tecnica di formulare le giuste domande e proporre le scelte migliori. Solo in tal caso vi sarebbe la necessità dell'intervento dell'IA per interpretare le informazioni raccolte e formulare delle soluzioni per ottimizzare una situazione, determinare la migliore azione da intraprendere e perfezionare il processo decisionale.

---

[108] Tra le principali precauzioni che si consigliano, anche alla luce della intervista con l'esperta di cybersicurezza, vi sono:
- Stabilire una chiara politica di sicurezza dei dati che delinei l'uso appropriato degli strumenti di intelligenza artificiale e la gestione delle informazioni sensibili. Assicurarsi che la politica sia facilmente accessibile e compresa da tutti i dipendenti. Aggiornare regolarmente la politica per tenere il passo con le nuove tecnologie e le minacce emergenti;
- La formazione dei dipendenti sulle best practice per la sicurezza dei dati, sull'importanza della sicurezza dei dati e sui rischi associati alla condivisione di informazioni sensibili attraverso strumenti di intelligenza artificiale;
- l'utilizzo di strumenti di intelligenza artificiale sviluppati pensando alla sicurezza dei dati e assicurati di verificare le loro richieste di sicurezza. Cerca strumenti che crittografano i dati in transito e inattivi e prendi in considerazione strumenti che offrano funzionalità di elaborazione locale per ridurre al minimo il rischio di esposizione dei dati;
- limitare l'accesso ai dati sensibili implementando controlli di accesso basati sui ruoli, garantendo che solo il personale autorizzato possa accedere e condividere informazioni sensibili. Rivedere e aggiornare regolarmente le autorizzazioni di accesso per mantenere un ambiente sicuro;
- stabilire un sistema per il monitoraggio e il controllo dell'uso degli strumenti di intelligenza artificiale all'interno dell'organizzazione. Questo può aiutarti a identificare potenziali perdite di dati e accessi non autorizzati a informazioni sensibili. Controlla regolarmente i log e i report per assicurarti che i dipendenti utilizzino gli strumenti di intelligenza artificiale in conformità con le policy e le best practice di sicurezza dei dati.

[109] Come riferito dall'esperto di IA, vi sono diversi esempi di provider di cloud che di per sé esplorano i dati, li analizzano, li classificano e danno suggerimenti o report sulle azioni da compiere. Inoltre, una terza fase eventuale, comunque presente in taluni tool è quella della modellazione: lo strumento, grazie all'impiego dell'IA applicato alla statistica o, se il problema è meno complesso con forme analitiche, sarebbe in grado di predire in anticipo trend o azioni future. Degli esempi di provider di cloud in grado di sostenere tali operazioni sono come Azure di Microsoft, Amazon Web Services (AWS), Google Cloud Platform (GCP). In tal caso, il cloud provider sarebbe designato di proteggere questi dati, grazie alle loro capacità in tal senso e avrebbe tutto l'interesse a proteggerli, per garantire la sua reputazione.
Tuttavia, laddove si applicasse poi l'IA, il software potrebbe svilupparsi sulla base dei dati inseriti, con la possibilità sottesa che qualcuno che usi la stessa interfaccia e ne entri in possesso.

Tuttavia, anche nel caso di utilizzo di tool di BDAA che non adoperino l'IA, potrebbe potenzialmente esservi un problema di tracciabilità dei dati inseriti manualmente sul loro sistema, che non potrebbero essere più pienamente controllabili, in quanto caricati su di un *cloud* e più vulnerabili, nonostante i server forniscano delle garanzie di sicurezza[110].

Adoperare i *cloud* non solo per memorizzare i dati in uso delle Forze Armate, ma anche per effettuare le analisi descrittive e predittive risulterebbe sicuramente l'opzione più vantaggiosa in termini di fattibilità: si rimetterebbe ad una società di consulenza terza il processo di migrazione dati, messa in sicurezza degli stessi e le analisi su di essi. Tuttavia, sentiamo di escludere sin d'ora questa opzione in quanto consentirebbe di collezionare solo limitatamente dati classificati e sensibili, essendo esposta a rischi – seppur remoti - a livello di sicurezza e, inoltre, richiederebbe la remissione del controllo sulla sicurezza a terzi, ossia sarebbe "*outsourced*".

La traiettoria futura parrebbe muoversi nel senso dei *computing clouds*, che però si declinino e si adattino alle esigenze delle Forze Armate: a mero titolo di esempio, si riporta quanto descritto dall'esperta di cybersicurezza nell'intervista, ossia l'alleanza strategica tra i *cloud providers* Lockeed Martin e Microsoft con il *Departement of Defense* statunitense in alcuni campi critici come innovazioni nel *cloud* classificato, AI/ML e capacità nel campo del *Modeling e Simulation*.

L'accordo prevede che Microsoft, per Lockeed Martin, realizzi un *cloud* secondo lo stesso standard impiegato per realizzare il *cloud* segreto del DoD. In questo modo si dovrebbero velocizzare tutte le procedure di "Compliance" per i progetti classificati, abbreviando i tempi di realizzazione dei programmi militari.

Ciononostante, considerate le esigenze attuali delle Forze Armate italiane, le risorse potenzialmente allocabili e la fattibilità, anche in termini di tempistiche, sarebbe preferibile percorrere altre strade, meno pioneristiche e più salde.

Piuttosto, si analizzerebbero due possibilità alternative: adoperare sistemi impieganti anche l'IA per processare dati non sensibili (dunque, se del caso, declassificando i dati o destinando a tale analisi solo dati non classificati), ovvero, analizzare e processare anche dati classificati ma con sistemi diversi, possibilmente non su *cloud* ma *on premise*. In tal caso, sia i dati inseriti che il *server* sarebbero locali e fisicamente presenti in un dato luogo, non accessibili da *cloud* ma solo tramite il supporto fisico. Ciò, chiaramente, come

[110] Spostando grandi quantità di dati sensibili in un ambiente cloud connesso a Internet, si profilano talune minacce informatiche: *in primis*, gli attacchi *malware*, poi la perdita o *leakage* di dati per cui è consigliabile che la sicurezza di alcuni dei dati critici dell'organizzazione si rimetta a qualcuno al di fuori del reparto IT. Uno dei rischi per la sicurezza più impattanti che il *cloud* deve affrontare è il potenziale di una violazione dei dati. Questi sono il risultato di scarse misure di sicurezza che consentono agli attori malintenzionati di accedere a dati sensibili attraverso i server *cloud*.

confermato anche dall'esperta di cybersicurezza e dall'esperto dell'EDA, consentirebbe di avere una raccolta dati molto più sicura rispetto a quella sul *cloud*, soprattutto se ci si riferisce a dati classificati, i quali possono essere memorizzati su *cloud* solo sino ad un determinato livello di classificazione.

Partendo dal presupposto che l'IA potrebbe adoperarsi, ma non risulta indispensabile per le attuali esigenze delle Forze Armate, si procederebbe, dunque, all'attuale analisi in tal senso: concentrandosi su strumenti performanti ma che non utilizzino l'IA, analizzando, in conclusione, la possibile implementazione di sistemi di IA nel futuro.

A tal proposito, le possibilità possono racchiudersi in due opzioni: creare dei sistemi o piattaforme *ad hoc* per le forze armate italiane, ovvero adoperare strumenti già implementati ed in uso in seno ad altre forze armate, anche a livello sovranazionale.

5.2 L'implementazione di sistemi *ad hoc*

Potrebbe risultare utile creare ed implementare un sistema di analisi dati *in house*, ad uso pieno ed esclusivo delle Forze Armate italiane, che si adatti perfettamente all'attuale richiesta e che garantisca una trattazione sicura dei dati inseriti, anche se classificati.

Formalmente, la creazione ed implementazione di tale sistema protetto consentirebbe di certo di condurre analisi descrittive, predittive e, eventualmente, grazie all'impiego di IA in un ambiente protetto, anche prescrittive.

A tal fine, sarebbe opportuno rivolgersi ad una società di consulenza o a privati che sviluppino e costruiscano un *software* ovvero una piattaforma, grazie all'intervento di *Data Architects*.

Nello specifico, come emerso dalle interviste con gli esperti, sarebbe opportuno convertire i documenti e *files* attualmente in uso delle Forze Armate in file strutturati e farli migrare, grazie ad un *tool*, in un apposito *database*.

Al fine di proteggere i dati, essi, una volta trasferiti sul *database*, subirebbero un processo c.d. di "mascheramento": per le informazioni classificate si implementa una chiave di cifratura al dato corrispondente, che sia in grado, appunto, di mascherare e di occultare l'informazione originaria, rendendola illeggibile all'esterno.

Anche in tal caso, sarebbe preferibile che i dati rimangano *on premise* e non vengano spostati su alcun *cloud*, per le ragioni poc'anzi menzionate.

In tal caso, la sicurezza degli stessi dati verrebbe totalmente rimessa alla società di consulenza, investita non soltanto del processo di migrazione dei dati su un diverso *database*, ma anche di garantire il trattamento dei dati classificati e della loro riservatezza nel corso del tempo.

Tale servizio di sicurezza informatica esternalizzato (c.d. in "*outsourcing*") che doti le Forze Armate di servizi di *cyber security as a service* garantirebbe una maggiore affidabilità e costanza in quanto il servizio di sicurezza sarebbe rimesso a esperti specializzati e certificati, aggiornati e formati e, tuttavia, sarebbe comunque rimesso a terzi.

Dal punto di vista operativo, sarebbe ideale una copertura 24x7x365, che rappresenta una garanzia di monitoraggio continuo della sicurezza sia per allerta preventiva su segnali sospetti ed indizi di pericolo, che per reportistiche sulle minacce.

Al fine di accomodare questa richiesta, considerando l'impatto finanziario che la stessa possa comportare, potrebbe essere utile adoperare i fondi normalmente destinati alla Ricerca e Sviluppo, orientandoli al fine di costituire tale *software*. Infatti, laddove si presenti il problema attuale, descrivendo le caratteristiche e le esigenze delle Forze Armate, esso potrebbe costituire una bozza di progetto da far implementare alla sezione Ricerca e Sviluppo, dal livello di prontezza tecnologica basso[111].

Una volta realizzata una bozza di progetto, esso può essere implementato in diversi progetti e linee di sviluppo.

Questo sistema consentirebbe di garantire la piena protezione dei dati – anche classificati – processati e lo scambio tra tutte le forze armate di essi, grazie ad un ambiente sicuro.

I punti di forza di tale opzione sarebbero di certo la sicurezza dei dati e l'abbattimento dei rischi connessi alla sicurezza, a spese tuttavia del livello di sofisticazione del sistema, che di certo risentirebbe di elaborazioni meno complesse ed all'avanguardia. Peraltro, tale opzione risulta essere anche quella più dispendiosa a livello di tempistiche e risorse, sia economiche che di personale.

Difatti, definiti i criteri e le esigenze, e istituito il *software*, lo stesso dovrebbe essere mantenuto grazie all'intervento di appositi sviluppatori o *developers*, che si occupino della piena manutenzione dello stesso.

Peraltro, vi è una incertezza sulla fattibilità dell'aggiunta, in futuro, di un *software* che utilizzi l'IA in un ambiente sicuro. Invero, in generale, la maggior parte dei *tool* IA forniscono solo l'API (*Application Programming Interfaces*).

---

[111] Il riferimento è al *Technological Readiness Level* (TRL), suddivisi in gamma da 1 (se l'idea è solo iniziale) a 9 (se il progetto è ready to use). Attraverso tale metodologia si identifica il livello di maturità di una determinata tecnologia o processo. Sono basati su una scala di valori da 1 a 9, dove 1 rappresenta la base della scalinata, mentre 9 ne rappresenta l'apice.
Di seguito viene riportata la definizione data dalla Comunità Europea, nel documento "Technology readiness levels (TRL), HORIZON 2020 – WORK PROGRAMME 2018-2020 General Annexes, Extract from Part 19 – Commission Decision C(2017)7124", per ognuno dei 9 livelli identificati, ed un approfondimento su ogni livello.

Per cui, sarebbe anche possibile usare API per connettere il *software* realizzato *ad hoc* per le Forze Armate al *software* che usa l'IA, ma esso avrebbe comunque "sede" al di fuori dell'ambiente protetto.

Si creerebbe una barriera, uno strumento che scherma Internet, lo metta in un ambiente confinato, prenda le informazioni e le copi in un sistema di confine, per poi installare un altro strumento ad esso collegato. Tuttavia, i dati classificati estratti dagli archivi possono essere utilizzati nell'ambiente classificato.

Potenzialmente, come rilevato dall'esperto informatico, nel futuro, si potrebbe dotare tale *software* di una API installata *on premise*, che riuscirebbe a comunicare ed inviare le informazioni all'API connessa con il *software* di IA. In tal caso non vi sarebbe rapporto diretto e reciproco tra API *on premise* e *software* di IA, ma sarebbe mediato dalla seconda API, consentendo alle informazioni necessarie, raccolte dal web, di introdursi nell'ambiente fisico, ma azzerando le possibilità che le informazioni fisiche siano inserite in Internet.

L'alternativa, piuttosto remota, sarebbe chiedere che la compagnia che gestisce il *software* adoperante l'IA lo dispieghi nell'ambiente classificato e fisicamente disconnesso in uso alle Forze Armate, ma in tal caso perderebbero il controllo sul proprio *software*.

Inoltre, risulterebbe dispendioso e particolarmente complesso per le Forze Armate dotarsi di un computing power talmente potente in un ambiente sicuro che consentirebbe l'applicazione di un *software* applicante l'IA.

In conclusione, tale opzione, per quanto consentirebbe di costruire da zero un sistema sicuro ed *ad hoc* che risponda alle esigenze delle Forze Armate, risulta essere complesso da implementare ed anche eccessivamente e inutilmente costoso, potendosi adoperare alternative valide come l'impiego di altri tool già disponibili.

5.3 L'impiego di strumenti già disponibili: l'esempio sovranazionale

L'EDA ha introdotto e gestisce una piattaforma, EUCLID (*European Union Collaboration In Defence*), in grado di catturare i piani, programmi, capacità e contributi diretti degli Stati membri e informazioni sul sistema operativo di questo tipo.

Tale sistema ha, tuttavia, molteplici scopi: non solo raccoglie i piani ed i programmi degli Stati membri, ma è anche adoperato per rendere accessibili a tutti i piani nazionali di attuazione dei singoli Stati membri.

È importante notare che EUCLID è composto da diversi moduli: l'approccio modulare garantisce che gli utenti abbiano accesso solo ai moduli a cui dovrebbero accedere, a meno che ciò non sia ritenuto necessario dalla loro autorità nazionale.

Vi è da precisare che EUCLID usa il supporto di taluni appaltatori, non invece sistemi adoperanti IA: gli Stati membri contribuiscono direttamente o popolano EUCLID da fonti aperte (*Open Sources*, OS) e, i *Project Officers* dell'EDA provvedono, a loro volta, a controllare sistemi operativi come piattaforme di notizie sulla difesa come Military Balance +, Janes Defence, defence24.com e ad estrarre informazioni pertinenti. Questi dati raccolti sono poi introdotti in EUCLID e contrassegnati come OS e gli Stati membri possono confermare le informazioni e assumerne la proprietà.

Inoltre, altre fonti pienamente attendibili da poter utilizzare sono il NATO *Defence Planning Process* (NDPP) e EU *Coordinated Annual Review on Defence* (CARD), entrambe iniziative volte alla raccolta di informazioni sui programmi nazionali di approvvigionamento della difesa, principalmente investimenti nel tempo (programmi di approvvigionamento).

Per ora, la raccolta dei dati viene eseguita manualmente, senza il supporto di IA ma con l'intervento ed il controllo umano. Tuttavia, l'esperto EUCLID non esclude che in futuro con un'interfaccia di programmazione delle applicazioni (API), EUCLID potrebbe utilizzare la moderna AI / ML per, in primo luogo, eseguire la raccolta dei dati e, in secondo luogo, la convalida dei dati (come nell'identificazione dei duplicati, soprattutto se le informazioni raccolte sono contraddittorie). In terzo luogo, AI / ML potrebbe essere utilizzato per il supporto decisionale: si potrebbero confrontare, ad esempio, i prezzi unitari, il costo dei servizi e trovare la corrispondenza più adatta alle esigenze individuali degli Stati membri.

I dati, una volta processati in EUCLID, sono in grado di estrapolare analisi, tendenze e influenzare futuri investimenti sulla base di indicatori standard automatici o personalizzati tramite PowerBI. A tal fine interviene anche l'*Aggregated Analysis* della CARD, che identifica le principali tendenze in ciascun settore operativo e informa su dove dovrebbero essere effettuati gli investimenti, sulla base delle opportunità di collaborazione precedentemente identificate proposte e confermate dagli Stati membri.

EUCLID è già un'applicazione piuttosto complessa, che consente molte funzioni e casi d'uso e garantisce sicurezza adoperando i più recenti protocolli di sicurezza in Internet. Tuttavia, l'esperto conviene che lo spostamento dell'applicazione in un ambiente classificato ne aumenterebbe ulteriormente la sicurezza, posto che la maggior parte degli Stati membri classifica i propri programmi di difesa, ciò consentirebbe una maggiore raccolta e sfruttamento dei dati.

Ad ogni modo, viene garantito che i dati non siano accessibili a persone non autorizzate anzitutto attraverso un approccio modulare: solo se ad una persona venisse concesso l'accesso al rispettivo modulo, dietro previa autorizzazione di un rappresentante governativo dello Stato membro, vedrebbe i rispettivi dati.

In secondo luogo, attraverso la proprietà dei dati: lo Stato membro proprietario dei dati può limitarne l'uso anche ai singoli Stati membri. Ad esempio, l'esperto ci comunica che un amministratore italiano sarebbe in grado di limitare l'accesso alle singole voci del *database* solo agli utenti italiani, se lo ritiene opportuno.

Ciò detto, una possibilità sarebbe che gli Stati Membri adoperino EUCLID anche per uso nazionale, procedendo a popolare il sistema con i propri dati, non solo per condividere gli stessi con l'EDA o gli altri Stati membri, ma per averne un record proprio, di tal guisa pienamente sfruttando il sistema.

Difatti, EUCLID è a disposizione degli Stati membri che potrebbero beneficiare della sicurezza dei dati, garantita dal sistema e la supervisione da parte dei *Project Officers* dell'EDA. Inoltre, EUCLID appare un tool che, seppur non adoperante l'IA, offre una *perfomance* di analisi dati ed estrazione *trend* in linea con quanto attualmente necessario alle Forze Armate italiane.

Peraltro, laddove i dati in dotazione alle Forze Armate siano classificati, gli operatori preposti o i rappresentanti degli Stati membri potrebbero copiare EUCLID nell'ambiente classificato, ottenendone una versione *stand-alone* in un ambiente sicuro e con un *database* centrale. Secondo l'esperto, infine, EUCLID è talmente versatile da non deve necessariamente essere adoperato *in toto*, rappresentando piuttosto un *blue-print* per le esigenze degli Stati membri: il suo utilizzo può essere declinato in base a tali necessità, sfruttando solo taluni moduli, inserendo più dati, anche classificati, impostando l'accesso dei soli utenti nazionali e gli amministratori EDA a tali dati.

6. Conclusioni

Come abbiamo analizzato a più riprese, i sistemi e le soluzioni basate sull'IA si stanno moltiplicando, fornendo una chiara ottimizzazione di servizi offerti nel campo tecnologico da altri sistemi, consentendo ai sistemi di apprendere e monitorare dati e attività, sino a supportare e informare concretamente il processo decisionale.

Profondi cambiamenti tecnologici hanno avuto luogo negli ultimi due decenni, supportati da progressi dirompenti sia sul lato *software* che su quello *hardware*. La caratteristica dominante dei cambiamenti è l'integrazione del mondo virtuale con il mondo fisico attraverso l'*Internet of Things* (IoT). Lo sviluppo più recente è il radicale cambiamento di paradigma dalle "cose connesse" all'"intelligenza connessa".

L'analisi condotta nel corso di questa indagine ha messo in luce diverse considerazioni chiave riguardo all'impiegabilità di sistemi di intelligenza artificiale (IA) nel contesto del controllo operativo delle risorse finanziarie assegnate alle Forze Armate italiane.

La situazione attuale ha rivelato una mancanza di avanzamento nell'utilizzo delle nuove tecnologie, comprese quelle basate su IA e *machine learning*, per gestire l'ampia quantità di dati finanziari e contrattuali associati alle attività delle Forze Armate. Tuttavia, l'aumento delle voci di bilancio e la necessità di tenere traccia degli investimenti hanno reso fondamentale una migliore gestione dei dati finanziari.

Idealmente, inoltre, considerando che, come rilevato dal Generale nell'intervista annessa a livello nazionale e sovranazionale se ne è sprovvisti, si potrebbe altresì riflettere sulla possibilità di istituire un *Database on Defence Capability Development*. In tal caso, tutti i dati del sistema operativo, a livello nazionale o da organismi internazionali, dovrebbero essere raccolti in un *database* centrale e classificati per ricerca e sviluppo, approvvigionamento e anche linee di sviluppo di capacità come materiale, formazione e strutture.

Il *database* dovrebbe essere poi popolato da un servizio automatizzato che scherma le informazioni del sistema operativo da pagine Web dedicate per questo tipo di informazioni.

Dopo aver fornito una panoramica dei benefici e rischi connessi all'utilizzo dell'IA nell'ambito della BDAA, possiamo riassumere i principali svantaggi sottesi come inerenti all'approvvigionamento dei dati, all'opacità di funzionamento o "*black box*" e al modo di processare i dati, che, in taluni casi, potrebbero essere inavvertitamente condivisi o riutilizzati in altre ricerche. L'applicazione dell'IA per analizzare e processare i dati finanziari offre notevoli vantaggi, tra cui il supporto alle decisioni basate su dati più accurati ed

efficienti. Tuttavia, è importante riconoscere le sfide, come l'opacità dei sistemi algoritmici, la qualità dei dati e la sicurezza delle informazioni.

Come soluzione a queste problematiche di certo un modo potrebbe essere quello di garantire la supervisione da parte di sistemi umani dell'apprendimento di tali sistemi, così da evitare anzitutto l'approvvigionamento di dati non veritieri, l'interpretazione erronea di dati storici o la minaccia di "indottrinamento malizioso" a causa di algoritmi erronei. Tale supervisione potrebbe anche estendersi ex post alle decisioni o al supporto alle decisioni che i sistemi propongono basandosi sull'analisi dei dati a disposizione.

Sul piano pratico ed operativo, considerate le attuali esigenze delle Forze Armate, abbiamo scoraggiato ed escluso l'utilizzo di sistemi che adoperino IA e ML, perlomeno al momento in cui si scrive.

Difatti, i rischi connessi e sottesi all'utilizzo di tali sistemi, specialmente se declinati nell'ambito applicativo delle Forze Armate con la richiesta di processare dati che potrebbero essere sensibili, supera i benefici che potenzialmente se ne potrebbero trarre.

Alla luce dell'analisi condotta, si sono presentate diverse opzioni che le Forze Armate potrebbero adoperare per collezionare ed analizzare i dati ed estrarne: implementazione di un sistema *ad hoc on premise* e uso di sistemi sovranazionali già in uso.

È stata considerata l'opzione di creare un sistema *ad hoc* per le Forze Armate italiane, che garantirebbe un controllo totale sulla sicurezza dei dati ma richiederebbe risorse significative sia in termini finanziari che umani. L'implementazione di un sistema di questo tipo richiederebbe un'interfaccia di programmazione delle applicazioni (API) sicura per collegare i dati AI/ML con il sistema principale.

Una seconda opzione potrebbe consistere nell'adottare strumenti già disponibili, come il sistema EUCLID gestito dall'EDA, che raccoglie dati sui programmi di difesa degli Stati membri dell'Unione Europea. EUCLID è modulare e offre la sicurezza dei dati attraverso autorizzazioni di accesso limitate e la proprietà dei dati. Tuttavia, attualmente, non utilizza l'IA per l'analisi dei dati, ma questa opzione potrebbe essere esaminata in futuro.

In sintesi, entrambe le opzioni offrono vantaggi e sfide specifiche, ma è fondamentale bilanciare l'efficacia nell'analisi dei dati con la sicurezza delle informazioni.

La scelta tra l'implementazione di un sistema *ad hoc* o l'adozione di strumenti esistenti dovrebbe essere basata sulle esigenze specifiche delle Forze Armate italiane e sulla disponibilità di risorse. La considerazione di implementare l'IA dovrebbe essere attentamente valutata in termini di sicurezza e praticità per garantire una gestione finanziaria efficiente e sicura.

Le opzioni dovrebbero essere concretamente valutate in futuro, per scegliere quale di queste possa essere effettivamente intrapresa dalle Forze Armate, anche sulla base dell'analisi SWOT (*Strenghts, Weaknesses, Opportunities, Threats*), sincerandosi su quali siano i punti di forza, debolezza, gli obiettivi e le minacce di ciascuna. Inoltre, un fattore importante che potrebbe influenzare la decisione riguarda l'allocazione di risorse per questo nuovo ambito e le tempistiche necessarie per la sua implementazione ed utilizzo.

Ad ogni buon fine, sarebbe auspicabile, *pro futuro*, condurre un apposito studio successivo, che prenda le mosse dalle considerazioni sinora qui esposte. Difatti, al fine di rendere operativa una delle opzioni menzionate, si dovrebbero condurre le analisi del caso, che, in tale sede è stato possibile, per ragioni di brevità, fornire solo in maniera rudimentale e collaterale al principale oggetto dell'indagine.

Annesso: Interviste

1. Intervista al Gen. B. A. Antonio Caruso, Stato Maggiore dell'Aeronautica, 6 reparto

D. (Domanda) L'elaborato deve tendere a conoscere il possibile utilizzo di IA e ML per sfruttare fonti aperte di informazioni sullo sviluppo di capacità e dati di approvvigionamento per supportare il processo decisionale?

R. (Risposta) Corretto. Al momento, le Forze Armate stanno sperimentando una mole di dati particolarmente corposi, in quanto si tende a storicizzare e mantenere contratti di acquisizione di beni e di servizi. La finalità dell'indagine servirebbe a comprendere come le nuove tecnologie possano essere usate per calcolare e processare i dati storici ed estrarne trend e pattern, di modo da verificare se le scelte fatte sono corrette o se, invece, i soldi allocati in un investimento possano essere usati in altro.

D. Sarebbe utile, a tal fine, conoscere quanto gli altri Stati membri investano in un certo tipo di capacità militari derivate da contratti con fornitori di difesa?

R. Certo, sarebbe possibile. Ma il focus è come l'innovazione digitale e gli algoritmi usati possano portare delle soluzioni.

D. Si può procedere alla verifica comparatistica di come altri Stati procedono? Ad esempio, valutando se nel panorama internazionale vi siano già esempi di Paesi che procedono in tal senso?

R. Certo. Si può procedere ad una ricognizione anche se non assolutamente collimante.

D. Parliamo nell'elaborato di Big Data delle Forze Armate. Quali sono le voci che sono prese in considerazione?

R. Risorse svariate come acquisto di carburanti, bollette, investimenti, acquisizione di sistemi, valutando in che numero, che funzione etc. I Big Data rappresentano dunque la mole di dati derivanti dalle spese effettuate.

D. Esiste, ad oggi, a livello nazionale, un portale o una piattaforma per la raccolta dati unitaria?

R. No, al momento ne siamo sprovvisti. Consideri che prima del 2016, anno in cui agli Stati membri della Nato è stato richiesto l'impegno di incrementare le proprie spese per la difesa fino al raggiungimento dell'obiettivo del 2% delle spese per la difesa rispetto al PIL, l'ambito finanziario era molto più limitato, per cui non se ne avvertiva la necessità.

2. Intervista a Senior Consultant presso Ernst & Young, AI expert

D. Posto che la necessità delle forze armate sia utilizzare nuove tecnologie al fine di processare la grande mole di dati risultante dalla gestione finanziaria per ottenere la valorizzazione di dati storici di gestione, trend e simulazioni sulla performance dell'organizzazione, quale sistema lei adopererebbe?

R. A mio parere, quello di cui le Forze Armate necessiterebbero è ottenere un semplice "business insights" dei dati storici collezionati, largamente in uso tra le grandi aziende private, che consenta di estrarre dati quali stagionalità e correlazione. A tal proposito, si parla di Big Data Advanced Analytics (BDAA). L'applicazione di IA appare, a mio dire, superflua per tale analisi, in quanto la sofisticazione dei sistemi di IA è molto più avanzata e serve altri scopi.

D. Cosa mi dice della BDAA?

R. La BDAA rappresenta l'insieme dei metodi e strumenti avanzati per analizzare e interpretare grandi quantità di dati, noti come Big Data. L'obiettivo principale dell'analisi avanzata dei Big Data è quello di estrarre informazioni significative, identificare modelli, tendenze e relazioni nei dati. Questo può essere fatto attraverso tecniche di analisi statistiche, data mining, elaborazione del linguaggio naturale, visualizzazione dei dati, e così via. BDAA si concentra sull'ottimizzazione delle analisi dei dati per trarre informazioni utili e prendere decisioni basate sui dati.

D. Quali sono le forme di analisi?

R. Le analisi che possono insistere sui dati, al fine di esplorarli, sono diverse. Anzitutto, vi è la c.d. "analisi descrittiva", la più semplice, in grado di esplorare i dati, analizzarli, dal valore prettamente informativo. Tale tipologia di analisi implica la formulazione di domande non complesse e dirette quali "cosa è successo?", "in quale quantità?" ed adopera tecniche statistiche e matematiche di base per ottenere indicatori chiave di prestazione che mettano in luce le tendenze dei dati storici di gestione. A tal fine si possono usare strumenti comuni anche come Excel, PowerBi o Tableu.

La seconda analisi, "predittiva" manipola i dati estratti dall'analisi descrittiva per compiere una analisi o stima di predizioni con forme analitiche. Tale modello prende comunque in considerazione il modello descrittivo e tuttavia, al contrario di questo, non appare ancorato ai dati storici, prendendo in considerazione per il processo decisionale dati strutturati e non provenienti da svariate fonti. Questa tipologia di analisi consentirebbe alle Forze Armate di prendere decisioni informate, non solo basandosi e fornendo un resoconto onnicomprensivo degli storici, ma analizzando tramite indagine probabilistica la fattibilità ed utilità di taluni investimenti. Comprendono vari modelli statistici avanzati e concetti

matematici sofisticati come foreste casuali, GBM, SVM, GLM, teoria dei giochi, wargaming ecc ed i modelli comunemente adoperati sono: RapidMiner, R, Python, SAS, Matlab, Dataiku DSS, e molti altri.

L'ultima, quella più complessa, è l'analisi "prescrittiva", che è l'unica per cui si applicano sistemi di IA. Difatti, quest'ultima, prevede un processo di modellazione, anche basato sulla statistica, che doti il modello di capacità non solo predittive, ma che suggerisca attivamente all'utente quale scelta intraprendere. Tale sistema, come detto, adopera la modellazione con IA nei casi di problemi complessi. In ultimo, l'analisi prescrittiva rappresenta il tipo più sofisticato di analisi, che adopera l'ottimizzazione e la simulazione stocasistica per valutare le opzioni possibili e consigliare la migliore azione possibile, data la situazione fattuale. In tal caso, le domande poste sono del tipo: "Cosa dovrei fare in tale data situazione?".

D. Quali possono essere i possibili esempi di software adoperanti BDAA?

R. Software che conducano BDAA, capaci di estrarre dati ed analizzarli sono molto diffusi tra le aziende private, come dicevo. Esempi applicativi possono essere forniti dai maggiori cloud providers (come Azure di Microsoft, Amazon Web Services (AWS), Google Cloud Platform (GCP). Tali piattaforme non solo salvano il dato in cloud, ma automatizzano i processi di esplorazione, estrazione degli insights.

D. Possono elaborarsi nuovi software, con la specifica idea di destinarli alle Forze Armate?

R. Volendo, sì. Bisognerebbe, a tal fine, rivolgersi ad una società di consulenza che si occupi di costruire un software o una piattaforma che, grazie all'intervento di Data Architects e developers possa essere implementato. Prima di ciò, servirebbe estrarre i dati, attualmente contenuti fisicamente in alcuni documenti, convertirli in file strutturati con un tool e inserirli nel database. Tutte operazioni rimesse sicuramente ai consulenti.

D. Quali sono i rischi connessi per la sicurezza?

R. Di certo, se si decide di adoperare uno dei cloud proposti dalle grande aziende, si rischia che i dati vengano ivi caricati e che ne si perda parzialmente il controllo. A quel punto, se le garanzie di sicurezza che tali cloud providers non risultano sufficienti, converrebbe adottare un software on premise: sia i dati che i server rimarrebbero fisicamente presenti in locale.

L'alternativa, come dicevo, è affidarsi ad una società di consulenza che garantisca tale sicurezza. È la società di consulenza poi a curare gli eventuali rischi connessi alla sicurezza e, per garantire la riservatezza, si firmano accordi in tal senso e si individuano dei responsabili del trattamento dei dati. I dati dovrebbero essere trasferiti sul database dopo

averli mascherati. Se le informazioni sono classificate, si procede ad implementare chiave di cifratura per nascondere il dato, che risulta poi illeggibile.

D. In futuro, potrebbero installarsi a margine di tali sistemi on premise software adoperanti l'IA, al fine di migliorarne la performance?

R. Questi sistemi o piattaforme on premise, o che siano forniti da cloud providers o creati e ad uso esclusivo delle Forze Armate, potrebbero eventualmente comunicare con sistemi adoperanti l'IA. Si dovrebbe installare, a tal fine, una API on premise, che possa comunicare con la rispettiva API del sistema adoperante l'IA, non consentendo, tuttavia, un trasferimento dei dati in rete, ma mantenendoli in loco.

3. Intervista a CARD Project Officer presso European Defence Agency (EDA):

D. How does the Coordinated Annual Review on Defence, or CARD work?

R. The CARD reviews EU member states defence plans and programmes: capability development incl. R&T and procurement plans are collected to landscape where MS invest their budget in. On one hand, we can see trends and figures and derive analysis from that. In the last CARD iteration, for instance, we saw a significant increase in the EU defence budgets, mainly triggered by the Russian military attack on the Ukraine. This led to most MS announcing further increases to their defence investment, having increased their budgets already in 2014 – post Crimea. With these announced increases, the investment gap that was created after the financial crisis in 2008 could have been closed within a year.

On the other hand, where MS plans match in terms of substance and timelines, we propose options for cooperation – so called “collaborative opportunities”. In simple terms: if we see that Italy wants to introduce a new main battle tank, Germany wants to do the same and so does France, why not doing that together to safe cost and increase interoperability? We then propose to set up European programmes with all interested MS for all identified topic. Last round, these were 127 areas for cooperation.

D. How does EUCLID work?

R. EUCLID – the “European Union Collaboration in Defence” platform serves multiple purposes. Firstly, EUCLID gathers MS defence plans, programmes and In-Service capabilities. This information is used for CARD. Secondly, EUCLID is used for PESCO, to make the national implementation plans of individual MS accessible to all and also to propose and monitor PESCO projects. Thirdly, EUCLID hosts several “modules” with similar functions, for instance the German-Led Framework Nation Concept. In this case, Germany manages contributions from other MS into their defence capability clusters and to larger formations formed around FNC.

It is important to note that EUCLID is composed of different modules. The modular approach ensures that users have only access to the modules they are supposed to access. For instance: a user of PESCO won’t see CARD data nor FNC data. However, users can access multiple modules if this is deemed necessary by their national authority. EUCLID is fully MS driven and hosted and developed by the EDA.

D. How is data collected for EUCLID?

R. Member States either contribute directly or we populate EUCLID from open sources (OS). We screen OS such as defence news platforms like Military Balance+, Janes Defence, defence24.com and extract relevant information. These are introduced into EUCLID and marked as OS. MS can confirm the information and take ownership.

We are mainly looking into who does what and how much does it cost. For example: Austria purchases AW169 helicopters from Leonardo for a specific amount. We would collect how many Austria purchases, what they invest, if there are any options on more, when the delivery is started, when finalised, if there are service contracts or if there is collaboration with Italy, e.g. in the area of helicopter pilot training on the new type.

For now, the data collection is done manually. I believe this could be done better by using AI/ML tools. With an Application Programming Interface (API), EUCLID could utilise modern AI/ML to, first, do data collection, and to, second, do data validation (as in identifying duplicates – there are often more than one sources for the same piece of information, and they are sometimes contradicting). Thirdly, analysis of matches (of similar projects of different MS) or trends could be done AI/ML supported. Lastly, AI/ML could be used for decision making support. One could compare e.g. unit prices, cost of services and find the best suitable match for individual MS needs.

D. Can EUCLID collect also classified data?

R. Yes, sure. EUCLID is able to collect all data unlike cloud providers, who often have limited power to collect classified data, or at least up to an intermediate level, as they cannot collect and process secret or top secret data.

D. Can you extrapolate analysis and trend from data processed in EUCLID and inform future investments?

R. Yes, certainly. On standard indicators automatically or customised through PowerBI. The CARD AA identifies major trends in each operational domain and informs on where investment should be made, based on previously identified collaborative opportunities proposed and confirmed by MS.

D. How could one invest into EUCLID?

R. EUCLID s already a quite complex application, allowing for many functions and use cases. Almost a decade of development and investment of several million Euros have been made. The most appropriate improvement is in my view the use of AI/ML through APIs.

Also, since EUCLID currently operates in the internet, investment should go – and actually goes – into transferring the application into a classified environment. As most MS classify their defence programmes, this would enable more thorough data collection and exploitation.

D. How safe is EUCLID?

R. EUCLID uses the latest safety protocols on the internet and is quite safe. However, moving the application to a classified environment would further increase its security.

D. How do you ensure that data cannot be accessed by unauthorised persons?

R. Firstly, through a modular approach. Only if a person is granted access to the respective module, he would see the respective data. A user who has access to PESCO, cannot see CARD data. Therefore, he needs also access to the CARD module.

Secondly, through data ownership. The MS who owns the data can restrict its use to: CARD, PESCO or FNC, and also to individual MS. For instance, an Italian administrator would be able to restrict access to individual database entries to Italian users only, if he deems that appropriate. He can add France or Germany, but Austria wouldn’t have access.

4. Intervista a Annita Larissa Sciacovelli, Professoressa di Diritto Internazionale presso Università degli studi di Bari, AG European Union Agency for Cybersecurity (ENISA):

D. Le forze armate hanno espresso la necessità di utilizzare nuove tecnologie al fine di processare la grande mole di dati risultante dalla gestione finanziaria per ottenere la valorizzazione di dati storici di gestione, trend e simulazioni sulla performance dell'organizzazione. Ciò detto, lei ritiene che sia opportuno adoperare, a tal fine, sistemi impieganti l'Intelligenza Artificiale o, per ragioni di sicurezza, sarebbe preferibile usare altri tool capaci di garantire una analisi prescrittiva/descrittiva senza l'intervento dell'IA? Quali sono, in generale, le sue considerazioni a riguardo dell'applicazione dell'IA?

R. Anzitutto, inizio col dire che l'IA rappresenta, ad oggi, un game-changer, potendo migliorare l'accessibilità dei dati, fruibili da tutti i sistemi operativi, comportando pulizia, catalogazione ed etichettatura degli stessi. L'IA e il ML appare dunque fondamentale per la raccolta dei dati: a tal fine risulta significativa l'espressione americana "we need to liberate data from traditional sylos". Bisognerebbe utilizzare IA e ML per sfruttarne il pieno potenziale in tale ambito.

D. Considerato che i dati manualmente inseriti dagli operatori nel sistema potrebbero essere confidenziali o segreti, come pensa si possano prevenire minacce incidenti sulla sicurezza di tali dati? Basterebbe limitare l'utilizzo dei cloud e adoperare sistemi on premise? O risulterebbero necessarie ulteriori precauzioni come creare ambienti sicuri [es. classified environments]?

R. Al momento i governi si stanno impegnando al fine di trasferire i dati, anche classificati, su cloud: basi pensare che nel 2022 l'Ufficio Segretario Difesa degli Stati Uniti ha comunicato che vi sarà l'impegno per costituire un secret cloud che consenta lo scambio di informazioni su un cloud classificato in tempo reale.

Ciononostante, al momento, sarebbe preferibile il sistema on premise, non su cloud. A tal fine, le informazioni classificate sarebbero conservate nelle diverse ambasciate di Stati alleati, per evitare attacchi fisici da parte di terzi.

D. Che ruolo svolge la cybersicurezza nell'assicurare che l'IA nell'analisi avanzata dei Big Data sia utilizzata in modo sicuro e che i dati siano protetti da minacce cibernetiche?

R. Vi sono diversi sistemi che potrebbero essere implementati, come, a titolo di esempio, firewall, server di ingresso, sicurezza con 18 punti di accesso con infrastrutture di rete. Valga notare come il Cyber Security Intelligence Index di IBM ha rivelato che più del 90% di tutti gli incidenti di sicurezza deriva da una qualche forma di errore umano: utilizzo di link di phishing, visite a siti web dannosi, attivazione di virus e di altre minacce APT (Advanced Persistent Threats). Per cui nella maggior parte dei casi di attacchi cibernetici è

la disattenzione del funzionario ad essere imputabile, pertanto, il fattore umano è quello in cui serve investire per cybersecurity awareness.

D. In quale modo si potrebbero mitigare i rischi associati all'adozione di queste tecnologie all'interno delle organizzazioni?

R. La sicurezza potrebbe essere utilmente garantita da operatori selezionati. Anche in tal caso, tuttavia, sarebbe preferibile che gli operatori siano interni e non che si rimetta il controllo in outsourcing perché non si ha personale sufficiente, in quanto questo potrebbe causare altri problemi. Quando si creano le strutture vi deve essere personale autorizzato ad accedere, anche se possono esservi rischi di attacchi cybernertici anche dall'interno (es. Membro della Marina Militare con codici segreti ai russi). Vi sono sistemi di controllo per cui è possibile (come fanno le aziende) controllo e accesso [segmentazione dei dati per come vengono raccolti, ognuno può accedere al proprio settore di competenza] e criptazione dei dati stessi.

Bibliografia

Monografie, Volumi e Curatele:

- Akgül A. (1990). *Artificial Intelligence: Military Applications*. Ankara Üniversitesi SBF Dergisi 45.
- Barr A., Feigenbaum E. (1981) *The Handbook of Artificial Intelligence*, vol. 1, Stanford: Butterworth-Heinemann.
- Bawden, D. (2008). Origins and concepts of digital literacy. Digital Literacies: Concepts, Policies and Practices. Bern: Peter Lang Publishing.
- Boyd J. R. (1996). A Discourse on Winning and Losing. Alabama: Air University Press Maxwell AFB.
- Brownlee J. (2011) *Clever Algorithms: Nature-Inspired Programming Recipes.* Wuhuan: Lulu.
- Ciotti, F. Roncaglia, G. (2008). *Il mondo digitale. Introduzione ai nuovi media*. Roma-Bari: Laterza.
- Clifton P. O. (1985), *Artificial Intellifence A "User Friendly" Introduction*. Alabama: Air University Press.
- De Landa M. (1991). *War in the Age of Intelligent Machines*. New York: Zone Books.
- Dell'Utri M. (2019) Principi generali e condizioni di liceità del trattamento dei dati personali. In Cuffaro V., D'Orazio R., Ricciuto V., a cura di, *I dati personali nel diritto europeo*, Torino: Giappichelli.
- Di Resta F. (2018) *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Torino: Giappichelli.
- Flammini F., Setola R., Franceschetti G. (2013). *Effective surveillance for homeland security*. Boca Raton: CRC Press.
- Genesereth M. R., Nilsson N. J. (1987). *Logical Foundations of Artificial Intelligence*. Burlington: Morgan Kaufmann Publishers.
- Giusti E. (2020). Intelligenza artificiale e sistema sanitario. In Dorigo S., a cura di, *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa: PaciniEditore.
- Goodfellow-Y. I. Courville Bengio-A. (2016) *Deep Learning*, Cambridge: Cambridge Press.
- Joshi R., Sanderson A. C. (1990) Multisensor data fusion. Singapore: World Scientific.
- Lesmo L. (1991). *ad vocem IA. Grande Dizionario, Appendice V*. Torino:UTET.

- Lexcellent C. (2019) *Artificial intelligence versus human intelligence: are humans going to be hacked?*. Berlino: Springer.
- Luke S. (2013) *Essentials of Metaheuristics*, Wuhan: Lulu Enterprises.
- Pasquale F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge: Harvard University Press.
- Pizzetti F. (2016) *Privacy e il diritto europeo alla protezione dei dati personali*, *Dalla direttiva 95/46 al nuovo Regolamento europeo*. Torino: Giappichelli.
- Pizzetti F. (2018) *Intelligenza Artificiale, protezione dei dati personali e regolazione.* Torino: Giappichelli.
- Resta F. (2018), *Sub* art. 5. In: Riccio G.M, Scorza G., Belisario E., a cura di, *Commentario GDPR e normativa privacy*, Milano: Wolters Kluwers.
- Romano G. (2020), Diritto, robotica e teoria dei giochi: riflessioni su una sinergia. In Alpa G., a cura di, *Diritto e Intelligenza Artificiale*, Pisa: PaciniEditore.
- Roy R., Paul A., Bhimjyani P., et al. (2020) A short review on applications of *Big Data* analytics. In: Mandal J.K., Bhattacharya D. et al., a cura di, *Emerging technology model graph*. Singapore:Springer.
- Russell S., Norvig P. (2005) *Intelligenza Artificiale un approccio moderno*, Milano: Pearson.
- Schutzer D. (1987) *Artificial Intelligence An Application-Oriented Approach*. New York: Van Nostrand Reinhold.
- Szegedy C., Zaremba W., Sutskever I. et al (2013) *Intriguing properties of neural networks*. Cornell: Cornell University.
- Van den Hoven J., Blaauw M., Pieters W., Warnier M., (2020) Privacy and information technology. In: E.N. Zalta, a cura di, *The Stanford Encyclopedia of Philosophy, Metaphysics Research Lab*, Stanford:Stanford University.
- Winston P. H. (1977) *Artificial Intellifence*. Reading: Addison Wesley Publishing Co.
- Yang X.S. (2010) *Nature-Inspired Metaheuristic Algorithms*. Bristol: Luniver Press.

<u>Atti di Conferenze, Convegni o Studi Condotti da Istituti di Ricerca:</u>

- Boucher P. (2019) How Artificial Intelligence Works; Scientific Foresight Unit; EPRS | European Parliamentary Research Service, European Union.
- Brownstein B. J. et al. (1983) “Technological assessment of future battlefield robotic applications”, in Procesedings of the army Conference on Application of AI to Battlefield Information Management, US Navy Surface Weapons Center, White Oak.

- Coldeway D. (2016) “Carnegie Mellon’s Mayhem AI Takes Home $2 Million from DARPA’s Cyber Grand Challenge,” TechCrunch Conference, August 5, 2016.
- Cottle M., Hoover W., Kanwal S., et al (2013) Transforming health care through Big Data: strategies for leveraging big data in the health care industry. Institute for Health Technology Transformation - iHT.
- Flammini F. (2018) Artificial Intelligence (Ai) Applicata Agli Autonomous Systems, Report per il Centro Militare di Studi Strategici, CASD Roma.
- Gérard W., Alexandre D. (2009) Torinji: Automated Exploitation Malware Targeting Tor Users. Radu State University of Luxembourg.
- Gevarter W. B. (1983) An Overview of Artificial Intelligence and Robotics. NASA Scientific and Technical Braanch, Washington.
- Lovergine S. (2022) Breve disamina degli algoritmi di intelligenza artificiale. Aspetti tecnologici e metodologici, Rapporto dell’Istituto Nazionale per Analisi Politiche Pubbliche (INAPP).
- Markowitz J., Schmidt A. C., Burlina P. M. et al (2017) “Combining deep universal features semantic attributes and hierarchical classification for zero-shot learning” in Conference proceedings of 2017 IAPR MVA Conference.
- Martin E. W. (1983) “Artificial Intelligence and Robotics for Military Systems” in proceeding of the army conference on application or artificial intelligence to Battlefield Information Management, US Navy Surface Weapons Centre.
- Mohiuddin A. K. M. (2003) “Expert system for the thermal design of mechanical devices” in Conference proceedings Intell. Eng. Syst. (INES), 212-214.
- Morgan F. E., Boudreaux B., Lohn A.J. et al. (2020) Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. Santa Monica: RAND Corporation.
- Salisbury A. B. (1983) “Opening remarks on artificial intelligence”, in Proceedings of the Arm Conference on Application of Artificial Intelligence to Battlefield Information US Navy Surface Weapons Center, White Oak
- Song C., Ristenpart T., Shmatikov V. (2017) “Machine Learning Models that Remember Too Much” Conference CS ‘17, Dallas, TX, USA.
- Touretzky, D., Gardner-McCune, C., Martin, F., & Seehorn, D. (2019). “Envisioning AI for K-12: What Should Every Child Know about AI?” paper for the Thirty-Third AAAI Conference on Artificial Intelligence (AAAI-19), 33, 9795–9799.
- Turek M. (2016). Explainable Artificial Intelligence (XAI). Defence Advanced Research Project Agency 16(53).

- W.-Y. Yang, H. Zhang, D.-Z. Song and F.-N. Lai (2018) “Review of face recognition methods” in Conference Modeling Simulation Optim. Technol. Appl. 560-564.
- Wang Y., Chen Z. (1999) Genetic algorithm (GA) based flight path planning with constraints, Beijing University of Aeronautics and Astronautics 25(3), 355–358, 1999.
- Zhu J., Liapis A., Risi S., Bidarra R., Youngblood G., (2018) “Explainable ai for designers–A human-centered perspective on mixed- initiative co-creation” in IEEE Conference on Computational Intelligence and Games (CIG)

Saggi da riviste o siti Internet:

- Abiyev R. H., Kaynak O. (2008) Fuzzy wavelet neural networks for identification and control of dynamic plants—A novel structure and a comparative study. IEEE Transactions on Industrial Electronics, 55(8): 3133–3140.
- Aizpurua J.I., McArthur S.D.J., Stewart B.G., et al. (2019) Adaptive power transformer lifetime predictions through machine learning and uncertainty modeling in nuclear power plants. IEEE Transactions on Industrial Electronics, 66(6):4726–37.
- Alkaissi H., McFarlane S.I. (2023) Artificial Hallucinations in ChatGPT: Implications in Scientific Writing. Cureus 19, 15(2).
- Alom M. Z.; Taha T. M.; Yakopcic C.,et al (2019) A state-of-the-art survey on deep learning theory and architectures. Electronics, 8: 292.
- Angehrn A. A., Dutta S. (1998) Case-based decision support, Communications of the ACM, 41(5), 157–165.
- Barredo Arrieta A., Díaz-Rodríguez N., Del Ser J. et al. (2020) Explainable Artificial Intelligence (xai)–Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58:82-115.
- Bello, O.; Holzmann, J.; Yaqoob, T.; Teodoriu, C. (2015). Application of artificial intelligence methods in drilling system design and operations: A review of the state of the art. Journal of Artificial Intelligence and Soft Computing Research. 5: 121–139.
- Bengio Y. (2009) Learning Deep Architectures for AI. Foundations and Trends in Machine Learning, 2(1): 10.
- Bonczek R. H., Holsapple C. W., Whinston A. B. (1980) The evolving roles of models in decision support systems, Decision Sciences, 11(2), 337–356.
- Castelvecchi D. (2022) Are ChatGPT and AlphaCode going to replace programmers? Nature.
- Cavoukian A. (2012). Privacy by design origin and evolution. IEEE Explore.

- Chang C. W., Lee H. W.; Liu C.H. (2018) A review of artificial intelligence algorithms used for smart machine tools. Inventions, 3: 41.
- Chen H., Chiang R. H., Storey V. C. (2012) Business intelligence and analytics: From big data to big impact. MIS quarterly, 36(4): 1165-1188
- Chen S.H.; Jakeman A.J.; Norton J.P. (2008) Artificial intelligence techniques: An introduction to their use for modelling environmental systems. Mathematics and Computers in Simulation. 2(78): 379–400.
- Claudino J.G., Cardoso F. C.A., Boullosa D., et al. (2021) The role of veracity on the load monitoring of professional soccer players: a systematic review in the face of the big data era. Applied Science 11:6479.
- Colmeraue A. (1985), Prolog in 10 figures. Communications of the ACM, 28(12).
- Cuomo S., Biagini G., Ranieri M. (2022) Artificial Intelligence Literacy, che cos'è e come promuoverla. Dall'analisi della letteratura ad una proposta di Framework. Media Education 13(2): 161-172.
- Dang L., Piran M., Moon D.H.K.M.H. (2019) A survey on internet of things and cloud computing for healthcare. Electronics, 7:768.
- De Spiegeleire S., Maas M., Sweijs, T. (2017). Artificial Intelligence and the Future of Defense – Strategic Implications for Small- and Medium-Sized Force Providers. The Hague Centre for Strategic Studies (HCSS).
- Dhillon G., Backhouse J. (2001) Current directions in is security research–Towards socio-organizational perspectives. Information System Journal, 11:127-153
- Dignum V. (2017) Responsible Artificial Intelligence: Designing AI for human values. ITU Journal 1.
- Dorri A., Kanhere S.S., Jurdak R. (2018) Multi-agent systems: A survey. IEEE Access, 6: 28573–28593.
- Dourish P., Anderson K., Collective information practice: Exploring privacy and security as social and cultural phenomena. Human Computer Interaction 319-342.
- Endsley M. R., Praphrcul G. (1999) 'Supporting situation awareness in aviation systems,' Brit. J. Occupational Therapy, 5(62), 131–135.
- Endsley M. R., Praphrcul G. (1999) op. cit. Brit. J. Occupational Therapy, 5(62), 131–135.
- Gerber M., von Solms R. (2005) Management of risk in the information age. Computer Security, 24:16-30,
- Gordijn B. (2023) Have HT. ChatGPT: evolution or revolution? Medical Health Care Philosophy.

- Harel J., Koch C., Perona P. (2007) Graph-based visual saliency. Advances in Neural Information Processing Systems 19, 545.
- Holzinger A., Biemann C., Pattichis C.S., Kell D.B. (2017) What do we need to build explainable AI systems for the medical domain?. Computer Science.
- Horowitz M. C., Kahn L., Mahoney C. (2020) The Future of Military Applications of Artificial Intelligence: A Role for Confidence-Building Measures?. Foreign Policy Research Institute, 532.
- Iachello G., Hong J. (2007) End-user privacy in human-computer interaction Found. Foundations and Trends® in Human–Computer Interaction, 1:1-137,
- Javed K., Gouriveau R., Zerhouni N. (2015) A new multivariate approach for prognostics based on extreme learning machine and fuzzy clustering. IEEE Transactions on Cybernetics, 45(12):2626–39.
- Jiang Y., Li X., Luo H., Yin S., Kaynak O. (2022) Quo vadis artifcial intelligence?. Discover Artifcial Intelligence, 2:4.
- Joyce J. (2005). Data crunching. Scientific Computing and Instrumentation 22(8):47.
- Kubick W.R.(2012) Big Data, Information and Meaning. Clinical Trial Insights, pp. 26–28.
- Kuriscak E., Marsalek P., Stroffek J., Toth PG. (2015) Biological context of Hebb learning in artificial neural networks, a review. Neurocomputing. 152:27–35.
- Lee H., Kim Y., Kim C.O. (2017) A deep learning model for robust wafer fault monitoring with sensor measurement noise. IEEE Transactions on Semiconductor Manufacturing, 30(1):23–31.
- Leung Y. (2009) Fuzzy set and fuzzy logic. International Encyclopedia Human Geography, 32(4): 283-287.
- Levine S., Pastor P., Krizhevsky A., Quillen D. (2017) Learning Hand-Eye Coordination for Robotic Grasping with Deep Learning and Large-Scale Data Collection. International Journal of Robotics Research, 37(4–5): 421–436.
- McCarthy J., Minsky M.L., Rochester N., Shannon C.E. (1995) A proposal for the Dartmouth summer research project on artifcial intelligence. Stanford: AI Magazine.
- Moretti A. (2018) Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679. Diritto dell'informazione e dell'informatica, 4-5
- Ng, D. T. K., Leung, J. K. L., Chu, S. K. W., & Qiao, M. S. (2021). Conceptualizing AI literacy: An exploratory review. Computers and Education: Artificial Intelligence, 2.
- Nilsson N. J. (1982) Artificial Intelligence: engineering, science or slogan. AI Magazine, vol. 3, n. 1, p. 2-9.

- Osamy, W., Khedr A. M., Salim A., et al (2022) Recent Studies Utilizing Artificial Intelligence Techniques for Solving Data Collection, Aggregation and Dissemination Challenges in Wireless Sensor Networks: A Review. Electronics, 11(3): 313.
- Panciroli, C., Rivoltella, P. C., Gabbrielli, M., Zawacki Richter, O. (2020). Artificial Intelligence and education: new research perspectives. Form@re - Open Journal Per La Formazione in Rete, 20(3): 1-12.
- Peluso M. G. (2022). Intelligenza Artificiale e dati di qualità: la tecnologia come valido alleato. Medialaws – Rivista di diritto dei media, 2.
- Provost F., Fawcett, T. (2013). Data science and its relationship to big data and data-driven decision making. Big data, 1(1), 51-59.
- Rajšp A., Fister I. (2020) A systematic literature review of intelligent data analysis methods for smart sport training. Applied Science 10:3013.
- Samuel A.L. (2000) Some studies in machine learning using the game of checkers. IBM Journal, 44(1.2):206–26.
- Searle J. R. (1980) Minds, brains, and programs. Behavioral and Brain Sciences (3).
- Semantha F.H., Azam S., Yeo K.C., Shanmugam B. (2020) A systematic literature review on privacy by design in the healthcare sector. Electronics, 3:452.
- Steinbauer, G., Kandlhofer, M., Chklovski, T., Heintz, F., & Koenig, S. (2021). A Differentiated Discussion About AI Education K-12. KI - Künstliche Intelligenz, 35(2): 131–137.
- Stokel-Walker C (2023) ChatGPT listed as author on research papers: many scientists disapprove. Nature. 613(7945):620-621.
- Stokel-Walker C. (2022) AI bot ChatGPT writes smart essays – should professors worry? Nature.
- Szabadföldi I. (2021) Artificial Intelligence In Military Application – Opportunities And Challenges. Revista Academiei Forţelor Terestre. 2 (102), 162.
- Trevisi C. (2018). La regolamentazione in materia di intelligenza artificiale, robot, automazione: a che punto siamo, Medialaws – Rivista di diritto dei media, 2.
- Van Deursen N., Buchanan W.J., Duff A. (2013) Monitoring information security risks within health care, Computer Security, 37:31-45.
- Wang W., Liu H., Lin W., et al (2020) Investigation on Works and Military Applications of Artificial Intelligence. IEEE Access. 8.
- Yao M., Zhao M. (2015) Unmanned aerial vehicle dynamic path planning in an uncertain environment. Robotica 33(3) 611–621.

- Zhang L., Zhang B. (1990) A geometrical representation of McCulloch-Pitts neural model and its applications. IEEE Transact Neural Networks,10(4): 925–9.
- Zhang T., Su G., Qing C., et al (2021) Hierarchical lifelong learning by sharing representations and integrating hypothesis. IEEE Transactions on Semiconductor Manufacturing, 51(2):1004–14.

Nota sull'IRAD e Nota sull'Autore

IRAD[112]

L'Istituto di Ricerca e Analisi della Difesa (IRAD) è l'Organismo che gestisce, nell'ambito e per conto del Ministero della Difesa, la ricerca su temi di carattere strategico.

Costituito come Centro Militare di Studi Strategici (Ce.Mi.S.S.) nel 1987 e riconfigurato come IRAD nel 2021 a seguito dell'entrata in vigore della Legge 77/2020 - art. 238 bis, l'IRAD svolge la propria opera avvalendosi di esperti civili e militari, italiani ed esteri, in piena libertà di espressione di pensiero.

Quanto contenuto negli studi pubblicati riflette quindi esclusivamente l'opinione del Ricercatore e non quella del Ministero della Difesa.

Autrice

Stefania Rutigliano ha conseguito la laurea con lode in Giurisprudenza (2018) ed il Dottorato di Ricerca in Principi giuridici ed istituzioni fra mercati globali e diritti fondamentali, curriculum in Diritto Internazionale e dell'Unione Europea (2023) presso l'Università degli Studi di Bari Aldo Moro. Ha conseguito il titolo di avvocato dal 2021 e la sua area di competenza è principalmente la causa transfrontaliera con applicazione del diritto dell'Unione europea, del diritto penale e processuale. Durante il percorso accademico, ha svolto diverse esperienze lavorative all'estero, tra cui un tirocinio presso l'Agenzia Europea per la Difesa (*European Defence Agency*, EDA), terminato nel 2023 ed uno stage per il Comitato politico e di sicurezza della Rappresentanza permanente d'Italia presso l'Unione europea a Bruxelles nel 2018.

È attiva collaboratrice e curatrice di articoli scientifici in materia di diritto internazionale e dell'Unione europea.

[112] http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pagine/default.aspx


9 791255 150831