CENTRO ALTI STUDI
PER LA DIFESA

CENTRO MILITARE
DI STUDI STRATEGICI

**Cap. Giovanni FRISO**

# "Una Difesa digitale, in un mondo fatto di bit" – prospettive, vulnerabilità e implicazioni.

**(Codice AP-SMD-04)**

Il Centro Militare di Studi Strategici (Ce.Mi.S.S.), costituito nel 1987 e situato presso Palazzo Salviati a Roma, è diretto da un Generale di Divisione (Direttore), o Ufficiale di grado equivalente, ed è strutturato su due Dipartimenti (Monitoraggio Strategico - Ricerche) ed un Ufficio Relazioni Esterne. Le attività sono regolate dal Decreto del Ministro della Difesa del 21 dicembre 2012.

Il Ce.Mi.S.S. svolge attività di studio e ricerca a carattere strategico-politico-militare, per le esigenze del Ministero della Difesa, contribuendo allo sviluppo della cultura e della conoscenza, a favore della collettività nazionale.

Le attività condotte dal Ce.Mi.S.S. sono dirette allo studio di fenomeni di natura politica, economica, sociale, culturale, militare e dell'effetto dell'introduzione di nuove tecnologie, ovvero dei fenomeni che determinano apprezzabili cambiamenti dello scenario di sicurezza. Il livello di analisi è prioritariamente quello strategico.

Per lo svolgimento delle attività di studio e ricerca, il Ce.Mi.S.S. impegna:

a) personale militare e civile del Ministero della Difesa, in possesso di idonea esperienza e qualifica professionale, all'uopo assegnato al Centro, anche mediante distacchi temporanei, sulla base di quanto disposto annualmente dal Capo di Stato Maggiore dalla Difesa, d'intesa con il Segretario Generale della Difesa/Direttore Nazionale degli Armamenti per l'impiego del personale civile;
b) collaboratori non appartenenti all'amministrazione pubblica, (selezionati in conformità alle vigenti disposizioni fra gli esperti di comprovata specializzazione).

Per lo sviluppo della cultura e della conoscenza di temi di interesse della Difesa, il Ce.Mi.S.S. instaura collaborazioni con le Università, gli istituti o Centri di Ricerca, italiani o esteri e rende pubblici gli studi di maggiore interesse.

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 guide per l'attività di analisi e di collaborazione con le istituzioni omologhe e definendo i temi di studio da assegnare al Ce.Mi.S.S..

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.

**Cap. Giovanni FRISO**

# ''Una Difesa digitale, in un mondo fatto di bit'' – prospettive, vulnerabilità e implicazioni.

(Codice AP-SMD-04)

# “Una Difesa digitale, in un mondo fatto di bit” – prospettive, vulnerabilità e implicazioni.

## 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 dal **Centro Militare di Studi Strategici**

Direttore: **Gen. S.A. Stefano Vito SALAMIDA**

Vice Direttore - Capo Dipartimento Ricerche: **Col. c.(li.) s.SM Andrea CARRINO**

Progetto grafico: **Massimo Bilotta – Capo 1^ cl. Massimo LANFRANCO**

Autore: **Cap. Giovanni FRISO**

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

Centro Militare di Studi Strategici
Dipartimento Ricerche
Palazzo Salviati
Piazza della Rovere, 83 - 00165 – Roma
tel. 06 4691 3203
e-mail: caporicerche.cemiss@casd.difesa.it

**chiusa a settembre 2020**

**ISBN 978-88-31203-48-7**

**Indice**


**Sommario** 7

**Abstract** 9

**Capitolo 1** 11

**Il dominio tecnologico per una Difesa digitale** 11

**Dati, informazioni, conoscenza** 11

**Dati per interpretare fenomeni** 13

**Potenziali sfide tecnologiche** 14

**Modelli di Difesa a confronto** 15

**Approcci all'Intelligenza Artificiale** 17

**Intelligenza Artificiale militare** 18

**Sistemi di Comando e Controllo intelligenti** 20

***Situation Awareness* ed interazioni uomo-macchina** 21

***Intelligence* Militare per una Difesa digitale** 24

**Minacce cibernetiche e Intelligenza Artificiale** 25

***Vulnerability Intelligence*** 27

***Blockchain* per la Difesa** 28

***Environment* Strategici digitali** 29

**Portfolio Strategico di una Difesa Digitale** 31

**Info-struttura della Difesa e *Covid-19*** 32

**Capitolo 2** 34

**Il fattore umano per una Difesa digitale** 34

**Coltivare talenti digitali** 34

**Sinergia con Università e Industria nazionale** 36

**Innovazione proattiva** 38

**Il problema etico** 39

**Capitolo 3** **43**

**La *leadership* organizzativa per una Difesa digitale** **43**

**Approcci al *change management* digitale** **43**

**Impatti sui processi di *Decision Making*** **45**

**Cambiamento culturale per una Difesa Digitale** **46**

**Metodologie per la definizione di business case** **47**

**Conclusioni** **49**

**Elenco delle principali abbreviazioni e degli acronimi** **51**

**biblio/emero/web-grafia** **52**

# Sommario

Il livello di pervasività delle *Information Technology* e l'impatto del mondo ICT (*Information Communication Tecnologies*) hanno evidenziato negli ultimi anni una crescente rilevanza strategica del dominio cibernetico; dopo terra, aria e spazio extra-atmosferico, il *cyberspace* è divenuto cruciale per il potere nel XXI secolo. Nell'era del cosiddetto quinto dominio, infatti, i paesi altamente informatizzati hanno raggiunto un elevato grado di interconnessione e interdipendenza a vari livelli (politico, strategico nazionale, strategico militare, operativo, tattico) per far fronte ai mutevoli scenari geopolitici con la necessaria efficacia.

Queste interconnessioni permettono di far scalare rapidamente informazioni tattiche fino al livello politico ma presentano, dal punto di vista strategico, un "prezzo da pagare" che consiste nella minaccia alla sicurezza di tipo trasversale, ovvero che riguarda l'intera catena di Comando e Controllo senza alcuna esclusione.

Per garantire un vantaggio militare in questo nuovo ambiente operativo digitale, la Difesa nel suo complesso deve dimostrarsi adattiva, innovativa ed in grado di esprimere senza soluzione di continuità le sue capacità in contesti eterogenei in termini di scenari, minacce e vincoli. L'analisi svolta in questo studio scompone il problema osservandolo da tre punti di vista apparentemente separati ma sostanzialmente relazionati tra loro: il dominio tecnologico, il fattore umano ed i cambiamenti culturali dell'organizzazione.

Nel primo capitolo di questo studio verranno affrontate le potenziali sfide tecnologiche in termini di prospettive, implicazioni e conseguenti minacce e vulnerabilità. La costante e persistente necessità di raccolta, analisi e interpretazione di una mole crescente e sempre più eterogenea di dati mette continuamente in evidenza il concetto dei cosiddetti "*environment* strategici digitali". Quelle info-strutture, ovvero installazioni, strutture, edifici, nodi della rete informatica, sistemi operativi, data center, server, dati e, astrattamente, algoritmi di analisi, che se resi vulnerabili da un attaccante, nella sua più ampia accezione, possono risultare una minaccia allo Stato e alla Sicurezza Nazionale. Le stesse info-strutture che, nel quinto dominio, possono costituire l'arma vincente per una superiorità a tutti i livelli, trasformando semplici dati in informazioni fruibili e costituendo condizione necessaria all'esecuzione di una missione affidabile in condizioni di persistenti minacce informatiche. Per raggiungere un tale livello di ambizione è di vitale importanza puntare sulle capacità tecnologiche emergenti con un approccio orientato all'innovazione proattiva, allo scopo di disporre di infrastrutture e servizi ICT agili, resilienti, sicuri e senza soluzione di continuità.

Nel secondo capitolo verrà affrontato un altro aspetto cruciale per la riuscita di una rivoluzione digitale dell'Amministrazione Difesa all'altezza delle sfide geopolitiche attuali, ovvero il fattore umano. Qualsiasi tecnologia emergente non potrà dar frutto alle necessarie capacità operative al servizio della Difesa se non opportunamente governata da personale altamente competente, formato e costantemente aggiornato per essere una forza lavoro digitale pronta alle nuove sfide. Elementi fondamentali per un efficace raccordo tra tecnologie, competenze e sistemi sono le Università, volano delle tecnologie emergenti, e l'Industria nazionale che dalle tecnologie produce capacità. Solo con l'adozione di un piano strategico che garantisca la massima sinergia in tal senso, l'Amministrazione Difesa potrà rispondere alla competitività internazionale in campo di competenze digitali del proprio personale; andranno strutturati piani di formazione specifici per il quinto dominio che abbraccino progressivamente un bacino crescente di personale, allo scopo di strutturare una sempre più ampia forza lavoro digitale che vada incontro alle sfide attuali ed emergenti in campo digitale.

Il terzo capitolo dello studio affronta il tema della *leadership* organizzativa e dei necessari adattamenti che sono imposti da una rivoluzione digitale dell'Amministrazione Difesa; dovranno essere valutati i nuovi approcci al *change management*, migrando da un approccio pianificato al cambiamento ad uno sistemico piuttosto che emergente. In un dominio dove la tecnologia è governata in modo inversamente proporzionale rispetto all'attuale *leadership* organizzativa, dove il bacino di talenti digitali è costituito per la quasi totalità da personale anagraficamente giovane, vanno riconsiderati fenomeni di *leadership* connettiva basata su una forte interazione tra individui dell'organizzazione.

Nelle conclusioni si raccordano i diversi approcci dello studio evidenziando come sia fondamentale ribaltare il concetto negativo di asimmetria del dominio cibernetico sfruttandone le caratteristiche intrinseche, allo scopo di guadagnare resilienza nel mondo della *Cyber Security* ed espandere la competitività nella cosiddetta *Digital Arena*.

# Abstract

The pervasiveness of Information Technology has highlighted how the strategic importance of the cyber domain has grown in recent years. After Earth, Air and Space domains, cyberspace has become crucial to power in the 21st century.

In the era of the “fifth domain”, computerized and digitalized countries have achieved a high degree of interconnection and interdependence at various levels (political, national strategic, military strategic, operational, tactical) to effectively cope with an ever-changing geopolitical scenario.

These interconnections allow tactical information to rapidly scale up to the political level; from a strategic point of view, this implies a cross-cutting security threat that affects the entire Command and Control chain without exceptions.

To guarantee a military advantage in this new digital operational environment, the Defense must prove itself adaptive, innovative and able to seamlessly express its capabilities in heterogeneous contexts in terms of scenarios, threats and constraints.

This paper breaks down the problem by observing it from three apparently separate points of view: the technological domain, the human factor and cultural changes in the organization.

The first chapter will address potential technological challenges in terms of implications, threats and vulnerabilities. The constant and persistent need for the collection, analysis and interpretation of a growing and increasingly heterogeneous amount of data highlights the concept of “digital strategic environments”. It includes info-structures, i.e. installations, structures, buildings, computer network nodes, operating systems, data centers, servers, data and, abstractly, algorithms which, if made vulnerable by an attacker, can be a threat to National Security. Those info-structures can be the winning weapon for achieving superiority at all levels, transforming simple data into usable information. For such a level of ambition, it is vital to focus on emerging technological capabilities with an innovative proactive approach, in order to have agile, resilient, secure and seamless ICT infrastructures and services.

In the second chapter the human factor will be addressed, which is another crucial aspect for the success of a digital revolution of Defense suitable for the current geopolitical challenges. Any emerging technology will not be able to produce the necessary operational capabilities unless suitably governed by highly competent, trained and constantly updated personnel.

In this process, the fundamental elements for an effective connection between technologies, skills and systems are the Universities, the flywheel of emerging technologies, and the Industry that produces skills from technologies.

Only through the adoption of a strategic plan that guarantees maximum synergy in this sense, the Defense will be able to respond to international competitiveness; specific training plans for the “fifth domain” will have to be structured, in order to foster the growth of a digital workforce that can meet current and emerging challenges in the digital field.

The third chapter deals with the theme of organizational leadership and the necessary adaptations that are imposed by a digital revolution in Defense; new approaches to change management will have to be evaluated, migrating from a planned approach to change to an emerging one. In a context in which the pool of digital talents is almost entirely made up of young staff, connective leadership phenomena based on the interaction between individuals in the organization must be reconsidered.

The conclusions connect the different approaches, highlighting how fundamental it is to overturn the negative concept of asymmetry of the cyber domain by exploiting its embedded characteristics, in order to gain resilience in the world of Cyber Security and expand competitiveness in the so-called Digital Arena.

# Capitolo 1

# Il dominio tecnologico per una Difesa digitale

## Dati, informazioni, conoscenza

Un famoso detto popolare recita che "viviamo nell'era dell'informazione"; in realtà stiamo vivendo nell' "era dei dati"[1]. Diversi studi quantificano l'esplosione del volume di dati prodotti da utenti e imprese nell'ordine dei quintilioni di *byte* che si riversano quotidianamente nelle reti informatiche e nei variegati dispositivi di archiviazione per effetto di interazioni legate al mondo degli affari, dell'economia, della scienza, dell'ingegneria, della medicina, di qualsivoglia ambito, finanche quello militare.

Questa crescita esplosiva del volume di dati disponibili è il risultato dell'informatizzazione della nostra società e del rapido sviluppo di potenti strumenti di raccolta e archiviazione dei dati. Le aziende di tutto il mondo generano giganteschi set di dati per gestire transazioni di vendita, registri di trading prodotti, profili commerciali, *feedback* dei clienti. Le comunità scientifiche ed ingegneristiche sviluppano una mole dell'ordine dei *petabyte*[2] di dati provenienti ininterrottamente da strumenti di telerilevamento, misurazioni di processo, esperimenti scientifici, analisi prestazionali, osservazioni e monitoraggio di fenomeni. Gli stessi utenti con le proprie ricerche supportate dai motori di ricerca, i social media ed i social network sono diventati fonti di dati che, potenzialmente, possono essere sfruttati a vantaggio di terzi.

Per poter creare valore aggiunto da una tale mole di dati sono necessari strumenti potenti e versatili che automaticamente identifichino ed estrapolino da tali dati informazioni utili per accrescere la conoscenza del cosiddetto "decisore".

Uno studio del centro di innovazione digitale *CEFRIEL* del Politecnico di Milano[3] ha stimato in circa trentacinquemila il numero di decisioni che mediamente una persona prende ogni giorno. Nonostante molte riguardino scelte semplici e ordinarie, spesso, soprattutto nel campo professionale, l'impatto maggiore è dato dalla complessità dell'informazione da trattare che comporta processi decisionali più complessi e articolati.

La prima regola dell'arte del *Decision Making* è quella di disporre dell'informazione giusta al momento giusto per avere l'adeguato livello di conoscenza del dominio di

1 Jiawei Han, Micheline Kamber, Jian Pei "Data-Mining. Concepts and Techniques" 3rd Edition Morgan Kaufmann 2011 p. 38-39

2 Il petabyte è un'unità di misura dell'informazione o della quantità di dati, il termine deriva dalla unione del prefisso SI peta con byte e ha per simbolo PB. Il prefisso peta deriva dal termine greco penta a indicare la quinta potenza di 1.000. Per definizione 1 petabyte equivale a mille terabyte, a un milione di gigabyte e a un biliardo di byte.

3 https://www.techeconomy2030.it/2019/12/19/data-driven-decision-making-come-fare-con-quali-benefici/

riferimento, allo scopo di prendere il più velocemente possibile la decisione corretta. Pertanto, disporre di una mole elevata di dati può risultare inutile se non si è supportati da strumenti tecnologicamente avanzati che permettano di sfruttarli per alimentare il processo decisionale. Il processo che consente di prendere decisioni partendo dai dati è il cosiddetto *Data Driven Decision Making*, un insieme di strumenti che consente di ridurre la complessità dei dati a disposizione grazie a specifiche metodologie di analisi, estrarre informazioni rilevanti dai dati e comunicare queste informazioni tramite sistemi di *Data Visualization* di rapida interpretazione.

Condizioni necessarie affinché i dati possano supportare il processo decisionale sono la chiarezza dell'obiettivo da comunicare, l'adozione di un approccio di analisi rigoroso, la corretta scelta dei dati per comprendere adeguatamente fenomeni, correlazioni e relazioni di causalità e la consapevolezza del background di chi dovrà leggere e interpretare l'informazione ricevuta, ovvero l'esperienza, la cultura e la preparazione. Con questi prerequisiti, l'attività di *Data Analysis* può estrarre informazioni rilevanti a partire dai dati, sfruttando strumenti e metodologie della *Data Science*, del *Machine Learning* e, più in generale, dell'Intelligenza Artificiale. Con il termine *Data Science* si intendono quelle tecniche basate sui principi statistici di analisi dei dati che permettono la comprensione e la previsione di specifici fenomeni. Algoritmi di apprendimento dati che deducono come comportarsi sulla base di esperienze note sono detti di *Machine Learning*. Con Intelligenza Artificiale si racchiudono le teorie e le tecniche il cui obiettivo è quello di riprodurre le capacità cognitive umane mediante delle macchine, anche modellando il funzionamento di reti neurali. Già nei primi anni '80 il Manuale di Intelligenza Artificiale di Avron Barr e Edward A. Feigenbaum[4] affermava:

> *"L'*Intelligenza Artificiale *è la parte della scienza informatica che si occupa della progettazione di sistemi informatici intelligenti, vale a dire sistemi che esibiscono le caratteristiche che associamo all'intelligenza tipica del comportamento umano - comprensione della lingua, apprendimento, ragionamento, risoluzione dei problemi e così via."*

4 Barr, Avron and Edward A. Feigenbaum. "The Handbook of Artificial Intelligence, Volume 1". Los Altos, California: William Kaufmann, Inc.

**Dati per interpretare fenomeni**

Un efficiente processo di analisi e visualizzazione dei dati può portare a comprendere il passato, ovvero capire cosa sia successo in uno specifico arco temporale ed identificare "*insight*", ovvero intuizioni, utili a migliorare gli approcci di lavoro.

Al contempo si può ragionare sul presente analizzando gli *input* forniti dai dati arrivando a poter prendere decisioni in tempo reale comprendendo dove intervenire e cosa cambiare. Infine, attraverso l'analisi dei dati è possibile fare attività previsionale sul futuro, ovvero anticipare fenomeni, ridurre o gestire potenziali rischi, aumentare l'efficienza e, più in generale, influenzare il *course of action*.

Pertanto, le decisioni basate sui dati, in funzione dell'accuratezza delle analisi, possono portare benefici anche inattesi in termini di maggior valore sul patrimonio informativo stesso, piuttosto che potenzialità di business del tutto inesplorate. È ampiamente dimostrato da diversi studi di settore che un'azienda o un'organizzazione che investe sui processi di *Data Driven Decision Making*, ovvero sulla considerazione che raccogliere, utilizzare e decifrare informazioni, costituisce un *enabler* di immense proporzioni per il proprio *business*.

Lo stesso Piano nazionale innovazione 2025 pubblicato dal Ministero per l'nnovazione Tecnologica e la Digitalizzazione promuove la tematica dell'efficienza che possono garantire tecniche di Intelligenza Artificiale e big data.

In particolare:

> *"L'*Intelligenza Artificiale *e i big data sono in grado di guidare i decisori pubblici verso scelte sempre più consapevoli, gestendo in maniera efficiente una serie di procedimenti amministrativi, specie se ripetitivi e a bassa discrezionalità.*
>
> *Progettare, sviluppare e sperimentare soluzioni di* Intelligenza Artificiale *applicata ai procedimenti amministrativi e alla giustizia eticamente e giuridicamente sostenibili significa dare attuazione moderna ai principi costituzionali che vogliono un'amministrazione efficiente e un processo giusto trasparente e breve. Non è qualcosa che si possa scegliere se fare o non fare, è qualcosa che si deve fare."*[5]

5 Piano nazionale innovazione 2025, Ministero per l'Innovazione Tecnologica e la Digitalizzazione, Release Stabile, 13 febbraio 2020. https://innovazione.gov.it/assets/docs/MID_Book_2025.pdf p.12

**Potenziali sfide tecnologiche**

Chris Anderson, direttore della rivista statunitense Wired nel 2008 scriveva:

> *"Sessanta anni fa i computer permisero che le informazioni potessero essere lette; vent'anni fa internet permise che le informazioni potessero essere ricercate; dieci anni fa i primi crawler dei motori di ricerca permisero di raggruppare le informazioni in un'unica banca dati; ora Google e le aziende che la pensano allo stesso modo stanno setacciando l'età più misurata della storia, trattando questo enorme corpus come un laboratorio della condizione umana. Sono gli albori dell'età dei Petabyte."*

e proseguiva coniando il concetto di "*Big Data*":

> *"Questo è un modo in cui enormi quantità di dati, uniti alle scienze matematiche applicate, sostituiscono ogni altro strumento che possa essere sfruttato (…) contro ogni teoria del comportamento umano, della linguistica e della sociologia. Dimenticando la tassonomia, l'ontologia e la psicologia. (…) chissà perché le persone fanno quello che fanno. Il punto è che lo fanno, e possiamo seguirlo e misurarlo con una fedeltà senza precedenti. Con abbastanza dati, i numeri parlano da soli."*[6]

Nella cosiddetta "*Petabyte Age*", uno dei requisiti fondamentali per comprendere la dimensione del cambiamento è slegare il "concetto di dato" come di qualcosa che possa essere visualizzato nella sua interezza. Lo sforzo da farsi è quello di vedere in prima battuta il dato in un'ottica analitica, per poi, successivamente, definirne il contesto. L'assunto è che, indipendentemente dal contesto applicativo, sia esso sociale, commerciale, politico, militare, strategico, operativo, finanche tattico, l'arma vincente per la superiorità è disporre di dati migliori e di strumenti di analisi migliori. La mole di dati di cui si dispone porta ad abbandonare le classiche e auto esplicative relazioni "causa effetto"; scontrandosi con i *Big Data*, l'approccio scientifico basato su ipotesi, modello e test diventa del tutto obsoleto, in piena analogia con quanto successo in fisica quando il modello newtoniano è stato superato dalle teorie quantistiche. Non esiste una soluzione migliore, ma strumenti di correlazione che abbandonano i modelli ed analizzano i dati senza supporre ipotesi sul comportamento di un fenomeno. Le capacità computazionali attuali permettono di immettere dati nei *cluster*[7] di elaborazione più potenti mai esistiti e di lasciare che gli algoritmi di *data science*, *Machine*

6 Wired USA, volume July 2008, https://www.wired.com/2008/06/pb-theory/.

7 In informatica un computer cluster, o più semplicemente cluster è un insieme di computer connessi tra loro tramite una rete telematica. Scopo del cluster è distribuire un'elaborazione molto complessa tra i vari computer, aumentando la potenza di calcolo del sistema e/o garantendo una maggiore disponibilità di servizio, a prezzo di un maggior costo e complessità di gestione dell'infrastruttura: per essere risolto il problema che richiede molte elaborazioni viene infatti scomposto in sotto problemi separati i quali vengono risolti ciascuno in parallelo.

*Learning* e più in generale di Intelligenza Artificiale trovino modelli dove la scienza classica non può.

Imparare a sfruttare i computer in questa scala può essere complicato, ma apre ad enormi opportunità: la disponibilità di enormi quantità di dati e di strumenti estremamente complessi di analisi, spesso basati su reti neurali che puntano a funzionare in analogia al cervello umano, offre nuove possibilità di comprendere fenomeni e prevedere scenari. In conclusione, la correlazione sostituisce il principio di causalità, e, grazie a queste tecnologie, la scienza può progredire anche senza modelli coerenti, teorie unificate e, nei casi limite, senza una spiegazione meccanicistica.

**Modelli di Difesa a confronto**

Apprezzare dal punto di vista militare i vantaggi di queste tecnologie emergenti porta naturalmente a processi di ottimizzazione della Difesa nel suo complesso, al fine di incrementare e rendere più efficienti le sue capacità. Fornire capacità ICT con maggiore efficienza assicurando prestazioni elevate per la Difesa necessita una riforma del modello con cui quest'ultima attualmente opera. In particolare, la valutazione e l'implementazione delle cosiddette *best practices* e delle comprovate tecnologie già in uso in settori di influenza (industria nazionale, accademia, partner NATO, paesi UE.) devono subire una forte accelerazione per mitigare il rischio di perdere competitività nella *Digital Arena*.

Come ampiamente descritto nella strategia di ammodernamento digitale del DoD americano[8], la Difesa statunitense è orientata a mutare la sua attuale struttura cosiddetta "*Component Centric*" verso un modello di Difesa e Operazioni "*Enterprise-wide*". Al riguardo, l'obiettivo strategico che il DoD d'oltreoceano si è posto è, quindi, di passare a un modello operativo e di Difesa di tipo aziendale, attraverso diverse fasi che prevedono la riprogettazione dei *Data Center*, l'ottimizzazione della produttività del lavoro d'ufficio e delle capacità di collaborazione, ivi compresi gli strumenti di *video* e *voice conference*, il rafforzamento della *partnership* con l'industria nazionale e dei processi di gestione finanziaria del comparto IT (*Information Technology*).

La *vision* di una tale ridefinizione in chiave strategica della struttura del DoD è la seguente:

> *"La vision è quella di garantire che i comandanti militari, la leadership civile, i soldati, i partner della Coalizione e altri partner di missione autorizzati non-DoD abbiano accesso alle informazioni e ai dati forniti in un ambiente informativo sicuro, affidabile e*

8 DoD Digital Modernization Strategy, DoD Information Resource Management Strategy Plan FY 19-23, ed. jul 12, 2019, p. 24-26

*agile per consentire le funzioni di Comando e Controllo di forze che eseguono operazioni del cyberspazio.(…) È prevista una soluzione di gestione dei servizi IT completamente convergente per supportare la gestione del cambiamento, delle risorse, della conoscenza e dei livelli di servizio"*[9].

Un recente "*food for thought paper*" a firma di diverse nazioni appartenenti *all'European Defence Agency* (EDA)[10] ha evidenziato l'importanza della digitalizzazione e dell'applicazione dell'Intelligenza Artificiale nel campo della Difesa per lo sviluppo delle capacità di domani. Secondo questo studio, queste nuove tecnologie impongono un approccio orientato ai sistemi *Commercial Off-The-Shelf* (COTS) di tipo duale che potranno essere usate in un modo innovativo per scopi militari. Il focus, quindi, viene spostato sul processo di integrazione di tali sistemi per le Forze Armate, presupponendo però una conoscenza duplice delle tecnologie COTS e delle piattaforme e Sistemi d'Arma della Difesa. La tesi del citato documento è che, considerando estremamente critica la creazione di queste tecnologie nel settore commerciale civile, risulta essere fondamentale guadagnare competitività come Europa nei confronti dei principali investitori attuali quali USA e Cina. In particolare:

*"(…) Lo sviluppo della digitalizzazione e dell'*Intelligenza Artificiale *nella Difesa (Europea) richiederà necessariamente dei fattori abilitanti, tra i quali un'infrastruttura a supporto, che includa qualsiasi aspetto dall'energia, all'hardware, ai software, alle risorse di networking, così come la garanzia di una elevata quantità e qualità dei dati."*

La digitalizzazione, quindi, offre alle forze armate nuove capacità e opportunità sia sul campo di battaglia fisico che nella *Digital Arena*. La diffusione delle tecnologie digitali aumenta la superiorità delle informazioni e migliora le capacità militari, nonché la solidità e la reattività delle forze armate su un campo di battaglia.

Risale a giugno 2019 il lancio del progetto "*Tactical Edge Networking*" (TEN), con il quale Germania e Paesi Bassi hanno siglato un *Memorandum of Agreement* (MOA) per l'avvio di un processo di digitalizzazione congiunta dei rispettivi eserciti il cui orizzonte temporale è fissato per il 2030 e per il quale il solo *Deutsches Heer* ha stanziato 12 miliardi di Euro. Nato nel 2018 originariamente come il progetto unilaterale tedesco *Digitizing Land-Based Operations* (D-LBO), ha rapidamente acquisito una dimensione bilaterale includendo una serie di sviluppi spiralizzati incentrati sul sostegno ai soldati che operano a livello tattico

9 Ibidem
10 Food for Thought Paper by Finland, Estonia, France Germany and the Netherlands, EDA, 17.5.19

e che hanno manifestato come esigenza primaria l'interoperabilità con le forze delle nazioni alleate.

In un'intervista alla testata Shephard Media[11], Christian Peters, il *Program Manager* del programma TEN-DLBO ha presentato la filosofia del programma, ovvero, consentire ai comandanti di operare in modo sicuro ed essere interoperabili ed efficaci nell'assolvimento delle loro missioni.

> *"(…) Abbiamo bisogno di una mentalità diversa per trovare una soluzione per migliorare il più rapidamente possibile le nostre attrezzature e rinnovare le tecnologie. L'ambizione (del programma) è quella di abilitare le nuove tecnologie dell'informazione ed equipararle ad un Sistema d'Arma primario da schierare in operazioni. (…) Questo è il motivo per cui costruiamo questa nuova struttura bilaterale. Entrambi i ministri della Difesa in Germania e nel Paesi Bassi hanno riconosciuto la necessità di un diverso modo di lavorare e lo hanno riconosciuto con la firma dell'accordo per seguire congiuntamente il percorso di modernizzazione, (…) un traguardo chiave."*

## Approcci all'Intelligenza Artificiale

Prima di affrontare il tema delle applicazioni in campo militare dei paradigmi dell'Intelligenza Artificiale occorre analizzare la differenza tra gli approcci cosiddetti "*machine driven*" e "*data driven*". Il concetto di "*machine driven*" si riferisce al modo in cui una specifica attività viene svolta, ovvero un'attività connessa, automatizzata e controllata da una macchina e dall'attuazione di specifici modelli o algoritmi; coincide con la fase finale del processo di industrializzazione e automazione. Il concetto di "*data driven*", invece, coincide con il passo successivo, ovvero con il vincolare qualsiasi progresso in un'attività ai dati piuttosto che all'intuizione o all'esperienza. Come evidenziato da diversi studi sulla digitalizzazione nelle aziende[12] appare evidente come la trasformazione digitale passi attraverso queste due fasi. Il primo passo è identificare specifiche attività sulle quali applicare l'approccio "*machine driven*" e sulle quali procedere con la digitalizzazione dei dati, ovvero la conversione delle informazioni in un formato digitale leggibile automaticamente. Il risultato sono i dati digitalizzati sotto forma di numeri binari, che facilitano l'elaborazione del computer e altre operazioni guidate dalla macchina.

La digitalizzazione dei dati è di fondamentale importanza per l'elaborazione, l'archiviazione e la trasmissione dei dati poiché consente di trasportare informazioni di tutti i tipi e in tutti i

**11** https://www.shephardmedia.com/news/digital-battlespace/germany-continues-pursuit-tactical-edge-networ/
**12** Data Science Strategy, Ulrika Jägare, John Wiley & Sons, Inc., ed. 2019, p.112

formati con la stessa efficienza. I dati digitalizzati, a differenza dei dati analogici (che in genere perdono qualità ogni volta che vengono copiati o trasmessi), possono, con una ragionevole approssimazione, circolare un numero indefinito di volte senza alcun degrado della qualità. La digitalizzazione, in sostanza, permette di utilizzare tutte le informazioni a disposizione come *input* per l'analisi dei dati, portando a un esponenziale incremento di efficienza dell'organizzazione.

Dopo questa fase di digitalizzazione si può passare all'automatizzazione di una parte dei processi o flussi di lavoro di un'organizzazione; in questo modo, avviene un passaggio di responsabilità della singola azione dall'uomo alla macchina, ma resta in seno all'uomo la decisione dell'approccio e dei passi che la macchina dovrà svolgere. Il passaggio alla fase successiva avviene con l'assegnazione di specifiche capacità alle macchine, le cosiddette intelligenze artificiali, ovvero progettare algoritmi e modelli per sfruttare il patrimonio informativo e realizzare uno specifico target; in questo caso il focus non è più il modo in cui raggiungo un obiettivo, ma l'obiettivo stesso, e impone un passaggio di responsabilità maggiore alla macchina.

**Intelligenza Artificiale militare**

Negli ultimi anni è stata individuata una miriade di possibili applicazioni dell'Intelligenza Artificiale per soluzioni della Difesa e dei sistemi militari, principalmente basati su strumenti complementari all'uomo inteso non solo come soldato nel campo di battaglia ma anche come decisore strategico. I principi trainanti per l'utilizzo delle applicazioni di tali tecnologie includono il raggiungimento di capacità militari superiori, ovvero maggiore efficienza in termini di costi e riduzione del carico di lavoro umano, particolarmente ricercato in un periodo storico di forte contingentamento sul fronte del personale[13].

In particolare, i sistemi informativi militari potrebbero sfruttare gli strumenti di *Data Mining* e Intelligenza Artificiale per derivare i loro aggiornamenti interpolando dati da sistemi di apprendimento automatico, motori di inferenza e strumenti di "*knowledge discovery*". Ciò si può tradurre in un'espansione capacitiva in tutti i settori della Difesa, dall'aumento di consapevolezza del campo di battaglia, all'efficientamento delle risorse, alla previsione di eventi e scenari a supporto dei processi decisionali. Quindi i progressi nel campo del *Data Mining* e dell'Intelligenza Artificiale hanno evidenziato fin da subito i potenziali vantaggi a tutti i livelli della catena di Comando e Controllo.

13 Legge n. 244 del 31/12/2012: "La revisione dello strumento militare".

Già nel 2000 Marion G. Ceruti, *data scientist* del *Navy's Space and Naval Warfare Systems*, intravedeva la possibilità di combinare i progressi tecnologici delle telecomunicazioni, del telerilevamento medico e gli algoritmi di *Data Mining* per sviluppare dispositivi portatili di cui dotare i soldati in grado di identificare potenziali attacchi batteriologici sulla base dei monitoraggi biometrici ed ambientali prodotti dai sensori sul campo[14].

La rete di comunicazioni militari costituisce uno dei pilastri fondamentali per il raggiungimento della superiorità informativa nella *Digital Arena*. Quindi, poter analizzare e valutare l'efficacia di un sistema di comunicazione in operazioni è un elemento cruciale per valutare l'impatto di scelte tecnologiche da implementare. Nasce da questo presupposto uno studio proposto dall'Istituto delle Società di Ingegneria dei Sistemi Elettronici di Pechino[15] che propone un *framework* per il supporto alle decisioni basato sull'Intelligenza Artificiale; in particolare viene analizzata la possibilità di predisporre un *data warehouse*[16] per la valutazione dell'efficacia dei sistemi di comunicazione militari utilizzando diverse sorgenti informative prevenienti da *testbed*, risultati simulati e esercitazioni operative. Sulla base dei dati raccolti e di algoritmi di *Data Mining* viene creato la cosiddetto *Intelligent Decision Support System* (IDSS), ovvero vengono trasformati i dati di efficienza dei sistemi in informazioni di supporto alle decisioni. Vengono inoltre previsti diversi stadi di *Data Mining* potenzialmente applicabili, dalla semplice aggregazione, alla *cluster analysis*[17] fino all'estrazione automatica di informazioni implicite.

Gli algoritmi di Intelligenza Artificiale, *Data Mining* e *Deep Learning* possono, inoltre, essere applicati dalla Difesa nel campo logistico con notevoli potenziali valori aggiunti, in termini di riduzione del carico di lavoro umano, velocizzazione dei processi e supporto alle decisioni strategiche grazie a strumenti di simulazione della sostenibilità logistica in scenari

---

14 M. G. Ceruti, "The relationship between artificial intelligence and data mining: application to future military information systems,"*Smc 2000 conference proceedings. 2000 IEEE international conference on systems, man and cybernetics. 'cybernetics evolving to systems, humans, organizations, and their complex interactions' cat. no.0*, Nashville, TN, 2000, pp. 1875 vol. 3.

15 T. Hong and Z. Jie, "A Framework of Intelligent Decision Support System of Military Communication Network Effectiveness Evaluation," 2008 Fifth International Conference on Fuzzy Systems and Knowledge Discovery, Shandong, 2008, pp. 518-521.

16 In informatica, all'interno dei sistemi informativi, nella pratica della business intelligence per data warehouse si intende in generale una collezione o aggregazione di dati strutturati, provenienti da fonti interne operazionali (DBMS) ed esterne al sistema informativo, utili ad analisi e rapporti informativi, prima adattati tramite strumenti appositi di trasformazione dei dati, e poi analizzati tramite strumenti di analisi di tipo OLAP (query multidimensionali) o data mining, tipicamente ad uso strategico nei processi decisionali.

17 In statistica, il clustering o analisi dei gruppi (dal termine inglese cluster analysis introdotto da Robert Tryon nel 1939) è un insieme di tecniche di analisi multivariata dei dati volte alla selezione e raggruppamento di elementi omogenei in un insieme di dati. Le tecniche di clustering si basano su misure relative alla somiglianza tra gli elementi. In molti approcci questa similarità, o meglio, dissimilarità, è concepita in termini di distanza in uno spazio multidimensionale. La bontà delle analisi ottenute dagli algoritmi di clustering dipende molto dalla scelta della metrica, e quindi da come è calcolata la distanza. Gli algoritmi di clustering raggruppano gli elementi sulla base della loro distanza reciproca, e quindi l'appartenenza o meno a un insieme dipende da quanto l'elemento preso in esame è distante dall'insieme stesso.

operativi. Ad esempio, il campo della manutenzione fornisce un tipico caso d'uso di come le moderne tecnologie possano essere applicate favorevolmente; attraverso una fusione della tecnologia e dell'elevato livello di competenze tecniche del personale manutentore dei Sistemi d'Arma, la Difesa potrebbe essere in grado di fornire ad ogni tecnico le condizioni per operare. Questo porterebbe in primo luogo un aumento dell'efficienza logistica delle linee di manutenzione con una conseguente crescita esponenziale della capacità operativa dello strumento militare; in secondo luogo, usando sistemi basati sulla conoscenza, si avrebbe la possibilità di suggerire *way ahead* sulla base delle decisioni prese in passato in scenari simili in tempi estremamente contenuti[18].

**Sistemi di Comando e Controllo intelligenti**

In quanto centro nevralgico del sistema di combattimento, il sistema di Comando e Controllo in un'analogia anatomica può essere identificato come il cervello di un'operazione militare. Pensare, quindi, a una sua intellettualizzazione è la chiave per migliorare la competitività nel campo di battaglia e garantire ai decisori un *enabler* di immense proporzioni. La graduale applicazione delle tecnologie di Intelligenza Artificiale in campo militare porterà a nuove forme di conflitti, nuove razionalizzazioni di risorse e diversi processi di Comando e Controllo.

La continua espansione della scala e delle dimensioni dei conflitti, unita alla crescente complessità delle operazioni e all'uso di strumenti e Sistemi d'Arma cosiddetti "*unmanned*" impone, quindi, una rivisitazione del concetto di Comando e Controllo; infatti, il Comando e Controllo così come concepito finora, ovvero basato sul controllo uomo-macchina, con il progressivo ampliamento dello scenario multidimensionale (terra, mare, aria, spazio, cyber..) deve ritenersi superato perché sono ampiamente raggiunti i limiti di elaborazione della figura umana del Comandante e delle sue organizzazioni di staff e, pertanto, l'uso delle nuove tecnologie diventerà una delle opzioni inevitabili. Già oggi, un gran numero di attività nel processo di Comando e Controllo potrebbe essere assistito o, persino diretto da strumenti di Intelligenza Artificiale, come, ad esempio, l'interpretazione dei dati di *Situation Awareness*, la generazione dinamica della pianificazione operativa, il controllo agile della risposta ai *task* o la valutazione in tempo reale degli effetti di un'azione in un conflitto.

18 K. A. Carlton, "Artificial intelligence supportability (Air Force application)," in *IEEE Aerospace and Electronic Systems Magazine*, vol. 3, n. 12, pp. 25-32, Dec. 1988.

In un recente studio della *National University of Defence Technology* di Xian[19] sono stati analizzati i principali passi tecnologici da percorrere per una possibile architettura di sistemi di Comando e Controllo intelligenti: in primo luogo devono essere sviluppate elevate capacità di interazione tra l'uomo e le tecnologie di Intelligenza Artificiale attraverso, ad esempio, l'implementazione di sistemi computerizzati indossabili dagli uomini sul campo e la realizzazione di una nuova generazione di software e hardware a supporto dell'interazione efficiente tra soldati e sistemi di Comando e Controllo. Successivamente devono essere potenziati gli strumenti tecnologici che assistono i processi decisionali; nell'era dei dati, è cambiata anche la modalità dei conflitti, che si basano sul concetto di superiorità informativa e sul controllo dei dati. Strumenti di supporto alle decisioni che effettuino rapidamente simulazioni di scenari e assicurino dati ed informazioni al Comandante più velocemente e accuratamente dell'avversario possono determinare l'andamento e l'esito di un'operazione. L'ultimo passo è lo sviluppo di tecniche di previsione e *Situation Awareness* che rispondano alle caratteristiche di complessità e mutevolezza degli scenari futuri di un campo di battaglia. Saranno sempre più necessari strumenti di *Deep Learning* e *computer vision* che applichino modelli cognitivi e incrementino le loro capacità previsionali sulla base dell'esperienza maturata dagli eventi passati. Collateralmente a questo progresso tecnologico è necessario disporre di tecnologie in grado di fondere dati eterogenei, provenienti da svariate fonti e sensori, ed analizzare, mappare e processare specifiche informazioni sulla base della necessità decisionali in maniera del tutto automatica.

### ***Situation Awareness*** **ed interazioni uomo-macchina**

Come anticipato nel paragrafo precedente, con il rapido sviluppo della tecnologia dell'informazione è diventato un tema cruciale per l'esito di un'operazione la disponibilità di una capacità di *Situation Awareness* in grado di estrarre in modo indipendente dati e informazioni, nonché di percepire le situazioni del contesto operativo usando strumenti di *Deep Learning*. L'incremento della capacità computazionale a disposizione unito all'enorme quantità di dati a disposizione fornisce, pertanto, un ottimo ambiente di impiego dell'Intelligenza Artificiale. L'essenza del concetto alla base del *Deep Learning*, infatti, è l'uso massivo di dati di *training* e la costruzione di modelli cosiddetti "a strati annidati" per

19 B. Su, H. Zhao, T. Qi, X. Liu and R. Yu, "Research on Architecture of Intelligent Command and Control System," *2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, Jishou, China, 2019, pp. 362-364.

apprendere efficacemente le caratteristiche dei dati, allo scopo di incrementare l'accuratezza della previsione.[20]

Uno dei principali metodi che sono stati utilizzati negli ultimi anni sono le cosiddette Reti Neurali Convolutive, le quali combinano reti neurali alla teoria del *Deep Learning* nel campo del riconoscimento di immagini. A differenza dei metodi di classificazione tradizionali, le reti neurali convolutive non hanno bisogno dell'intervento manuale di estrazione di oggetti da immagini e quindi, oltre ad assicurare ottimi risultati possono gestire problemi la cui risoluzione manifesta caratteristiche di urgenza. È questo il caso della percezione del campo di battaglia, un processo che in tempo reale riguarda lo schieramento di assetti e l'equipaggiamento di armi basandosi sui dati ambientali (terreno, meteorologia, idrologia) provenienti direttamente dalle truppe sul campo o dalle forze di supporto. Oltre ai processi tradizionali di *intelligence*, sorveglianza e ricognizione, targeting e valutazione del danno, sono sempre più coinvolti anche la condivisione e il controllo dei dati, delle risorse e delle informazioni. Vengono utilizzate queste capacità per comprendere e prevedere scenari e situazioni, controllare l'andamento di un'operazione e trarre vantaggi operativi.

Per mantenere la necessaria competitività nella citata *Digital Arena*, le Forze Armate devono incrementare lo sviluppo di questi sistemi. Negli ultimi anni molti studi hanno analizzato il potenziale impiego di algoritmi di *Deep Learning* per la *situational awareness* di un campo di battaglia[21][22]; in particolare, le principali sfide tecnologiche sono: da un lato la classificazione di *target*, dall'altro il rilevamento e l'identificazione di veicoli a pilotaggio remoto o droni.

La classificazione di target si traduce nell'analisi di immagini provenienti da sensori piuttosto che da *frame* di registrazioni o *live streaming* (cosiddetto *Full Motion Video*). Gli attributi delle immagini (forma, trama, colore e altre informazioni visive, così come scale di invarianza e gradienti) non sono specifici per alcune tipologie di immagini o peculiari di alcuni metodi di classificazione, pertanto, in condizioni di scene complesse e nonostante la varietà di modelli di reti neurali convolutive a disposizione (as esempio LeNet[23], AlexNet, GoogleNet, VGG-Net[24], SENet[25]), è estremamente difficile trovare gli oggetti artificiali che

20 Q. L. Yin and J. W. Wang, "An overview of the application of deep learning in the field of image processing," J. Higher Educ., vol. 1, no. 9, pp. 11–15, Oct. 2018.

21 M. Andrew, "Situational awareness — From the battlefield to the corporation," Comput. Fraud Secur., vol. 9, no. 1, pp. 13–16, Sep. 2016.

22 T. P. Hanratty et al., "Enhancing battlefield situational awareness through fuzzy-based value of information," in Proc. 46th Hawaii Int. Conf. Syst. Sci., vol. 1, n. 1, pp. 13–18, Jan. 2013.

23 Lecun Y, Bottou L, Bengio Y, et al. Gradient-based learning applied to document recognition (J). Proceedings of the IEEE, 1998, 86 (11):2278-2324.

24Karen Simonyan, Andrew Zisserman. Very Deep Convolutional Networks for Large-scale Image Recongnition (C). International Conference of Learning Representation. 10 Apr 2015.

25 Hu J, Shen L, Sun G. Squeeze-and-excitation Networks(J). ar Xiv preprint ar Xiv: 1709.01507, 2017.

descrivano accuratamente l'immagine *target*. La scelta del corretto metodo in funzione del contesto applicativo è fondamentale per assicurare un'identificazione accurata, rapida ed efficace dei target. Un recente studio dell'università di Wuhan[26] ha sviluppato un modello da applicare a un sistema di *Situation Awareness*, allo scopo di identificare le posizioni e classificare cinque tipologie di oggetti sul campo di battaglia (elicotteri, missili, serbatoi, soldati e armi). Tale modello riconosce e categorizza gli obiettivi dalle immagini target risolvendo problemi di regressione tramite le reti neurali convolutive e definendo il livello di confidenzialità della previsione ottenuta. Nei test effettuati sono stati raggiunti livelli di accuratezza di categorizzazione e posizione superiori all'80% e una velocità notevolmente maggiore rispetto ai modelli tradizionali di identificazione di *target*.

Veicoli aerei commerciali a controllo remoto e droni stanno diventando sempre più popolari negli ultimi anni e la loro accessibilità può portare a una serie di problematiche tecniche e di sicurezza dei *environment* strategici, compresi quelli della Difesa. Di conseguenza, il rilevamento e l'identificazione dei droni riveste sempre più un carattere cruciale per il sistema paese e la difesa delle sue istituzioni. In letteratura sono stati proposti diversi approcci al problema, dall'analisi delle emissioni audio a quelle elettromagnetiche, all'analisi visuale; ciascuno di questi presenta restrizioni o limitazioni legate a fenomeni di rumore, distanza o interferenze. Con l'introduzione delle tecniche di Intelligenza Artificiale sono state sfruttate le reti neurali profonde (*Deep Neural Network*) chiamante anche *Multilayer Perceptron* (MLP) per ricercare la presenza di droni attraverso l'analisi di registrazioni a circuito chiuso, immagini di videosorveglianza[27][28] e processando l'effetto doppler generato[29].

In sostanza, la necessità di avere sistemi intelligenti per l'identificazione di *Unmanned Aerial Vehicles* (UAV) e droni con un'adeguata accuratezza è una capacità tecnologica di cui la Difesa dovrà dotarsi per rispondere alle sfide del prossimo futuro, in linea con le linee guida dettate dal CaSMD nel recente concetto strategico[30]:

> *"(…) Un* trend *che implicherà per le Forze Armate la necessità ancora più stringente di mantenere e rafforzare capacità militari maggiormente attinenti alle funzioni di*

26 H. Peng, Y. Zhang, S. Yang and B. Song, "Battlefield Image Situational Awareness Application Based on Deep Learning," in IEEE Intelligent Systems, vol. 35, n. 1, pp. 36-43, 1 Jan.-Feb. 2020.
27 C. Aker and S. Kalkan, "Using deep networks for drone detection," 2017 14th IEEE Int. Conf. Adv. Video Signal Based Surveillance, AVSS 2017, n. August, 2017.
28 N. Shijith, P. Poornachandran, V. G. Sujadevi, and M. M. Dharmana, "Breach detection and mitigation of UAVs using deep neural network," 2017 Recent Dev. Control. Autom. Power Eng. RDCAPE 2017, vol. 3, pp. 360–365, 2018.
29 B. K. Kim, H. S. Kang, and S. O. Park, "Drone classification using convolutional neural networks with merged doppler images," IEEE Geosci. Remote Sens. Lett., vol. 14, no. 1, pp. 38–42, 2017.
30 Il Concetto Strategico del Capo di Stato Maggiore della Difesa, ed. gennaio 2020.

*difesa, ampliandone lo spettro d'azione in maniera progressiva ed elevandone contestualmente la specializzazione capacitiva e tecnologica (…)"*

### ***Intelligence*** **Militare per una Difesa digitale**

L'avanzamento tecnologico nel campo della *Data Analysis* investe anche il dominio dell'*Intelligence,* la cui peculiarità consiste nel ricercare informazioni dai dati a disposizione; con l'incremento dei numeri e delle tipologie di sensori intesi come fornitori di dati si è introdotto il concetto di *Military Intelligence Fusion* (MIF), ovvero l'insieme di processi, metodologie e algoritmi di interpolazione e fusione dei dati militari. Dal punto di vista strettamente militare, la definizione di fusione di informazioni coincide con l'ottimizzazione, la combinazione e l'aggregazione di dati provenienti da diverse tipologie di fonti in una rappresentazione omogenea, allo scopo di ottenere le posizioni accurate di un obiettivo, la stima dello stato di un oggetto sul campo di battaglia, la convalida dell'identità di un individuo, la valutazione della situazione e del livello di minaccia. A differenza del processo consolidato di gestione del ciclo *intelligence,* l'applicazione del concetto di fusione, grazie all'aggregazione di dati eterogenei di diverse sorgenti e all'introduzione del dominio temporale, permette di incrementare il patrimonio informatico complessivo e di correggere gli errori e le imprecisioni di dati provenienti da una fonte fino a quel momento ritenuta autoritativa.

Come ampiamente prospettato da illustri "strategisti" le guerre del prossimo futuro avranno caratteristiche del tutto inedite rispetto a quelle del passato, ovvero multidimensionalità, rapidità, connettività, trasparenza del campo di battaglia; questo impone la disponibilità di nuove capacità tecnologiche anche nel dominio dell'*Intelligence* e della fusione dei dati a scopi militari. Le sfide in questo campo sono molteplici:

- Multidimensionalità: il campo di battaglia delle sfide moderne è esteso e multiregionale e per il buon esito di un'analisi *intelligence* è necessario conoscere una vasta mole di dati dell'intero scenario di operazione.
- Real Time: il cosiddetto *Battle Rhythm* dei conflitti moderni non è mai stato più rapido; questo impone alla capacità *intelligence* una reattività estremamente sfidante che può essere assicurata solo con il supporto di strumenti e tecnologie di *Data Analysis* e *Data Mining* allo stato dell'arte per evitare di arrivare dopo gli avversari;
- Accuratezza: la stessa velocità dei conflitti moderni impone al decisore di rispondere prontamente al cambiamento di scenario con ordini precisi ed efficaci; l'accuratezza, pertanto, è determinante per il risultato di un'operazione ma, a fronte della mole

eterogenea e complessa di dati, è altrettanto difficile da raggiungere vista la vastità del patrimonio informativo a disposizione;

- Disponibilità e affidabilità: raccogliere, decifrare, analizzare dati è a tutti gli effetti il core business di innumerevoli attività e può identificarsi come l'arma vincente per una superiorità strategica, operativa e tattica. Quindi, la disponibilità e affidabilità dei servizi e delle infostrutture che garantiscano queste capacità sono da considerarsi un vincolo per la buona riuscita di una qualsiasi operazione militare moderna.
- Integrazione: i conflitti moderni vedono sul campo di battaglia Sistemi d'Arma estremamente complicati, tecnologicamente complessi il cui valore aggiunto è strettamente legato al dominio netcentrico nel quale operano. Un'*intelligence* Integrata garantisce la necessaria *Situation Awareness* ai diversi attori in gioco a tutti i livelli della catena di Comando e Controllo.

**Minacce cibernetiche e Intelligenza Artificiale**

In questa prospettiva di rivoluzione digitale della Difesa, rivestono carattere strategico gli aspetti relativi alla *Cyber Security*, che sono decisivi non solo nell'uso delle soluzioni di Intelligenza Artificiale per contrastare gli attacchi informatici, ma anche in senso più ampio per contrastare le sfide alla sicurezza derivanti dallo sviluppo di queste tecnologie, come, ad esempio, garantire l'integrità dei dati, fondamentale nella citata "era dei dati".

Negli ulti anni, infatti, nel campo della *Cyber Security* c'è stata una transizione dallo stadio della *Cyber Criminality* a quello della *Cyber War* che ha imposto anche alla Difesa una adeguata transizione delle tecniche di *Cyber Defence* alle tecnologie militari[31]. Innanzitutto, questa transizione riguarda la percezione dell'analisi delle minacce nel cosiddetto modello "*cyber kill chain*", nonché l'applicazione della tradizionale tecnologia di *intelligence* militare. Inoltre, lo scenario cyber attuale presenta potenziali avversari dotati di risorse adeguate e addestrati a condurre campagne di attacco, intrusione e raccolta dati, anche su base pluriennale, rivolte a informazioni di carattere economico, sociale e di sicurezza nazionale. Le tecniche di difesa delle infostrutture critiche che sfruttano la conoscenza di questi avversari possono creare un circuito virtuoso di *feedback* di *intelligence*, che consenta ai difensori di stabilire uno stato di superiorità informativa e

31 ENISA Threats Landscape Report 2016: 15 Top Cyber-Threats and Trends, ENISA, 2017. ENISA Threat Landscape 2017 fornisce una raccolta completa delle 15 principali minacce informatiche incontrate nel periodo dicembre 2016 - dicembre 2017. Il documento contiene le principali minacce informatiche, insieme a informazioni su kill-chain, agenti di minaccia e vettori di attacco. Vengono inoltre fornite alcune informazioni sullo stato di avanzamento di Cyberthreat Intelligence (CTI). https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape.

diminuire la probabilità di successo dell'avversario a ogni successivo tentativo offensivo. Questo livello di ambizione, come palesato dalla maggioranza degli esperti del settore, non può prescindere da una transizione qualitativa ai nuovi strumenti di *Cyber Defence* con un uso diffuso dei metodi di Intelligenza Artificiale per analizzare le informazioni scambiate, i flussi di rete e le fonti di minacce e per pianificare misure efficaci anche di tipo proattivo.

La preparazione dell'*intelligence* in un contesto operativo cibernetico è un processo sistemico e continuo di analisi di possibili minacce per identificare attività sospette che possano intaccare sistemi, reti, informazioni fornendo mezzi per identificare, analizzare e valutare i diversi input provenienti dai sensori della rete. Questo processo, se correttamente implementato, identifica le potenziali minacce e assiste i responsabili della sicurezza dell'organizzazione nel definire le strategie di difesa ideali in funzione degli scenari. Il SANS Institute ha definito il "*Cyber Threats Intelligence*" come un modello a supporto della strategia di gestione del rischio cibernetico di un'organizzazione basato su quattro fasi[32]:

- definizione dell'ambiente operativo inteso come sistemi e strumenti utilizzati;
- dettaglio delle vulnerabilità dell'ambiente operativo e dell'interazione tra i suoi diversi componenti;
- valutazione delle possibili minacce cibernetiche;
- sviluppo delle cosiddette "*Course of Action*".

In quest'ottica le moderne tecniche di Intelligenza Artificiale possono essere considerate fattori abilitanti per lo sviluppo di soluzioni computerizzate autonome che si adattino al contesto operativo, si auto configurino ottimizzando i propri parametri e, nel campo della *Cyber Security,* rappresentano il terreno idoneo per rafforzare le misure di sicurezza del cyberspazio. Nell'ambito della sicurezza informatica le soluzioni di Intelligenza Artificiale possono essere classificate in due categorie:

- metodi distribuiti (agenti *multi-intel*, reti neurali, sistemi immunitari artificiali e algoritmi genetici);
- metodi compatti (*Machine Learning*, metodi associativi, classificazione *bayesiana*[33], algoritmi di riconoscimento di *pattern*, logica *fuzzy*).

Tenendo conto di questa varietà di metodi, è di particolare importanza che vengano selezionati criteri adeguati alla valutazione e selezione di una specifica applicazione in

32 Brian P. Kime Threat Intelligence: Planning and Direction, SANS Institute, 2015.

33 Un classificatore bayesiano è un classificatore basato sull'applicazione del teorema di Bayes. Il classificatore bayesiano richiede la conoscenza delle probabilità a priori e condizionali relative al problema, quantità che in generale non sono note ma sono tipicamente stimabili. Se è possibile ottenere delle stime affidabili delle probabilità coinvolte nel teorema, il classificatore bayesiano risulta generalmente affidabile e potenzialmente compatto. Spesso viene detto "classificatore bayesiano completo" (full Bayes classifier o anche belief network). Per costruzione, il classificatore bayesiano minimizza il rischio di classificazione.

funzione del contesto. Mutuando il contesto dei livelli di Comando e Controllo, anche l'*intelligence* applicata alle minacce cibernetiche può essere sviluppata su tre livelli, strategico, operativo e tattico; ciascun livello avrà specifiche soluzioni di Intelligenza Artificiale che prevarranno sulle altre per il contesto di impiego e gli output desiderati valorizzando il patrimonio informativo a disposizione in funzione delle esigenze.

### *Vulnerability Intelligence*

Nella digitalizzazione della Difesa un elemento cruciale consiste nell'abilità di prevenire minacce cyber adottando strumenti e tecnologie che proattivamente, ovvero sulla base dei sensori sulla rete, catturino, analizzino, condividano dati per decifrare ed anticipare le mosse avversarie. Ai giorni d'oggi, infatti, il codice software distribuito sui Sistemi d'Arma costituisce un elemento cruciale della catena di sicurezza e pertanto deve essere analizzato al pari di qualsiasi altro elemento potenzialmente ostile utilizzabile da un attaccante. Gli utenti di tali sistemi, siano essi satelliti, assetti di 5ª generazione, navi, carri armati, missili balistici, ecc., dipendono nelle loro azioni da una miriade di componenti *software*, eseguiti da diverse piattaforme, più o meno complessi e annidati nei sistemi. Una vulnerabilità in una componente di questa pletora di programmi software può provocare danni o perdite consistenti di dati che, come detto, sono l'indice di superiorità dell'era moderna[34]. Pertanto, la ricerca di strumenti automatici di scoperta di vulnerabilità software ha spinto diverse società del campo dell'Internet Of Things (IoT) a forti investimenti nel settore. La principale criticità è legata al fatto che questo tipo di analisi debba essere svolta su codice binario, dal momento che il software può essere stato offuscato, chiuso o risultare comunque sconveniente da utilizzare per via dei lunghi processi di preparazione e pulizia; in alcuni casi il codice può non essere reso disponibile, in altri le fasi di *software optimization* finalizzate alle performance in fase di elaborazione possono portare a alterazioni della struttura del programma creando un disallineamento tra il codice sorgente ed il file effettivamente compilato. Un'analisi di tipo binario, invece, permette di tenere traccia delle fasi di esecuzione del programma ed è utilizzato in diversi altri contesti rispetto all'analisi di vulnerabilità quali, ad esempio, la ricerca di codice clonato o la rilevazione di malware; di contro, per una efficace ed efficiente analisi binaria è fondamentale l'implementazione di approcci basati sull'Intelligenza Artificiale sfruttando modelli di *Deep Learning*.

34 S. M. Ghaffarian and H. R. Shahriari, "Software vulnerability analysis and discovery using machine-learning and data-mining techniques: A survey" ACM Comput. Surv., vol. 50, n. 4, 2017, Art. n. 56

Uno dei primi esperimenti in questa direzione è stato pubblicato a marzo 2020[35] ed è frutto di una cooperazione tra università australiane e cinesi; è stato evidenziato come sia possibile identificare vulnerabilità dal codice binario attraverso due fasi: l'estrazione di funzioni binarie e la costruzione di un modello appropriato di predizione.

In questo quadro di complessità, dinamicità e scala dei moderni scenari geopolitici nei quali è integrata la Difesa, sono sempre più presenti strategie di attacco informatico e cosiddetti *Autonomous Intelligent Malware* (AIM); nel caso in cui questi attacchi cibernetici dovessero avere successo nell'inconsapevolezza degli operatori umani o nell'incompetenza tecnologica per poterli affrontare tempestivamente, verrebbe compromesso l'esito di una missione o un'operazione. Pertanto sono sempre più necessarie nuove dottrine e tecnologie di difesa cibernetica autonoma. In ambito NATO è stata introdotta la cosiddetta *Autonomous Cyber Defence* (ACyD), un nuovo campo di ricerca tecnologica guidato dal dominio militare orientato a prevedere le potenziali minacce a infrastrutture, sistemi e operazioni militari. Tale approccio è basato sulla *Autonomous Intelligent Cyber-Defence Agents* (AICA) *Reference Architecture*[36] e prevede l'implementazione di sciami di agenti distribuiti nelle reti che combattono autonomamente gli AIM.

### *Blockchain* per la Difesa

Quanto finora prospettato in termini di potenziali capacità esprimibili con lo stato dell'arte della tecnologia informatica e le sue prospettive future richiede soluzioni sicure, robuste ed affidabili di protezione e di scambio del patrimonio informativo. Al riguardo, il dominio tecnologico della "*Blockchain*"[37] offre un terreno fertile per una rivisitazione dei modelli di sviluppo del sistema militare nel suo complesso. Come già ampiamente trattato precedentemente, l'elemento cruciale per un "sistema Difesa" competitivo nello scenario geopolitico contemporaneo è la disponibilità di sistemi di Comando, Controllo, Computer, Comunicazione e *Intelligence* che non trascuri anche gli aspetti *Cyber*, alla luce delle

35 S. Liu, M. Dibaei, Y. Tai, C. Chen, J. Zhang and Y. Xiang, "Cyber Vulnerability Intelligence for Internet of Things Binary," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2154-2163, March 2020.

36 A. Kott, P. Theron, M. Drašar, E. Dushku, B. LeBlanc, P. Losiewicz, A. Guarino, L. V. Mancini, A. Panico, M. Pihelgas and K. Rzadca, "Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture, Release 2.0," US Army Research Laboratory, Adelphi, MD, 2019.

37 La blockchain (letteralmente "catena di blocchi") è una struttura dati condivisa e immutabile. È definita come un registro digitale le cui voci sono raggruppate in blocchi, concatenati in ordine cronologico, e la cui integrità è garantita dall'uso della crittografia. Sebbene la sua dimensione sia destinata a crescere nel tempo, è immutabile in quanto, di norma, il suo contenuto una volta scritto non è più né modificabile né eliminabile, a meno di non invalidare l'intera struttura. Tali tecnologie sono incluse nella più ampia famiglia delle Distributed Ledger, ossia sistemi che si basano su un registro distribuito, che può essere letto e modificato da più nodi di una rete. Le caratteristiche che accomunano i sistemi sviluppati con le tecnologie Blockchain e Distributed Ledger sono digitalizzazione dei dati, decentralizzazione, disintermediazione, tracciabilità dei trasferimenti, trasparenza/verificabilità, immutabilità del registro e programmabilità dei trasferimenti.

potenziali fragilità dei sistemi in termini di attacchi cibernetici e manipolazione incontrollata di dati; concetto riassumibile dall'acronimo C5ISR. La manipolazione dei dati, infatti, è il *core business* dei sistemi decisionali basati su grosse quantità di dati, quindi, la tracciabilità e la trasparenza di tali processi è fondamentale per un output affidabile ed efficace per le decisioni. Sebbene i moderni *data base* offrono strumenti e funzionalità specifiche per combattere questo tipo di minacce, la vulnerabilità persiste al livello di trasporto e rete di comunicazione. A questo livello entrano in gioco le soluzioni basate sul modello *blockchain*, in ampia diffusione in diversi settori commerciali per archiviare, organizzare ed elaborare le informazioni in modo sicuro. Il paradigma della decentralizzazione tipico della *blockchain* da un lato migliora l'accessibilità dei dati, dall'altro irrobustisce l'architettura rendendo l'intero sistema più resiliente agli attacchi. Infatti, gli approcci basati sulla decentralizzazione connettono nodi della rete distribuiti geograficamente e dotati dello stesso livello di capacità, garantiscono transizioni tra nodi solamente se approvate attraverso una collaborazione tra diverse entità, bloccano qualsiasi richiesta che non venga considerata valida da specifici controlli di sicurezza e assicurano l'accessibilità ai dati anche in caso di inefficienza o perdita di un nodo della rete. Implementare soluzioni tecnologiche nativamente integrate con il paradigma *blockchain* implica, quindi, un cambio di direzione nello sviluppo di sistemi militari che aggiunga al concetto di "*security by design*" quello di "*secure data manipulation by design*" che quindi sposta il focus della sicurezza alle interazioni tra sistemi e non solo sui sistemi stessi.

### *Environment* Strategici digitali

La proiezione strategica della Difesa a un modello "digitale" non può prescindere dalla ridefinizione di quelli che possano essere ritenuti gli *environment* strategici digitali del Dicastero. A fronte di un tale cambio di paradigma che vede il possesso e la condivisione controllata di informazioni l'arma vincente per una superiorità a tutti i livelli, risulta fondamentale l'introduzione di nuove priorità in termini di *assets* strategici da proteggere. Questo approccio rispecchia pienamente quanto previsto dal DL 105/2019 in materia di "Perimetro di sicurezza nazionale cibernetica"[38] a tutela di tutti quei soggetti e servizi che svolgono o assicurano funzioni essenziali dello Stato.

**38** Il D.L. 105/2019 ha istituito il perimetro di sicurezza nazionale cibernetica, con il fine di assicurare la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato o la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, o dall'utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

I vantaggi descritti finora nel campo del *Decision Making*, *information sharing*, Intelligenza Artificiale, *Data Analysis* e *Data Mining* dipendono da quanto i dati a disposizione della Difesa siano visibili, accessibili, interpretabili, affidabili ed interoperabili. I proprietari dei dati e le corrispondenti comunità di interesse (ISR, *Air*, *Maritime*, *Land*, finanziario, logistico, sanitario, personale, ecc.) sono i responsabili della disponibilità dei dati di competenza quali fonti autoritative. In questo scenario, i Sistemi *hardware*, strumenti *software*, registri, algoritmi e processi che assicurino questo servizio essenziale possono essere considerati *environment* strategici.

La Difesa dispone di centinaia di installazioni, strutture, edifici per mezzo dei quali conduce operazioni in tutte le "*business area"*, al punto da poter essere assimilata ad una complessa rete di relazioni; migrare al paradigma di una Difesa digitale impone una maggiore sinergia nei nodi di questa rete relazionale. Dal punto di vista informatico, questa maglia si concretizza in centinaia di sistemi operativi e *data center*, migliaia di *server* e decine di migliaia di *workstation* e dispositivi mobili; lo sforzo dovrà essere quello di un coordinamento per una maggior interoperabilità, condivisione di informazioni e, ove necessario, capacità computazionale.

I benefici attesi dall'implementazione delle tecnologie emergenti finora descritte (*Big Data Analytics*, *Deep Learning*, *Machine Learning*, IoT...) possono essere raggiunti solamente con la disponibilità di una info-struttura adeguata nel suo complesso, anch'essa definibile strategica. L'ammodernamento non può prescindere da un incremento delle reti in termini di *performance*, capacità di banda, agilità e sicurezza preferendo soluzioni a ridotto impatto economico e a limitata complessità che favoriscano soluzioni consolidate, efficienti e sicure in grado di affrontare le sfide operative attuali e future.

Anche il comparto *mobile* dovrà mantenere il passo con l'evoluzione tecnologica che può garantire opportunità impensabili nel recente passato dal punto di vista dei vantaggi operativi della Difesa. Infatti, attraverso un rapido accesso all'informazione da ogni posizione e all'elevata capacità computazionale dei dispositivi portatili, le unità sul campo possono essere sempre più in grado di operare in contesti ostili grazie a dati disponibili in tempo reale e strumenti situazionali ricchi di livelli informativi costantemente aggiornati, le forze amiche possono essere identificate con una elevatissima precisione limitando al minimo fenomeni fratricidi, le strumentazioni a disposizione del soldato possono aumentare il patrimonio informativo a disposizione dei decisori; più in generale, con la tecnologia mobile possono essere espresse capacità abilitanti per il successo di un'operazione nella *Digital Arena* al punto da considerarla parte integrante degli *environment* strategici digitali della Difesa da salvaguardare.

**Portfolio Strategico di una Difesa Digitale**

Lo sviluppo e il rilascio di capacità digitali con elevati indici di efficienza e performance prevede una ridefinizione dei processi dell'intero sistema della Difesa; in particolare, la valutazione e l'implementazione di soluzioni tecnologiche, opportunamente sostenute sul fronte economico, devono subire una forte accelerazione e avere necessariamente carattere *Joint* piuttosto che orientata alle singole componenti, allo scopo di ottimizzare gli investimenti e il ritorno in termini di capacità prodotte e disponibili. La *vision* è quella di assicurare ai comandanti militari, alla *leadership* politica, ai soldati sul campo di battaglia e ai partner di coalizione l'accesso alle informazioni e ai dati a disposizione in modo sicuro, affidabile e agile al fine di assicurare un efficace sistema di Comando e Controllo delle forze durante le operazioni nel cyber spazio.

I passi propedeutici alla creazione di un ambiente in grado di rispondere prontamente alle sfide finora citate sono legate ad una precisa strategia di gestione delle risorse informative della Difesa; in prima battuta dovranno essere ottimizzati i *data center* attraverso un puntuale processo di validazione, armonizzazione, clusterizzazione e migrazione dei sistemi e degli strumenti, allo scopo di aumentare le performance e ridurre i costi di gestione. Anche la rivisitazione degli strumenti di *Office Productivity*, le piattaforme di collaborazione e le capacità *voice* e *video* costituisce un passaggio fondamentale per una Difesa Digitale e un incremento di interoperabilità nel rispetto degli aspetti di *Cyber Security*, con una conseguente razionalizzazione delle ridondanze, l'incremento di efficienza del sistema Difesa complessivo e un ingente risparmio economico che permetterebbe un maggior investimento nel campo delle tecnologie emergenti.

Il problema di progettare un efficiente sistema di Difesa è stato più volte oggetto di studi di diversi analisti nell'ottica di pesare gli elementi in gioco. Una metodologia che viene spesso impiegata in questo settore è l'ottimizzazione del cosiddetto portafoglio strategico, in base alla quale l'obiettivo dell'analisi dovrebbe portare alla selezione di un insieme diversificato di assetti che massimizzi il ritorno dell'investimento iniziale; nella fattispecie del campo della Difesa, l'utile sul capitale investito si traduce in termini di capacità operative che gli investimenti produrranno. Mentre le tecniche di ottimizzazione del portafoglio, in generale, sono ben consolidate, le applicazioni nel settore della Difesa, come descritto in precedenza, pongono sfide uniche e inedite in altri domini applicativi.

Gli obiettivi della Difesa, in generale, sono diversificati tra loro, difficilmente riducibili a valori singoli quantificabili, specifici in funzione della missione da assicurare o dell'ambiente

operativo in cui si opera e, più in generale, caratterizzati da un certo livello di incertezza legato anche alle interdipendenze tra le diverse capacità; inoltre, la scelta dell'ottimo in termini di applicazioni e tecnologie nel settore della Difesa, a differenza di una statica teoria dei giochi, risente di una complessità aggiuntiva legata ai diversi livelli di approvazione e supervisione durante il processo decisionale. Una interessante panoramica delle principali sfide associate alla definizione di un portafoglio dei sistemi della Difesa è stata ampiamente affrontata di recente da un gruppo di ricercatori dell'università di Canberra supportata dal DoD australiano[39]; l'output dell'analisi ha portato ad una classificazione delle sfide secondo criteri di incertezza (scenario, distribuzione geografica,..), di valutazione (costo, gestione del rischio, opportunità,..), di dinamicità (variabilità nel tempo, tecnologie in arrivo,..), di vincoli in essere ( economici, categorico, temporali,..) e di molteplicità di obiettivi (goal setting, importanza della partecipazione).

Di certo, la variabilità che caratterizza lo scenario tecnologico attuale impone un processo di sviluppo e rilascio capacitivo che sia al passo con i tempi, ovvero che garantisca a tutti i livelli la tecnologia idonea per la superiorità informativa. Questo vincolo riflette la perenne sfida dei processi di acquisizione che tipicamente impediscono di adottare nuove tecnologie in tempi brevi: un approccio per affrontare questa problematica ci viene offerto dalla strategia per la digitalizzazione della Difesa americana[40], che prevede una razionalizzazione del processo di approvazione delle soluzioni tecnologiche sfruttando pratiche di sviluppo tecnologico tipiche dell'ingegneria digitale.

### Info-struttura della Difesa e *Covid-19*

Per far fronte all'emergenza epidemiologica da *Covid-19*, i provvedimenti che si sono succeduti hanno prodotto disposizioni volte a favorire il ricorso al lavoro agile, cosiddetto "*smart working*". In particolare l'art. 87 del Decreto Legge n. 18 del 2020 disponeva che, per il periodo dello stato di emergenza, il lavoro agile costituisse la modalità ordinaria di svolgimento della prestazione lavorativa delle pubbliche amministrazioni le quali, pertanto:

- limitano la presenza del personale negli uffici per assicurare esclusivamente le attività che ritengono indifferibili e che richiedono necessariamente la presenza sul luogo di lavoro, anche in ragione della gestione dell'emergenza[41];

39 K. R. Harrison et al., "Portfolio Optimization for Defence Applications," in IEEE Access, vol. 8, pp. 60152-60178, 2020.

**40** DoD Digital Modernization Strategy, DoD Information Resource Management Strategy Plan FY 19-23, ed. jul 12, 2019, p.27-28

41 Il Dipartimento della funzione pubblica ha avviato il monitoraggio dello stato di attuazione del lavoro agile nelle pubbliche amministrazioni nel periodo gennaio-aprile 2020, finalizzato a verificarne la diffusione prima e dopo l'emergenza COVID-19.

- consentono che la prestazione lavorativa in lavoro agile si svolga anche attraverso strumenti informatici nella disponibilità del dipendente qualora non siano forniti dall'amministrazione stessa[42].

Questa condizione globale di emergenza che ha visto un'esplosione del numero di lavoratori in modalità agile, ivi compresi una quota parte del personale della Difesa in grado di lavorare in efficienza anche in modalità remota, è paragonabile a una accademia a cielo aperto, a livello nazionale, che ha consentito contestualmente il distanziamento fisico e la vicinanza sociale attraverso le info-strutture a disposizione; queste info-strutture si sono dimostrate *assets* strategici per gran parte delle attività produttive, formative e istituzionali a garanzia di un sistema paese costantemente attivo nonostante le condizioni emergenziali. Nei casi in cui l'info-struttura non si è dimostrata adeguata a sostenere i processi delocalizzati questo ha implicato forti rallentamenti in termini di operatività con conseguenze drasticamente negative sulla produttività dell'organizzazione coinvolta.

Inoltre, la precipitosa migrazione verso lo svolgimento del lavoro in forma digitale, portata dalla pandemia, è esplosa in un momento storico di profonda trasformazione dei sistemi produttivi. La cosiddetta quarta rivoluzione industriale aveva già accelerato i processi di digitalizzazione i cui obiettivi a medio-lungo termine andavano nella direzione di una connettività totale (tutto è interconnesso secondo il paradigma *anything, anywhere, anytime*), della raccolta, elaborazione ed utilizzo di una grande massa di dati e delle "*Smart Factories*", fabbriche intelligenti operate dall'Intelligenza Artificiale.

In questa prospettiva, lo *smart working*, implica una riorganizzazione del lavoro in termini di reingegnerizzazione dei processi basata sulle tecnologie digitali ovvero di inserimento in questi processi del lavoro a distanza in termini di complementarietà del lavoro in presenza in funzione delle diverse fasi dei processi. Senza una tale riorganizzazione si rischia di mappare, con un approccio miope, l'attività in lavoro agile come la sola quota parte che può essere svolta in un luogo diverso da quello abituale con il supporto degli stessi strumenti normalmente a disposizione.

42 In tali casi l'articolo 18, comma 2, della richiamata legge n. 81 del 2017, secondo cui il datore di lavoro è responsabile della sicurezza e del buon funzionamento degli strumenti tecnologici assegnati al lavoratore per lo svolgimento dell'attività lavorativa, non trova applicazione.

# Capitolo 2

# Il fattore umano per una Difesa digitale

## Coltivare talenti digitali

Una delle grandi aspettative sul futuro è quella sull'Intelligenza Artificiale, che, come ampiamente analizzato nel corso di questo studio, coincide con la possibilità di approssimare per via tecnologica alcune funzioni cognitive dell'essere umano. Queste tecniche hanno avuto una crescita esponenziale legata per lo più alla enorme disponibilità di dati e di grandi capacità di calcolo. Risulta però ancora lontana la comprensione profonda del linguaggio naturale e di tutte le sue peculiari caratteristiche per cui l'unica opportunità attualmente perseguibile per trarre vantaggi effettivi da queste tecnologie emergenti è quella di riuscire a integrare le capacità intellettive e di apprendimento basate sulle reti neurali, ambito in cui l'Intelligenza Artificiale è estremamente competitiva, con la capacità di ragionare, tipica dell'intelligenza umana.

I sistemi di apprendimento automatico ampiamente descritti di *Machine Learning* e *Deep Learning* approssimano in modo sempre più efficace le capacità intellettive di riconoscimento e classificazione di dati sensoriali. Secondo l'*AI Index Annual Report* della *Stanford University*[43], già nel 2018 l'Intelligenza Artificiale ha equiparato e in alcuni casi superato l'intelligenza umana nel riuscire a riconoscere le immagini. Nell'ultimo biennio diverse società di *Business Analytics* hanno cercato di mappare i possibili ambiti di impiego delle tecnologie legate all'Intelligenza Artificiale; ad esempio, uno studio della società *Cognilytica LLC*[44] ha identificato sette filoni interessati al cambiamento quali: riconoscimento immagini, interazioni e conversazioni con umani, analisi predittive e supporto decisionale, sistemi orientati agli obiettivi, sistemi di guida autonoma, ricerca di anomalie e pattern significativi, profilazione e classificazione degli individui.

Per gestire questo portafoglio di potenziali capacità tecnologiche e tradurle in valore aggiunto per la Difesa vi è la necessità di guidare il processo dall'interno dell'organizzazione, attraverso competenze specifiche che permettano di affrontare il cosiddetto *skill-gap*[45] e gestire la trasformazione verso la digitalizzazione. Vi è pertanto la necessità di dotarsi di figure strategiche nel processo di trasformazione digitale che conoscano l'ambiente applicativo, le tecnologie emergenti e sappiano estrarre dai dati le informazioni utili.

43 http://cdn.aiindex.org/2018/AI%20Index%202018%20Annual%20Report.pdf;
44 https://www.cognilytica.com/2019/04/04/the-seven-patterns-of-ai/;
45 https://www.bloomberg.com/graphics/2016-job-skills-report/;

Uno studio del *World Economic Forum* del 2018[46] ha mappato le principali capacità tecniche che verranno richieste nel 2022 proiettando il trend tecnologico in essere nel settore civile. Le principali evidenze sono legate al fatto che il progresso tecnologico ha portato a una progressiva accelerazione del processo di gestione del cambiamento, al punto da richiedere alle organizzazioni, al mondo aziendale e ai singoli lavoratori di approcciarsi in modalità proattiva ad una nuova modalità di lavoro; si dovrà essere nelle condizioni di guidare i cambiamenti, accelerare l'adozione di tecnologie emergenti, investire nel mondo della robotica a supporto dei processi e cambiare i ruoli e le mansioni degli attuali lavoratori con una conseguente spinta al cosiddetto *re-skilling*. Nella classifica delle dieci capacità emergenti di cui non si potrà fare a meno nel 2022 vi sono, in ordine, *Data Analysts and Scientists*, specialisti in Intelligenza Artificiale e *Machine Learning*, *Big Data Analysts*, *Digital Transformation Analysts* e *New Technology Specialists*.

Il focus della problematica alla base del processo di trasformazione digitale consiste nel coltivare talenti digitali che non comprendano solamente argomenti spiccatamente tecnici, ma anche tecnologici e culturali, in grado di vincere la fisiologica resistenza al cambiamento tipica di una sfida organizzativa dal carattere sostanziale e ben descritta dal premio Nobel per l'economia Milton Friedman che la paragona a una tirannia[47].

L'obiettivo, quindi, è diffondere la cultura digitale che possa portare tutti gli elementi dell'organizzazione a sentirsi parte del cambiamento; se da un lato è fondamentale dotarsi delle opportune competenze per guidare i processi di trasformazione digitale, dall'altro è altrettanto importante dotare gli altri elementi dell'organizzazione degli strumenti per accogliere il cambiamento tecnologico.

Nel 2019 l'Università La Sapienza di Roma in collaborazione con la *Business School Master and Skills* ha avviato un esperimento sociale durante il quale ha campionato circa cinquecento professionisti nel campo dell'analisi dei dati sondando la loro confidenza nei confronti di trenta temi legati alle seguenti aree funzionali: business, tecnologia, progettuali, matematiche e sistemiche; i risultati di tale campionamento statistico hanno evidenziato quanto siano variegate le competenze di figure professionali appartenenti alle stesse classificazioni (manager, sviluppatori, creativi e ricercatori) e di come non sia possibile disporre di tutte le competenze in un unico profilo. Ciascuna tipologia di figura professionale si caratterizza per un approccio al problema tecnologico da un preciso punto di vista che porta ad un'analisi il cui valore aggiunto può essere sostanziale solo se messo a fattor

46 http://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf;
47 Friedman, M. and Friedman R.D., "Tyranny of the Status Quo", 1985, Harpercollins;

comune con gli altri. Da un lato i manager approcciano il problema tecnologico dal punto di vista della governance, del business e del budget, gli sviluppatori sono orientati dagli aspetti tecnologici e progettuali, mentre i ricercatori si concentrano sugli aspetti matematici e sistemici. Questo, come molti altri studi di settore, evidenzia quanto si debba puntare su un portafoglio capacitivo anche sul fronte del personale al fine di rendere efficiente il sistema Difesa nel suo complesso attraverso una elevata trasversalità di competenze e *background*. Una delle professionalità fondamentali nel processo di digitalizzazione di un'organizzazione complessa come la Difesa è quella del cosiddetto *Innovation Manager*: si tratta di una figura ibrida, orizzontale, con competenza tecnologiche, manageriali e di analisi quantitativa che comprenda le potenzialità di una nuova tecnologia e le sappia applicare con efficacia nel contesto organizzativo sfruttando al meglio l'intero portafoglio capacitivo a disposizione.

Questa necessità riveste ancora più importanza a fronte dello scenario estremamente competitivo tipico della *Digital Arena* che richiede un continuo adattamento del potenziale tecnologico ed è caratterizzato da una elevata variabilità dei requisiti operativi; risulta fondamentale quindi disporre di un idoneo portafoglio capacitivo in termini di risorse umane professionalmente competenti e addestrate sul dominio applicativo per garantire una interpretazione univoca di concetti, principi, e applicazioni e poter valorizzare e difendere il dominio informativo della Difesa, rispondendo alle esigenze di *Cyber Security* attraverso una ridefinizione del concetto di prontezza militare.

### Sinergia con Università e Industria nazionale

L'importanza di una sistemica digitalizzazione è stata recepita in modalità incrementale da diversi Stati, organizzazioni internazionali e nazionali che hanno avviato programmi di ricerca e sviluppo orientati ad un approccio sinergico che raccordi tecnologie, competenze e sistemi, e produca capacità.

Ad esempio, nel documento programmatico pluriennale della Difesa per il triennio 2018-2020, il Ministro della Difesa sottolineava l'importanza di una visione sistemica che integri competenze specialistiche nel settore industriale della Difesa, dell'Università e dei settori di ricerca ed industria[48]. L'anno successivo nel documento programmatico pluriennale della Difesa per il triennio 2019-2021[49] veniva marcata l'importanza di una stretta collaborazione con gli altri Ministeri/Organismi e del supporto dell'accademia, dell'industria, della ricerca e dei settori pubblico e privato, presupposti per consentire il transito concettuale

48 Documento Programmatico Pluriennale per la Difesa per il triennio 2018-2020, Ministero della Difesa, ed. 2018;
**49** Documento Programmatico Pluriennale per la Difesa per il triennio 2019-2021, Ministero della Difesa, ed. 2019;

e operativo dalla attuale concezione a Forze Armate 4.0, cioè adatte ad affrontare in maniera efficace, efficiente e sostenibile il "nuovo" che avanza; in particolare:

> *"Essere 4.0 significa dotarsi di uno strumento "persistente e a potenza variabile", facilmente modulabile per essere impiegato nell'intero spettro delle moderne minacce – dall'ibrido, alla sicurezza cyber-energy, alla hyperwar[50], senza naturalmente dimenticare le più classiche situazioni di crisi convenzionali."*

In tale contesto, l'incredibile velocità di sviluppo e diffusione delle cosiddette *emerging e disruptive technologies* identificate accademicamente con l'acronimo BRINE[51], e la sempre più estesa disponibilità di tecnologie digitali per uso militare, rendono via via più difficoltoso il mantenimento del vantaggio tecnologico della Difesa, acuendo l'esigenza di strutturare in maniera sinergica la cooperazione con il mondo accademico e l'industria.

Nel recente piano nazionale innovazione 2025 uno dei tre obiettivi alla base della sfida dello sviluppo inclusivo e sostenibile è il seguente:

> *"L'automazione e l'innovazione stanno trasformando il mondo del lavoro, contribuendo alla creazione di nuovi lavori che richiedono nuove competenze e aggiornamento continuo. Percorsi di formazione verso gli studenti ma anche formazione continua e reskilling dei lavoratori, così come forme di tutela dei lavoratori impegnati nelle nuove tipologie di lavoro, permettono di sviluppare le competenze necessarie per far fronte ai lavoratori del futuro."*[52]

Questo crescente coinvolgimento del mondo universitario e della ricerca, costituisce l'ambiente ideale non solo per lo sviluppo di tecnologie e sistemi, ma anche per formare e aggiornare il patrimonio di competenze del fattore umano necessario alla Difesa per il salto tecnologico, sistemico e organizzativo verso la digitalizzazione. D'altro canto, in questo processo l'industria nazionale riveste un ruolo fondamentale perché trasforma e raccorda tecnologie in capacità esprimibili dalla Difesa. Solo l'adozione di un piano strategico che garantisca la massima sinergia di questi tre pilastri, Difesa, accademia ed industria nazionale, potrà rispondere alla competitività internazionale nel campo della *Digital Arena* garantendo la progettazione di sistemi e soluzioni integrate *ab initio* con un lungimirante sguardo al futuro.

---

50 "Progressiva sostituzione dell'elemento umano nel processo decisionale nel c.d. Observe-Orient-Decide-Act (OODA) loop con elementi tecnologici a complessità e autonomia crescenti", ibidem

51 Biology, biotechnology and medicine; Robotics, artificial intelligence, new smart weapons, and human enhancement; Information and Communication Technology (ICT), surveillance and cognitive science; Nanotechnology and advanced materials; and Energy technology.

52 Piano nazionale innovazione 2025, Ministero per l'Innovazione Tecnologica e la Digitalizzazione, Release Stabile, 13 febbraio 2020. https://innovazione.gov.it/assets/docs/MID_Book_2025.pdf p.7.

Lo scenario finora descritto evidenzia chiaramente l'esigenza di incrementare lo scambio di informazioni in termini di "domanda tecnologica" e "offerta" delle tecnologie emergenti e dirompenti già disponibili o in corso di sviluppo, allo scopo di incentivare le sinergie tra i Centri di ricerca militari e civili, le Università, i Distretti e i Poli Tecnologici, l'industria nazionale, il mondo finanziario e le analoghe realtà internazionali. Un fattore abilitante è necessariamente la condivisione degli obiettivi sulle tecnologie in fase di sperimentazione, per favorire una forma di cooperazione strutturata già nelle fasi iniziali dell'innovazione tecnologica dove la curva degli investimenti raggiunge il picco. Per quanto riguarda gli scopi prettamente militari questa condivisione non può che essere guidata dalla Difesa a cui è richiesta una postura strategica che imponga priorità in termini di attività di ricerca in funzione delle esigenze capacitive; contestualmente deve esserci uno sforzo da parte della Ricerca pubblica nell'intercettare le linee di interesse militari e delle imprese per garantire un accesso conveniente alle Ricerca e al trasferimento tecnologico.

**Innovazione proattiva**

La principale sfida che le ampiamente citate tecnologie emergenti e dirompenti pongono sullo scenario della Difesa, riguarda la necessità sostanziale di non perdere terreno nei confronti dei potenziali competitor; pertanto, la costante collaborazione tra Difesa, Università e industria nazionale descritta nel paragrafo precedente costituisce la condizione necessaria affinché l'innovazione di sistemi e assetti non rincorra le capacità tecnologiche disponibili sul mercato ma si faccia portatrice di idee e intuizioni dal carattere proattivo sulle quali la sinergia tra accademia e componente industriale possono portare un enorme valore aggiunto.

In Italia la ricerca nel campo dell'Intelligenza Artificiale presenta dei picchi di eccellenza in specifici settori che fanno percepire le intrinseche capacità del Sistema Paese di affrontare tematiche così spinte e all'avanguardia; quindi, nella cosiddetta "corsa all'Intelligenza Artificiale militare" a cui si assiste in campo internazionale, l'Italia potrebbe esprimere importanti capacità. Il fattore abilitante, pertanto, non è la specializzazione in settori tecnologicamente avanzati, ma piuttosto nella capacità di avviare un circolo virtuoso di trasferimento tecnologico nel vasto ecosistema di attori coinvolti (università, centri di ricerca pubblici e privati, *Competence Center*, *Technology Cluster*, *Digital Innovation Hub*, poli tecnologici). In primo luogo devono essere quindi favoriti i luoghi, fisici e virtuali, dove esploratori, *Data Scientist*, esperti del domino applicativo possano interfacciarsi, identificare opportunità, creare nuovi modelli di business e moltiplicare le capacità singole;

successivamente deve essere garantito, nell'ambito del contesto applicativo di riferimento, un ambiente di produzione stabile che consenta a strumenti e algoritmi di funzionare come parte integrante della realtà operativa dell'organizzazione.

Nell'ambito del processo di digitalizzazione della Difesa questo si traduce nella possibilità per un piccolo nucleo di personale, opportunamente supportato dall'organizzazione e in coordinamento sinergico con l'ecosistema abilitante, di fare la differenza e diventare volano per lo sviluppo di nuove capacità operative e stimolo per altri elementi dell'organizzazione. Viene pertanto ribaltato il concetto che l'asimmetria tipica del dominio cibernetico sia un elemento esclusivamente negativo, a favore di un approccio che sfrutti le competenze giuste nelle corrette posizioni, allo scopo di guadagnare resilienza nel mondo cibernetico ed espandere la competitività nella Digital Arena. In linea del tutto teorica, così come un singolo individuo può costituire una minaccia per uno Stato in un contesto di lotta asimmetrica, una singola unità della Difesa può diventare una risorsa strategica per assicurare la missione dell'organizzazione e garantire senza soluzione di continuità l'esercizio della funzione essenziale di difesa dello Stato.

**Il problema etico**

In un contesto globale dominato dalla crescente rivalità tra Stati Uniti e Cina, l'Unione Europea si è gradualmente ritagliata un ruolo di difensore dell'uso responsabile della tecnologia, nonché di un approccio teso a considerare tecnologie emergenti come l'Intelligenza Artificiale come mezzo e non come fine. Lo sforzo di orientare lo sviluppo normativo in questo ambito ha progressivamente spostato l'attenzione dal tema dell'etica dell'Intelligenza Artificiale al più ampio dibattito internazionale relativo alla sua affidabilità, essenzialmente basata sulla necessità di proteggere i diritti fondamentali dell'individuo e sullo sviluppo sostenibile.

Con il recente documento di proposte per una strategia digitale[53] l'Italia tenta di definire un piano strategico nazionale in risposta al citato sforzo della Comunità Europea; in particolare:

> *"A fronte della pandemia, di un tessuto industriale da rivitalizzare e di un'emergenza sociale che si presenza quasi impossibile da fronteggiare, l'Italia ha la possibilità di ritrovarsi come sistema paese in grado di governare la tecnologia digitale e utilizzarla per modernizzare l'amministrazione pubblica.(…) Tutti i paesi industriali e gli esperti concordano nel considerare l'*Intelligenza Artificiale *come un'opportunità senza*

53 Proposte per una Strategia italiana per l'intelligenza artificiale, MISE, 2020

*precedenti per incrementare la produttività del lavoro e consentire progressi straordinari (…) Allo stesso tempo vi è la consapevolezza che può , se utilizzata in modo incauto, generare notevoli rischi per la società, per la Democrazia e per l'ordine globale".*

Uno dei rischi collaterali più critici riguarda l'utilizzo dell'Intelligenza Artificiale ai fini militari, sia nel contesto della *cyberwarfare* che nell'aggiornamento delle armi tradizionali; questa doppia applicabilità della tecnologia sia in tempo di guerra che di pace, la rende classificabile come "duale". Nel contesto della *cyberwarfare* l'uso di tecnologie dirompenti può portare quindi a un altrettanto dirompente problema etico: è questo il caso di strumenti di Intelligenza Artificiale finalizzato al raggiungimento di fini illegali come la violazione di diritti fondamentali, la realizzazione di attacchi informatici, le citate campagne di disinformazione. Il problema di attribuzione della responsabilità dell'azione è estremamente complesso per l'intrinseca difficoltà di identificazione dei soggetti che hanno progettato o implementato il sistema di Intelligenza Artificiale. Infatti, l'abilità di controllare un sistema e i suoi conseguenti effetti nello scenario di impiego è la condizione necessaria per l'assegnazione di responsabilità; ciononostante con l'evoluzione tecnologica di questo tipo di strumenti emergenti si va nella direzione in cui l'uomo non è più nella condizione di controllare i sistemi automatici e automatizzati, e quindi, paradossalmente, a non essere più ritenuto responsabile di eventuali azioni sanzionabili.

Dal punto di vista dell'aggiornamento delle armi tradizionali e, più in generale, nella progressiva sostituzione del capitale umano in capitale digitale, il problema etico viene inquadrato come un progressivo processo di perdita di competenze (*de-skilling*), ovvero un eccessivo affidamento di compiti e responsabilità alle macchine cosiddette intelligenti che porta in casi estremi ad impedire all'essere umano di sostituirsi rapidamente a un sistema quando questo finisca fuori controllo.

In estrema ipotesi, nei sistemi avanzati che incorporano al loro interno algoritmi di Intelligenza Artificiale, reti neurali e strumenti di *Machine Learning*, gli utenti ma anche gli stessi sviluppatori potrebbero non essere nelle condizioni di controllare o predire tutti i possibili comportamenti, dal momento che non è chiaro il percorso ottenuto per definire gli output.

La limitata capacità umana di influenzare il comportamento dei sistemi autonomi può quindi creare una discrepanza tra i concetti di ruoli e responsabilità negli eventi; questo può essere legato alla scarsa autorità dell'uomo sull'intero processo, piuttosto che all'impossibilità di controllare o intraprendere le necessarie azioni per influenzare il *Course of Action* a causa di fattori esterni incerti e probabilistici che non possono essere governati

pur disponendo di adeguata autorità. In sostanza, la progressiva crescita funzionale delle citate tecnologie emergenti ha creato un cosiddetto gap di responsabilità[54].

Un altro rischio etico che una forte spinta alla digitalizzazione della Difesa può far emergere, velatamente anticipato dagli effetti dell'emergenza epidemiologica da *Covid-19*, è quello di dare all'organizzazione una caratteristica di asincronia; digitalizzare e delocalizzare la forza lavoro sfruttando l'info-struttura digitale può portare a un crescente distanziamento sociale e relazionale che, nel lungo termine, potrebbe inficiare l'organizzazione stessa, dal benessere psicofisico del personale, all'assenza di confronto quale motore del progresso di processi e sistemi.

I sistemi sviluppati con le tecnologie basate sui concetti dell'Intelligenza Artificiale possono costituire, opportunamente governati, un grosso valore aggiunto in un'operazione militare per risolvere i cosiddetti "*three D's problems*", ovvero *dull*, *dirty* e *dangerous*. Si tratta di tutte quelle attività che inevitabilmente portano a elevati stress psicofisici del personale come, ad esempio, lavori che richiedono elevata concentrazione e necessitano di fisiologici momenti di pausa piuttosto che manovre estreme su velivoli vincolate da limiti fisici gravitazionali imposti dal personale a bordo; tutte queste attività potrebbero essere sostituite efficientemente da strumenti, sistemi o macchine. Diverse proiezioni portano a stimare un incremento nei prossimi anni di macchine che potranno svolgere le stesse funzioni attualmente di pertinenza dei soldati, con svariati punti di vantaggio in termini di prontezza e rapidità di risposta in caso di pericolo, capacità analitica e computazionale e resistenza fisica.

Allo stesso tempo dal punto di vista dei decisori, ci si troverà sempre più alle prese con scelte pre-analizzate da strumenti informatici intelligenti, in grado di processare enormi quantità di dati in tempi estremamente contenuti. Realizzare queste capacità intelligenti porta inevitabilmente a un paradosso intrinseco. Da un lato il *leader vuole* strumenti e macchine intelligenti come i soldati, in grado di imparare dall'esperienza e decidere in una situazione complicata; dall'altro non vuole che siano troppo creativi e possano uscire dal controllo del *leader.*

La frontiera dello sviluppo delle citate tecnologie dirompenti sono le cosiddette *Autonomous Weapon Systems* (AWS), ovvero quei Sistemi d'Arma che, una volta attivati, possono selezionare e ingaggiare un target in piena autonomia senza alcun ulteriore

54 N. Douer and J. Meyer, "The Responsibility Quantification Model of Human Interaction with Automation," in *IEEE Transactions on Automation Science and Engineering*, vol. 17, n. 2, pp. 1044-1060, April 2020.

intervento umano.[55] Durante il *Xiangshan Forum 2018*, un alto dirigente della società NORINCO, la terza più grande industria della Difesa cinese, ha stimato che i sistemi AWS potranno essere di uso comune già nel 2025.[56] Già nel 2013 l'Unione Europea ha costituito un gruppo di esperti per analizzare la problematica etica dei Sistemi d'Arma Autonomi, e il 12 settembre 2018 il Parlamento Europeo ha adottato un testo per spingere l'Unione Europea e gli Stati Membri a diffidare dall'uso di tali tecnologie.

55 United Nations Human Rights Council, "Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns," 09.04.2013. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-7_en.pdf

56 G. C. Allen, "Understanding China's AI Strategy. Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security," Center for a New American Security, 06,02,2019.

# Capitolo 3

# La *leadership* organizzativa per una Difesa digitale

## Approcci al *change management* digitale

Il *change management* è una disciplina emergente che studia in maniera strutturata il cambiamento negli individui, nei gruppi, nelle organizzazioni e nelle società; il cambiamento è un processo di transizione da uno stato corrente a uno stato futuro attraverso uno specifico percorso.

Il teorico organizzativo Gareth Morgan, noto come l'ideatore del concetto di "metafora organizzativa", sostiene che l'approccio al cambiamento è funzione diretta del modo in cui viene percepita un'organizzazione. In particolare ha identificato quattro metafore organizzative[57]:

- organizzazione come organismo: questa metafora si contestualizza in caso di sistemi adattivi in funzione dell'ambiente in cui sono immersi;
- organizzazione come macchina: in questa classificazione rientrano i sistemi razionali, ovvero governati da logiche lineari;
- organizzazione come sistema politico: rientrano in questa categoria i sistemi di potere con interessi in conflitto;
- organizzazione come flusso e trasformazione: questa metafora contempla i sistemi aperti, immersi nell'ambiente.

In letteratura, il cambiamento viene affrontato da un punto di vista tridimensionale: manifestazione (cambiamento pianificato o emergente), frequenza (cambiamento episodico o continuo) e portata (cambiamento evolutivo, di transizione o trasformativo).

Uno dei primi modelli di *change management*, teorizzato da Kurt Lewin[58], è il cosiddetto "approccio pianificato al cambiamento": si tratta di un modello *top-driven* composto da tre fasi sequenziali (*unfreeze, change e refreeze*). Partendo dalla definizione dello *status quo*, si definisce una *vision* che descriva la situazione finale desiderata e si identificano le forze a favore e quelle contrarie al cambiamento per poi passare alla fase di implementazione. In questo modello che riflette la metafora dell'organizzazione come organismo, ogni cambiamento deve essere imposto dall'alto.

57 Gareth Morgan, "Images of Organization", Sage Publications, 1986
58 Center for Strategic Business Studies, Managing change, Winchester, CSBS, 1998

Un altro modello basato sull'approccio pianificato al cambiamento è quello proposto da Bullock e Batten, che rappresenta la metafora di organizzazione come macchina ed è basato su quattro fasi sequenziali (*exploration, planning, action, integration*)[59].

Le principali critiche a questi modelli si basano sulle caratteristiche estremamente rigide legate ad approcci meccanicistici e lineari; negli anni '90 del secolo scorso, emerge un nuovo modello di *change management* a firma di J.P. Kotter, professore di *leadership* presso la Harvard Business School, che stigmatizza i principali errori che pregiudicano il successo di ogni implementazione del cambiamento in un'organizzazione. Questo modello si pone l'obiettivo di individuare un percorso guidato per costruire le capacità di *leadership* indispensabili all'implementazione del cambiamento nelle organizzazioni complesse.

La recente alternativa ai modelli di *change management* di tipo pianificato viene definita "cambiamento emergente": questo approccio riflette l'elevata rapidità e imprevedibilità richiesta ai processi di cambiamento che necessariamente deve rispondere agli svariati stimoli di cambiamento provenienti da diverse direzioni intere ed esterne all'organizzazione. Il focus si sposta, quindi, dalla modellazione di iniziative di cambiamento pre-pianificate al livello di prontezza e reattività al cambiamento delle organizzazioni.

Un dominio come quello dell'informatica e della digitalizzazione applicato alla Difesa, che può essere considerata un sistema complesso basato su fitte relazioni e interazioni tra individui, non può che essere inquadrata in un processo di trasformazione di tipo emergente, dove, quindi, il cambiamento non può essere *top-driven*; in riferimento alle metafore organizzative, in questo caso l'organizzazione può essere vista come flusso e trasformazione. In uno scenario del genere non ci possono, quindi, essere spinte esterne che portino a cambiamenti così sostanziali, così come non può essere il singolo individuo a farsi carico del cambiamento stesso ma può influenzarlo attraverso il suo reticolo di relazioni.

L'approccio di una Difesa digitale fatta di *bit*, può essere facilmente considerato un esempio di cambiamento *down-driven*, la quale impatta sulle competenze che la *leadership* organizzativa deve mettere in campo a tutti i livelli dell'organizzazione per guidare efficientemente la transizione e contrastare il rischio omeostatico di ritorno allo *status quo*.

59 Maya Larissa Paul. The Future of Organizational Change Management, University of Twente The Netherlands. https://essay.utwente.nl/67268/1/Paul_BA_BMS.pdf.

**Impatti sui processi di *Decision Making***

La materia delle tecnologie digitali è in costante evoluzione, al punto che inseguire la tecnologia per un *policymaker* è spesso una scelta perdente, posto che qualsiasi regola eccessivamente dettagliata e prescrittiva non può che diventare obsoleta in tempi estremamente contenuti. Scrivere regole puntuali per le tecnologie emergenti e dirompenti finora descritte non può essere considerato un approccio efficace di *Decision Making*; al contrario, definire regole basate su principi cardine, sufficientemente invariabili nel medio periodo è un indicatore di una *leadership* agile e lungimirante.

Tali tecnologiche, se opportunamente governate, possono espandere esponenzialmente il portafoglio capacitivo a disposizione dei decisori, perché consentono di unire domini finora incorrelati, virtualizzare ed efficientare prodotti e processi organizzativi, snellire e velocizzare i processi decisionali.

L'ambizione di trasformare la Difesa in veste digitale, passa attraverso le diverse fasi ampiamente descritte in questo studio, ma impone in prima analisi un radicale cambio di prospettiva da parte dei decisori. Dal punto di vista della *leadership*, vi è la necessità di creare nel contesto organizzativo le condizioni favorevoli a un cambiamento emergente, modificando dall'interno il tessuto connettivo dell'organizzazione ed i modelli di relazioni tra gli individui.

Disporre, infatti, di dati digitali direttamente disponibili per le decisioni presuppone una diffusione di consapevolezza che il singolo elemento dell'organizzazione contribuisce attivamente all'efficienza dell'intero sistema Difesa; deve quindi esserci una decisa e sentita sensibilizzazione a tutti i livelli della bontà dei dati da inserire nei sistemi informativi, allo scopo di evitare un effetto tsunami di dati sporchi, corrotti o errati sulle decisioni finanche strategiche che possono essere prese sulla base di quel patrimonio informativo.

La disponibilità tecnologica di strumenti evoluti di *Data Analysis*, *Data Mining* e, più in generale, di Intelligenza Artificiale, unitamente all'enorme quantità di dati che un'efficace digitalizzazione della Difesa potrebbe verosimilmente portare, determinano un ulteriore impatto sui processi di *Decision Making*; strumenti e algoritmi che prevedono scenari sulla base di serie storiche, esperienza maturata, o semplicemente una grande mole di dati, implicano una ragionevole dose di fiducia da parte del decisore sulla bontà della soluzione dell'algoritmo, a fronte dell'impossibilità di poter verificare esplicitamente il processo che ha portato a quell'output. Il cambio di focus dal processo al risultato può portare al paradosso di mancanza di fiducia sul sistema previsionale, almeno fintanto che la realtà dimostri, *ex-post* la bontà della previsione.

Supportare il processo decisionale sfruttando i dati a disposizione, consente di ridurre la complessità della mole di bit a disposizione, estraendo informazioni rilevanti dai dati. Questo processo, già descritto in questo elaborato come *Data Driven Decision Making*, dal punto di vista dei decisori non può prescindere dalla disponibilità di strumenti di *Data Visualization* efficaci; l'obiettivo è quello di presentare in maniera chiara fenomeni complessi, derivanti da molteplici sorgenti, allo scopo di rendere più immediato il processo decisionale.

**Cambiamento culturale per una Difesa Digitale**

Nei paesi più avanzati dal punto di vista tecnologico questi processi di trasformazione del settore militare sono stati avviati più o meno celermente; il rimanere indietro in questo senso porterebbe inevitabilmente a un progressivo scollamento tecnologico e a una conseguente inferiorità capacitiva. Applicando questo paradigma al cosiddetto OODA Loop[60], si nota come queste tecnologie emergenti stiano accelerando sensibilmente i processi decisionali militari, spostando il focus del problema dal lato tecnico a quello dottrinale; vi è la necessità di mettere in campo tutte quelle forze che per loro funzione hanno la facoltà decisionale di adottare una strategia coordinata tale da fattorizzare le risorse in termini di generazione, raccolta, gestione, analisi e condivisione di dati, nell'ottica di una efficace digitalizzazione ed innovazione della Difesa. Il concetto stesso di "innovazione" è inteso come l'arte di combinare invenzioni già fatte per farle diventare modelli di business, servizi o prodotti attagliati a specifiche esigenze. A differenza del concetto di invenzione che è un fenomeno di poche persone, l'innovazione ha un carattere sociale, deve, cioè, coinvolgere tante persone affinché si raggiungano gli obiettivi sperati. A tal proposito, per una efficace spinta verso una Difesa digitale risulta necessario diffondere a tutti i livelli organizzativi la cultura dell'informatica come bacino di innovazione per l'intera organizzazione, e contribuire a far sentire tutto il personale parte attiva del cambiamento.

Diviene quindi fondamentale e di primaria importanza diffondere la cultura IT, far crescere la consapevolezza digitale in termini di sicurezza, di gestione del patrimonio informativo della Difesa e di tutela in ambito di *Cyber Security*, attraverso un graduale processo di familiarizzazione, coinvolgimento e sensibilizzazione, adottando tutti i canali comunicativi a disposizione.

60 L'espressione OODA loop (in italiano ciclo OODA) o ciclo di Boyd si riferisce al ciclo decisionale "osservare, orientare, decidere e agire", sviluppato dallo stratega militare dell'aeronautica degli Stati Uniti col. John Boyd, che ha applicato questo concetto alle fasi del combattimento, spesso in operazioni militari a livello strategico.

Un sostanziale cambiamento culturale per una Difesa digitale efficiente richiede il superamento del concetto di “componente”, che spesso fraziona, isola e contrappone risorse; in un paragone informatico è come se si disponesse di diversi computer ciascuno con una propria capacità computazionale e non la si sfruttasse in parallelo con un’efficiente orchestrazione delle risorse.

**Metodologie per la definizione di business case**

L’adozione di una particolare soluzione tecnologica nell’ambito di un ampio e complesso processo di digitalizzazione di un’organizzazione passa attraverso specifiche fasi ben definite dalla dottrina:

- Sviluppo *Business Case*: in questa fase si analizzano le potenziali opportunità di *improvement* tecnologico e funzionale del sistema informativo, attraverso l’identificazione dei *key business driver* e delle *business benefit area*, attraverso metriche e informazioni interne per una stima iniziale dei livelli di *benefit*. I *business benefit* possono essere classificati in funzione delle aree impattate: persone (incremento della produttività individuale, sviluppo di nuove capacità, riduzione dello stress), processi (riduzione “*lead time*” dei processi, eliminazione delle attività non a valore aggiunto, minimizzazione degli errori e del *re-working*, standardizzazione dei processi), tecnologia (incremento dell’affidabilità e della qualità, riduzione della complessità, contenimento della curva sviluppo-costi, riduzione *Total Cost of Ownership* (TCO) *software*), management (miglioramento del supporto alle decisioni, dell’attività di controllo, misurazione e reporting). Altri *business benefit* hanno, invece, carattere trasversale e riguardano caratteristiche infrastrutturali, scalabilità e flessibilità.
- *Team building*: un elemento fondamentale per valutare singoli progetti di digitalizzazione e per fare una corretta valutazione dei vantaggi e dei costi di un investimento è quello del *team building*, ovvero la formalizzazione, al livello adeguato, di specifici team composti dalle figure idonee ad affrontare problematiche complesse e articolate, scomporle e semplificarle per favorire le fasi successive.
- *Gap analysis* su tecnologie e funzionalità: si sviluppano analizzando i servizi IT, l’infrastruttura e le tecnologie a disposizione e le funzionalità dei sistemi e degli strumenti. In prima battuta deve essere fatta un’analisi dello scenario “*as is*”, con cui si devono identificare processi cosiddetti *business critical*, dettagliare il portafoglio applicativo in termini di capacità espresse e mappare l’architettura tecnologica a disposizione: successivamente va definito lo scenario “*to be*” che dovrà descrivere i nuovi servizi,

sistemi, *framework*, piattaforme potenzialmente disponibili, definire la nuova architettura tecnologica e le capacità aggiuntive che ci si pone come obiettivo.

- Misurazione dei *Business Benefit*: attraverso una puntuale attività di raccolta dati e definizione di parametri e indicatori viene valutato il valore aggiunto della potenziale implementazione di un cambiamento tecnologico.
- Elaborazione *Business Case*: sulla base delle analisi precedenti vengono condivise le assunzioni alla base delle stime dei costi e dei benefici, definito l'orizzonte temporale oggetto del business case e convertiti i *business benefit* in indicatori di redditività o risultati economici.

# Conclusioni

In questo studio si è cercato di approfondire il concetto di “Difesa digitale”, ovvero quel processo complesso di ammodernamento delle Forze Armate orientato alla gestione efficace della sfera della digitalizzazione e dei dati. L’analisi svolta ha fatto emergere la necessità di considerare il problema da tre diverse prospettive: il dominio tecnologico, il fattore umano e la *leadership* organizzativa.

Partendo dalla definizione di “dato” e dalle potenzialità che una gestione efficiente e strutturata del patrimonio informativo a disposizione può dare ad un’organizzazione come la Difesa, è stato analizzato il dominio tecnologico, ovvero le tecnologie emergenti e dirompenti come l’Intelligenza Artificiale nella sua accezione più ampia, gli approcci, le potenzialità e le minacce di sfide tecnologiche come il machine learning e il deep learning in campo militare. Sono stati trattati gli aspetti di *Cyber Security* che hanno evidenziato una crescente rilevanza strategica del dominio cibernetico ed è stato introdotto il concetto di *environment* strategici digitali per identificare tutti gli *asset* considerabili *enabler* per qualsivoglia operazione nella *Digital Arena*.

L’analisi è proseguita affrontando il problema della digitalizzazione della Difesa dal punto di vista delle risorse umane. Governare tecnologie emergenti e dirompenti altamente specializzate e dal carattere esplosivo in termini di capacità esprimibili, non può prescindere dal disporre di capitale umano all’altezza di questa sfida; per gestire il portfolio strategico di una Difesa Digitale e trasformare tecnologie in capacità è fondamentale guidare il processo dall’interno dell’organizzazione, attraverso la fusione di competenze opportunamente formate, che possa affrontare lo *skill-gap* e gestire la trasformazione verso la digitalizzazione. In questo scenario, quindi, è tanto importante la conoscenza dell’ambiente applicativo su cui andranno a operare gli output delle tecnologie emergenti, quanto la competenza tecnologica e culturale in grado di vincere la fisiologica resistenza al cambiamento tipica di una sfida organizzativa di tale portata. Vi è pertanto la necessità di disporre, al pari del portfolio di capacità tecnologiche, anche di un portfolio di capacità tecniche in termini di risorse umane costantemente al passo con le evoluzioni tecnologiche, allo scopo di valorizzare e difendere il dominio informativo della Difesa nonché ridefinire il concetto di prontezza militare. A differenza di altri contesti applicativi dove il fattore quantitativo fa la differenza, nella Digital Arena è la qualità delle competenze a determinare il successo o il fallimento di un’operazione. Il focus dell’analisi è poi passato sull’esigenza intrinseca di un continuo, efficace e proattivo scambio di informazioni in termini di “domanda

tecnologica" e "offerta" delle tecnologie emergenti; questo si traduce in un costante incremento della sinergia tra la Difesa, i Centri di ricerca militari e civili, le Università, i Distretti ed i Poli Tecnologici e l'industria nazionale; la peculiarità delle capacità militari che si traducono in "domanda tecnologica", impone che una tale condivisione di informazioni sia guidata dalla Difesa, a cui è richiesta una postura strategica tale da poter imporre priorità sulle ricerche tecnologiche in funzione delle esigenze capacitive da raggiungere. Una volta avviato un tale processo, anche un team interno ridotto opportunamente costituito, supportato dall'organizzazione e in coordinamento sinergico con l'ecosistema abilitante, può fare la differenza e diventare un volano per lo sviluppo di nuove capacità operative e stimolo per altri elementi dell'organizzazione; in questo modo viene completamente ribaltato il preconcetto negativo relativo all'asimmetria del dominio cibernetico, tramutandolo in peculiarità da sfruttare a vantaggio del sistema per guadagnare resilienza e competitività nella *Digital Arena*.

Il terzo punto di osservazione di questo studio è stato quello relativo alla *leadership* organizzativa ideale per un cambiamento sostanziale, drastico e repentino come quello che viene chiesto per una Difesa digitale. Dopo aver analizzato gli approcci al *chance management* applicati al contesto di digitalizzazione di un'organizzazione complessa come la Difesa, è emersa chiaramente la necessità di un approccio al cambiamento sistemico di tipo emergente. In un mondo sempre più guidato dall'informatica e dalla proliferazione dei dati, risulta evidente come le tecnologie emergenti siano governate da un bacino di talenti digitali costituito da personale anagraficamente e professionalmente giovane; pertanto, per permettere una crescita evolutiva dello strumento militare in un'ottica digitale, è opportuno riconsiderare fenomeni di *leadership* connettiva basati sull'interazione di individui, che porta a far emergere idee altamente espressive dal punto di vista capacitivo provenienti da qualsiasi livello dell'organizzazione.

In conclusione, lo studio dei settori di influenza e delle implicazioni tecnico-operative portate dalla digitalizzazione e dalle tecnologie emergenti analizzate hanno evidenziato prospettive, vulnerabilità e implicazioni che impattano il sistema Difesa nel suo complesso. Questo impone un approccio proattivo che spinga verso una rivoluzione digitale l'intera organizzazione, ovvero che non si limiti agli aspetti tecnici ma coinvolga la sfera dottrinale e culturale. Il rimanere indietro tecnologicamente porta ad una progressiva ed incrementale inferiorità capacitiva, colmabile solo da un'organizzazione pronta al cambiamento in termini di *leadership*, investimento sul capitale umano, priorità di investimenti, influenza sul mondo dell'Università e della Ricerca e sinergia con l'industria nazionale.

# Elenco delle principali abbreviazioni e degli acronimi

| | |
|---|---|
| ACYD | Autonomous Cyber Defence |
| AI | Artificial Intelligence |
| AICA | Autonomous Intelligent Cyber-Defence Agents |
| AIM | Autonomous Intelligent Malware |
| AWS | Autonomous Weapon Systems |
| BRINE | Biotechnology Robotics Information Nanotechnology Energy |
| C2 | Comando e Controllo |
| C5ISR | Comando Controllo Comunicazioni Computer Cyber Intelligence Sorveglianza ricognizione |
| CaSMD | Capo di Stato Maggiore della Difesa |
| CeMiSS | Centro Militare di Studi Strategici |
| COTS | Commercial Off-The-Shelf |
| CTI | Cyberthreat Intelligence |
| DBMS | Database management system |
| D-LBO | Digitizing Land-Based Operations |
| DL | Decreto Legge |
| DoD | Dipartimento della Difesa |
| EDA | all'European Defence Agency |
| ENISA | European Union Agency for Cybersecurity |
| FMV | Full Motion Video |
| IA | Intelligenza Artificiale |
| ICT | Information Communication Tecnologies |
| ICVRIS | International Conference on Virtual Reality and Intelligent Systems |
| IDSS | Intelligent Decision Support System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IOT | Internet Of Things |
| ISR | Intelligence Surveillance Reconnaissance |
| IT | Information Technology |
| MIF | Military Intelligence Fusion |
| MISE | Ministero dello Sviluppo Economico |
| MLP | Multilayer Perceptron |
| MOA | Memorandum of Agreement |
| NATO | North Atlantic Treaty Organization |
| OLAP | On-Line Analytical Processing |
| OODA | Observe Orient Decide Act |
| REGISCC | Reparto Gestione ed Innovazione Sistemi di Comando e Controllo |
| TCO | Total Cost of Ownership |
| TEN | Tactical Edge Networking |
| UAV | Unmanned Aerial Vehicles |
| UE | Unione Europea |

# Biblio/emero/web-grafia

## Articoli e pubblicazioni


B. Su, H. Zhao, T. Qi, X. Liu and R. Yu, "Research on Architecture of Intelligent Command and Control System," 2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), Jishou, China, 2019, pp. 362-364

Barr, Avron and Edward A. Feigenbaum. “The Handbook of Artificial Intelligence, Volume 1”. Los Altos, California: William Kaufmann, Inc.

Brian P. Kime Threat Intelligence: Planning and Direction, SANS Institute, 2015

C. Aker and S. Kalkan, “Using deep networks for drone detection,” 2017 14th IEEE Int. Conf. Adv. Video Signal Based Surveillance, AVSS 2017, no. August, 2017

Center for Strategic Business Studies, Managing change, Winchester, CSBS, 1998

Data Science Strategy, Ulrika Jägare, John Wiley & Sons,Inc., ed. 2019, p.112

ENISA Threats Landscape Report 2016

Food for Thought Paper by Finland, Estonia, France Germany and the Netherlands, EDA, 17.5.19

Friedman, M. and Friedman R.D., "Tyranny of the Status Quo", 1985, Harpercollins

G. C. Allen, “Understanding China’s AI Strategy. Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security,” Center for a New American Security, 06 02 2019

Gareth Morgan, “Images of Organization”, Sage Publications, 1986

H. Peng, Y. Zhang, S. Yang and B. Song, "Battlefield Image Situational Awareness Application Based on Deep Learning," in IEEE Intelligent Systems, vol. 35, no. 1, pp. 36-43, 1 Jan.-Feb. 2020

Hu J, Shen L, Sun G. Squeeze-and-excitation Networks(J). ar Xiv preprint ar Xiv: 1709.01507, 2017

Jiawei Han, Micheline Kamber, Jian Pei “Data-Mining. Concepts and Techniques” 3rd Edition Morgan Kaufmann 2011 p.38-39

K. A. Carlton, "Artificial intelligence supportability (Air Force application)," in IEEE Aerospace and Electronic Systems Magazine, vol. 3, no. 12, pp. 25-32, Dec. 1988

K. R. Harrison et al., "Portfolio Optimization for Defence Applications," in IEEE Access, vol. 8, pp. 60152-60178, 2020

Karen Simonyan, Andrew Zisserman. Very Deep Convolutional Networks for Large-scale Image Recognition. International Conference of Learning Representation. 10 Apr 2015

Lecun Y, Bottou L, Bengio Y, et al. Gradient-based learning applied to document recognition(J). Proceedings of the IEEE, 1998, 86(11):2278-2324.

M. Andrew, “Situational awareness—From the battlefield to the corporation,” Comput. Fraud Secur., vol. 9, no. 1, pp. 13–16, Sep. 2016

M. G. Ceruti, "The relationship between artificial intelligence and data mining: application to future military information systems," Smc 2000 conference proceedings. 2000 IEEE international conference on systems, man and cybernetics. 'cybernetics evolving to systems, humans, organizations, and their complex interactions' cat. no.0, Nashville, TN, 2000, pp. 1875 vol.3

Maya Larissa Paul. The Future of Organizational Change Management, University of Twente The Netherlands. https://essay.utwente.nl/67268/1/Paul_BA_BMS.pdf

N. Douer and J. Meyer, "The Responsibility Quantification Model of Human Interaction With Automation," in IEEE Transactions on Automation Science and Engineering, vol. 17, no. 2, pp. 1044-1060, April 2020

N. Shijith, P. Poornachandran, V. G. Sujadevi, and M. M. Dharmana, “Breach detection and mitigation of UAVs using deep neural network,” 2017 Recent Dev. Control. Autom. Power Eng. RDCAPE 2017, vol. 3, pp. 360–365, 2018

Q. L. Yin and J. W. Wang, “An overview of the application of deep learning in the field of image processing,” J. Higher Educ., vol. 1, no. 9, pp. 11–15,Oct. 2018

S. Liu, M. Dibaei, Y. Tai, C. Chen, J. Zhang and Y. Xiang, "Cyber Vulnerability Intelligence for Internet of Things Binary," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2154-2163, March 2020

S. M. Ghaffarian and H. R. Shahriari, “Software vulnerability analysis and discovery using machine-learning and data-mining techniques: A survey” ACM Comput. Surv., vol. 50, no. 4, 2017, Art. no. 56

T. Hong and Z. Jie, "A Framework of Intelligent Decision Support System of Military Communication Network Effectiveness Evaluation," 2008 Fifth International Conference on Fuzzy Systems and Knowledge Discovery, Shandong, 2008, pp. 518-521

T. P. Hanratty et al., “Enhancing battlefield situational awareness through fuzzy-based value of information,” in Proc. 46th Hawaii Int. Conf. Syst. Sci., vol. 1, no. 1, pp. 13–18, Jan. 2013

Wired USA, volume July 2008, https://www.wired.com/2008/06/pb-theory/

**Siti**

http://cdn.aiindex.org/2018/AI%20Index%202018%20Annual%20Report.pdf

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-7_en.pdf

http://www3.weforum.org/docs/WEF_Future_of_Jobs_2018.pdf

https://essay.utwente.nl/67268/1/Paul_BA_BMS.pdf

https://innovazione.gov.it/assets/docs/MID_Book_2025.pdf

https://www.bloomberg.com/graphics/2016-job-skills-report/

https://www.cognilytica.com/2019/04/04/the-seven-patterns-of-ai/

https://www.shephardmedia.com/news/digital-battlespace/germany-continues-pursuit-tactical-edge-networ/

https://www.techeconomy2030.it/2019/12/19/data-driven-decision-making-come-fare-con-quali-benefici/

https://www.wired.com/2008/06/pb-theory/

**Normativa e direttive**

Decreto Legge 105/2019

Documento Programmatico Pluriennale per la Difesa per il triennio 2018-2020, Ministero della Difesa, ed. 2018

Documento Programmatico Pluriennale per la Difesa per il triennio 2019-2021, Ministero della Difesa, ed. 2019

DoD Digital Modernization Strategy, DoD Information Resource Management Strategy Plan FY 19-23, ed jul 12, 2019

Il Concetto Strategico del Capo di Stato Maggiore della Difesa, ed. gennaio 2020

Legge n. 81 del 2017

Legge N.244 del 31/12/2012: “La revisione dello strumento militare”

Piano nazionale innovazione 2025, Ministero per l'Innovazione Tecnologica e la Digitalizzazione, Release Stabile, 13 Febbraio 2020. https://innovazione.gov.it/assets/docs/MID_Book_2025.pdf

Proposte per una Strategia italiana per l’Intelligenza Artificiale, MISE, 2020

United Nations Human Rights Council, “Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns,” 09 04 2013. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-7_en.pdf

## NOTA SUL Ce.Mi.S.S. e NOTA SULL'AUTORE

### Ce.Mi.S.S.[61]

Il Centro Militare di Studi Strategici (Ce.Mi.S.S.) è l'Organismo che gestisce, nell'ambito e per conto del Ministero della Difesa, la ricerca su temi di carattere strategico.

Costituito nel 1987 con Decreto del Ministro della Difesa, il Ce.Mi.S.S. svolge la propria opera valendosi si 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.

### Cap. G.A.r.n. Giovanni FRISO

Il Cap. Giovanni Friso si è arruolato in Aeronautica Militare nel 2005 come Allievo Ufficiale del Ruolo Normale del Genio Aeronautico nel corso accademico Falco V.

Ha conseguito la laurea specialistica in Ingegneria Elettronica presso l'Università degli Studi di Napoli – Federico II ed ha perfezionato le sue competenze tecniche e professionali con diversi percorsi formativi post-laurea nel campo dell'informatica e la digitalizzazione, dell'organizzazione, management ed innovazione nelle Pubbliche Amministrazioni, della *leadership* e analisi strategica e del *Data Intelligence* applicato alle strategie decisionali.

Dal 2010 lavora presso il Reparto Gestione ed Innovazione Sistemi di Comando e Controllo (Re.G.I.S.C.C.) dell'Aeronautica Militare nel campo dello sviluppo e della sperimentazione di soluzioni tecnologiche all'avanguardia per l'innovazione dei sistemi C5-ISR della F.A. e della Difesa. Dal 2014 rappresenta l'Amministrazione Difesa nel consesso *NATO C3 Board* quale membro tecnico permanente al *Data Management Capability Team*.

61 http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pagine/default.aspx

ISBN 978-88-31203-48-7