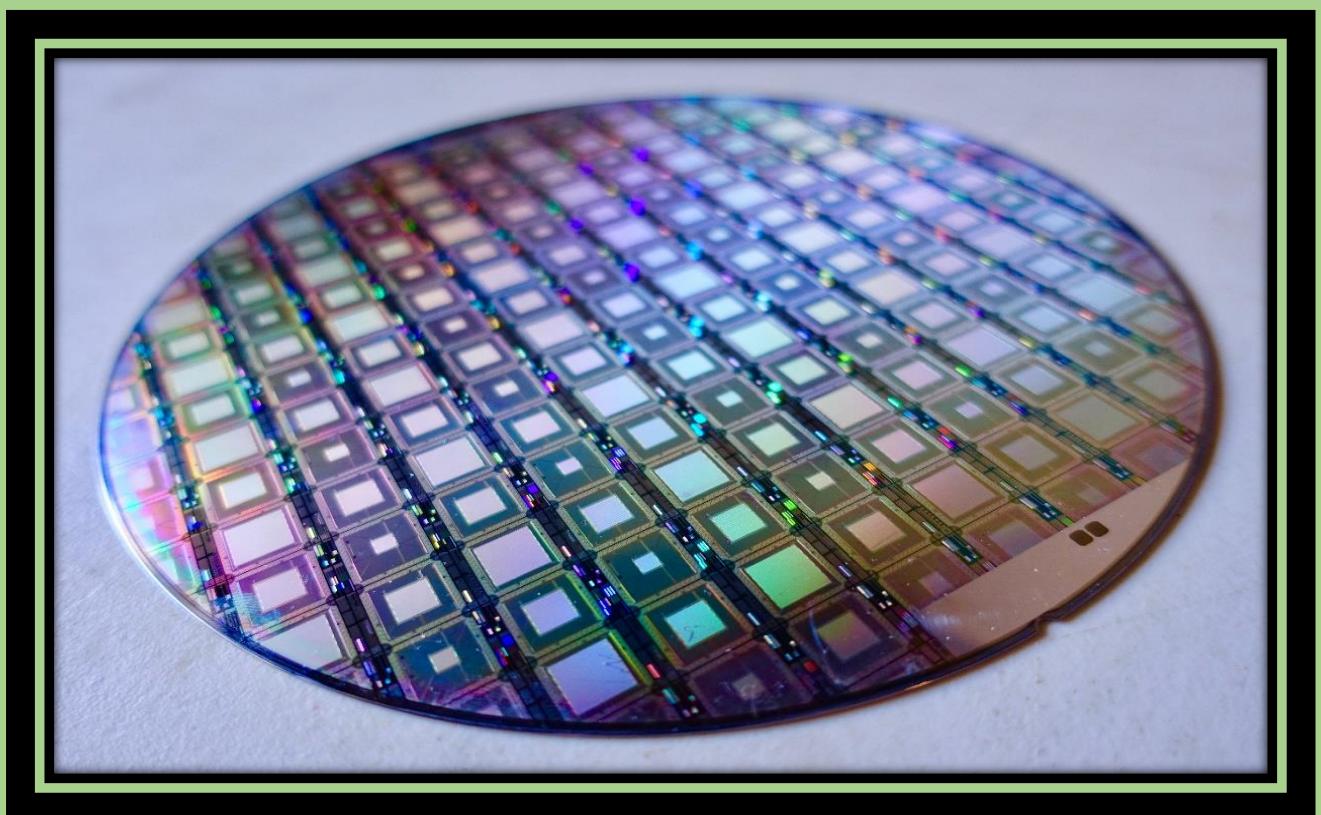


STATO MAGGIORE DELLA DIFESA



L'impatto delle Emerging & Disruptive Technologies (EDTs) sulla Difesa

Edizione 2022

PREFAZIONE DEL CAPO DI STATO MAGGIORE DELLA DIFESA



“L’innovazione tecnologica, caratterizzata da una crescita esponenziale, procede così rapidamente da non dare l’opportunità di comprenderne il reale cambiamento, tantomeno le conseguenze correlate. Tale velocità è la principale sfida che dovrà essere affrontata accettandone le grandi opportunità offerte e traguardando quello che sarà il futuro scenario di riferimento attraverso una concreta trasformazione culturale e cognitiva.

Un’accelerazione tecnologica “dirompente” che ha spinto le organizzazioni e le strutture

ad individuare nuove forme di adattamento, rivoluzionando i propri processi operativi fino a toccare i settori della formazione, dell’impiego del personale e della leadership con una sostanziale ed importante necessità di mindset change.

In questo scenario, le Emerging and Disruptive Technologies (EDTs) rappresenteranno la spina dorsale di un’evoluzione che se guidata, opportunamente controllata e correttamente impiegata, non potrà che permettere al Paese, e quindi anche alla Difesa, di saper fronteggiare le sfide del futuro con sicurezza, resilienza e risolutezza.

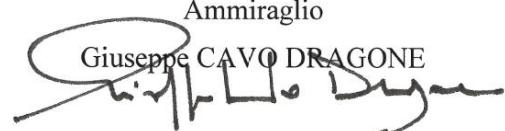
La gestione dell’enorme mole di dati oggi disponibili (Data Governance), la definizione del nuovo rapporto tra essere umano ed Intelligenza Artificiale (Human Autonomy Teaming), l’impiego dei Sistemi Autonomi in supporto o sostituzione del militare, la regolamentazione del nuovo dominio Spazio, l’impatto strategico della minaccia ipersonica, le nuove potenzialità della tecnologia quantistica e l’applicazione delle biotecnologie al contesto civile e militare sono solo alcune delle tematiche sviluppate che richiedono specifici approfondimenti in termini di implicazioni per la Difesa e la Sicurezza nazionale.

Agli albori di una nuova rivoluzione e trasformazione tecnologica, appare quindi inevitabile un profondo cambiamento culturale che sicuramente richiederà nuove priorità, coraggio e determinazione, velocità e adattamento a nuovi livelli di rischio, investimenti e una sempre maggiore ricerca di concrete ed efficaci sinergie.

In questo senso la Difesa dovrà rispondere attraverso una Cultura dell’Innovazione aperta al mondo esterno (c.d. Open Innovation), che potenzi la capacità di comprendere i fenomeni e sia in grado di elaborare risposte rapide ed efficaci per affrontare le nuove sfide e le potenziali minacce per la Sicurezza nazionale. Il ritmo accelerato dell’innovazione e dello sviluppo tecnologico è contraddistinto da un marcato coinvolgimento del settore privato e rende, pertanto, indispensabile la creazione di un nuovo approccio teso a cogliere le opportunità di questa complessità. L’identificazione dei principali trends di sviluppo e delle correlate implicazioni, non emerge da un processo lineare di causa-effetto, bensì da un percorso articolato (c.d. modello Innovation Journey) che cogliendo le opportunità, fronteggi le sfide di questa evoluzione e che sia in grado di prevedere le minacce con tempistiche e capacità reattive adeguate alla crescente e continua competizione internazionale. Un percorso che consenta l’esplorazione dei futuri in un contesto Multidominio dinamico ed interconnesso dove le tecnologie rappresentano un elemento determinante e discriminante negli equilibri in essere per cercare di giungere a conclusioni che delineino non solo i futuri preferibili, frutto delle influenze dell’oggi, ma cerchino di trarre futuri probabili e plausibili.

Questo documento concettuale rappresenta, quindi, un ulteriore passo significativo nel processo di evoluzione del Pensiero Strategico Innovativo della Difesa e potrà contribuire a diffondere la consapevolezza dell’importanza delle tecnologie emergenti tra tutti gli attori istituzionali in modo da coglierne appieno le sfide, ma soprattutto le opportunità”.

Ammiraglio
Giuseppe CAVO DRAGONE



INDICE

Introduzione SCENARIO TECNOLOGICO	1
CULTURA DELL'INNOVAZIONE	1
CLASSIFICAZIONE DELLE TECNOLOGIE	2
SVILUPPO DELLE <i>EMERGING & DISRUPTIVE TECHNOLOGIES</i>	5
Capitolo 1 BIG DATA	8
1.1 PERVASIVITÀ DEI DATI	8
1.2 GESTIONE DEI DATI (<i>DATA ANALYTICS</i>)	10
1.3 QUALI TECNOLOGIE USERANNO I DATI?	14
1.4 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA	15
Capitolo 2 INTELLIGENZA ARTIFICIALE	19
2.1 UN'EVOLUZIONE “DARWINIANA”	19
2.2 IMPLICAZIONI ETICHE, MORALI E GIURIDICHE	20
2.3 TRUST	22
2.4 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA	23
Capitolo 3 SISTEMI AUTONOMI	28
3.1 LIVELLI DI <i>REASONING</i>	28
3.2 TIPOLOGIE DI SISTEMI AUTONOMI	30
3.3 INTERFACCIA UOMO-MACCHINA E METRICHE PER I LIVELLI DI AUTONOMIA	30
3.4 IMPLICAZIONI ETICHE E GIURIDICHE	32
3.5 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA	34
Capitolo 4 TECNOLOGIE SPAZIALI	38
4.1 LO SPAZIO E LE TECNOLOGIE ABILITANTI	38
4.2 CAPACITÀ STRATEGICHE PER OPERARE NELLO SPAZIO	42
4.3 MINACCE ALLE INFRASTRUTTURE SPAZIALI	45
4.4 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA	48

Capitolo 5 TECNOLOGIE IPERSONICHE	51
5.1 UN “IMPATTO FULMINEO”	51
5.2 LA PROTEZIONE DELLE FORZE	52
5.3 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA	54
Capitolo 6 TECNOLOGIE QUANTISTICHE	57
6.1 LA SECONDA RIVOLUZIONE QUANTISTICA	57
6.2 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA	59
Capitolo 7 BIOTECNOLOGIE	63
7.1 CAMPI DI APPLICAZIONE DELLE BIOTECNOLOGIE	63
7.2 BIOINFORMATICA, BIOSENSORI E BIOELETTRONICA	65
7.3 POTENZIAMENTO UMANO	66
7.4 BIOLOGIA SINTETICA	69
7.5 CONTROMISURE MEDICHE E TECNOLOGIE BIOMEDICHE	70
7.6 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA	72
CONCLUSIONI	75
LE TECNOLOGIE EMERGENTI E DIROMPENTI NEL NUOVO CONTESTO MULTIDOMINIO	75
NUOVO MODELLO DI INNOVAZIONE	78
Allegato METODOLOGIA DI LAVORO E BIBLIOGRAFIA	80

Introduzione

SCENARIO TECNOLOGICO

“CULTURA DELL’INNOVAZIONE”

Il progresso e l’innovazione tecnologica comportano molteplici sfide ed offrono grandi opportunità. La società, l’economia, la politica ed il mondo militare sono modificati ed influenzati dalla pervasività delle nuove tecnologie, senza peraltro comprenderne appieno il reale cambiamento né l’entità delle conseguenze. Non tutte le invenzioni hanno apportato i vantaggi e le trasformazioni auspicati ma, al contrario, alcune hanno dato origine ad instabilità, criticità e generato nuove ed eterogenee forme di minaccia. La realtà è che l’uomo, nella sua abilità di progredire ed innovarsi, deve necessariamente aumentare le proprie capacità di adattamento e concentrarsi sulla previsione degli effetti che le sue azioni possono generare.

L’evoluzione delle tecnologie (innovative, emergenti o dirompenti che siano) muta ad una velocità sorprendente e la principale sfida, soprattutto per le future generazioni, sarà quella di operare con velocità, in modalità predittiva e, purtroppo, convivendo con un potenziale grado di indeterminatezza, di insicurezza e di rischio sempre maggiore. Risulta, pertanto, fondamentale individuare e studiare quegli indicatori che, se colti ed intercettati in tempo utile, consentiranno di anticipare i mutamenti in corso e quelli che probabilmente si manifesteranno nel futuro a medio e lungo termine. E’indispensabile, dunque, sostenere una concreta trasformazione culturale e cognitiva che ci porti a sviluppare una vera e propria **”Cultura dell’Innovazione”**.

In questo senso, la capacità di immaginare il futuro (sia dal punto di vista delle opportunità così come delle possibili minacce) diventa un potente ed efficiente sistema di sviluppo dell’innovazione che può trarre vantaggio anche dall’utilizzo di metodologie di analisi concettuali con il concorso costante di competenze ed esperienze espresse da molteplici settori della società. Il bilanciamento tra la necessità di “usare il microscopio”, per acquisire il dettaglio delle attuali conoscenze (e strumenti) già a disposizione per affrontare le sfide del presente, e quella di “usare il telescopio”, per prevedere e prepararsi alle sfide del futuro, non può che essere dinamico: proprio per questo, oggi più che mai, ogni istituzione ed organizzazione deve possedere un efficace sistema di intuizione, di capacità di pensiero *“out of the box”* e di anticipazione degli scenari futuri.

Questo processo di previsione ed anticipazione degli sviluppi scientifici e tecnologici deve essere continuamente ed adeguatamente sostenuto e guidato, non solo per le importanti ricadute sul settore della Difesa, ma anche sulle strutture ed infrastrutture nazionali. Un’azione importante diventa perciò quella di selezionare quelle tecnologie che, emergendo dal sistema della Ricerca e dell’Innovazione, più

di altre potranno poi avere un impatto dirompente ed inaspettato: alcune tecnologie emergenti, infatti, sono sviluppate in strutture ben note (se non appartenenti) agli enti preposti alla Difesa e alla Sicurezza; altre sono, invece, concepite e sviluppate in laboratori accademici o in piccole aziende (spesso *spin-off* o *start-up*) che, per essere individuate ed eventualmente coinvolte in progetti istituzionali, richiedono una sistematica opera governativa di monitoraggio e *scouting* rivolta non solo al panorama nazionale, ma anche alle realtà internazionali che rientrano negli interessi strategici nazionali.

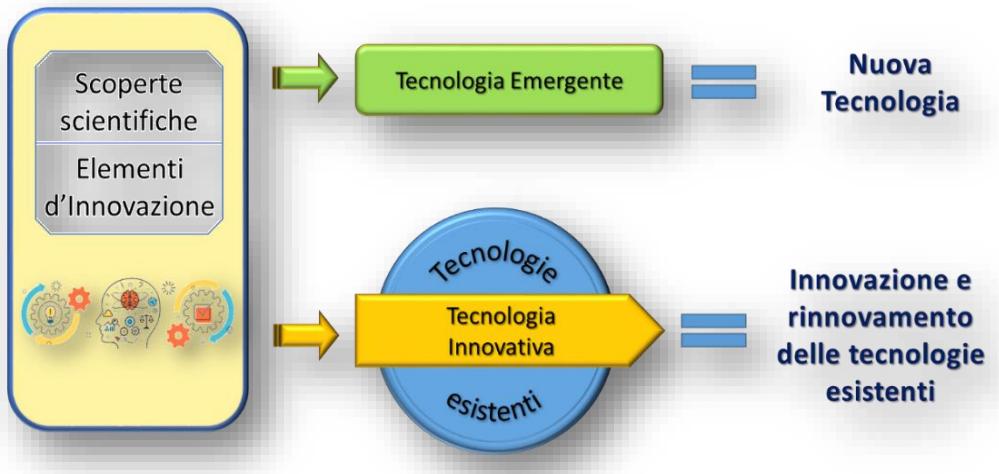
In questo scenario, le cosiddette Tecnologie Emergenti e Dirompenti (*Emerging and Disruptive Technologies* – EDTs) rappresenteranno la spina dorsale di un’evoluzione che, se guidata, opportunamente controllata e correttamente impiegata, non potrà che permettere al Sistema Paese, e quindi anche alla Difesa, di saper fronteggiare le sfide e le opportunità del futuro.

CLASSIFICAZIONE DELLE TECNOLOGIE

Nel categorizzare le differenti tecnologie è necessario considerare fattori e variabili che possono risultare più o meno influenti: tra queste la disponibilità delle materie prime, la possibilità economica di realizzazione, le restrizioni imposte dai creatori o dagli investitori di settore, l’effetto sulla “rete” (inteso come area d’interesse), la maturità del prodotto in termini di accessibilità e diffusione (standardizzazione delle specifiche tecniche) e, non ultimo, il consolidamento del suo utilizzo.

In tal senso sono state comunemente standardizzate le seguenti definizioni:

- **Tecnologie Emergenti** che si affermano per la prima volta in un dato ambito, la cui scoperta e realizzazione costituisce un elemento di novità (non conosciuto prima). La loro nascita ed il loro sviluppo richiedono normalmente un orizzonte temporale medio-lungo ed il loro consolidamento dipende da numerosi fattori (interesse, diffusione, commercializzazione, costi di produzione, ecc.).
- **Tecnologie Innovative** che hanno un contenuto di novità tale da cambiare, perlopiù in meglio, lo stato delle cose già esistenti, producendo rinnovamento e progresso. Il loro sviluppo è abbastanza rapido poiché frutto di una spinta spesso trasversale, influenzata da molteplici fattori (tra cui, oggi, domina quello economico-commerciale derivante dalle competizioni industriali). Di contro, il loro ciclo di vita può essere particolarmente breve. Basti pensare, ad esempio, all’ammodernamento dell’ottica (fotocamera) di uno *smartphone* che, innescando la produzione di nuovi modelli, genera la veloce obsolescenza dei vecchi originando una corsa tra i produttori alimentata e supportata dal commercio. È altresì possibile che il loro sviluppo sia frutto di nuove esigenze, come spesso accade nel mondo militare, dove il mutamento degli scenari e l’evoluzione delle tipologie di minacce impongono la revisione (quindi la ricerca) e l’ammodernamento dei sistemi con il fine di mantenere un vantaggio sul “competitore”.

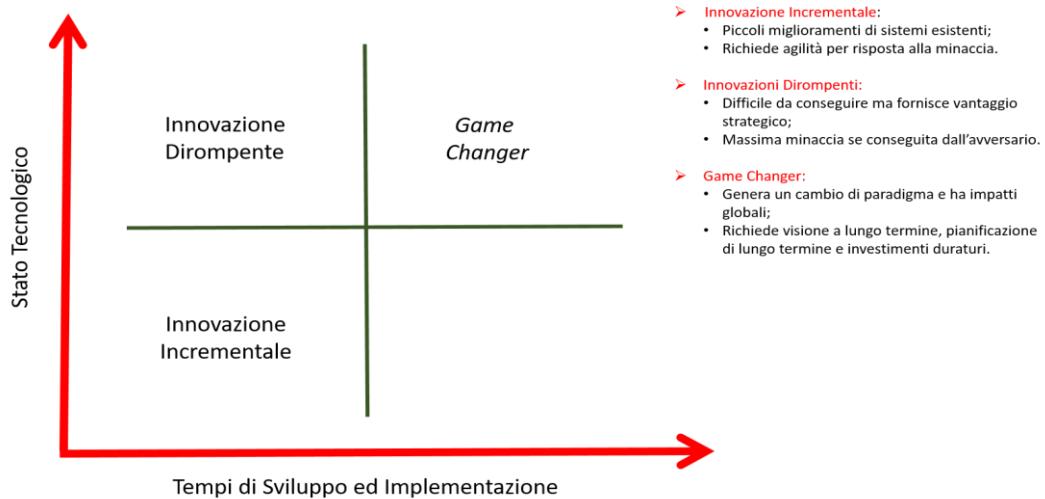


➤ **Tecnologie Dirompenti** la cui identificazione è correlata alla tipologia d'impatto ed effetto che possono produrre. Sono, infatti, quelle che stravolgono il sistema nel quale sono applicate e, talune volte, ne alterano in modo imprevedibile ed in breve tempo l'equilibrio (c.d. *game changer*). Sono le più complesse e critiche poiché possono ingenerare “sorprese strategiche”, mutamenti improvvisi con evidenti conseguenze di destabilizzazione, sia nel settore specifico di applicazione (magari rendendo obsolete alcune delle tecnologie esistenti), sia in altri settori strettamente interconnessi (come ad esempio quello economico, sociale, etico e politico), attraverso un impatto diretto, trasversale o di riflesso. Dirompente, ad esempio, è stata l'introduzione dell'energia nucleare che, da “mera” scoperta scientifica, si è velocemente tramutata in un volano strategico (chi possedeva, e ancora oggi possiede, munizionamenti nucleari detiene un deterrente politico-strategico ineguagliabile, forse superabile solo dagli agenti biologici).

È importante sottolineare che l'effetto “dirompente” può essere anche frutto di una spinta trasversale operata su di un settore tecnologico a sua volta emergente. Un forte interesse economico-industriale, o anche politico, può dar vita a uno sviluppo capacitivo specifico e mirato che, probabilmente, punta proprio a destabilizzare una situazione a vantaggio di un'altra.

Numerose tecnologie dirompenti nascono in ambienti impensabili, sono realizzate a basso costo e al di fuori di processi d'innovazione strutturati. Risultano, nella loro forma embrionale, di poco interesse per le grandi aziende poiché queste si interessano soprattutto al mantenimento delle posizioni di controllo dei mercati, gestendo i prodotti e le tecnologie esistenti, cercando di competere con i concorrenti unicamente migliorandole o inventando nuovi prodotti basati sull'evoluzione delle tecnologie già note. Per questo motivo, si procede aggiornando i prodotti, introducendo funzionalità aggiuntive o migliorandone alcuni attributi, focalizzandosi sulla variazione di valore (es. come l'aumento della velocità del processore o della risoluzione del sensore di una fotocamera).

Le tecnologie innovative ed emergenti posseggono una loro intrinseca prevedibilità poiché si manifestano e si consolidano gradualmente, seguendo lo sviluppo delle ricerche e delle scoperte scientifiche che, normalmente, impiegano anni per



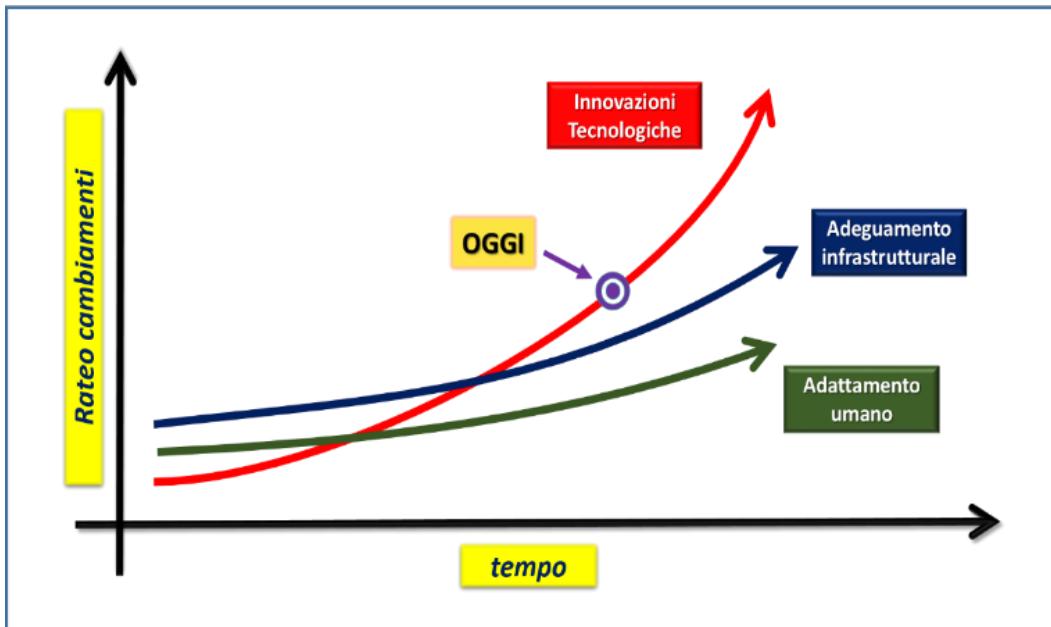
consolidarsi e produrre effetti. Di contro, le implicazioni associate alle tecnologie dirompenti, siano esse etiche, legali, economiche o sociali, così come le reali interconnessioni e le potenziali minacce, non sempre emergono immediatamente o risultano facilmente prevedibili, ma si manifestano con il tempo, in relazione alla diffusione e all'impiego, rendendo così indispensabile l'identificazione di idonei indicatori per anticiparne la globalità degli effetti trasversali e trovare soluzioni rapide ed efficaci.

Le risposte che saremo in grado di fornire ai mutamenti, sia graduali che repentina, dovranno essere necessariamente frutto di un approccio organizzativo e tecnologico “preventivo” che, in considerazione della velocità dei mutamenti, diviene essenziale per anticipare e poter attuare le necessarie pianificazioni e le dovute predisposizioni.

L'attenzione verso il settore delle tecnologie, nella loro natura emergente e dirompente, ha dato vita all'acronimo **EDTs** (*Emerging and Disruptive Technologies*) divenuto nel 2019 una delle principali priorità della NATO e dell'Unione Europea.

SVILUPPO DELLE *EMERGING & DISRUPTIVE TECHNOLOGIES*

L'impiego delle *Emerging and Disruptive Technologies* (EDTs) sta radicalmente trasformando ed innovando numerosi settori, tra cui l'intera sfera della Sicurezza e della Difesa. L'inevitabile progresso tecnologico genererà un concreto impatto su molte delle capacità che oggi impieghiamo e che presto vedranno un'obsolescenza



Progressione delle innovazioni, adeguamento infrastrutturale e adattamento umano

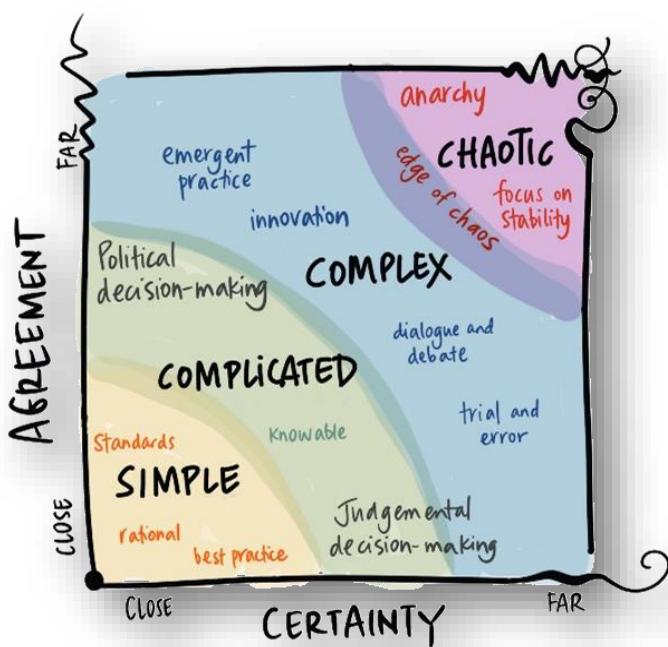
anticipata. La corsa all'adozione d'innovazioni altamente avanzate, sia in ambito civile che militare, sta divenendo un obiettivo determinante per molti attori internazionali che mirano ad acquisire una supremazia tecnologica ed un rilevante vantaggio strategico. Raggiungere e mantenere una predominanza nel settore della ricerca scientifica e tecnologica significa poter competere "ad armi pari" e sostenere obiettivi politici, militari ed economico-industriali.

Sia la NATO che l'UE stanno redigendo strategie e piani implementativi atti ad intraprendere iniziative capacitive che, oltre a modernizzare gli attuali strumenti militari, forniscano concreto impulso alle industrie, ma anche al settore della Ricerca e dello Sviluppo (R&D - *Research & Development*).

In quest'ultimo settore, la rivoluzione è ancora più marcata poiché se è vero che fino al secolo scorso l'innovazione tecnologica era trainata dall'industria militare, è altrettanto vero che in altri settori, ad oggi, è l'industria privata ad averne il monopolio. Il mercato globale ha imposto un'accelerazione alla quale le organizzazioni militari devono adattarsi, rivoluzionando le proprie strutture, i propri processi di acquisizione e di implementazione operativa. Una rivoluzione che, in realtà, abbraccia anche il settore della formazione, dell'impiego del personale e della *leadership*, trasformandosi in un sostanziale ed importante *mindset change*.

Un cambiamento radicale che l'Italia deve affrontare e che prevede un rafforzamento della collaborazione con l'industria, l'accademia e tra tutti gli attori governativi (nazionali ed internazionali), per individuare sinergie e soluzioni concrete, sostenibili e velocemente implementabili.

Lo sviluppo tecnologico segue una progressione inarrestabile ed esponenziale. I presupposti e le ipotesi che oggi vengono formulati e discussi in ambito scientifico ed internazionale dipingono – in linea di massima – scenari ben più critici di quelli che ci circondano o che possiamo immaginare. Si è transitati da eventi e scenari “complicati”, intesi come costituiti da un insieme di parti difficili da codificare, a situazioni ed implicazioni “complesse” che hanno origine dall'intreccio di elementi che interagiscono fra loro, creando disorientamento e provocando incertezza. I mutamenti all'orizzonte richiederanno sempre di più la necessità che l'uomo, sino ad oggi unico artefice di trasformazioni, sbilanciamenti e degradazioni “ambientali” (geografici, sociali, naturali ed economici), individui un suo nuovo ruolo nel quale la sinergia tra tecnologie e le proprie capacità cognitive dovrà trovare un necessario ed indispensabile compromesso, equilibrio e un vantaggio (*Human-Machine Teaming*).



Stacey Matrix adapted by S. Bradd and D. Finegold

Le innovazioni tecnologiche, che hanno contribuito al miglioramento delle condizioni di vita, sono il risultato dello sviluppo evolutivo e dell'operato dell'uomo. In considerazione della dirompente forza insita nelle EDTs, siamo chiamati a governare e gestire al meglio il loro sviluppo e il loro impiego futuro.

Nello specifico, i lavori degli esperti nella redazione di questo documento concettuale hanno teso a fornire risposte a domande precise, riassumibili nella identificazione dei motivi per cui il nostro sistema di Difesa deve fare uso delle EDTs e nella previsione delle loro evoluzioni. Tutto ciò è stato inserito nell'analisi del contesto industriale e della ricerca nazionale senza, ovviamente, trascurare il panorama internazionale; quest'ultimo è servito da riferimento per le considerazioni su ipotetici scenari sia collaborativi (in ambito bilaterale e multilaterale) che di possibile confronto (a vari livelli di intensità).

Le tecnologie emergenti e dirompenti individuate sono:

- **BIG DATA**
- **INTELLIGENZA ARTIFICIALE**
- **SISTEMI AUTONOMI**
- **TECNOLOGIE SPAZIALI**
- **TECNOLOGIE IPERSONICHE**
- **TECNOLOGIE QUANTISTICHE**
- **BIOTECNOLOGIE**

Appare evidente che i suddetti ambiti tecnologici non sono tutti analizzabili con la medesima metodologia, in ragione di alcune loro differenze strutturali. Le tecnologie per l'analisi dei dati, ad esempio, possono evolversi rapidamente con dotazioni finanziarie ed infrastrutturali molto meno imponenti di quelle richieste per realizzare progressi “dirompenti” nelle tecnologie per lo Spazio, nei velivoli ipersonici oppure nei sistemi quantistici. In un certo senso, quindi, alcune tecnologie sono più “democratiche” di altre, così come alcune presentano caratteristiche di elevata applicabilità trasversale, se non persino di “mattone tecnologico” fondamentale per le altre. Ne sono prova la simbiosi tra Intelligenza Artificiale e Sistemi Autonomi, l'applicabilità dell'analisi ed elaborazione dei dati ad ogni contesto progettuale e la pervasività degli strumenti satellitari negli ambiti delle applicazioni delle altre tecnologie.

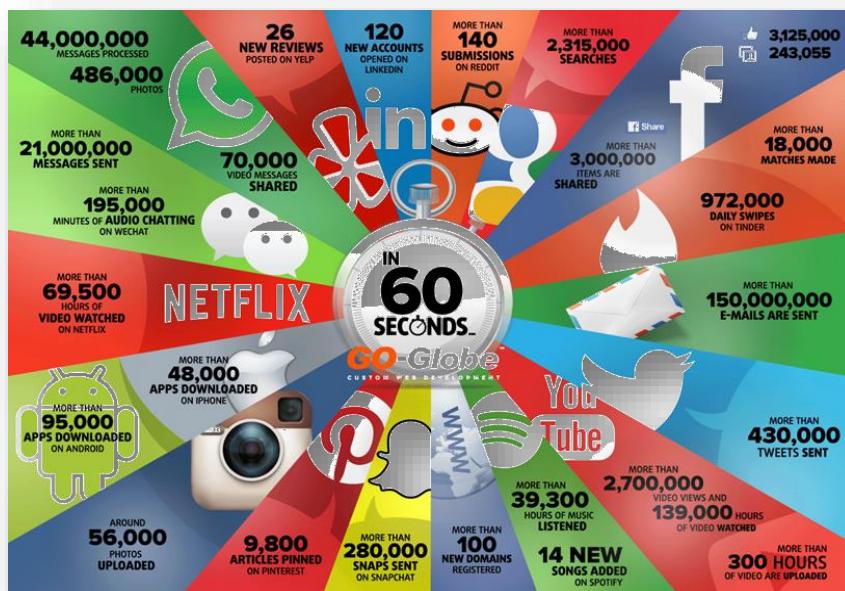
Capitolo 1

BIG DATA

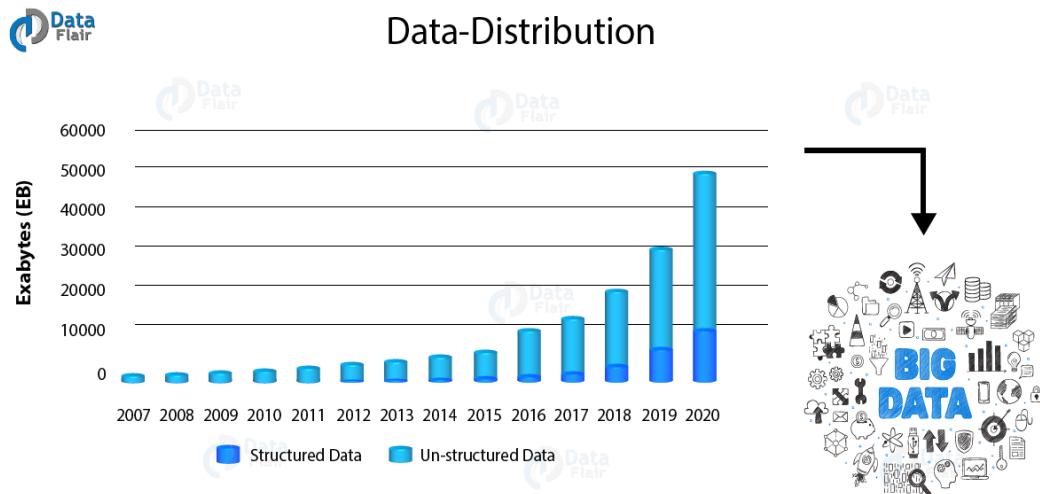
1.1 PERVASITÀ DEI DATI

La diffusione dei Dati, genericamente denominati *Big Data*, afferisce, con buona approssimazione, ad ogni aspetto della realtà e della società in cui viviamo. Nel corso degli ultimi anni diversi fenomeni hanno moltiplicato in maniera decisamente significativa la mole dei dati disponibili ed utilizzabili dai più, tra questi:

- la proliferazione e la diffusione di nuove tecnologie, l'ampia disponibilità di strumenti di accesso alla rete sempre più sofisticati e dalle prestazioni avanzate, l'incremento esponenziale dei sensori a basso costo di produzione e con significative capacità di raccolta e condivisione dei dati (*smart-phone*, *tablet*, sistemi di videosorveglianza, tele-rilevamento aereo, ecc.);
- la condivisione dei dati personali ed il loro conferimento ad aziende/società private in modo automatico e/o involontario (le norme sui *cookies* che spesso vengono accettate acriticamente e che spesso stanno alla base di attività di profilazione particolarmente aggressive nei riguardi dell'utente);
- l'esplosione dei *social media* quale piattaforme virtuali per l'interazione sociale tra le persone, la creazione e la condivisione di contenuti *online*, la commercializzazione di prodotti e servizi, la creazione di dimensioni e realtà virtuali (es. *social networks*, *weblogs*, *content communities*, *virtual social worlds*, *virtual game worlds*, *metaverse*, ecc.).

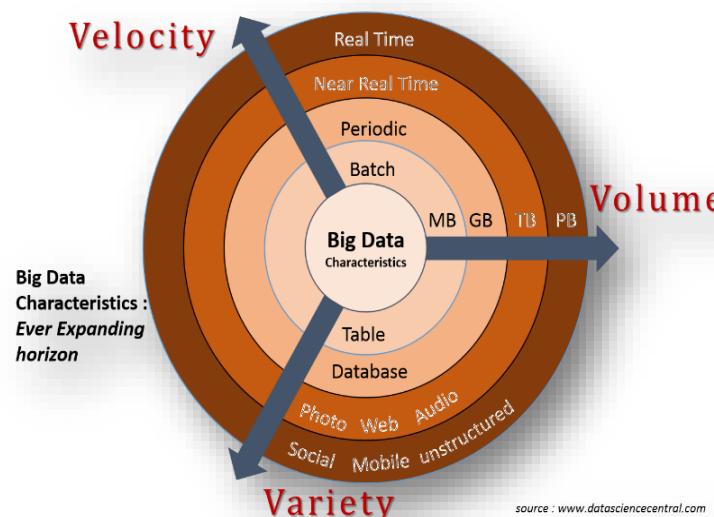


A titolo di esempio, nel biennio 2016-2018 è stato generato il 90% dei dati presenti nel mondo. Ogni giorno, poi, si aggiungono alle sole reti di *Big Data* 2,5 quintilioni di nuove notizie, di cui l'80% sono dati non-strutturati (e quindi di difficile aggregazione ed utilizzo).



La nozione di *Big Data* ha iniziato a farsi largo nell'ambito dell'*Information Communication and Technologies* (ICT) solamente all'inizio degli anni 2000, quando l'americano *Doug Laney* ne ha teorizzato la nozione secondo il c.d. paradigma delle 3V:

- Volume: quantità di dati generati da varie sorgenti eterogenee;
- Varietà: *format* dei dati (strutturati, non strutturati, numerici nei database tradizionali, ecc.) che vengono generati, memorizzati ed utilizzati;
- Velocità: rapidità con cui i nuovi dati vengono generati.



Al modello di *Laney* sono poi state successivamente aggiunte caratteristiche che hanno contribuito a specificare e meglio descrivere il concetto di *Big Data*, ovvero:

- Veridicità: qualità dei dati e possibili difficoltà (provenendo essi da fonti diverse) di collegare, abbinare, pulire e trasformare i dati tra i sistemi;
- Valore: capacità di trasformare i dati in valore;
- Variabilità: mutevolezza dei dati;
- Complessità: dimensione del *dataset* e complessità di gestione.

Ad oggi si potrebbe aggiungere una ulteriore specificazione, la Pervasività, intendendo con questo termine la sempre maggiore diffusione dominante che i *Big Data* hanno in tutti i settori della vita, pubblica e privata.

I *Big Data* si presentano in vari formati e strutture e, dal punto di vista della quantità dimensionale, non è univocamente definita una soglia di riferimento prestabilita, ma convenzionalmente si può parlare di *Big Data* quando “l'insieme di dati è talmente grande e complesso che richiede la definizione di nuovi strumenti e metodologie per estrapolare, gestire e processare informazioni entro un tempo ragionevole”.

In ultimo, oltre alla varietà dei formati e delle strutture in cui sono disponibili, i *Big Data* presentano anche una varietà di fonti e sensori da cui sono generati/tratti: possono essere sostanzialmente suddivisi in *human-generated* (acquisiti mediante sistemi che agiscono nella sfera del sociale quali piattaforme di *social network*, *blog*, ecc.), *machine-generated* (prodotti da sensori eterogenei quali centrali di monitoraggio di eventi meteorologici, strumenti scientifici, dispositivi biomedicali, ecc.) o *business-generated* (dati a qualsiasi titolo generati internamente ad un'azienda, che registrano tutte le attività *data-driven* dei processi di *business* aziendale).

1.2 GESTIONE DEI DATI (DATA ANALYTICS)

Le organizzazioni commerciali e industriali da tempo hanno cominciato a sfruttare i *Big Data* includendoli nei processi aziendali come *best practice*. Sotto tale prospettiva, i dati vengono considerati non soltanto una risorsa da utilizzare, ma piuttosto come un bene o *asset* che deve essere opportunamente gestito al pari di un qualsiasi altro elemento fisico in termini di integrità, sicurezza, resilienza e fruibilità. E' quindi necessario strutturare processi di *governance* in grado di garantire tali proprietà attraverso l'intero ciclo di vita del dato (*Data Life Cycle*).

Mentre l'adozione delle tecnologie per la gestione e l'analisi dei dati nell'ambito delle organizzazioni civili e commerciali/industriali è matura e consolidata, solo più recentemente un numero crescente di agenzie ed organizzazioni governative sta trasformando i processi ed i sistemi interni per sfruttare al meglio questa nuova risorsa. Si tratta della gestione e dell'analisi delle informazioni su larga scala, tali da superare la capacità delle tecnologie tradizionali di elaborazione dei dati.

La gestione dei dati o *Big Data Analytics* è in grado di produrre conoscenze operative su vasta scala grazie ai progressi tecnologici nell'archiviazione, nell'elaborazione e nell'analisi degli stessi, con particolare riferimento a:

- rapido ed esponenziale aumento negli ultimi anni dello *storage* e della potenza della CPU/GPU, con significativi benefici associati alla riduzione dei costi;
- flessibilità ed efficacia dei *data center* e delle architetture *cloud computing* per il calcolo e la memorizzazione delle informazioni;
- sviluppo di *suites* di prodotti che consentano agli utenti significativi vantaggi in termini di calcolo distribuito e di memorizzazione di grandi quantità di dati attraverso una elaborazione parallela e flessibile.

Il primo aspetto, pertanto, che appare subito in tutta la sua importanza è la necessità di memorizzazione dei dati e di garantire un accesso rapido agli stessi. Tale mole di dati per poter essere impiegata deve,



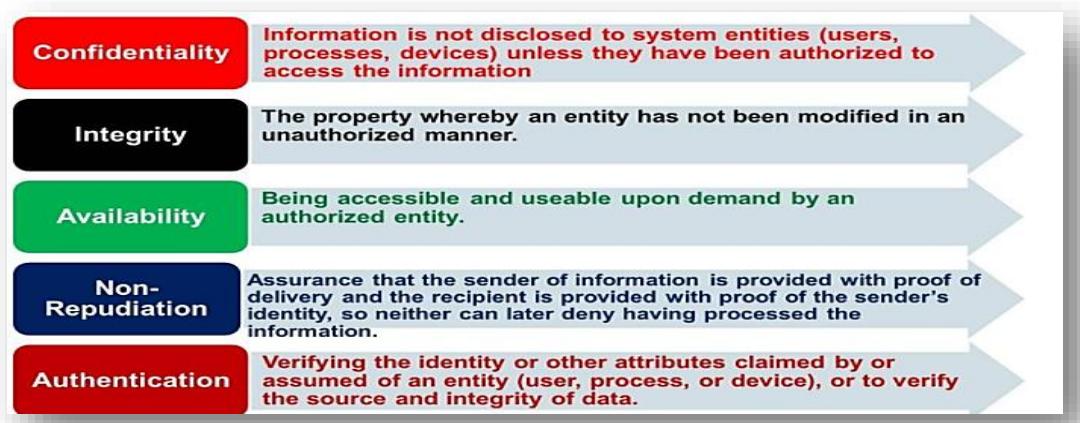
infatti, essere riversata su adeguati (in termini di dimensione e velocità di accesso) supporti di *storage* dotati di connettività tale che ne permetta l'impiego nei tempi compatibili con le applicazioni che li richiederanno.

Il secondo aspetto decisamente importante è quello della sicurezza che, nella sua accezione più ampia e completa, include:

- la confidenzialità (es. *privacy*);
- l'integrità (certezza che il dato non venga alterato durante il suo ciclo di vita);
- la disponibilità (il dato, da cui i sistemi e servizi associati, deve essere sempre disponibile);
- il non ripudio (necessità che le transazioni non possano essere negate da una o da entrambe le parti);
- l'autenticazione (controllo degli accessi ai dati).

Tralasciando gli ultimi due caratteri, molto importanti ma più tecnici, riuscire a garantire la confidenzialità, l'integrità e la disponibilità di una mole immensa e sempre crescente di dati è certamente un impegno decisamente complicato, ma fondamentale, che deve prevedere l'applicazione di concetti di sicurezza quali, ad esempio, quello di “*Security by design*”.

Un altro aspetto importante è rappresentato dalla capacità di gestione dei dati (*Data Governance*) ossia l'insieme dei processi, delle *policy*, degli standard e delle responsabilità che assicurano la qualità e la sicurezza dei dati impiegati all'interno di un'organizzazione civile e militare.



In ultimo la questione della *privacy*, legata soprattutto ai notevoli impatti sulle attività, le opinioni e le scelte delle singole persone attraverso l'analisi dei dati. Molto spesso la *privacy* è già protetta dalle leggi nazionali o dai trattati internazionali, cui le applicazioni *Big Data* sono tenute a conformarsi anche se ciò non elimina completamente i potenziali rischi legati ad un uso illegale dei dati sensibili. Al fine di tutelare la riservatezza dei dati personali l'UE, nel 2002, ha emanato la Direttiva *ePrivacy* (attualmente in fase di revisione con lo scopo di emanare un nuovo Regolamento *ePrivacy*) volta a garantire la riservatezza delle comunicazioni e dei dati personali nel settore delle comunicazioni elettroniche. Nel 2016 il Parlamento Europeo ed il Consiglio hanno adottato l'ormai noto Regolamento 2016/679, meglio conosciuto come *GDPR – General Data Protection Regulation* che, realizzando la definitiva armonizzazione della regolamentazione in tema di protezione dei dati personali all'interno dello spazio UE e richiamando i concetti di *accountability*, *data protection by design* e di *data protection by default*, ha fortemente condizionato tutti i soggetti che trattano dati personali di cittadini europei prevedendo, in caso di violazione, pesanti sanzioni economiche. A tal proposito va ricordato che, a seguito dell'approvazione del Trattato di Lisbona il quale ha riconosciuto alla Carta di Nizza (o Carta dei diritti fondamentali dell'Unione Europea) lo stesso valore giuridico dei trattati, la protezione dei dati personali ha assunto, sulla base degli art.7 e 8 della Carta, il rango di diritto fondamentale dei cittadini dell'Unione¹. La tutela dei dati personali, inoltre, si

¹ Nell'ambito della tutela dei dati personali, si inserisce la recente pronuncia della Corte di Giustizia Europea la quale ha ritenuto il *Privacy Shield*, ossia l'accordo UE - USA sullo scambio dei dati, insufficiente ad assicurare una adeguata protezione dei dati personali dei cittadini UE. Le due parti, infatti, adottano un approccio concettuale differente sul tema. Mentre l'UE, attraverso il *GDPR*, ha impostato un sistema eguale e centralizzato per la protezione dei dati dei propri cittadini, in cui la tutela risulta essere anticipata attraverso il meccanismo del consenso preventivo alla raccolta e alla trattazione, gli Stati Uniti regolano tale questione solo in relazione a specifici aspetti giuridici. Da ciò ne consegue che la protezione dei dati è collegata a generici strumenti rimediali e non è considerata, come in Europa, un diritto fondamentale del cittadino.

inserisce nell’ambizioso progetto dello *European Data Strategy* orientato a creare, all’interno dello spazio europeo, un mercato unico dei dati dove questi possono circolare ed essere condivisi liberamente, in maniera trans-settoriale, a vantaggio di vari soggetti quali imprese, pubbliche amministrazioni, ricercatori ed organizzazioni. Gli obiettivi della strategia sono individuabili nella definizione di regole chiare ed eque sull’accesso ed sul riutilizzo dei dati, nell’investimento in strumenti ed infrastrutture per archiviare ed elaborare i dati implementando la capacità *cloud* europea (con l’importante iniziativa *Gaia-X*²), nella condivisione dei dati europei in settori chiave, con spazi dati comuni ed interoperabili, e nel riconoscimento agli utenti di diritti, strumenti e competenze per mantenere il totale controllo dei propri dati³. Per attuare tale progetto, nel 2020, la Commissione Europea ha emanato una proposta di Regolamento denominata *Data Governance Act*, che ha trovato recente approvazione da parte del Parlamento Europeo, volta a regolare la disponibilità dei dati nel settore pubblico ed a far crescere la fiducia nei servizi di intermediazione dei dati in tutta l’UE, anche allo scopo di fornire un modello di gestione dei dati alternativo a quello adottato dalle *Big Tech*. Al *Data Governance Act* è seguita, nel 2022, la presentazione della proposta per una legge europea sui dati (*Data Act*) avente lo scopo di introdurre norme armonizzate per l’accesso equo agli stessi ed in merito al loro utilizzo, riaffermando così la costante acquisizione di consapevolezza circa il fondamentale ruolo dei dati nella società del futuro. Inoltre, la Commissione Europea, nell’ambito della *European Digital Strategy* della UE, ha presentato due proposte normative finalizzate all’aggiornamento della regolamentazione UE nel settore digitale: il *Digital Services Act* ed il *Digital Market Acts*. Quest’ultimo, in particolare, in relazione al quale è stato recentemente raggiunto l’accordo tra Consiglio e Parlamento UE per un’approvazione definitiva entro il 2023, ha come obiettivo quello di limitare pratiche sleali nel caso queste siano attuate dai cd. *Gatekeepers*. Questi ultimi, essendo i possessori delle piattaforme *online* attraverso le quali devono transitare i servizi di altre aziende più piccole, nonché di una ingente mole di dati, possono esercitare condotte anticoncorrenziali a vantaggio di alcuni e a discapito di altri. Questi, inoltre, avranno anche l’obbligo di condividere i dati con gli utenti *business* che operano sulle loro piattaforme. Tutto ciò allo scopo di rendere il mercato più concorrenziale ed impedire la creazione di un sistema monopolistico dello stesso basato sul possesso privatistico dei *Big Data*. Nonostante i tentativi di rendere l’intero sistema il più equilibrato possibile, sarà impossibile non considerare il ruolo che, nel prossimo futuro, le grandi aziende dell’*hi-tech* avranno nel contesto internazionale. Occorrerà, quindi, adottare un approccio che tenga conto delle esigenze e delle dinamiche sia del settore pubblico che del settore privato per realizzare una sinergia vantaggiosa a favore di tutti gli attori coinvolti, cittadini *in primis*.

² La Fondazione GAIA-X è un’organizzazione internazionale con sede in Belgio che si propone di sviluppare un progetto europeo, guidato da Francia e Germania, per la prossima generazione di un’infrastruttura di dati per l’Europa e promuovere la sovranità digitale degli utenti europei dei servizi *cloud*.

³ C. Polito, “La governance globale dei dati e la sovranità digitale europea”, IAI Istituto Affari Internazionali.

1.3 QUALI TECNOLOGIE USERANNO I DATI?

Quello che ora appare decisamente interessante è anche l'esame di un possibile uso futuro (a medio e lungo termine) che probabilmente faremo di questa massa smisurata di dati. Volendo rifarsi ad altre tecnologie attualmente in fase di studio o agli albori della sperimentazione e ponendoci su un piano di logicità, ne esistono alcune che avrebbero poco senso di esistere (o addirittura non ne avrebbero) in assenza di dati.

In primis l'Intelligenza Artificiale, una tecnologia alla cui base esiste la possibilità di "istruire" delle macchine in modo che le stesse possano reagire e comportarsi in modo simile al cervello umano. Questa fase iniziale di "istruzione" (*machine learning*) è strettamente legata al grande flusso di dati fornito alla macchina senza il quale tutte le fasi successive non avrebbero alcun senso. Facendo un parallelismo, l'istruzione iniziale è molto simile a quella di un neonato che, immerso nell'ambiente familiare e, successivamente anche nel mondo esterno, acquisisce continuamente delle informazioni (dati) che gli permettono di imparare, migliorarsi e prepararsi per la vita futura che sarà caratterizzata, sempre più, di scelte e decisioni che dovrà prendere in modo indipendente. Un neonato che crescesse in un ambiente fortemente chiuso e con limitatissimi contatti con l'esterno riceverebbe un flusso informativo molto ridotto e lo sviluppo cerebrale sarebbe fortemente compromesso,

esattamente come per la fase di *learning* di una Intelligenza Artificiale che non ricevesse un idoneo flusso di dati.

Un'altra tecnologia che, per induzione, diventerebbe poco utile in assenza di dati è certamente quella legata ai Sistemi Autonomi.

Tali sistemi, infatti, si

basano fondamentalmente sull'Intelligenza Artificiale e, per i motivi già evidenziati precedentemente, non potrebbero assolutamente essere sviluppati in un ambiente privo di una idonea quantità di dati.

Esiste almeno un'altra tecnologia che in assenza dei dati perderebbe molto del proprio *appeal*: la tecnologia quantistica. Tale tecnologia, infatti, nasce per velocizzare enormemente i processi di calcolo, finalità questa che, in prima approssimazione, sembrerebbe disgiunta dalla questione dei *Big Data*. In realtà vi sono molte situazioni in cui lo scopo di impiegare una velocità di calcolo così elevata è legata alla necessità di elaborazione di dati in tempi molto ridotti (si pensi, ad esempio, alla tecnologia quantistica applicata all'Intelligenza Artificiale). Appare, quindi, evidente, anche in questo caso, come l'assenza di una idonea



quantità di dati diventi elemento discriminante per l'uso delle tecnologie quantistiche (almeno per talune applicazioni).

Volendo affrontare il discorso da un punto di vista più generale, tutte le tecnologie (siano esse EDTs o altro), tutti i sistemi e tutti i servizi già esistenti, ed a maggior ragione quelli che avremo nel futuro, necessitano di dati forniti in quantità sempre maggiore, ipotizzando un rateo di crescita di tipo esponenziale. Questo aspetto di “proliferazione esponenziale” di dati ci porta a dover affrontare alcuni aspetti molto importanti legati, fondamentalmente, alla sicurezza degli stessi in un’ottica di Difesa nazionale e Sicurezza.

1.4 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA

La natura stessa dei *Big Data* rende assai difficile ed estremamente sfidante inquadrarne e delimitarne i potenziali impieghi agli attuali cinque domini delle operazioni militari (terrestre, marittimo, aereo, cibernetico e spaziale), essendo i dati trasversali a tutti i sistemi e servizi utilizzati nei diversi domini, il cui funzionamento non può prescindere dalla presenza di dati stessi.

Proprio il riconoscimento del *Cyber* e Spazio ha dato il via ad una iniziale esplorazione in questi due nuovi domini attraverso l’acquisizione di un significativo quantitativo di dati che necessariamente vanno raccolti, memorizzati, analizzati, valorizzati, protetti e messi a sistema con quelli provenienti dai domini “classici”. Tutto questo al fine di dare all’utente finale (decisore o attuatore che sia) un complesso di informazioni coerenti che gli forniscano la piena *Situational Awareness* dello scenario in cui egli opera, adattando la propria linea d’azione e le proprie decisioni in funzione dell’*end state* da raggiungere e dei riscontri dal campo delle azioni poste in essere (*measures of effectiveness*).

È, quindi, evidente che, ognualvolta ci si troverà ad approcciare un nuovo ambiente di azione/dominio di operazioni, trarremo da questo una nuova e significativa mole di dati che contribuirà ad accrescere il nostro patrimonio informativo. Ciò è particolarmente vero se si prende in considerazione il progressivo sviluppo delle *Cyber and ElectroMagnetic Activities* (CEMA) e l’ineluttabile aumento dei dispositivi connessi in rete (*Internet of Things* IoT e *Internet of Military Things* IoMT), che contribuiranno a rendere ancora più complesse le dinamiche del confronto militare necessitando di sistemi avanzati di Intelligenza Artificiale e *big data analysis* per consentire ai livelli decisionali di avere una *picture completa*.

Nei prossimi anni la Difesa dovrà quindi, con un approccio trasversale e multidisciplinare, monitorando costantemente l’evoluzione tecnologica nel campo dell’ICT, concentrare le proprie attenzioni su:

- sviluppo, mantenimento e aggiornamento della capacità di raccolta, memorizzazione e trattazione dei dati (ad esempio, sistemi basati su tecnologie *edge computing* o future sue evoluzioni, impiego di reti neurali e di sistemi di Intelligenza Artificiale flessibili ed efficaci);

- sviluppo di sistemi di analisi e strumenti predittivi basati su tecnologie allo stato dell’arte in grado di supportare adeguatamente l’azione del decisore, sia esso politico che militare, nello sviluppo delle operazioni in ambiente Multidominio e nella cooperazione civile/militare. I sistemi dovranno essere flessibili ed efficaci e potranno essere accessibili a seconda dell’esigenza di conoscere dell’attore, quindi sempre più specifici ed attagliati all’ambiente/dominio di riferimento⁴ (*need to know e need to share*);
- sviluppo di adeguate forme di protezione dei *Big Data* che, in concorso con gli attori nazionali che operano nel settore della raccolta informativa, consentano di prevenire/contrastare efficacemente le minacce poste dai sempre più numerosi attori che agiscono nel cyber-spazio per sottrarre dati a fini di lucro/vantaggio informativo;
- impulso allo sviluppo/ridefinizione di aspetti etico-giuridici per rivedere il *corpus normativo* in ottica Multidominio ed interagenzia;
- definizione di chiari processi di *Data Governance*.

Per quanto attiene, invece, alle operazioni militari, queste presuppongono la disponibilità di informazioni/notizie ad ampio spettro sul dominio o domini nei quali si deve andare ad operare che devono essere raccolte, valorizzate e rese disponibili (disseminate) ai decisori per la condotta delle operazioni stesse. Le informazioni devono essere costantemente o, al limite, periodicamente aggiornate al fine di disporre sempre di una *Situational Awareness* e di un correlato *Situational Understanding* omnicomprensivo, dinamico ed esaustivo del dominio/i di azione. In questo senso il processo OODA loop (*Observe, Orient, Decide, Act*), basato sulle capacità di osservare, orientare, decidere ed agire più velocemente dell’avversario da parte di una organizzazione, può essere così declinato in base ai dati che va dall’acquisizione delle informazioni fino al momento decisionale attraverso le seguenti fasi:

- ***Observe***: prevede la raccolta di dati da varie fonti quali sensori, IoT (*internet of things*)/IoMT (*Internet of Military Things*) e altri dispositivi nelle tre dimensioni di riferimento (fisica, virtuale e cognitiva) quale base informativa per il proseguo del processo. I sensori sono considerati nel modo più ampio, includendo anche i *social media* e le altre forme di raccolta dati (de)strutturata. Per avere un valore questi dati devono essere verificati e fusi all’interno di un’unica *picture* mediante un’infrastruttura in grado di gestire una grande quantità di dati su molteplici livelli di sicurezza.
- ***Orient***: questa fase prevede l’utilizzazione di sistemi di *big data analysis* e algoritmi in grado di realizzare, in tempi brevi, una rapida analisi e l’elaborazione dei dati acquisiti, funzionale alla generazione di una visione unificata e dettagliata della situazione, frutto di una ingente mole di dati condensata ed aggregata in informazioni.

⁴ In alcuni Paesi (ad es. gli USA) si stanno invece rendendo i flussi informativi “*platform agnostic*” proprio per garantire la massima fruibilità, attraverso sistemi di rete diversi e connessi *on-the-fly*, dell’informazione.

- Decide: dopo essere state elaborate, le informazioni necessitano di essere presentate all'utilizzatore in modo tale da supportare il processo di *decision making*. Il decisore, oltre ad avere la necessità di acquisire una dettagliata consapevolezza situazionale nelle tre dimensioni di riferimento, deve disporre anche delle *future CoAs (Course of Actions)*, proprie e degli avversari, basate sulla fusione dei dati, sui modelli e sulla conoscenza in generale, attraverso anche l'impiego di sistemi di Intelligenza Artificiale quale strumento di *decision support*.
- Act: una volta che i dati sono stati raccolti (anche attraverso *feedback*), elaborati e trasformati in informazioni, è possibile procedere all'esecuzione delle azioni prese in considerazione per conseguire gli obiettivi predeterminati. In questo contesto l'evoluzione dei sistemi di Intelligenza Artificiale sarà sempre più importante anche in relazione al ruolo dell'essere umano nella scelta delle azioni da compiere.

L'obiettivo da perseguire è, dunque, quello di elaborare processi basati su nuove tecnologie in grado di realizzare un ecosistema che permetta di analizzare ed integrare i dati raccolti per poi essere utilizzati nei vari contesti operativi, incrementando le capacità di C2. Tale obiettivo sta assumendo sempre maggiore importanza con l'avvento del concetto delle *Multi Domain Operations* (MDO), in cui la disponibilità di informazioni aggiornate “giace e si nasconde” su diversi *layers* e non in un unico dominio/*layer*. Una tale mole di dati, va da sé, costituisce un aspetto strategico che deve adeguatamente essere tutelato e reso sicuro per impedirne l'acquisizione e l'uso contro la nazione stessa da parte di terze parti per trarne profitto o minare la sicurezza stessa dello Stato. Tutelare questo patrimonio informativo assume, quindi, un valore strategico, soprattutto per quanto attiene agli aspetti inerenti la Difesa. La disponibilità di dati costantemente aggiornati raccolti nei domini di operazioni, adeguatamente analizzati e memorizzati e resi disponibili ai decisori, mettono l'attore che li possiede in condizione di applicare efficacemente i concetti di “*information superiority*⁵” e “*information dominance*⁶”, fondamentali



⁵ L'*Information Superiority* è la capacità di raccogliere, elaborare e diffondere un flusso ininterrotto di informazioni sfruttando o negando la capacità di un avversario di fare lo stesso.

⁶ L'*Information Dominance* è quel grado di *Information Superiority* che consente al possessore di utilizzare sistemi e capacità di informazione per ottenere un vantaggio operativo in un conflitto o per controllare la situazione in operazioni diverse dal conflitto negando tali capacità all'avversario.

per l’acquisizione di quella posizione di vantaggio informativo che consentirà, nel dominio in cui ci si confronta, di raggiungere l’obiettivo negandone, di converso, il raggiungimento all’avversario.

Il complesso delle strutture CIS della Difesa, funzionali all’esercizio del Comando e Controllo delle operazioni, andrà quindi considerato come “infostruttura critica”, la cui efficienza/efficacia, aggiornamento e protezione andranno garantite senza soluzione di continuità 24/7. Nello specifico occorrerà:

- valutare la migliore tipologia di architettura da implementare, scalabile e facilmente aggiornabile in funzione dell’evoluzione della tecnologia legata alla gestione dei *Big Data* ed al loro incremento nel corso del tempo. Sarà, inoltre, necessario prevedere un’architettura in grado di garantire la capacità di elaborazione di una grande mole di dati, acquisita a livello decentralizzato, soprattutto in quei contesti operativi dove la connettività è pregiudicata o fortemente ridotta (non sempre, infatti, è possibile procedere alla elaborazione dei dati allo stesso livello nel quale questi sono stati acquisiti⁷);
- studiare e successivamente adottare tutte le misure tecniche e, laddove non sufficienti, procedurali atte a prevenire l’accesso, la cancellazione e l’estrazione, volontaria o involontaria, dei dati;
- considerare sempre gli aspetti inerenti alla *minaccia cibernetica* rappresentata da un numero crescente di attori che tentano ogni giorno di acquisire una grande mole di dati per poi utilizzarli a proprio favore, generalmente illeciti, per ottenere un vantaggio economico o di posizionamento strategico nello scacchiere internazionale;
- mettere in atto delle nuove procedure di *procurement* per l’acquisizione / aggiornamento delle capacità infostrutturali e, più in generale, di *networking* tra *sensors* ed *effectors*. Esse dovranno essere infatti sufficientemente rapide da tenere il passo con la citata “crescita esponenziale” dei *Big Data*, pena l’essere operativamente irrilevanti. Inoltre, dovranno seguire flussi di aggiornamento indipendenti dai singoli sistemi d’arma che ne fruiscono (ad es. “*platform agnostic*”), elevandosi di per sé al rango di “abilitanti strategici” e, quindi, meritevoli di finanziamenti specifici (si pensi, ad esempio, nei contesti futuri di tipo *denied* come l’A2/AD, dove è irrealistico non prevedere tentativi di *disruption* dei flussi informativi da parte di un *peer competitor*).

⁷ Attualmente l’orientamento è verso architetture decentralizzate o distribuite (*edge computing*), integrando il concetto di architetture centralizzate (*data center / cloud computing*). In realtà si parla di infrastrutture ibride, dove il concetto di *data center* rimane e coesiste con l’*edge computing* al fine di ridurre sia i tempi garantendo agli utenti finali risposte immediate e prestazioni migliori a prescindere dalla banda a disposizione.

Capitolo 2

INTELLIGENZA ARTIFICIALE

2.1 UN'EVOLUZIONE “DARWINIANA”

“L’Intelligenza Artificiale sarà la nuova elettricità”: con questa predizione il professor Andrew Ng dell’Università di Stanford⁸, uno dei più grandi esperti di Intelligenza Artificiale (IA) al mondo, sta indicando chiaramente come questa nuova tecnologia possa rivoluzionare il mondo e la società nei prossimi anni. Già oggi è possibile vedere (o si è vicini a vedere) interessanti applicazioni dell’IA, impensabili fino a pochi anni o decenni fa in settori molto diversi (se non nei film di fantascienza), come il riconoscimento di oggetti in tempo reale (auto, moto, barche) avendo come *input* delle normali telecamere di sorveglianza; il riconoscimento del linguaggio naturale e facciale per svariate applicazioni; la realizzazione di un incremento di risoluzione di immagini e video mediante sofisticate

tecniche di
estrapolazione;
l’ottenimento di
foto e video
montaggi
estremamente
realistici (fino ad
arrivare ai *deep
fake*). Analoghi
innovativi risultati
si stanno
ottenendo
nell’automazione



industriale, nell’*healthcare* (soprattutto nell’ausilio alla diagnostica per immagini), nella logistica (*predictive maintenance*), nell’aviazione (es. nel *training* dei futuri piloti di aerei attraverso la realtà aumentata), nel *automotive* e nella guida autonoma dove interpretare in tempo reale grosse moli di informazioni provenienti da svariati sensori è molto difficile o impossibile per operatori umani, nell’*Internet of Things* (IoT) attraverso la gestione e le correlazioni di dati (*data analytics*) e, naturalmente, nel settore militare, come negli *autonomous decision support systems*, nel *mission planning*, nel *Manned Unmanned Teaming* (MUM-T)⁹ e nel *Loyal Wingman* (LW)¹⁰.

⁸ Andrew Ng: “Why AI Is the New Electricity”.

⁹ Teaming of manned aircraft with unmanned air systems (<https://www.japcc.org/manned-unmanned-teaming/>).

¹⁰ Loyal Wingman: un drone fatto volare insieme ad un assetto pilotato, per agire quale assetto complementare o quale decoy per proteggere l’assetto *manned* contro misure di difesa aerea offensiva.

Molteplici sono i vantaggi potenziali per la società dal diffondersi della IA: la possibilità per i cittadini di avere servizi più sicuri, più personalizzati, più ottimizzati e più economici; per le aziende, il poter mettere sul mercato prodotti tecnologici più competitivi, riducendo al contempo i costi economici del ciclo di vita e della *toolchain* di tali prodotti; in ambito militare si potranno avere missioni maggiormente efficaci ed efficienti, soprattutto in scenari operativi complessi e poco conosciuti a priori, con minore rischio per le vite umane.

In termini di prospettiva futura (*foresight*) è interessante delineare l'ambito del “dove” l’Intelligenza Artificiale si diffonderà, così come del “quando” e con quale accelerazione. Nel merito del “dove” abbiamo conferma che, dal contesto militare all’*education*, dai processi ripetitivi a quelli creativi, dai dipinti alla musica, dalla diagnosi oncologica alla polizia predittiva, l’Intelligenza Artificiale è già attiva. In questi processi i risultati suggeriti dai più moderni sistemi di elaborazione (*mainframe*) - citiamo *Watson*, *Alfa Go* e *Tencent* - sono in grado di superare analisi cliniche fatte da gruppi di specialisti in termini di acutezza di indagine e, soprattutto, di indicazione terapeutica. Se si tratta di giocare al più complesso gioco di strategia, l’asiatico *Go*, dopo un relativamente breve periodo di apprendimento automatico, ha dimostrato la prevalenza del sistema informatico sul campione del mondo umano. Un ulteriore esempio è stato, inoltre, il rilascio di un sistema accessibile che parla con cadenza e accento della voce di Albert Einstein e risponde a quesiti complessi di teoria della relatività.

Sul “quando”, invece i dubbi sono molto più ampi, perché appare impossibile fare previsioni su sviluppi esponenziali tanto che le eventuali analisi devono essere caratterizzate da uno spirito cautelativo.

2.2 IMPLICAZIONI ETICHE, MORALI E GIURIDICHE

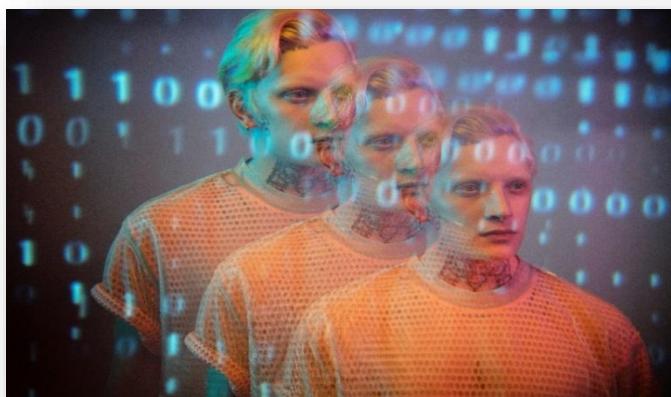
La crescente presenza e rilevanza dei sistemi di Intelligenza Artificiale nelle società contemporanee presenta risvolti che trascendono l’aspetto tecnologico e che possiedono un profondo potenziale trasformativo delle stesse, sollevando interrogativi di carattere etico, giuridico, organizzativo e morale. Infatti, tutte queste applicazioni sono senza dubbio di portata rivoluzionaria e aprono scenari ricchi di ulteriori potenzialità, ma al tempo stesso implicano diversi rischi, spesso inerenti alle questioni etiche, legali e di accettazione sociale, la cui interpretazione non è univoca, né è unanime il modo con cui approcciarla.

Tra le questioni più dibattute, per esempio, vi è quella della responsabilità di eventuali danni causati da dispositivi che facciano uso di IA (del costruttore? del proprietario? del programmatore degli algoritmi?). Numerosi approcci risolutivi sono stati proposti, tutti dipendenti dal grado di autonomia e dal contesto applicativo (tra questi ve ne è uno che suggerisce l’istituzione di una “personalità elettronica”).

Altre problematiche riguardano i valori da usare come riferimento per la valutazione etica dell'IA (una possibile risposta potrebbe essere quella di utilizzare la Carta dei Diritti Fondamentali dell'Unione Europea) e l'eticità o meno dell'uso di robot in ambito militare, tematiche altamente divisive in cui motivazioni convincenti possono annoverarsi in entrambe le posizioni.

Ulteriori problematiche si riferiscono al trattamento dei dati personali attraverso il riconoscimento facciale e la profilazione molto particolareggiata di individui, al fine di capire interessi e propensioni all'acquisto dei prodotti, che possono portare a pregiudizi (*bias*) determinati dalla tipologia di dati che sono stati utilizzati per effettuare il *training* degli algoritmi di IA. La possibilità di effettuare previsioni sul futuro stato di salute di un individuo sulla base dei suoi dati sanitari mediante tecniche di *data analytics* e, inoltre, nel medio termine vi è la possibilità che sempre più posti di lavoro vengano sottratti da macchine dotate di IA.

Non a caso, ha assunto notevole importanza nel dibattito sulle nuove tecnologie il tema della riproposizione inconsapevole di pregiudizi discriminatori derivanti da *bias* cognitivi che, riflettendosi nella tipologia di dati immessi e, quindi, negli algoritmi, di fatto annullerebbero la supposta imparzialità dei sistemi di IA. Tali condizionamenti comprendono una pluralità di caratteristiche umane quali la razza, l'appartenenza etnica, l'età, il genere, l'orientamento sessuale e/o religioso. In sostanza, dal momento in cui il funzionamento degli algoritmi si basa sull'immissione di dati "storici", il rischio che tali dati riflettano pregiudizi e distorsioni sociali storicamente acclarate è molto alto. Negli algoritmi, che basano le proprie capacità generalizzanti e predittive su di un meccanismo di *input-output*,



dove l'*input* è appunto rappresentato dai dati con cui vengono "nutriti" gli algoritmi, è chiaro che la "qualità" di tale *input* è dirimente, anche in relazione alla capacità di apprendimento dei sistemi di IA (*machine learning*). Noto è il caso dell'algoritmo

elaborato per automatizzare i processi di selezione del personale presso Amazon, il quale risultava preferire in modo netto candidati di sesso maschile per posizioni da software *developer* o altri ruoli tecnici.

Un ulteriore livello di problematicità deriva dalla segretezza e della inesPLICabilità che connota la maggioranza degli algoritmi di IA, che rende pressoché impossibile l'individuazione degli eventuali pregiudizi contenuti nei processi decisionali derivanti dagli algoritmi stessi.

È ormai assodato che la disuguaglianza di genere sia una questione trasversale ad ogni società ed attività umana, al punto che il *gender mainstreaming* – ovvero la necessità di adottare un approccio analitico che tenga conto della dimensione di genere – è ormai largamente considerato necessario ai fini di un’elaborazione equa ed obiettiva delle politiche pubbliche e della valutazione del loro impatto. Il rischio che i sistemi di IA (ovvero i *dataset*, gli algoritmi ed i dispositivi di addestramento dell’IA) perpetuino, diffondano e rafforzino gli stereotipi di genere, introducendo sostanzialmente ulteriori discriminazioni e marginalizzazioni ai danni delle donne – che, è bene ricordarlo, costituiscono metà della popolazione mondiale – è stato esplicitamente rilevato dall’UNESCO, la prima agenzia delle Nazioni Unite ad interrogarsi sulla questione. Già nel 2019, prendendo in esame alcuni tra i più comuni assistenti vocali digitali come *Alexa*, *Cortana* e *Siri*, l’Agenzia aveva rilevato come gli stessi contribuiscano a rafforzare una rappresentazione stereotipata e “servile” del genere femminile, avviando così un dibattito a livello globale sulla necessità di considerare la prospettiva di genere in relazione all’Intelligenza Artificiale.

Un’altra questione fonte di dibattito è l’eventuale capacità dell’IA di sviluppare autocoscienza grazie alla quale, nel lungo termine, essa possa arrivare addirittura “ribellarsi” all’umanità e tentare di soggiogarla, anche se tale questione è oggettivamente una eventuale problematica molto remota nel tempo e legata a un’ipotetica futura realizzazione di un’Intelligenza Artificiale Forte (o Generale). Si discute anche della prospettiva che l’IA possa creare dei brevetti, aprendo un altro ulteriore fronte di competizione.

Per poter, quindi, permettere che l’IA rappresenti pienamente un’opportunità, tali questioni andranno affrontate e risolte in modo approfondito (ma ragionevolmente veloce) dalle autorità politiche e di regolamentazione. Ciò consentirà di evitare che si possa inutilmente ostacolare lo sviluppo tecnologico e ritardare gli innegabili vantaggi che l’IA può portare, oltre che causare un vantaggio competitivo a favore di altre regioni nel mondo con diversi orizzonti valoriali che sapranno essere più agili nell’affrontarle.

2.3 TRUST

Un altro tema di rilievo riguarda il confine tra la fiducia (*trust*) nell’Intelligenza Artificiale e nel relativo algoritmo e la comprensione dello stesso. Anche in questo caso il confine è dinamico: tanto più si avranno decisioni prese dai sistemi che agiranno in modo super veloce e verosimilmente senza analitica comprensione dello schema di giudizio e dell’attuazione, ma con un risultato coerente con le attese umane, tanto più progressivamente aumenterà la fiducia e quindi l’integrazione e la positiva ibridizzazione uomo-macchina. Se, al contrario, ci saranno forzature secondo valori etici non condivisi, e quindi basati su pregiudizi (*bias*) non rispondenti alle attese umane, si andrà su un percorso negativo e per nulla risolutivo. Su questo scenario l’impegno generale delle istituzioni deve essere più attivo, ma

soprattutto più veloce con un’accelerazione del pensiero e della cultura umana che si ponga come obiettivo la riduzione del *gap* ancora in continua crescita tra accelerazione tecnologia e suo umano utilizzo. Da subito, quindi, è necessario un potenziamento e un’estensione della formazione culturale a tutte le tecnologie emergenti e soprattutto all’Intelligenza Artificiale, affinché il potenziale dirompente non divenga distruttivo.

Più nello specifico, dato l’impatto sociale delle decisioni prese per mezzo di algoritmi, grande preoccupazione desta il fatto che le reti neurali processano informazioni in modo poco interpretabile. Da un punto di vista tecnico, “l’opacità” dei sistemi rende impossibile una chiara comprensione di quali siano le correlazioni su cui effettivamente sono basate le elaborazioni finali e quindi le decisioni (c.d. *blackbox*). Preoccupa, innanzitutto, la possibilità che decisioni dall’impatto rilevante siano prese e applicate senza che esista un *framework* di fiducia che le governino e senza che se ne possa esporre una giustificazione comprensibile ai più, non solo dai tecnici, ma anche dall’utente medio. Ciò, infatti, non determina solo un impatto negativo sul diritto dell’utente umano all’autodeterminazione, ma anche il sospetto che alcune correlazioni su cui la decisione è basata possano incorporare pregiudizi eticamente condannabili e causare discriminazioni, trattamenti non equi e ingiustizie. In questo senso sono in corso numerosi studi verso un “*explainable Artificial Intelligence*” che permetta di individuare le motivazioni alla base delle scelte effettuate dagli algoritmi, in maniera da aumentare la fiducia negli stessi (c.d. *whitebox*).

2.4 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA

Risulta oltremodo consolidato che l’Intelligenza Artificiale, nel prossimo decennio, sarà una delle tecnologie impattanti sugli aspetti strategico-operativi delle operazioni militari. Le intrinseche potenzialità che essa detiene, in termini di possibile miglioramento delle *performance*, portano il mondo della ricerca e l’industria ad investire continuamente sia nell’ottimizzazione dei noti algoritmi di *machine learning* (siano essi basati sulle Reti Neurali, sul *Random Forest* o sugli Algoritmi Genetici), sia nello sviluppo di quelli più recenti sul *deep learning*, basati su un approccio più diretto al problema dell’apprendimento, focalizzandosi sull’interno *set* di dati disponibili anziché sull’estrazione delle caratteristiche più significative.

L’IA ha possibili applicazioni in molteplici ambiti, civili e militari. Tuttavia, è prevedibile che troverà un massivo sviluppo nei settori ove risulta vitale assumere decisioni in tempi ristrettissimi, nonché in contesti nei quali non è possibile avere un controllo diretto degli eventi, in *real time*, da parte dell’uomo. Per cogliere quanto appena assunto è sufficiente menzionare quanto avvenuto al velivolo della *NASA Perseverance*, il piccolo drone inviato su Marte che ha eseguito da solo l’atterraggio sul “Pianeta Rosso”: il ritardo di dieci minuti nelle comunicazioni tra la Terra e il sito di approdo non avrebbe infatti permesso di gestire eventuali piccoli

errori e, quindi, tutto è stato affidato all’Intelligenza Artificiale, sviluppata allo stato dell’arte dagli ingegneri dell’agenzia statunitense. A similitudine di quanto avvenuto a milioni di chilometri dal nostro pianeta, anche sulla Terra esistono zone remote che non possono essere servite, in *real time*, da una infrastruttura di comunicazione. Basti pensare agli abissi marini che assumeranno sempre più valenza strategica nel nostro secolo, definito anche il *Blue Century*.

Si tratta di un dominio nel quale, oggi, transitano il 97% delle informazioni della rete Internet, nonché buona parte delle risorse energetiche attraverso le condutture di gas e petrolio. Su tale rete “comunicativo-energetica”, vitale per la sicurezza e l’economia di una nazione, posata sul fondo, in un ambiente ostile e dalle caratteristiche fisiche assolutamente non permissive anche per le trasmissioni e le comunicazioni, devono operare dei sistemi *unmanned* che siano in grado di prendere decisioni in maniera completamente autonoma ed indipendente. A differenza di un sistema automatico, in cui l’azione è programmata ed eseguita regolarmente, un sistema autonomo è in grado di prendere decisioni sulla base della propria conoscenza (fatti e regole).

Nello specifico ambito della Difesa è auspicabile che siano eseguite dai sistemi intelligenti tutte quelle attività che possono compromettere l’incolumità fisica di esseri umani nell’esercizio di attività operative in aree a rischio. È il caso delle missioni di *Intelligence, Surveillance and Reconnaissance* (ISR) e delle attività di bonifica di ordigni improvvisati (*Improvised Explosive Device*, IED) tipicamente svolte dagli artificieri. I benefici derivanti dall’impiego di tecnologie abilitanti di IA riguardano anche altri casi d’uso: la possibilità di delegare ad agenti razionali l’analisi *real time* dell’enorme quantitativo di dati ambientali riguardanti un determinato teatro operativo per massimizzarne la *situational awareness* e l’efficientamento dell’impianto logistico dei nuovi sistemi d’arma.

Funzioni come il riconoscimento dei bersagli, lo sfruttamento dei dati della missione, il monitoraggio delle minacce e la *context awareness*, il supporto decisionale e l’autonomia della missione diventano indispensabili per condurre una missione ISR, mantenendo al minimo il carico di lavoro degli operatori e lo stress psicologico. Attraverso il *machine learning* e *deep learning* si prevede che questo tipo di capacità possa essere adottato all’interno di un sistema di gestione di missione adatto a piattaforme medio-grandi e senza equipaggio (*Unmanned Vehicles*) di tipo aereo, navale e terrestre e a sistemi di controllo/supporto di terra, espandendo le funzionalità dei sistemi di missione verso l’esecuzione di missioni potenziate e autonome.

Autonomous Target Detection, Recognition e Identification Systems possono essere ampiamente supportati dall’IA. Analisi di *background* e *foreground*, rilevamento e movimento di analisi di *pixel* (gruppi), confronto con forme semplici o referenziate, controllo rispetto alle librerie (ad es. analisi ISAR¹¹), co-registrazioni per

¹¹ *Inverse Synthetic Aperture Radar*

rilevazioni di cambiamenti coerenti e incoerenti (ad es. analisi SAR¹²) rappresentano aspetti adatti per essere affrontati e risolti con i metodi di Intelligenza Artificiale per generare *mission alerts* e *events monitoring*.

Le decisioni sugli eventi possono comportare condizioni per la ripianificazione o l'impostazione tempestiva di *payload resources* (ad es. sensori) e comunicazioni o piani di volo/rotte su eventi di missione (malfunzionamenti del sistema di recupero, rilevamenti di anomalie e identificazione del bersaglio, compiti prioritari, gestione delle armi, ecc.), prendendo in considerazione anche l'aspetto dell'HMI (*Human Machine Interface*) avanzato (come gli *Smart Operator Virtual Assistant*). La trasformazione digitale degli attuali laboratori nei laboratori intelligenti del futuro diventa impossibile da implementare se gli assistenti personali virtuali non saranno utilizzati per controllare le apparecchiature di rete e i sistemi.

La gestione dei *Big Data* e il *data mining* sono termini ampiamente menzionati oggigiorno quando è necessario analizzare un'enorme quantità di dati per scoprire la relazione tra i dati (scoperta della conoscenza) e per stabilire preziose informazioni come il *pattern reference* finalizzato al rilevamento di anomalie di dati di missione su cui dovrebbe essere richiesto un sistema di missione avanzato per prendere decisioni. L'impiego di algoritmi di *machine learning* e *deep learning* consente alle “macchine digitali” di elaborare significative moli di dati ed eseguire in autonomia analisi ed elaborazioni su di esse in modo tale da poter fornire un adeguato supporto al *decision maker*. L'implementazione di tali tecniche predittive può essere efficacemente impiegata in diversi ambiti *dual-use*, tra cui: *Predictive Situational Awareness*, analisi dello spettro a *Radio Frequency* (RF) (ambito SIGINT¹³), *Surveillance Systems*, *Predictive Maintenance*, *Image Analysis & Object Recognition* (ambito IMINT¹⁴), *Battlefield Healthcare* e *Cybersecurity*.

L'*Information Superiority* diventa una questione fondamentale per applicazioni di IA usate per il processo decisionale, ovvero il *planning* e *re-planning* delle risorse proprie del sistema di missione per raggiungere la superiorità contro un avversario. In questo caso, l'elaborazione e il *database* a bordo di una singola piattaforma potrebbero non essere sufficienti per comprendere autonomamente l'evoluzione dello scenario. Molte più informazioni, disponibili a distanza in *database* proprietario o piattaforme cooperanti (*Command, Control, Communications, Collaboration and Intelligence, C4I*) e/o come informazioni *open source* sul *web*, se elaborate in modo intelligente, dovrebbero fornire una visione più ampia dello scenario della missione (schemi di correlazione) e della sua evoluzione rispetto a quanto può fare il sistema di missione per mezzo dell'elaborazione dei dati che può produrre singolarmente. Le vulnerabilità possono portare alla perdita anche di informazioni militari classificate e danni ai sistemi militari, mentre i sistemi dotati di Intelligenza Artificiale possono rilevare autonomamente eventuali attacchi

¹² Synthetic Aperture Radar

¹³ Signals Intelligence

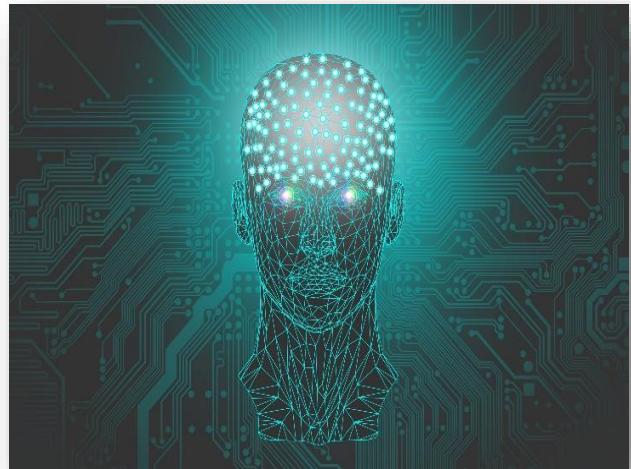
¹⁴ Imagery Intelligence

informatici, proteggere reti, computer, programmi e dati da accessi non autorizzati. Inoltre, i sistemi di sicurezza *web* abilitati IA possono registrare il modello di attacchi informatici e sviluppare strumenti di contrattacco per affrontarli. Un *Information Superiority Framework* sarà quindi auspicabile all'interno di un contesto interoperabile e di sicurezza informatica per ottenere i migliori risultati di missione.

La domanda “*What role do we want humans to play in wartime lethal decision making?*” posta da un esperto durante un forum sulle *Lethal Autonomous Weapons Systems*, in futuro potrebbe essere sempre più spesso parafrasata così: “*What role do we want senior military leadership to play in wartime decision making?*” ed essere riferita al “ruolo” che si vorrà dare alla *Senior Leadership* militare nella conduzione di operazioni complesse e al suo atteggiamento verso l’IA. Lo sviluppo tecnologico sempre più innovativo e l’impiego massiccio della IA in campo militare pongono quindi un dubbio relativo alla sua applicazione ai massimi livelli di Comando Strategico/Operativo, quale ad esempio quello di un *Joint Force Commander*. Se da un lato possiamo solo sottostimare lo sviluppo tecnologico cui assisteremo nel medio e lungo periodo, per rispondere al quesito posto dobbiamo concentrarci sull’essere umano e sulla sua “umanità” quale elemento di vantaggio o svantaggio: “Esisteranno nella guerra futura decisioni che lasceremo ancora ad un Comandante militare o si potrà delegare tutto agli *Autonomous Systems*? oppure “Potrà un sistema artificiale sostituire in toto un *senior leader*? Non è un azzardo riconoscere come oggi l’Intelligenza Artificiale non sia compresa a fondo dai *leader* (inclusi quelli militari) dei paesi occidentali, che ancora faticano a delineare un chiaro modo di procedere al riguardo. Tentativi iniziali sono stati fatti negli Stati Uniti, con la creazione del *Joint Artificial Intelligence Center* e con il rapporto rilasciato dal *Congressional Research Service* nel 2019, nel quale si riafferma l’importanza che i *leader* militari valutino gli sviluppi dell’IA ed esercitino un’adeguata supervisione delle tecnologie emergenti. Ciò li obbliga a capire cosa sia l’IA, cosa non sia e il modo migliore per sfruttarla a proprio vantaggio, ma soprattutto se sia possibile affidare la direzione di una operazione a sistemi completamente autonomi. Non si parla di utilizzare droni o l’IA per rendere efficienti i processi organizzativi e logistici o, in generale, per scopi tattici, utilizzo ormai largamente diffuso come provato dal successo del *Project Maven*¹⁵. Si parla invece di strutturare una operazione, darle un *Operational Design* e soprattutto stabilire un *end-state* e definire il *Commander’s Intent*, tutti aspetti che rappresentano il vero banco di prova di un Comandante e che lo caratterizzano rispetto ai colleghi. Lo stesso *Project Maven* ci offre un chiaro riferimento in tal senso, laddove il processo di ingaggiare con *Automated Systems* i *target* riconosciuti con la IA non è stato autorizzato.

¹⁵“*Project Maven*”, anche conosciuto come *Algorithmic Warfare Cross-Function Team* è un progetto del Pentagono finalizzato all’utilizzo dell’IA per la gestione delle immagini e dei *full motion video* per incrementare le capacità dei droni/APR sul campo di battaglia.

Partendo dal convincimento che passeranno anni prima di assegnare una operazione alla sola IA, appare opportuno chiedersi cosa fare ora nel breve termine. Una prima indicazione può essere ripresa dalle parole del *Lt. Gen. Michael Groen*, primo direttore del *Joint Artificial Intelligence Center* (JAIC): *"Se vogliamo che l'IA sia il nostro futuro, dobbiamo iniziare a costruire oggi le sue basi...[...] Dobbiamo avere un approccio comprensivo di tutti gli aspetti ed iniziare a connettere tutti i processi che riusciamo man mano ad automatizzare...[...] Dobbiamo modernizzare l'intero modo di rivedere l'approccio al warfighting in modo da mettere a disposizione dei decisi sistemi di supporto alla decisione che permettano di usufruire della infinita mole dei dati a disposizione...[...] È il sistema che supporta i decisi che deve evolvere"*. Questo aspetto ci porta quindi ad analizzare la struttura dello *staff* operativo che, per essere orientato all'utilizzo della IA, deve mutare notevolmente rispetto all'attuale composizione, ancora focalizzata quasi completamente all'analisi umana dei dati. Bisogna iniziare a prevedere la presenza di scienziati (*scientists*) necessari per selezionare e adattare i processi di IA, anche se questi potrebbero non disporre di alcuna prospettiva operativa. E' opportuno avviare un percorso progressivo di informazione e formazione nei confronti del personale della Difesa a tutti i livelli, al fine di evidenziare potenzialità e benefici risultanti dall'impiego di tale tecnologia e condividere valutazioni circa il rischio derivante da un drastico cambio di paradigma. Bisognerà introdurre figure quali quelle di un *Chief Data Officer* che sappia orientare le scelte del proprio Comandante verso dati pertinenti e verso la loro efficace ridistribuzione ai livelli più bassi. Tutto ciò evidenzia l'urgenza di rivedere anche la formazione e l'addestramento dei nostri *Senior Leader* per far sì che si costruisca la necessaria fiducia sia nei confronti di professionalità ora non prese in considerazione, sia nella stessa IA, scongiurando quindi il rischio che una naturale diffidenza verso questa tecnologia si trasformi in uno svantaggio militare irrecuperabile.



Capitolo 3

SISTEMI AUTONOMI

3.1 LIVELLI DI REASONING

Il concetto di “autonomia” associato ad un determinato sistema è strettamente legato (anche se distinto) a quello dell’Intelligenza Artificiale (IA). Ad oggi, non esiste una definizione univoca e condivisa di IA, ma seguendo un approccio pragmatico è possibile identificarla come “la capacità di taluni sistemi digitali di avere un comportamento riconducibile a quello umano ovvero di ragionare (*reasoning*) e/o di agire come un essere umano con l’obiettivo di prendere decisioni in modo autonomo”. Il punto è che lo stesso essere umano utilizza diversi livelli di *reasoning* in base alla complessità e alla criticità dell’azione da compiere. La definizione concettuale di IA proposta va, poi, necessariamente integrata con la considerazione che un essere umano non sempre ha un comportamento razionale ovvero non sempre decide di compiere l’azione “più giusta” rispetto alla conoscenza del contesto operativo e agli obiettivi che intende perseguire o che gli sono stati assegnati.

La finalità è, pertanto, quella di implementare, all’interno dei sistemi “intelligenti”, logiche comportamentali in grado di poter agire contestualmente in modo “autonomo” e “razionale”. Il concetto di razionalità è strettamente correlato alla misura della *performance* intesa come la capacità del sistema di IA di massimizzare il risultato atteso. È possibile distinguere diversi di comportamento umano in termini di *reasoning* ed il limite di separazione tra livelli contigui è sovente sfumato, non sempre così chiaramente definito. Estendendo¹⁶ la tassonomia inizialmente presentata da Rasmussen nel 1983¹⁷ è possibile individuare i seguenti quattro livelli di *reasoning*: *skill-based*, *rule-based*, *knowledge-based* ed *expertise-based*. E’ possibile, quindi, affermare che un sistema “intelligente” sia un sistema che



¹⁶ M. L. Cummings, “Man versus Machine or Man + Machine?” – IEEE Computer Society, 2014.

¹⁷ Jens Rasmussen, “Skills, Rules and Knowledge: Signals, Signs and Symbols and other distinctions in human performance model” – IEEE Transaction Systems, Man and Cybernetics. Vol.n.3, maggio 1983.

implementa (in modo più o meno spinto) i suddetti livelli di *reasoning*, mutuabili con le diverse modalità di comportamento della mente umana.

Indipendentemente dal livello di *reasoning* implementato e dal grado di autonomia raggiunto, ogni sistema “intelligente” è dotato di un agente razionale che consente al sistema stesso di raggiungere gli obiettivi prefissati in funzione della conoscenza acquisita sul contesto operativo (*perception*), della sua capacità di organizzare e rappresentare tali informazioni (*modelling*) e, infine, in base alla consapevolezza delle azioni che il sistema con i suoi organi attuatori è in grado di eseguire. La “razionalità” dell’agente risiede nella capacità di individuare le azioni più adeguate a conseguire l’obiettivo assegnato massimizzando la *performance*.

In definitiva, lo sviluppo di un sistema “intelligente” dotato di un determinato livello di “autonomia” presuppone l’assegnazione degli obiettivi che esso stesso deve conseguire, la definizione dei criteri e delle metriche con cui misurare la *performance* e, infine, l’individuazione delle variabili da monitorare in grado di caratterizzare adeguatamente l’ambiente operativo di riferimento. In ambito NATO¹⁸ si associa l’autonomia alla “*abilità di un sistema a rispondere a situazioni incerte, selezionando e combinando diverse opzioni possibili al fine di conseguire gli obiettivi assegnati, in base alla conoscenza e alla comprensione del contesto e della situazione in cui esso stesso opera*” mentre per la NASA come “*la capacità di un sistema di raggiungere degli obiettivi operando in assenza di controllo esterno*”¹⁹. Inoltre, l’autonomia è caratterizzata dai diversi gradi di autodeterminazione del sistema che vanno dal “completamente manuale” al “pienamente autonomo”, per cui è intuibile come tra i due estremi vi siano numerosi livelli di autonomia.

In sintesi, è possibile affermare che mentre un sistema automatico si può comportare in modo deterministico secondo un predeterminato e finito *set* di regole, un sistema autonomo nelle sue diverse declinazioni (dipendenti dai livelli di autonomia) può impiegare la capacità di autoapprendimento per assumere decisioni su problematiche non note a priori, escludendo l’intervento umano. In definitiva, i sistemi autonomi devono poter gestire l’incertezza (legata ad una rappresentazione parziale o disturbata dell’ambiente operativo) seguendo un approccio probabilistico e risolvere le ambiguità presenti sul campo in base a capacità di discernimento e giudizio acquisiti da precedenti esperienze.

¹⁸ NATO Science & Technology Trends 2020-2040.

¹⁹ “NASA Technology Roadmaps. Introduction, Crosscutting Technologies, and Index” – National Aeronautics and Space Administration, luglio 2015.

3.2 TIPOLOGIE DI SISTEMI AUTONOMI

I sistemi autonomi (*Autonomous Systems – AS*) possono essere classificati in funzione del loro modo di interagire con l’ambiente operativo in cui si trovano:

- Agente software (Bot) inteso come un programma in grado di eseguire attività molto spesso ripetitive e continuative che implicano l’elaborazione di una grossa quantità di dati in modo più veloce ed efficiente rispetto ad un operatore umano. Sono attualmente utilizzati nei motori di ricerca nel *web*, nelle *chatbot* e possono trovare un efficace impiego nei *task* di elaborazione dei dati ISR (*Intelligence Surveillance and Reconnaissance*).
- Sistemi senza pilota (unmanned vehicles-UxV)²⁰: trattasi di veicoli senza pilota a bordo, in grado di muoversi in domini fisici diversi dotati di agenti *software on-board* capaci di fornire un predeterminato livello di autonomia.
- Robot: sistemi, non necessariamente antropomorfi in grado di assumere comportamenti di tipo attuativo, paragonabili a quelli degli esseri umani. Componenti robotiche possono essere integrate nei sistemi senza pilota (es. braccio robotico nei *rover* utilizzati per la rimozione di esplosivi improvvisati durante lo svolgimento dei task counter IED).

Nell’ambito di questa suddivisione ha senso distinguere una componente “fisica” - rappresentata dall’autopilota, dalla sensoristica, dal sistema di propulsione e dagli organi attuatori – ed una “cognitiva”, derivante dalla implementazione delle logiche di IA (diversi paradigmi di *knowledge representation* e *reasoning*, tra cui *machine/deep learning*) e strettamente riconducibile all’agente *software*. Il livello di autonomia del sistema è fondamentalmente legato a quest’ultima componente.

3.3 INTERFACCIA UOMO-MACCHINA E METRICHE PER I LIVELLI DI AUTONOMIA

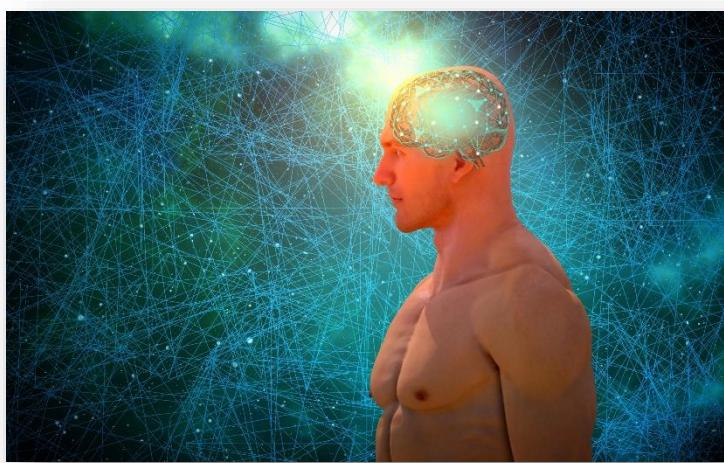
La capacità di un sistema di potere assumere autonomamente decisioni e, quindi, di autodeterminare i propri comportamenti rispetto a situazioni non note a priori, pone il problema di stabilire dei criteri per gestire il *decision-making loop*, individuando un adeguato bilanciamento di ruoli e funzioni fra il sistema (assimilabile al concetto di *machine*) e l’essere umano (*human*) rispetto alle esigenze della missione, al rispetto delle normative vigenti e ai presupposti di carattere etico e giuridico. A tal fine, è efficace considerare il sistema intelligente ed autonomo in modo macroscopico come l’insieme delle due entità, *human-machine*. L’essere umano può mantenere la supervisione della macchina attraverso dei processi di comunicazione e controllo con i livelli autoritativi²¹ di seguito riportati schematicamente:

²⁰ UxV: qualsiasi categoria di *Unmanned Vehicle*, aereo, navale e/o subacqueo, terrestre, spaziale.

²¹ R. A. Clothier, B. P. Williams, T. Perez, “Autonomy from a Safety Certification Perspective” - Autonomous Systems, Boeing Research & Technology (Australia), Febbraio 2019.

- *complete*: la macchina esegue senza riserve le direttive (i comandi) dell’operatore umano che svolge il ruolo di supervisione;
- *directed*: la macchina è in grado di suggerire alternative o compromessi rispetto agli *input* di controllo inviati dall’operatore umano che stabilisce quale debba essere la decisione finale da attuare;
- *suggestive*: la macchina può negoziare soluzioni alternative a quelle inviate dall’operatore umano e detiene la decisione prevalente;
- *none*: la macchina stabilisce se prendere in considerazione il comando inviato dall’operatore umano.

Nei livelli di libertà che il supervisore umano concede alla macchina è necessario introdurre metodologie atte a valutare, già nella fase preliminare di progettazione, i cosiddetti livelli di autonomia rapportandoli alle modalità di interazione uomo-macchina. Poiché si ritiene che il concetto di autonomia sia distinto (sebbene correlato) da quello di intelligenza, l’obiettivo di queste metodiche non è quello di misurare l’intelligenza del sistema, bensì il suo livello di autonomia ovvero la capacità di intraprendere un determinato piano di azioni senza che nessuna indicazione venga fornita da un operatore umano. L’intelligenza di un sistema è soprattutto legata alla capacità di analizzare il contesto operativo e di “imparare” situazioni pregresse, utilizzando tale conoscenza per decidere quale sia l’azione più adeguata ed efficace per risolvere una problematica non prevista e non nota a priori.



L’esigenza di introdurre criteri condivisi per classificare i livelli di autonomia di una macchina deriva da diversi ordini di motivi. È infatti necessario fissare delle metriche oggettive e standardizzate per poter effettuare

benchmarking fra soluzioni diverse, per indirizzare la fase di raccolta requisiti e di progettazione seguendo delle linee guida prefissate, per pianificare l’impiego dei sistemi autonomi e, infine, come utile supporto ai processi di certificazione rispetto alla gestione del *safety risk*. In relazione alla necessità di stabilire delle metriche condivise per distinguere i diversi livelli di autonomia per i sistemi *unmanned*, si riporta come utile riferimento quanto stabilito dall’EXTAC 102, contenuta nella

AXP 05²² e sviluppata in ambito NATO dal CMRE e dal CJOS COE²³, che contiene un'interessante suddivisione su sette livelli di autonomia. Altro spunto interessante è lo schema di *Schaub & Kristoffersen* (2017) o anche la SAE- J3016™ (2018) (*Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*). Quest'ultimo documento riporta le *recommended practices* dalla Society of Automotive Engineers sui veicoli a guida autonoma con riferimento alla possibilità di eseguire parte dei *dynamic driving tasks*, su base continuativa in un particolare dominio applicativo. Nel documento, congiuntamente ad una tassonomia comune, vengono definiti sei livelli di automazione, con riferimento al ruolo del *driver* e del sistema di guida autonoma.

Ulteriore elemento di attenzione è rappresentato dalla necessità di definire un articolato modello di interazione tra esseri umani e macchine in grado di governare la complessità, la caoticità e la criticità del nuovo “ambiente delle operazioni” ed il conseguente livello di *trust* che deve stabilirsi tra il *team manned* e le piattaforme *unmanned* durante lo svolgimento delle operazioni. L'obiettivo deve essere quello di rendere “sostenibili” ed efficaci le operazioni militari eseguite secondo il caratteristico paradigma *Manned-Unmanned Teaming* (MUMT).

3.4 IMPLICAZIONI ETICHE E GIURIDICHE

Robotica e sistemi autonomi sollevano importanti interrogativi etici e giuridici. In particolare, laddove si pensi di impiegare una IA interconnessa e dispositivi "autonomi", emerge – sia in ambito civile che militare – una sentita esigenza di sicurezza nel significato più pieno del termine: sicurezza dei dati, protezione dei sistemi, prevenzione da danni collaterali, mitigazione dei rischi. Sorgono inoltre domande sulla responsabilità legale in caso di fallimento del sistema autonomo, anche in relazione al fatto che i processi dettati dagli algoritmi alla base dell'IA sono di fatto trasparenti per l'essere umano. A tal riguardo, in relazione agli scopi militari, non avendo visibilità dei processi decisionali messi in atto dalla IA, risulta particolarmente critico assicurare la qualità dei dati in ingresso (certificati/criptati) allo scopo di evitare comportamenti imprevedibili e deleteri della IA. In tale ottica, si pone l'esigenza di prevenire il rischio di corruzione dei dati in ingresso tramite tecnologia *ad hoc* che ne certifichi la validità (es. *blockchain*). A tal proposito, assume ancor più valore il ruolo dell'uomo nel teatro di operazioni che, in prospettiva, sarà riservato sempre più all'esecuzione di compiti pregiati, attraverso uno *Human-Machine Teaming* vincolato al principio del *human in the loop* (breve periodo) che, nel lungo periodo, potrebbe evolvere nel *human on the loop* o, addirittura, nel *human out of the loop*. Nel campo civile si pensa altresì ad una IA etica che dovrà orientare il comportamento degli automi di fronte a scelte estreme

²² EXTAC (EXperimental TACtic) 102, contenuta nella pubblicazione AXP 05 “NATO EXPERIMENTAL TACTICS AND AMPLIFYING TACTICAL INSTRUCTIONS” (R).

²³ Centre for Maritime Research and Experimentation e il Combined Joint Operations from the Sea - Centre of Excellence.

che possono mettere in pericolo la vita umana (es. leggi di Asimov). In definitiva, la tematica relativa alla liceità/legalità dell’impiego di mezzi autonomi, soprattutto in relazione alla loro eventuale capacità di impiegare la forza letale, è una tematica di assoluta attualità ed interesse, le cui implicazioni legali presentano risvolti che, al momento, rimangono largamente irrisolti e non normati nel Diritto nazionale ed internazionale. Un esempio è il caso di effetti non voluti o danni causati da tali sistemi (indipendentemente dalla capacità o meno di ingaggio degli stessi) in cui si pone il problema della attribuzione di responsabilità.

Un altro aspetto è quello legato allo status di tali sistemi (senza “*human in/on the loop*”) e del rispetto da parte degli stessi di leggi e convenzioni: ad esempio per un veicolo autonomo marittimo si pone la questione del riconoscimento o meno dello stesso come “nave”²⁴ e i discendenti obblighi di rispetto dei vigenti portati normativi internazionali²⁵.

La discussione sugli aspetti etici, legali e di accettazione sociale dei sistemi autonomi porta poi al tema che oggi sistemi completamente autonomi non sarebbero in grado di garantire il rispetto dei principi/norme di diritto internazionale. In particolare, le regole di distinzione, proporzionalità e necessità militare sono strumenti particolarmente importanti per quanto riguarda la protezione dei civili dagli effetti della guerra e potrebbe essere complesso assicurare il rispetto di queste norme da parte di sistemi autonomi. Sono stati studiati e proposti diversi approcci e meccanismi per sopperire a queste mancanze, sia basati su algoritmi in grado di analizzare situazioni *combat*, sia su sistemi basati su “*strong AI*” o *Artificial General Intelligence*, ma la tecnologia non è ancora abbastanza soddisfacente da replicare processi cognitivi e di *decision making* tipicamente umani. Un altro aspetto parimenti importante e oggetto di discussioni in numerosi ambiti riguarda quello dell’*accountability*. Il quesito a cui trovare una risposta unitaria riguarda infatti quello della responsabilità in seguito ad una azione del sistema autonomo: le opzioni includono il Comandante militare, il programmatore *software*, il costruttore, l’operatore (qualora ci sia), il sistema autonomo stesso. Poiché non è stata ancora raggiunta una posizione comune su questi aspetti, la responsabilità legale di un atto di un sistema autonomo non è definita²⁶.

Vi sono, inoltre, una serie di problematiche ineludibili relative allo sviluppo e al mantenimento dei sistemi autonomi. Molte di queste sono comparabili a quelle di sistemi esistenti, ma l’evoluzione dei sistemi autonomi porta con sé una serie di questioni tecnico-etiche che accrescono la complessità della questione in modo esponenziale. Tra queste vi è *in primis* il fattore dell’affidabilità di un sistema autonomo (cd. *trust*): un efficace rapporto uomo-macchina si basa innanzitutto sulla fiducia progettuale (cd. *trust by design*), nella quale le funzioni del sistema

²⁴ Ref.: Dr. Christian Wesemann: *Legal Issues surrounding the use of Maritime Unmanned Systems*, Sett. 2020.

²⁵ Ref.: *International Regulations for Preventing Collisions at Sea (COLREG)*, *United Nations Convention on the Law of the Sea (UNCLOS)* e *International Convention for the Prevention of Pollution from Ships - MARPOL*.

²⁶ Considerazioni tratte dal report “*Losing Humanity The Case against Killer Robot*”

autonomo vengono prestabilite e mappate. Ma l'affidabilità riguarda, ovviamente, anche l'effettiva *performance* operativa del sistema, che essendo moltiplicatore di capacità diventa elemento difficilmente sostituibile o insostituibile *tout-court*.

Di pari passo con l'affidabilità dei sistemi autonomi, il fattore della prevedibilità gioca un ruolo altrettanto importante. Particolarmente in ambito cinetico, è presente la necessità di poter prevedere, con un alto margine di sicurezza/certezza, che determinate condizioni innescheranno una determinata azione; allo stesso modo, il sistema autonomo deve fornire garanzie, fin dalla fase di progettazione, che la presenza di altri parametri sarà sufficiente a limitare o inibire tale azione.

Il fattore affidabilità ed il fattore prevedibilità convergono in quella che è un'altra delle questioni centrali nel ruolo dei sistemi autonomi, ossia quella della manutenzione, riparazione ed eventuale *bypass* del sistema. Se da un lato la naturale integrazione di altre tecnologie nel contesto dei sistemi autonomi permette l'ottimizzazione dei cicli di manutenzione predittiva, dall'altro vi è la necessità di un sistema di diagnostica avanzata che permetta la riparazione e/o il recupero autonomo dell'eventuale piattaforma fisica, nonché la possibilità per un operatore umano di bypassare il sistema autonomo e prenderne il controllo in caso di necessità.

3.5 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA

I sistemi autonomi sono una delle tecnologie abilitanti per la condotta delle operazioni militari in grado di superare i limiti e le barriere a cui sono sottoposti gli esseri umani,

operando da e verso domini differenti ed in maniera trasversale agli stessi. In tale ottica, il *re-shaping* del “campo di battaglia” sarà ineludibile: in tal senso la crescita non solo numerica dei sistemi autonomi, oltre a ridurre il

livello di esposizione del personale – con contenimento della vulnerabilità e aumento del livello di resilienza – contribuirà a sviluppare le capacità di operare in tutti i domini (inclusi quello cibernetico e spaziale). La sfida sarà quella di evolvere la modalità di gestione delle crisi internazionali e di adeguare la stessa dottrina militare, in relazione all'impiego sistematico e strutturato dei sistemi autonomi, coniugato a quello dei sistemi *legacy*.



I sistemi autonomi sono particolarmente idonei alla condotta di Operazioni Multidominio, in ragione di intrinseche caratteristiche che risultano fortemente abilitanti nel caso di missioni prolungate in ambienti operativi ardui od ostili, per i quali l'impiego di mezzi con operatori umani a bordo risente fortemente di ineludibili limiti in termini di resistenza e persistenza. Ciò è particolarmente significativo nel caso di operazioni ad elevate distanze dalle infrastrutture di supporto logistico nazionale (fuori area), nel caso di adempimento di compiti gravosi, prolungati e ripetitivi tipici (es. dell'*Airborne ISR* e delle mappature dei fondali marini), nonché in ambienti problematici/proibitivi per l'essere umano, quali quello subacqueo, aereo o spaziale ovvero per sostituire gli umani nelle cosiddette missioni 3D (*Dull, Dirty or Dangerous*)²⁷.

Le applicazioni militari più immediate per i sistemi autonomi sono dunque quelle legate alla cosiddetta sostituzione dell'elemento umano in ambienti o attività ad alto rischio (EOD, supporto logistico in aree contese, ecc.) ed al completamento di compiti di routine che comportano un impiego significativo di forza-lavoro a dispetto di risultati a basso impatto (c.d. *low value tasks*). Ma vi sono altre applicazioni, già disponibili o in via di sviluppo, che dimostrano la vastità del panorama di prospettive d'impiego dei sistemi autonomi. Come indicato dalla *NATO Science & Technology Organization in Science & Technology Trends 2020-2040*, i sistemi autonomi offrono una serie di prospettive d'impiego che hanno un impatto diretto ed in molti casi potenzialmente dirompente tanto sull'assolvimento delle funzioni militari, quanto sulla struttura organizzativa stessa della Difesa. Tra queste l'accesso ad aree interdette all'operatore umano e la sua sostituzione; l'integrazione e l'assunzione di controllo *ad hoc* di piattaforme commerciali preesistenti; lo sviluppo di *software* autonomi in grado di gestire e ottimizzare *network* difensivi in ambito cibernetico; la gestione, organizzazione ed ottimizzazione del supporto ed il trasporto logistico a livello tattico, operativo e strategico, sviluppando inoltre la capacità di elaborare piani e strategie di manutenzione predittiva; il dispiegamento di sciami (c.d. *swarm*) in funzione di supporto, deterrenza o per generare massa nell'intento di rallentare o paralizzare determinate attività offensive o difensive degli avversari. Nello specifico lo sfruttamento del potenziale degli sciami implica anche un'esigenza di protezione: attaccare i flussi informativi vitali per la funzionalità dello sciame crea opportunità di manipolazione e *disruption*. Progressi nell'IA miglioreranno le contromisure elettroniche, cyber e spaziali; in alternativa, sistemi robotizzati potrebbero essere usati per formare reti di comunicazione *ad hoc* laddove altri sistemi siano stati degradati o distrutti.

²⁷ *Dull* (lett. *noisy*), sono attività di routine e/o lunga durata quali l'osservazione prolungata; *"dirty"* (sporche) sono attività nelle quali è presente il rischio di esposizione a minacce CBRN; *"dangerous"* (pericolose) sono invece quelle attività che comportano un alto rischio per il personale, quali ad esempio ISR in aree contese o le contromisure mine. Si veda *USA Congressional Research Service: Navy Large Unmanned Surface and Undersea Vehicles - Background and Issues for Congress, updated March 17, 2021*.

Se le opportunità di sviluppo di capacità autonome sono potenzialmente infinite, ritardi o *gap* capacitivi nel settore (così come nell'ambito più ampio delle EDTs) possono comportare una serie di rischi tattici, operativi, strategici e sistematici che vanno tenuti in considerazione. Carenze nello sviluppo dei sistemi autonomi comporterebbero una serie di rischi “comparativi” sia nei confronti degli avversari che in ambito EU/NATO: nel caso dei primi, il vantaggio portato dai sistemi autonomi come moltiplicatori di forza può determinare la capacità dell'avversario di mantenere l'iniziativa, dettando i tempi delle operazioni e manovrando ad un ritmo che non è sostenibile per una forza che non dispone di sistemi autonomi comparabili; nel contesto di *partnership* e alleanze, invece, il rischio di “mancare l'appuntamento” con l'integrabilità operativa dei sistemi di altre nazioni può ridurre significativamente l'impatto che una forza armata può avere sulla missione, e di conseguenza il ruolo all'interno della missione stessa.

La standardizzazione è un ulteriore elemento di potenziale criticità. A livello nazionale/interforze, un elevato grado di standardizzazione aiuta a ridurre i costi economici e logistici attraverso tutto il ciclo di sviluppo e impiego dei sistemi autonomi, ma al tempo stesso richiede un altrettanto elevato grado di modularità, per far fronte alle diverse esigenze operative esistenti. In ambito EU/NATO, come precedentemente menzionato, la necessità di mantenere il passo con gli sviluppi capacitivi messi sul campo dai principali *partner* e alleati internazionali sarà un fattore determinante nello stabilire il ruolo ricoperto in una missione.

Va inoltre sottolineato come il denominatore comune che collega tutte le criticità relative ai sistemi autonomi sia la necessità di basare il rapporto con tali sistemi su un approccio euristico nei confronti della sperimentazione: questo serve *in primis* a valutare affidabilità e prevedibilità dei sistemi, ma anche e soprattutto a identificarne potenziali sviluppi ed impieghi alternativi in grado di generare valore capacitivo aggiunto e potenzialmente dirompente.

Punto essenziale nell'adozione di tecnologie di AS è quello di poter fungere da “*force multiplier*” in ambiti complessi partendo dalla delegazione di compiti non prioritari e non supervisionati, in modo da liberare risorse per consentire una migliore concentrazione di capacità sul reale obiettivo della missione (es. il supporto ad una squadra di fanteria, in collaborazione con sistemi di trasporto e di logistica). Successivamente allo sviluppo tecnologico, legale e operativo si può immaginare l'utilizzo di questi sistemi anche in compiti maggiormente onerosi, o in sostituzione addirittura dell'operatore umano, in contesti particolarmente pericolosi. Il miglior vantaggio che l'AS presenta è una scalabilità della soluzione in sostituzione dell'essere umano.

Nel prossimo futuro, in ambito Difesa, è auspicabile la definizione di una strategia nazionale legata al sistematico impiego di AS ed alla contestuale individuazione di profili di missione in grado di sfruttarne appieno le potenzialità, focalizzandosi sui seguenti aspetti:

- salvaguardia della vita umana, innalzamento del livello di sopravvivenza, ottimizzazione del modello di interazione *manned vs. unmanned teaming* (MUMT);
- miglioramento delle capacità di individuare le *windows of opportunity* che caratterizzano le operazioni multidominio, minimizzando i tempi di reazione rispetto alla quantità crescente di dati da elaborare;
- capacità in *near real time* di classificare il rischio proveniente da una determinata tipologia di minaccia, grazie all’impiego di agenti *software* intelligenti e dotati di autonomia per l’elaborazione dei dati acquisiti dalla sensoristica (es. *force protection*);
- individuazione delle opportunità/potenzialità relative alla capacità di una medesima piattaforma UxV (anche sotto forma di *swarm*) di operare in domini fisici diversi (es. UAV in grado di navigare sulla o sotto la superficie marina);
- sviluppo di reti cooperative di UxV in grado di riconfigurarsi “autonomamente” in funzione della evoluzione della missione (*swarming*);
- previsione di adeguati sistemi di contromisura rispetto alla evoluzione dei sistemi *unmanned*, seguendo un *continuum process*;
- adeguamento delle catene C3 ed integrazione di *multi-domain task force*, con particolare riferimento a coniugare gli AS con le capacità in ambito *cyber* e lo spettro elettromagnetico.

Avvalersi degli AS nelle diverse declinazioni (agenti *software*, piattaforme *unmanned*, robot) implica evidentemente un adeguamento dei processi di formazione e di simulazione in relazione ai nuovi paradigmi di gestione e di conduzione delle operazioni Multidominio e all’introduzione dei nuovi strumenti operativi (*tools*, piattaforme, ecc.).

Capitolo 4

TECNOLOGIE SPAZIALI

4.1 LO SPAZIO E LE TECNOLOGIE ABILITANTI

Lo Spazio tradizionalmente svolge un ruolo trainante nelle tendenze di sviluppo tecnologico (c.d. *space driven*): le tecnologie spaziali sono infatti sviluppate per essere in grado di operare in condizioni ambientali estreme e sfidanti anche se sono sempre più frequenti i casi di adozione di prodotti di largo consumo e/o commerciali provenienti da tecnologie trasversali sviluppate in altri settori ad elevata specializzazione (c.d. *space related*). La sempre maggiore miniaturizzazione dei componenti e le crescenti performance dei *payload* rendono possibili prestazioni e capacità solo pochi anni fa inimmaginabili. Inoltre, l'avvento dell'Intelligenza Artificiale, di algoritmi di *machine learning* e delle tecnologie quantistiche, aprirà prevedibilmente la strada a un salto generazionale nei servizi spaziali.

La cosiddetta “democratizzazione dello spazio” conseguente all’abbassamento delle barriere di

accesso
(economiche,
tecnologiche e
normative) sta
consentendo (e lo
farà sempre più
nel prossimo
futuro) l’ingresso
di nuovi attori, tra
cui si segnala il
ruolo di entità
commerciali in
grado di cambiare



i tradizionali paradigmi che hanno caratterizzato il settore spaziale sin dagli albori. La messa in orbita di ingenti quantità di satelliti, specie di piccole/medie dimensioni, in mega costellazioni principalmente nelle orbite basse, da parte di attori statuali e no, renderà presto lo Spazio per gli assetti tradizionali (e.g. governativi, della Difesa) un ambiente operativo sempre più congestionato, competitivo e conteso.

In questo contesto, l'impatto tecnologico sullo Spazio può essere valutato nelle sue tre componenti essenziali:

➤ **Segmento di terra e lanciatori**

- Accesso allo Spazio

Per quanto attiene i lanciatori tradizionali, che continueranno a giocare un ruolo primario anche nel dispiegamento delle prossime mega-costellazioni, si segnalano decisive innovazioni nel campo delle tecnologie riutilizzabili, dello sviluppo di motori a propellente liquido di tipo “green” e dell’impiego sempre più esteso di stampanti 3D per la manifattura dei lanciatori. La miniaturizzazione dei satelliti e dei *payload*, già in corso, aprirà all’utilizzo di vettori più piccoli (ad es. *fighter type*) in alternativa ai lanciatori tradizionali (specie nelle operazioni di *replenishment* delle costellazioni sopra citate). Sono in fase di sviluppo a livello internazionale diversi lanciatori, di taglia piccola, basati a terra e da piattaforma mobile (aerea e navale).

- Space Control, Space Surveillance Tracking e Space Situational Awareness

Per la condotta delle operazioni da terra (*Space Control*), lo sviluppo di tecnologie ad Intelligenza Artificiale è specificamente teso alla mitigazione della prevista crescita di dati collezionati dallo Spazio (nella loro più ampia tipologia) e, quindi, dal carico computazionale che ne deriva. Questo in parte potrebbe essere svolto già a bordo (*in-orbit processing*) anche attraverso innovativi algoritmi di *data-fusion* e *automation*, ma anche con il supporto di processi di *Modeling and Simulation* (M&S). Questo nell’ottica di poter prevedere in anticipo con modelli accurati, e monitorando in *real time* con sensori di precisione, gli eventi di interesse sia nell’ambito della *Space Surveillance Tracking* (SST), sia quelli relativi allo *Space Weather* (SWx), al fine di contribuire sinergicamente nella più ampia ed ambiziosa capacità di *Space Situational Awareness* (SSA). In questo settore lo sviluppo delle tecniche Radar più avanzate consentirà, inoltre, di disporre di sensori *ground-based* ai quali si affiancheranno altrettanti strumenti *space-based* ottici o radar, per incrementare la capacità SSA/SDA (*Space Situational Awareness /Space Domain Awareness*) di una nazione.

➤ **Segmento spaziale**

- Satelliti e sensori

Nell’ambito dei sensori sono in corso di sviluppo nuove soluzioni di *payload* ad alta risoluzione spaziale basati, ad esempio, sulla tecnologia iperspettrale o SAR (*Synthetic Aperture Radar*), nonché sulle migliori potenzialità di ricezione e analisi di emissioni radio. L’integrazione dell’Intelligenza Artificiale e della maggiore capacità di calcolo offerta dal *quantum computing* renderà disponibili servizi sempre più efficienti ed efficaci, dotati di capacità di analisi e di previsione particolarmente promettente per le funzioni di ISR (*Intelligence Surveillance and Reconnaissance*) e di *targeting*, conseguibili

con i servizi *Position Navigation and Timing* (PNT), trasversalmente a tutte le componenti aerea²⁸, terrestre²⁹ e marittima³⁰.

- **Contromisure (attive e passive)**

Potranno essere garantiti sistemi per le contromisure elettroniche e per la protezione elettro-meccanica più performanti, in termini di rapporto peso/spazio, per la protezione delle infrastrutture più sensibili. I satelliti governativi dovranno essere dotati di sensori di prossimità, per identificare eventuali assetti ostili in avvicinamento e/o evitare collisioni con detriti spaziali orbitali (*debris*) e sensori per il monitoraggio continuo del proprio stato di integrità.

- **Sviluppo e impiego di materiali innovativi**

Materiali innovativi con spiccate proprietà di leggerezza e resistenza a temperature estreme, con componenti/sottosistemi realizzati anche tramite le tecniche di *3D Printing/Rapid Prototyping/Additive Layer Manufacturing*.

- **In Orbit Maintenance & Servicing**

Sviluppo di tecnologie per attività di *check-out, refueling, replacement, relocation* di grandi satelliti con tecnologia avanzata.

- **Active Debris Removal**

L'incremento delle attività spaziali e del conseguente affollamento delle varie orbite richiede lo sviluppo di sistemi avanzati per la rimozione di detriti orbitali (*debris*). Un sistema attivo potrebbe avere anche implicazioni militari come possibile tecnologia offensiva (come i sistemi *Anti-Satellite Weapons ASAT*).

- **Direct Energy Weapons**

Sviluppo di tecnologie basate su emissioni di energia nello spettro per eventuali azioni preventive/interdittive di assetti avversari. Tecnologie di questo tipo possono essere imbarcate su satelliti, ma anche su velivoli per *counterspace operations* (da preferirsi alle tradizionali ASAT con effetti cinetici più estesi)

- **Spacecraft e Stazioni spaziali**

Lo sviluppo del c.d. *commercial spaceflight* e l'ampliamento agli operatori commerciali rende possibile ipotizzare lo svolgimento di attività di R&D (*Research and Development*) e OT&E (*Operational Test and Evaluation*) per tecnologie abilitanti d'interesse militare nello spazio. Ciò può essere ottenuto realizzando piattaforme orbitanti (*unmanned*) in orbita bassa (*Low Earth Orbit - LEO*).

²⁸ Includendo la *Shared Early Warning* (SEW) per la rilevazione del lancio di missili balistici e/o armamento ipersonico.

²⁹ Per la situazione delle forze terrestri, coordinamento della manovra, sorveglianza delle forze avversarie e *targeting*.

³⁰ Nel contesto della compilazione della *Maritime Situational Awareness*.

- Sistemi di mobilità spaziale (*Advanced EVA*)

L’effettuazione di attività di *In-Orbit servicing* avverrà per lo più tramite sistemi automatizzati. Qualora vengano sviluppate capacità *manned*, sarà richiesto lo sviluppo di tecnologie per *Extra-Vehicular Activity (EVA)* come tute e sistemi di *man backpack* per spostamenti *unrestricted* all'esterno. Tali capacità (automatiche o *manned*) consentiranno di effettuare manovre estensive di manutenzione e supporto alle infrastrutture spaziali.

- Infrastruttura lunare e logistica associata

L’incremento dell’economia spaziale dalle orbite basse si estenderà nei prossimi anni al sistema Terra-Luna. Appare indispensabile, dunque, una capacità di monitoraggio, controllo e protezione degli interessi nazionali in ambito economia lunare.

- Propulsione ipersonica, materiali ablativi, GNC (Gas Naturali Compressi) per stabilità e controllabilità velivoli ad alti numeri di Mach-Reynolds³¹.

Si prevede che lo sviluppo tecnologico in materia di propulsione innovativa punti a sistemi di trasporto ipersonici, suborbitali e, in prospettiva a lungo termine, di vettori *Single-Stage-to-Orbit* (cosiddetti Spazioplani). Ciò richiede l'estensione notevole delle attuali tecnologie propulsive e dei materiali per altissime temperature per lo sviluppo di sistemi di volo in alta stratosfera a regime ipersonico *sustained (scramjet)* e per il rientro atmosferico. Tale sviluppo tecnologico dovrà ricercare un compromesso tra prestazioni e costi/manutenibilità/*reliability*.

➤ Link terra-spazio

L’elevata quantità di dati ottenibili dallo Spazio, da differenti fonti e con differente qualità/risoluzione/frequenza, permette di offrire informazioni a valore aggiunto sempre più preziose ai vari utenti commerciali ed istituzionali. La fornitura di servizi sarà sempre più “customizzata” sulle singole esigenze. Funzionale a questo sarà l’adozione di tecnologie di *Big Data Analytics*, *Machine/Deep Learning* ed anche *Distributed Ledger*, al fine di garantire univocità, veridicità e sicurezza dell’informazione stessa. La miniaturizzazione, la messa in orbita di mega-costellazioni e lo sfruttamento delle comunicazioni ottiche a larga banda (per es. Laser IR) non solo di tipo inter-satellite, ma anche verso le stazioni di terra, potrà offrire potenziali soluzioni in orbite basse, alternative alla *relay* geostazionario, con indubbi vantaggi sia sui tempi di latenza e di rivisita, sia sulla resilienza dell’architettura.

³¹ Il numero di *Reynolds* consente di valutare se il flusso di scorrimento di un fluido è in un regime laminare (valori più bassi di tale valore) o in un regime turbolento (valori più elevati) calcolati in base alla geometria del corpo investito dal flusso, la natura del fluido, le condizioni operative (temperatura e pressione) alle quali avviene l’esperienza.

4.2 CAPACITÀ STRATEGICHE PER OPERARE NELLO SPAZIO

➤ Accesso allo spazio

La sempre più veloce evoluzione dei lanciatori spaziali, con l'applicazione dei concetti di modularità e riutilizzabilità, l'impiego di propellenti *green* e quello massivo della stampa 3D additiva per parti strutturali, offrirà maggiori opportunità anche nel delicato settore dell'accesso allo spazio, vitale per l'autonomia strategica di un Paese e fattore abilitante in termini di potenziali cooperazioni ad ampio spettro, in supporto alle politiche nazionali nel comparto.



La parallela miniaturizzazione delle componenti elettroniche ha incrementato notevolmente le capacità dei piccoli/mini satelliti favorendo anche, in determinate condizioni, la possibilità di utilizzare vettori più piccoli, complementari ai lanciatori più grandi. Tali vettori potranno essere lanciati ancora da Terra, o da piattaforme mobili, qualora gli sviluppi tecnologici ne confermino il costo-efficacia. In questo contesto, l'impiego di lanciatori da piattaforma mobile (navale, aviotrasportati o terrestre) potrà essere, in futuro, una soluzione esplorabile per supportare la *policy* nazionale finalizzata a conseguire una eventuale capacità autonoma nazionale di accesso allo spazio³² anche in ottica di garantire la resilienza delle costellazioni attraverso i *responsive launch* (i lanci per sopperire all'eventuale perdita improvvisa di un satellite in una costellazione) e/o il lancio di costellazioni ad hoc.

In funzione del livello di ambizione nazionale fissato, una capacità di lancio *responsive* richiederà la disponibilità di *Space Launch Vehicle* (SLV) già pronti e pre-assemblati, con un tempo di approntamento molto basso, e la disponibilità di satelliti standardizzati e pronti per il dispiegamento (requisito di modularità e scalabilità).

➤ Space Traffic Management (STM)

Lo *Space Traffic Management* - internazionalmente riconosciuto quale “insieme delle disposizioni tecniche e regolamentari per promuovere l'accesso sicuro allo Spazio, la conduzione delle operazioni nello spazio ed il ritorno di oggetti provenienti dallo Spazio libero da interferenze di qualsiasi forma” - implica lo

³² L'Italia, di fatto, possiede un Centro Spaziale a Malindi (Kenya), con piattaforma *off-shore* per il lancio di piccoli vettori, anche se non più utilizzata dalla fine degli anni '80.

sviluppo di specifiche capacità ed appare un passo indispensabile in previsione di un forte incremento, nel prossimo futuro, dell'utilizzo dello Spazio che includa le mega costellazioni satellitari ed i voli suborbitali.

➤ **Servizi satellitari**

La crescente miniaturizzazione dei componenti, nonché le crescenti prestazioni dei *payload* rendono disponibili capacità solo pochi anni fa inimmaginabili. Inoltre, l'integrazione delle tecnologie emergenti e dirompenti (in particolare l'IA, il *Machine Learning* ed il *Quantum Computing*), apriranno, prevedibilmente, la strada ad un salto generazionale nei servizi spaziali.

- **Osservazione della Terra**

Nell'ambito dell'osservazione terrestre sono in corso di sviluppo nuove modalità/soluzioni di *payload* ad alta risoluzione basati, ad esempio, sulla tecnologia multi/iperspettrale, SAR elettro-ottica.

In prospettiva, queste maggiori performance dei *payload* satellitari, unitamente al consistente aumento del numero di *asset* satellitari disponibili (mega costellazioni, anche commerciali), miglioreranno il tempo di *refresh* delle informazioni su scala globale, permettendo una migliore e più aggiornata *Situational Awareness* dei vari domini operativi, contribuendo significativamente ad una sempre più efficace generazione della *Common Operational Picture*. Ciò avverrà attraverso l'ottenimento di informazioni di carattere puntuale, anche con tecniche di *image intelligence*, a partire da grandi quantità di dati globali (es. servizi di sfruttamento dei dati di osservazione di provenienza diversa, al fine di monitorare e sorvegliare infrastrutture ed aree critiche, come siti specifici, aree marine soggette a traffici e/o operazioni illegali, ecc.). Infine, si evidenzia la possibilità di rendere complementari gli strumenti e sensori tradizionali di terra ottici e radar con strumenti dedicati a bordo satellite al fine di fornire servizi di *Space Situational Awareness* e, quindi, una *Recognized Space Picture* omnicomprensiva, che tenga conto anche delle informazioni legate agli assetti spaziali provenienti dai rispettivi centri di controllo.

- **Comunicazioni satellitari**

Le comunicazioni satellitari rimangono un *asset* capacitivo ormai irrinunciabile, in particolare per la Difesa quando opera fuori dai confini nazionali. Queste comunicazioni sono affidate ai preziosissimi satelliti geostazionari che rimarranno vitali anche in futuro, alla miniaturizzazione dei satelliti, allo sfruttamento delle comunicazioni ottiche non solo di tipo intersatellitare, ma anche verso le stazioni di terra, che già oggi offrono soluzioni per mega costellazioni di satelliti per le telecomunicazioni in orbite basse, alternative al *relay* geostazionario. Ciò aumenterà la resilienza dell'intera architettura, ma avrà anche indubbi riflessi positivi sulla riduzione dei tempi di latenza e l'ampliamento della banda cruciali, ad esempio, per consentire operazioni remotizzate critiche quali il comando e controllo “*beyond line of*

sight” di aeromobili a pilotaggio remoto (APR), la telemedicina e l’implementazione dei nuovi protocolli di comunicazione per l’*Internet of Things*. Al riguardo sarà fondamentale l’esplorazione di nuove bande/tecniche di modulazione/trasmissione quali la banda Q/V, tecniche di quantum *key distribution*, tecniche trasmissive *spread spectrum* allo scopo di rendere efficiente la risorsa di banda e aumentare la quantità e la sicurezza dei dati trasmessi, oltre che l’utilizzo di sistemi di propagazione (antenne) idonee a garantire la miniaturizzazione dei dispositivi ricetrasmettenti utilizzati dagli utenti.

- **Position, Navigation & Timing (PNT)**

I sistemi globali di PNT satellitare (detti anche GNSS - *Global Navigation Satellite Systems*) costituiscono oggi un *asset* strategico a livello mondiale su cui si fonda l’esercizio di molteplici servizi ed applicazioni, civili e militari, al punto che è ormai difficile immaginare di poterne fare a meno. In generale, i servizi offerti dai GNSS supportano le Forze Armate in tutti gli ambiti di applicazione operativi, risultando indispensabili alla condotta delle operazioni. Tali sistemi generano la capacità di mantenere il coordinamento in termini di posizione, navigazione e tempo tra i vari reparti operanti ed il centro di comando, mediante lo sfruttamento di sistemi di navigazione globale satellitare in unione con sistemi di posizionamento e navigazione più tradizionali. Essi contribuiscono fattivamente al raggiungimento delle prestazioni desiderate da parte dei sistemi d’arma, all’ottimizzazione dei processi logistici ed all’efficace assolvimento di tutti i *task* tipicamente militari. Attualmente questi servizi sono assicurati da diverse costellazioni di satelliti, in particolare dal *Global Positioning System* (NAVSTAR GPS di proprietà USA) ed in prospettiva dal *Galileo Public Regulated Service* (realizzato/gestito dall’UE), da integrare in ricevitori a doppia costellazione (GPS-GALILEO) così da di aumentare la resilienza generale del servizio.

- **Space Domain Awareness (SDA), Space Situational Awareness (SSA) e Space Surveillance and Tracking (SST)**

La *Space Situational Awareness* (SSA)³³ contribuirà all’ottenimento di una *Recognized Space Picture* (RSP) omnicomprensiva a supporto del conseguimento di una *Space Domain Awareness* e, quindi, dell’autonomia decisionale operativa e strategica, nonché quale strumento di *augmentation* delle capacità offerte dai vari sistemi degli altri domini. In questo senso è necessario disporre di una capacità di *Space Surveillance and Tracking* (SST) e *Space Situational Awareness* (SSA) nazionale, in linea con le aspirazioni di autonomia strategica prefissate per una efficace cooperazione internazionale. Tuttavia, la capacità di osservare e tracciare i satelliti si basa, oggi, su sensori dislocati a terra limitati, ovviamente, dalla longitudine del nostro territorio.

³³ SSA: composta dalla *Space Surveillance and Tracking* (SST), dallo *Space Weather* (SWx) e dalla *Space Intelligence*.

Oltre ad eventuali capacità *space-based* dedicate che in futuro potranno integrare la rete nazionale, lo sviluppo di tecniche radar più avanzate potrebbe consentire, inoltre, di disporre di sensori imbarcati su sistemi terrestri, navali o aerei per incrementare la capacità SST e SSA.

- In-orbit servicing

In futuro, le evoluzioni tecnologiche potranno sostenere ulteriori servizi, come ad esempio il cosiddetto *In-orbit servicing*, che permetterà di manutenere gli assetti in orbita con lo scopo di estenderne la vita utile ovvero modificarne la missione, piuttosto che estendere gli attuali servizi.

4.3 MINACCE ALLE INFRASTRUTTURE SPAZIALI

L'importanza strategica dello Spazio ha portato alcune nazioni a costruire arsenali di armi “*counterspace*” per degradare, distruggere o negare l'utilizzo dei sistemi spaziali avversari. Di contro, tale valenza strategica dello Spazio ha stimolato alcune nazioni a compiere ogni sforzo per promuovere norme di comportamento responsabili che mantengano lo stesso come un ambiente sicuro e aperto in conformità con il Diritto Internazionale, il Diritto Internazionale Umanitario e l'*Outer Space Treaty*.

Le armi “*counterspace*”, in particolare quelle che producono detriti orbitali, rappresentano un serio rischio per l'ambiente spaziale e per la capacità di utilizzare lo Spazio per fini commerciali e civili. Di seguito le principali minacce alle infrastrutture spaziali.

➤ Armamento fisico cinetico

Le armi c.d. *counterspace* cinetiche hanno lo scopo di colpire direttamente o far esplodere una *warhead* vicino a un satellite o una stazione di terra. Le tre forme principali di attacco fisico cinetico sono le armi “*Anti-Satellite Weapons*” (ASAT) ad ascensione diretta che vengono lanciate da terra su una traiettoria suborbitale per colpire un satellite in orbita; le armi ASAT coorbitali che vengono prima messe in orbita e poi manovrate in prossimità o all'interno del bersaglio previsto; infine, gli attacchi alla stazione di terra mirati ai siti terrestri responsabili del comando e del controllo dei satelliti o della trasmissione dei dati delle missioni satellitari agli utenti.

Gli attacchi fisici cinetici tendono a causare danni irreversibili ai sistemi interessati e sono facilmente attribuibili. Inoltre, un attacco fisico cinetico nello spazio produrrà detriti orbitali, che possono colpire indiscriminatamente altri satelliti in orbite vicine. Questi tipi di attacchi sono una delle poche azioni *counterspace* che comportano potenzialmente la perdita di vite umane (sia riferendosi ad attacchi a stazioni di terra che a satelliti in orbita in cui sono presenti esseri umani, come la Stazione Spaziale Internazionale). Ad oggi, nessun paese ha condotto un attacco fisico cinetico contro il satellite di un altro paese, anche se Stati Uniti, Russia, Cina e India hanno testato con successo armi ASAT ad ascensione diretta.

➤ Armamento fisico non cinetico

Le armi “*counterspace*” non-cinetiche (laser, ordigni nucleari e disturbatori/ingannatori elettronici) sono quelle che producono effetti fisici sui satelliti o sui sistemi di terra senza stabilire un contatto fisico. I laser possono essere utilizzati per abbagliare temporaneamente o accecare permanentemente i sensori sui satelliti oppure causare il surriscaldamento dei componenti. In generale, un sistema laser “*counter-satellite*” richiede un'elevata qualità del

“beam”, un'ottica adattiva (se utilizzata attraverso l'atmosfera) e un complesso controllo di puntamento del raggio laser: si tratta quindi di tecnologie costose e ad alto livello di sofisticazione. Il sistema laser per essere efficace, deve trovarsi nel campo visivo del sensore posto sul satellite e, per tale motivo è possibile attribuire



l'attacco partendo dalla sua origine geografica approssimativa.

Le armi *High-Powered Microwave* (HPM) possono bloccare i sistemi elettronici di un satellite o causare danni permanenti ai circuiti elettrici e ai processori di un satellite. Un dispositivo nucleare fatto esplodere nello Spazio può creare un ambiente ad alta radiazione e un impulso elettromagnetico (*ElectroMagnetic Pulse* - EMP) che creerebbe effetti indiscriminati sui diversi satelliti nelle orbite interessate. L'uso di un'arma nucleare nello Spazio avrebbe effetti su larga scala che sarebbero facilmente attribuibili e visibili. Una detonazione nucleare nello spazio influenzerebbe immediatamente i satelliti nel raggio del suo EMP e creerebbe anche un ambiente ad alta radiazione che accelererebbe il degrado dei componenti satellitari a lungo termine per i satelliti non schermati nel regime orbitale interessato. Questi attacchi possono essere meno visibili a osservatori terzi e più difficili da attribuire perché l'attacco può provenire da diverse angolazioni, anche da altri satelliti che passano in orbita. I satelliti possono essere colpiti con armamento laser o HPM da siti terrestri, navali, piattaforme aeree o altri satelliti. Inoltre, l'attaccante potrebbe avere difficoltà a comprendere se l'azione ha avuto successo perché è improbabile che produca indicatori visibili.

L'armamento “*electronic counterspace*” colpisce lo spettro elettromagnetico attraverso il quale i sistemi spaziali trasmettono e ricevono dati. I dispositivi di disturbo interferiscono con le comunicazioni da o verso i satelliti, generando “rumore” nella stessa banda di radiofrequenza. Un *jammer uplink* interferisce con il segnale che va da terra al satellite (ad es. il *command and control uplink*), mentre i *jammer downlink* interferiscono con il segnale che da un satellite si propaga verso gli utenti sulla Terra. Lo *spoofing*, forma di attacco elettronico in cui l'aggressore inganna un ricevitore generando un segnale falso, può essere utilizzato per immettere false informazioni in un flusso di dati o per inviare falsi comandi a un satellite per interromperne le operazioni. Attraverso un tipo di *spoofing* denominato “*meaconing*” anche i segnali GPS militari crittografati possono essere falsificati. I terminali degli utenti con antenne omnidirezionali, come molti ricevitori GPS e telefoni satellitari, hanno un campo visivo più ampio e, pertanto, sono possibili di disturbi e *spoofing* in *downlink* da un'ampia gamma di direzioni. Le forme di attacco elettroniche possono essere difficili da rilevare o distinguere da interferenze accidentali, rendendone difficile l'attribuzione. Sia il *jamming* che lo *spoofing* sono forme di attacco reversibili perché una volta disattivati, le comunicazioni possono tornare alla normalità. La tecnologia necessaria per bloccare e falsificare molti tipi di segnali satellitari è disponibile in commercio ed è poco costosa, il che ne rende relativamente facile la proliferazione tra attori statuali e non statuali.

➤ Attacchi informatici

Mentre le forme elettroniche di attacco interferiscono con la trasmissione dei segnali in radiofrequenza, gli attacchi informatici prendono di mira i dati stessi e i sistemi che utilizzano, trasmettono e controllano il flusso di dati. Gli attacchi informatici ai satelliti possono essere utilizzati per monitorare i modelli di traffico dati, intercettare dati o inserire dati falsi o corrotti/danneggiati in un sistema. Questi attacchi possono colpire le stazioni di terra, le apparecchiature degli utenti finali oppure i satelliti stessi.

Sebbene gli attacchi informatici richiedano un alto grado di comprensione e conoscenza dei sistemi presi di mira, non necessitano di risorse significative per essere condotti e, pertanto, possono essere appaltati a gruppi privati o a singoli individui. In questo senso, quindi, anche se un attore statuale o non statuale non dispone di capacità informatiche interne, può comunque rappresentare una minaccia informatica.

Un attacco informatico ai sistemi spaziali può comportare la perdita di dati o servizi forniti da un satellite, che potrebbe avere effetti sistemici diffusi se utilizzato contro un sistema come il GPS. Gli attacchi informatici potrebbero avere effetti permanenti se, ad esempio, un avversario prendesse il controllo di un satellite attraverso il suo sistema di comando e controllo. Un aggressore potrebbe interrompere tutte le comunicazioni e danneggiare in modo permanente il satellite (ad es. consumando il propellente o impartendo comandi che danneggino i componenti elettronici e sensori). L'attribuzione precisa e

tempestiva di un attacco informatico può essere difficoltosa, perché gli aggressori possono utilizzare una varietà di metodi per nascondere la propria identità.

➤ Collisione in orbita accidentale

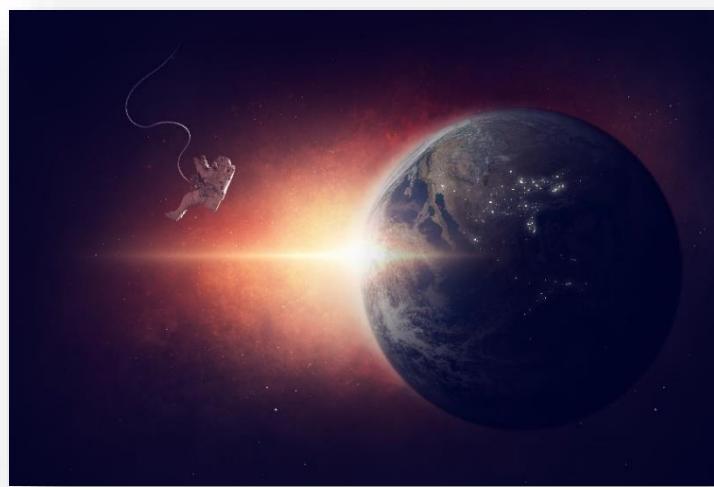
L'incremento del numero e delle dimensioni delle costellazioni satellitari, in particolare nell'orbita LEO (*Low Earth Orbit*), aumenta il rischio di collisioni con detriti spaziali (oggetti non controllati) e di collisioni involontarie con oggetti spaziali controllati. In tal senso diventa fondamentale prevedere il potenziamento dei sensori terrestri e, in prospettiva futura, anche di quelli posti in orbita sui satelliti controllati, utili alle operazioni di *Collision Avoidance*.

➤ Fenomeni naturali

Durante i periodi di intensa attività solare è possibile che le particelle energetiche provenienti dall'attività del sole possano colpire i satelliti, sovraccaricare i sensori, danneggiare le celle solari e degradare cablaggi e altre apparecchiature. Una soluzione è quella di monitorare l'attività solare ed effettuare previsioni di tali fenomeni (*Space Weather SWx*) distribuendo avvisi e bollettini dedicati agli operatori satellitari al fine di poter mitigare sia possibili disturbi sui vari servizi basati su capacità satellitari (es. SATCOM, PNT, ecc.) sia possibili danneggiamenti ai satelliti stessi tramite operazioni preventive di protezione (es. chiusura pannelli solari, disabilitazione temporanea di alcuni servizi e/o circuiti elettrici, ecc.).

4.4 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA

Il settore spaziale è in costante evoluzione ed il suo sfruttamento è passato da logiche prettamente governative e di affermazione politica a logiche commerciali, con scenari inediti e sfidanti con l'ingresso in scena di nuovi attori statuali e non statuali (c.d. “*new space*”). La nuova corsa commerciale vedrà, entro i prossimi 10-15 anni, l'estensione degli interessi strategici e degli investimenti nazionali e internazionali alla Luna e alle orbite circumlunari, con conseguenti ed ineludibili impatti in termini di Difesa e Sicurezza, prevedibili sin d'ora. Si rileva, pertanto, un costante incremento dei rischi e delle minacce nello



Spazio e verso le infrastrutture ad esso connesse, con un conseguente aumento della probabilità che si possano verificare eventi di indisponibilità dei servizi spaziali.

Nell'ambito della Strategia Spaziale della Difesa sono stati individuati dei settori specifici su cui focalizzare una particolare attenzione.

- **Osservazione della Terra**

L'integrazione dell'Intelligenza Artificiale e la maggiore capacità di calcolo offerta dal *Quantum Computing* renderà disponibili servizi sempre più efficienti ed efficaci dotati di capacità di analisi e previsione, con particolare riferimento alle capacità di *on-board processing*. I futuri *asset* spaziali da sviluppare in ambito Difesa dovranno consentire, ad esempio, di interpretare il “*pattern of life*” di obiettivi di interesse, individuare i comportamenti sospetti, correlare le informazioni per una più completa *Situational Awareness*. I nuovi *payload* multi/iperspettrali potranno consentire anche di potenziare il servizio cartografico nazionale, velocizzando e rendendo sempre più accurate, per esempio, la realizzazione della cartografia cartacea e digitale, inclusa la batimetria e il DTED (*Digital Terrain Elevation Data*).

- **Comunicazioni Satellitari**

Il dispiegamento di mega costellazioni in orbita bassa, gestite da operatori commerciali, porterà alla diffusione di sistemi satellitari a bassa latenza e a larga banda in funzione di *backhauling*³⁴ per aree servite con modalità *Fixed Wireless Access*: tale configurazione potrà per esempio asservire luoghi/comunità remote per applicazioni distribuite localmente in “*real time*” e centralizzate con *latency* accettabile (tipicamente 20 -30 ms).

- **Position, Navigation & Timing (PNT)**

I servizi di PNT sono e saranno sempre più importanti nelle operazioni militari. In questo senso, lo Strumento Militare ha la necessità di disporre con continuità di un monitoraggio costante della qualità e della certezza del segnale, disponendo anche di sensori che, utilizzando le capacità di elaborazione dei Centri di Comando e Controllo nazionali, siano in grado di assicurare informazioni certe sulla qualità dei segnali PNT.

- **Space Situational Awareness (SSA) e Space Surveillance and Tracking (SST)**

La capacità SSA/SST nazionale dovrà essere basata, oltre che sui dati forniti dagli accordi internazionali da stipulare/in vigore con i Paesi amici/alleati, anche sulla disponibilità autonoma di solide capacità sensoristiche e di elaborazione di SST studiate *ad hoc*. Oltre al potenziamento, quindi, delle capacità telescopiche e Radar site sul territorio nazionale, ivi inclusi i sensori civili/duali, potrà essere valutata l'implementazione ed integrazione nella rete SST di sensori distribuiti da mettere in orbita (*space-based*) ed eventualmente anche su altre piattaforme

³⁴ Una rete di *backhaul* o rete di ritorno è la porzione di una rete gerarchica che comprende i collegamenti intermedi tra la rete centrale e le piccole sottoreti ai "margini" della stessa rete gerarchica.

dislocate nei Teatri Operativi³⁵. Una rete di sensori distribuiti, imbarcabili su piattaforme aeree, navali e terrestri, da impiegare anche nei Teatri Operativi che agevolerebbe la compilazione della *Recognized Space Picture* contribuendo a fornire una solida base per la *Space Domain Awareness* (SDA).

- **Piccoli satelliti**

Dal punto di vista di soluzione tecnologica, i piccoli satelliti sono progrediti in modo significativo nell'ultimo decennio da piattaforme sperimentali a piattaforme operative con determinate capacità di missione. Questi satelliti sono significativamente più economici rispetto alle piattaforme di dimensioni maggiori e possono trovare più facilmente opportunità di volo a bordo dei lanciatori. In alcuni casi, i piccoli satelliti possono integrare le capacità degli assetti spaziali più grandi convenzionali e stanno diventando piattaforme utilizzabili per effettuare missioni militari specifiche. Essi possono operare individualmente, insieme in costellazioni o autonomamente in sciami per missioni di maggiore complessità. Al contrario dei satelliti singoli o in costellazione che vengono gestiti da terra sotto il diretto comando del Centro di Controllo Satellite, i piccoli satelliti possono operare autonomamente in sciami e rappresentano assetti intelligenti in grado di riconfigurare la loro missione ovvero il funzionamento dei loro *payload* in modo autonomo, ma sincronizzato, sulla base dell'osservazione/scoperta di eventi senza la necessità di una direzione/comando da terra, ma solo di operazioni di pianificazione e *monitoring*. Oggigiorno, vengono già utilizzati piccoli satelliti di diverse dimensioni e gradi di autonomia per le attività di raccolta ISR (*Intelligence Surveillance and Reconnaissance*), pur in presenza delle intrinseche limitazioni che caratterizzano tali assetti (ad esempio, per applicazioni Osservazione della Terra, la risoluzione geometrica spinta, richiesta specie in ambito *intelligence*, resta appannaggio degli assetti tradizionali).

- **Ground Segment**

Alla luce del crescente numero di piattaforme satellitari, l'infrastruttura terrestre della Difesa, devoluta alla condotta del segmento spaziale e alla gestione della missione (rispettivamente controllo assetto satellitare e gestione dei prodotti del *payload*), dovrà evolvere ed essere conseguentemente potenziata in modo da fornire servizi multi-missione e/o di interoperabilità tra segmenti di differenti missioni (sull'esempio del MUSIS-CIL – *Multinational Space-based Imaging System-Common Interoperability Layer* tra i sistemi di nuova generazione di Italia - *COSMO-SkyMed* Seconda Generazione e Francia - *Composante Spatiale Optique*), oltre a rinforzarne la protezione e la sicurezza contro le minacce citate in precedenza.

³⁵ Possono configurarsi assetti dedicati esclusivamente alla SST, oppure dotati di sensori con capacità SST *sensors*).

Capitolo 5

TECNOLOGIE IPERSONICHE

5.1 UN “IMPATTO FULMINEO”

La tecnologia sottesa ai missili ipersonici – in grado di muoversi entro i limiti superiori dell’atmosfera, a velocità vicine e superiori a *Mach 5* e manovrare con agilità imprevedibile – è ancora in fase di sviluppo. Tuttavia, non si può escludere che, già nei prossimi anni, essi non possano essere impiegati da attori statuali e non-statuali nella condotta di un’operazione.

Per comprendere le possibili implicazioni della minaccia ipersonica sulla condotta delle operazioni militari è necessario comprenderne le capacità, le potenzialità, nonché gli effetti diretti e indiretti. L’utilizzo di questi sistemi, grazie alle loro caratteristiche tecniche (velocità, traiettoria e imprevedibilità) permette di superare le tradizionali barriere di difesa missilistica costituendo un importante fattore per alimentare le strategie di *Anti-Access/Area-Denial* (A2/AD), nel caso di attore statuale, oppure di persuasione, nel caso di attore non-statuale.

Detta considerazione diventa ancora più marcata se si considera che il primo lancio potrebbe essere decisivo: in relazione al grado dei danni subiti, la capacità di risposta potrebbe infatti addirittura risultare inefficace ovvero impossibile. Va detto, inoltre, che i missili ipersonici potrebbero innescare una pericolosa *escalation* nella condotta dell’operazione, tale da comportare la transizione da uno scontro convenzionale ad uno di tipo nucleare.

Attualmente, le ricerche e gli sviluppi tecnologici sono concentrati su due principali tipologie di mezzi:

➤ ***Hypersonic Glide Vehicle – HGV***

Questi veicoli hanno bisogno di un *booster* del tipo a razzo per raggiungere l’alta atmosfera. Dopo che il veicolo ha raggiunto quasi 100 km di altitudine, il *booster* si stacca e il veicolo scivola sulla parte superiore dell’atmosfera a velocità di 8-10 *Mach*. Il profilo di volo viene scelto per ridurre al minimo la durata durante la quale gli attuali intercettori eso ed endoatmosferici possono ingaggiare la minaccia. Differiscono da una minaccia balistica per la loro capacità di



manovrare attraverso l'uso di *flap* o propulsori. Questi componenti di manovra consentono all'HGV di "saltare" in quota e lateralmente, scambiando velocità per opportunità di intercettazione ridotte. È anche difficile prevedere dove il veicolo potrebbe uscire nella serie di "salti" per eseguire un avvicinamento terminale.

➤ ***Hypersonic Cruise Missile – HCM***

Un *Cruise Missile* (CM) è un veicolo guidato senza equipaggio la cui missione principale è posizionare ordigni su un bersaglio predeterminato con propulsione continua fino al momento dell'impatto. I CM sostengono il volo tramite portanza aerodinamica per la maggior parte del profilo di volo. Poiché i CM sono bersagli che utilizzano l'aria quale comburente, rimangono in uno strato di atmosfera relativamente più basso. Sono anche in grado di volare su traiettorie non balistiche a velocità subsoniche, supersoniche o ipersoniche, dove la maggior parte del profilo di volo è a velocità costante. I motori *turbojet*, *turbofan*, *ramjet* e *scramjet* possono essere utilizzati per un CM.

Gli *Hypersonic Cruise Missile* (HCM) o i veicoli da crociera *boost* vengono rilasciati da velivoli o alimentati da razzi per raggiungere la velocità ipersonica e utilizzati per attacchi tattici da distanze di stallo. Passano quindi a un motore *scramjet* e navigano ad altitudini comprese tra 20 km e 40 km con manovra laterale. Nella loro fase terminale, possono rallentare tra *Mach 2* e *Mach 4* e immergersi sul loro bersaglio o eseguire voli a basso livello verso il bersaglio, alcuni con una traiettoria di volo *pull-up*³⁶. Gli HCM sono un tipo di veicolo con un motore senza parti in movimento, dove l'intero processo di combustione avviene in una camera di combustione. Poiché c'è una combustione a base di ossigeno, il veicolo deve volare relativamente più in basso nell'atmosfera per portare abbastanza ossigeno nella camera di combustione. La maggiore complessità dell'HCM, essendo veicolo a motore, porta a dover risolvere problemi legati alla durata strutturale, all'efficienza della propulsione, alla resistenza ed alla navigazione/guida per colpi di precisione.

5.2 LA PROTEZIONE DELLE FORZE

I sistemi ipersonici operano nel *gap* tra le tradizionali difese aeree e le difese da missili balistici. Le difese odierne (negli USA i sistemi *Patriot*, *THAAD*, *Aegis*, in Europa il *SAMP/T* e *PAAMS*, in Israele *l'Arrow2*, *Arrow3*, *David's Sling*), in grado di proteggere i siti sensibili e le forze militari dagli attacchi aerei e missilistici (talvolta anche balistici), trovano una reale minaccia nei missili ipersonici.

Le criticità della difesa dall'ipersonico nascono dai seguenti aspetti:

- il lancio dell'armamento ipersonico potrebbe non essere rilevato dagli attuali sensori a infrarossi spaziali, progettati per individuare il lancio di missili balistici

³⁶ La Russia, così come la Cina per proprio conto, ha testato il missile da crociera ipersonico *Zirkon* che ha raggiunto una velocità massima di *Mach 8* e un altro missile come il *Kinzhal* con una velocità massima di *Mach 10* e una gittata di 2000 km. Non è chiaro se i Russi abbiano superato i problemi associati all'uso di idrocarburi.

intercontinentali. Un *air-launched scramjet* o un missile ipersonico lanciato da una piattaforma “non balistica” potrebbe non sviluppare un *plume* infrarosso al lancio tale da venire rilevato dagli attuali sistemi;

- a causa della loro quota di volo e della curvatura della Terra, la distanza a cui è possibile rilevare i missili ipersonici è più breve rispetto ai missili balistici ed il tempo di tracciamento è sensibilmente inferiore rispetto ai *cruise missile*, a causa della elevata velocità;
- gli attuali sistemi di difesa contro i missili balistici utilizzano sensori che tracciano il missile fino al *burnout* e poi prevedono un punto di impatto che viene passato ai sensori a terra o in mare per riacquisirlo e tracciarlo fino all’obiettivo. Questo sistema funziona perché i missili balistici in questa fase non manovrano e la loro traiettoria di volo è prevedibile. Questo non è il caso delle armi ipersoniche, che sono in grado di manovrare, sia in termini di velocità che in direzione, rendendo queste armi imprevedibili su quale sia l’obiettivo e dove possano essere acquisite dai sensori di difesa terminali;
- a differenza dei missili balistici, i missili ipersonici volano a quote inferiori e variabili, sono più difficili da vedere, percorrono una rotta di volo non prevedibile (manovrata) e la loro velocità rappresenta una sfida per gli attuali sistemi di difesa. Anche se fosse possibile risolvere i problemi di prevedibilità e quota di volo aumentando il numero di sensori di ricerca, riuscire a tracciare un sistema ipersonico e fornire dati precisi per l’ingaggio in tempi ristretti è un’ulteriore criticità che rende il sistema altamente strategico.

Dal punto di vista, quindi, della protezione delle forze – intesa come l’insieme di tutte le misure e gli strumenti per preservare la capacità di combattimento delle unità nella condotta delle operazioni – la capacità di contrasto dei missili ipersonici richiede un approccio integrato volto a garantire in modo estensivo e bilanciato la “protezione in profondità”.

In particolare, in relazione alle caratteristiche della minaccia ipersonica, le principali forme di protezione da sviluppare sono:

- *Close contact*;
- *Standoff*;
- *Left of launch*.



Con riferimento all'area “*Close Contact*”, è possibile distinguere specifiche misure di natura passiva e attiva³⁷ per garantire un adeguato livello di protezione contro missili ipersonici. Le misure passive devono permettere di resistere agli effetti di un attacco o ridurre la probabilità che un avversario possa condurre detta azione (es. utilizzare il *camouflage* per ridurre l'esposizione alla vista oppure il diradamento delle forze). Le misure attive, invece, prevedono l'ingaggio dell'avversario (anche preventivamente) e la neutralizzazione delle sue capacità offensive.

Inoltre, il grado di efficacia aumenta in relazione all'estensione e all'integrazione di queste misure con le altre previste nell'ambito delle aree “*Standoff*” e “*Left of Launch*”. In particolare, in relazione alle Operazioni Multidominio e alle caratteristiche della traiettoria dei missili ipersonici, diventa di fondamentale importanza prevenire il lancio sfruttando anche le capacità disponibili nel dominio Spazio e *Cyber*.

In tale ambito, tenuto conto anche del *range* di un missile ipersonico, l'attività di *intelligence*, unita a quella ISR (*Intelligence Surveillance and Reconnaissance*), risulta di fondamentale importanza per fornire il corretto quadro informativo a supporto delle decisioni.

5.3 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA

La minaccia potrà essere evitata con una difesa passiva, provvedendo ad una stratificazione delle forze, aumentandone le capacità di scoperta delle diverse piattaforme di lancio, nonché la preventiva e più rapida dislocazione dei sistemi di contrasto a difesa delle forze militari e dei siti sensibili.

Le difese attive si compongono invece delle diverse componenti che devono far parte di un sistema equilibrato, integrato ed economicamente conveniente (la difesa dalla minaccia è

molto più
costosa della
minaccia stessa).

La protezione dai missili ipersonici deve essere intesa come
integrazione di molteplici attività svolte da diversi attori a diversi livelli e in profondità: deterrenza, prevenzione, sicurezza attiva, difesa passiva e mitigazione sono misure che non devono essere intese separatamente. Solo la stretta



³⁷ Applicando quanto previsto dall'AJP-3.14 “*Allied Joint Doctrine for Force Protection*”

correlazione e integrazione tra misure passive e attive contribuisce ad aumentare il grado di protezione delle forze.

Pertanto, si rende necessario:

- sviluppare CONOPS (*Concept of Operations*), simulazioni e *wargaming*, per valutare l'integrazione di qualsiasi nuova capacità con i sistemi esistenti identificando i cambiamenti richiesti alla dottrina e al supporto dell'Alleanza;
- garantire che i sistemi di difesa approvvigionati da parte NATO/EU siano interoperabili e che possano migliorare la copertura dei sensori, migliorare i tempi di reazione e supportare le intercettazioni;
- ottimizzare l'infrastruttura C2 per supportare le operazioni in un teatro di battaglia ampliato e in rapida evoluzione, consentendo la rapida fusione di dati di *intelligence* e sensori e la loro successiva diffusione ai decisori;
- incoraggiare la condivisione delle conoscenze e la cura dei dati in relazione alla ricerca emergente su materiali, sistemi di propulsione, guida e miglioramenti della modellazione all'interno dell'Alleanza;
- sviluppare e utilizzare modelli, simulazioni e dati di volo di prova per esplorare i limiti del profilo di volo delle minacce, per consentire la previsione anticipata delle zone di impegno e l'uso della controforza e per identificare dove apportare miglioramenti alle capacità odierne;
- sviluppare in ambito Industria nazionale, anche in cooperazione internazionale, una nuova *capability* costituita da sistemi di sensori e intercettori capaci di scoprire, tracciare e contrastare le nuove minacce ipersoniche;
- incoraggiare lo sviluppo delle strutture di prova e addestramento a terra, necessarie per supportare la difesa e l'attacco con armi ipersoniche, inclusi DEW (*Direct Energy Weapon*), Cyber ed EW (*Electronic Warfare*).

In termini di capacità specifiche, si identificano:

➤ **Comando & Controllo (C2)**

La componente C2 nel *counter-hypersonic missile* deve essere mantenuta a livello strategico-operativo ampliando ed integrando la consapevolezza di tale minaccia a livello interagenzia e multinazionale, al fine di sfruttare le sinergie connesse alla rete di *early warning* e garantire la piena e rapida capacità di risposta. Peraltra, tenuto conto delle sue caratteristiche peculiari, la capacità C2 deve sfruttare i sistemi della robotica e dell'Intelligenza Artificiale allo scopo di ricevere un consistente supporto decisionale, dove lo scambio di dati e di servizi tra sistemi e sensori (es. radar di nuova generazione, *cluster multisensore*) sarà essenziale.

➤ ***Intelligence, Surveillance and Reconnaissance (ISR)***

Sulla base delle caratteristiche della minaccia ipersonica, occorre porre in essere tutte le azioni necessarie per ricercare, identificare e riportare i sistemi e le piattaforme che possono essere utilizzati per il lancio di missili ipersonici. In questa prospettiva, le capacità ISTAR (*Intelligence, Surveillance, Target*

Acquisition and Reconnaissance) dello Strumento Militare dovranno essere in grado di individuare l'intero sistema sotteso al lancio di missili ipersonici. Queste attività, da sviluppare in forma integrata a livello multinazionale e internazionale, permetteranno di identificare gli anelli deboli del sistema sotteso al lancio di missili ipersonici e di agevolare il decisore nel delineare la possibile soluzione (non necessariamente di natura cinetica).

➤ Sensoristica

- Sensoristica spaziale: gli attuali satelliti di preallarme possono rilevare il lancio di veicoli, ma non sono adatti a seguirli durante la fase di planata. Solo i sensori spaziali possono fornire tracce di qualità per il controllo del fuoco per i missili ipersonici.
- Sensoristica terrestre: gli odierni radar per missili balistici di superficie sarebbero in grado di individuare un'arma solo una volta che attraversa l'orizzonte.
- Sensoristica navale: i sistemi radar imbarcati sono attualmente efficaci nei confronti della minaccia missilistica “convenzionale”, ma risultano ancora non ottimizzati per una minaccia estremamente veloce e manovriera come quella ipersonica. Risulta necessario, pertanto, verificare le reali capacità dei sistemi in linea nei confronti della minaccia ipersonica e individuare il *gap* capacitivo da colmare in termini di requisiti, studiando sia la fisica della formazione del plasma, sia la sua interazione con le onde elettromagnetiche prodotte dai radar.
- Sensoristica aerospaziale: risulterà necessario integrare ulteriormente la rete di sensori aerotrasportati (*Airborne Early Warning* e *fighter type*) per creare e potenziare una “*combat cloud*” capace di fornire una *picture* aggiornata. I sensori dovranno essere parte integrante di un sistema di sistemi dispiegabili in maniera dinamica su piattaforme sia *manned* sia *unmanned*.

➤ Reazione

- Intercettori: gli intercettori esistenti possono essere migliorati ma, certamente, dovranno essere sviluppati nuovi intercettori più adatti allo *stress* termico e all'ambiente di alta manovrabilità della missione. In particolare, potrebbero essere sviluppati intercettori endoatmosferici con propulsore a statoreattore tipo *ramjet* a velocità modulabile, con testa di ricerca (*seeker*) di tipo duale (RF/IR), capace di contrastare una pluralità di minacce (*Tactical Ballistic Missile*, *Hypersonic Cruise Missile*, *Hypersonic Glide Vehicle*).
- Armi ad energia diretta: le armi a energia diretta (*Direct Energy Weapons – DEW*) potrebbero potenzialmente prendere di mira minacce ipersoniche nella loro fase di crociera o bloccarle nella loro fase terminale, ma la complessità della missione determinerà quasi certamente sia effetti cinetici che non cinetici.

Capitolo 6

TECNOLOGIE QUANTISTICHE

6.1 LA SECONDA RIVOLUZIONE QUANTISTICA

Le prime applicazioni della meccanica quantistica hanno avuto, già nello scorso secolo, un impatto rilevante sui sistemi grazie all'utilizzo dei più importanti dispositivi realizzati dalla "prima rivoluzione quantistica" (basata sul comportamento di gruppi di quanti): tra essi transistor, semiconduttori, computer *chip*, laser e sistemi di visione.

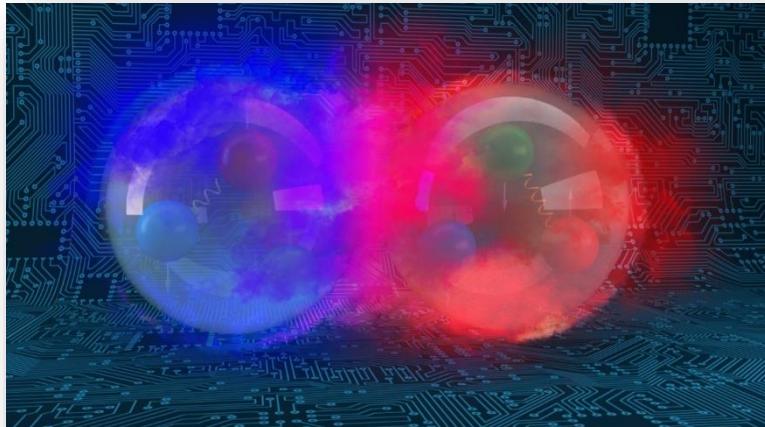
La "seconda rivoluzione quantistica" (fondata sul trattamento di singoli quanti, giunzioni superconduttrici, atomi freddi, intrappolamento di ioni, ecc.) offre ora nuovi e più sofisticati strumenti che basano il loro funzionamento su effetti totalmente assenti nella fisica classica e concettualmente non intuitivi: tra essi *l'entanglement* ("intrecciamento"), la sovrapposizione di stati quantistici e l'indeterminazione.

I settori nei quali queste tecnologie attualmente si prevede potranno avere maggior impatto sono quelli delle comunicazioni, del calcolo, della crittografia, della simulazione, della sensoristica, della metrologia e dei sistemi di rilevazione di oggetti (sistemi

radar, di visione, di creazione di immagini).

Sebbene le realizzazioni attuali si trovino, per la gran parte, a TRL ancora bassi³⁸, in alcuni settori (quali, ad esempio, le comunicazioni

per scambio di chiavi cifrate, dove il TRL pare già essere a ~ 6) va rilevata la disponibilità sul mercato di prodotti commerciali per l'implementazione di funzionalità di livello elevato. A ragione di ciò, tutte le grandi potenze hanno avviato programmi di finanziamento e sviluppo al fine di arrivare per prime a godere dei vantaggi



³⁸ TRL: *Technology Readiness Level* (livello di maturità tecnologica). È basata su una scala di valori da 1 a 9, dove 1 è il più basso (definizione dei principi base) e 9 il più alto (sistema già utilizzato in ambiente operativo).

tecnologici che certamente (se non altro per scopi specifici) alcuni dispositivi potranno offrire, in modo affidabile, come detto, già a breve.

In prospettiva, molti studi di *foresight* indicano, per il prossimo ventennio, un'entrata determinante delle tecnologie quantistiche anche nei domini delle altre EDTs e che, con elevata probabilità, le prime applicazioni dirompenti saranno quelle trasversali che accoppieranno tecnologie proprie di differenti domini disciplinari come Quantistica & Spazio oppure Quantistica & Biotehnologie o, ancora, Quantistica & Intelligenza Artificiale.

Va da sé che le applicazioni con maggiori ricadute commerciali (come nel supercalcolo e nella crittografia) saranno le prime ad apparire sui mercati e la Difesa si potrà trovare – come già accaduto in passato con i semiconduttori, le comunicazioni *wireless*, il 5G, ecc. – a dover/poter utilizzare le ricadute di investimenti tecnologici rilevanti, realizzati nel settore civile, generate sia da *start-up* e *spin-off* accademici o (come è nel caso del super-calcolo) da grandi gruppi industriali del settore *Big Data* o dell'Elettronica (*Google, Alibaba, IBM, Intel, ecc.*).

Al contrario, i tempi per la messa a disposizione di apparecchiature per esclusive/principali applicazioni operative nella Difesa potrebbero essere più lenti. In questo contesto, va quindi considerato un aspetto che, sebbene non direttamente connesso con la tecnologia e con le sue leggi, ne è strettamente correlato: l'accessibilità. Lo sviluppo delle tecnologie quantistiche rappresenta, come sopra accennato, una fetta di uno specifico mercato che muove enormi interessi economico-finanziari e che già sta portando sugli scenari internazionali attori nuovi e differenti da quelli statuali che attualmente detengono “ampie proprietà” in queste tecnologie. In un futuro medio-lungo, invece, grandi gruppi industriali potrebbero investire capitali ancora più ingenti e raggiungere una “autonomia quantistica” che inevitabilmente porterà a ridefinire equilibri geo-politici (ma non solo) in settori determinanti per la Sicurezza e la Difesa.

La costruzione di un ecosistema nazionale favorevole alle *Quantum Technologies* che coinvolga, insieme alle Istituzioni preposte anche il sistema della ricerca pubblica e del mondo industriale (dalle *start-up* alle consolidate aziende del settore della Difesa), è una scelta strategica che deve essere perciò implementata e costantemente potenziata.

L'Italia della Ricerca e dell'Innovazione è ottimamente inserita in programmi dell'Unione Europea avviati per studi ed applicazioni quantistiche, dispone di una Traiettoria Nazionale per le Tecnologie Quantistiche e di una dorsale in fibra ottica (IQB- *Italian Quantum Backbone*) per la comunicazione e la metrologia quantistica. Molte sono, inoltre, le realtà di eccellenza scientifica nella ricerca pubblica (Università e Politecnici, CNR- Consiglio Nazionale delle Ricerche, INFN- Istituto Nazionale di Fisica Nucleare, INRIM- Istituto Nazionale di Ricerca Metrologica) e in quella privata.

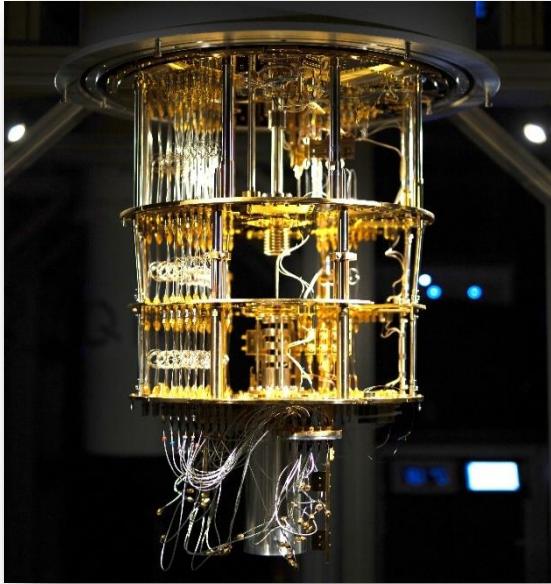
6.2 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA

➤ Calcolo

I computer quantistici offrono (soprattutto per problemi di ottimizzazione e simulazione) potenze di calcolo di ordini di grandezza superiori a quelli dei calcolatori “classici”, grazie al ricorso al principio quantistico della sovrapposizione di stati: si passa così dal bit (intesa come unità di informazione classica) al *qubit* - *Quantum Bit*, che non si presenta solo nei due stati 0 e 1, ma anche in tutte le possibili loro sovrapposizioni.

Ciò può fornire (nel rispetto di stringenti condizioni) una capacità di calcolo tale da permettere di decifrare (ad esempio) alcuni dei sistemi crittografici a chiave asimmetrica basati su problemi matematici intrattabili da un computer classico (come nel caso dell’algoritmo RSA - *Ronald Rivest, Adi Shamir e Leonard Adleman* – comunemente utilizzato per la protezione di transazioni ed accessi via Internet a siti bancari o che, comunque, trattino dati sensibili), ma anche fornire enormi ricadute su molte discipline, incluso il supporto ai processi decisionali, la simulazione/costruzione di molecole complesse di interesse per le scienze dei materiali e biologiche. Altri campi dove i computer quantistici

possono avere un impatto dirompente sono: l’ottimizzazione dei processi (logistica, allocazione di risorse, ecc.), Intelligenza Artificiale e *Machine Learning* (accelerazione del *training*, processo di enormi quantità di dati, ecc.), simulazioni con metodo Monte Carlo (valutazione dei rischi, modelli stocastici), e risoluzioni di sistemi lineari di equazioni. Le tecnologie attualmente utilizzate per la progettazione di computer



quantistici sono differenti, così come differenti sono gli oggetti fisici che possono fungere da *qubit*. In questa fase è ancora difficile prevedere quale delle piattaforme tecnologiche attualmente proposte (*chip* superconduttori, intrappolamento di ioni, circuiti fotonici, silicio, ecc.) sarà vincente o, semplicemente, sopravviverà nei prossimi anni alle richieste di aumento del numero di *qubit*, di efficienza e di riduzione del rumore quantistico (quindi della possibilità di errore). Certamente la capacità di implementare tecniche *di QEC – Quantum Error Correction* sarà fondamentale nei prossimi anni, come pure la possibilità di ottenere porte logiche quantistiche che operino a temperature

ambiente (come già dimostrato possibile al MIT – *Massachusetts Institute of Technology*). È comunque prevedibile che i primi sistemi che realmente saranno a disposizione saranno sistemi ibridi che accoppieranno computer classici e quantistici.

➤ **Sensori**

I sensori quantistici evidenziano, rispetto a quelli attuali, incrementi molto rilevanti di sensibilità e aprono nuove opportunità per lo sviluppo di rivelatori gravitazionali, magnetici, giroscopici ed acustici capaci di misurare le più piccole variazioni dei rispettivi campi. L'incremento, quindi, della *Situational Awareness*, attraverso elevate capacità di analisi spazio-temporali, obbligherà, già nel prossimo decennio, a modificare le tecniche per rendere meno individuabili velivoli, *bunker* e sommergibili, permetterà l'individuazione di mine/esplosivi, anche ad elevata profondità, renderà ancora più precise le rilevazioni da satellite, contribuendo a generare una *predictive intelligence* coerente e più vicina alla situazione reale.

Lo sviluppo di sensori per la navigazione inerziale (con precisa determinazione di accelerazioni e momenti angolari), uniti ad orologi ad altissima stabilità, permetterà inoltre la misurazione di precisione degli spostamenti, anche in assenza di segnali satellitari di geo-riferimento e con evidenti vantaggi di supporto alla manovra di unità e munizioni guidate. Infatti, operazioni di veicoli autonomi o in situazioni ambientali in assenza di segnali satellitari (ad esempio UUV sotto il ghiaccio, operazioni in *bunker* sotterranei o in edifici schermati) trarranno grande giovamento dal ricorso a questa tipologia di sensoristica quantistica. I sensori magnetici quantistici, ad esempio, basati su vacanze di atomi di azoto in nano-cristalli di diamante, possono essere impiegati per misurazioni ad altissima sensibilità di proprietà ambientali come, appunto, il campo magnetico (fino a valori di flusso dell'ordine dei femtotesla), la temperatura e i valori di campo elettrico. Il vantaggio rispetto ai sensori SQUID – *Superconducting Quantum Interference Devices* (che richiedono ingombranti sistemi di raffreddamento ad azoto o elio liquido per mantenere la condizione di supercondutività) risiede nella maggior compattezza derivata dalla loro capacità di funzionamento anche a temperatura ambiente che li rende adatti ad impieghi operativi. In aggiunta, le potenzialità di risoluzione spaziale si attestano intorno ai nanometri, prefigurando la possibilità di effettuare delle vere e proprie operazioni di *imaging* del campo magnetico. Tali caratteristiche rendono questa tipologia di sensori a nano-cristalli di diamante particolarmente importante negli impieghi di rilevazioni di anomalie magnetiche in ambiente sottomarino. I vantaggi di bassa segnatura magnetica posseduti, infatti, dagli attuali moderni sottomarini (ottenuti sia grazie a processi di *deperming* e *degaussing*, sia con l'impiego di materiali amagnetici) potrebbe, nel prossimo futuro, azzerarsi influenzando pesantemente le tattiche di *Anti Submarine Warfare* (ASW). È opportuno anche citare le potenzialità nel campo dell'*imaging* ottico, dove l'utilizzo della elevata correlazione generata dall'*entanglement* consente

l'utilizzo di raffinate soluzioni tecniche (ad esempio *Ghost Imaging*, *Quantum Illumination/Quantum Radar*) per la rilevazione, identificazione e *tracking* in condizione di visibilità estremamente bassa e/o con elevata luminosità di fondo anche contro bersagli cosiddetti “*stealth*” rispetto alla tecnologia radar attuale. Altre tecniche si fondano, invece, sulla raccolta e sull'identificazione temporale di fotoni diffusi dopo *scattering* multipli permettendo la ricostruzione e il riconoscimento di oggetti e minacce nascosti dietro ad ostacoli e, quindi, fuori della linea di vista (la così dette metodologie *Non Line of Sight* oppure *Behind the Corner*).

Per quanto è invece riferito ai recenti annunci di costruzione di radar quantistici, va sottolineato che i vantaggi dimostrati sono minimi e limitati a casi estremi di alto rumore di fondo.

➤ Comunicazioni

Un settore sul quale si evidenzia un impatto determinante è quello delle comunicazioni, soprattutto perché lo sfruttamento di fenomeni esclusivi della fisica quantistica apre la strada alla realizzazione di infrastrutture di comunicazione intrinsecamente sicure. Non ha mancato di suscitare attenzione il lancio, nell'agosto del 2016, del primo satellite quantistico cinese, Micius, dimostrando che la priorità accordata alla scienza dell'informazione quantistica è stata esplicitamente legata agli obiettivi di sicurezza nazionale (e in particolare di *cyber security*) oltre che di competizione economica.

Sfruttando l'*entanglement of quantum particles pairs* (effetto di “intrecciamento/interconnessione” tra le proprietà delle particelle), per lo scambio di chiavi crittografiche (*Quantum Key Distribution - QKD*) o per la trasmissione dell'informazione stessa (*Quantum Teleportation*), si possono, infatti, realizzare sistemi crittografici quantistici con la prospettiva futura di realizzare un *quantum-internet* costituito da reti di computer quantistici e sistemi di comunicazione, intrinsecamente sicuri.

In questo contesto, importanti sperimentazioni riguardanti la *Quantum Key Distribution (QKD)* sono da tempo in corso in molti Paesi e una vasta iniziativa europea, sostenuta congiuntamente dalla Commissione Europea (Direzione Generale CONNECT- Communications, Networks, Content and Technology) ed ESA- European Space Agency, è attualmente in corso. La sperimentazione è finalizzata alla progettazione e alla realizzazione di una Infrastruttura di Comunicazione Quantistica (Euro QCI) per lo scambio di chiavi cifrate che impieghi contemporaneamente *links* in fibra ottica su scala metropolitana/regionale e *links* satellitari in spazio libero su scala, invece, nazionale e internazionale, per determinare così una completa copertura continentale. Tale infrastruttura ibrida, che vede come primi esempi di uso le comunicazioni intergovernative e la protezione di infrastrutture critiche, si pone, come obiettivi di medio termine, l'utilizzazione di tecnologie già esistenti e la progettazione, attorno ad esse, di una rete continentale con funzionalità *end-to-end*.

La *Quantum Teleportation* (via satellite e via fibra ottica) costituisce il passo successivo verso una infrastruttura di comunicazione quantistica che sia in grado di garantire altre funzionalità al di là dello scambio chiavi (*Distributed Quantum Computing*, *Distribute Quantum Sensing*); essa necessiterebbe, tuttavia, di trasmettere, mantenendo la coerenza degli stati quantistici sulle lunghe distanze, potendo anche immagazzinarli in opportune memorie quantistiche.

Di particolare interesse, nell'ambito delle comunicazioni sicure, saranno certamente i recenti studi sulla comunicazione quantistica sottomarina attraverso l'impiego di nuove tecnologie di trasduttori acustici che potrebbero avere risvolti importanti nell'ambito dei veicoli *unmanned*, dove tendenzialmente si hanno a disposizione fonti energetiche limitate. Il passo successivo potrà essere nella direzione di utilizzare la *Quantum Teleportation* (fino ad oggi studiata solo nelle comunicazioni satellitari o via fibra ottica) anche nel dominio marittimo. Lo sviluppo di idonei *quantum repeaters* potrà consentire tutto ciò. La prospettiva è, tuttavia, almeno ventennale, in quanto le attuali criticità legate ad aspetti teorici, sperimentali e di protocolli di comunicazione non sono di poco conto.

Inoltre, sebbene possa apparire una riflessione ancora nelle fasi iniziali, è importante sottolineare alcuni aspetti della sicurezza che costituiscono una problematica comune a tutti i sistemi di comunicazione, indipendentemente dal fatto che essi si basino sulle leggi della meccanica quantistica o della fisica classica. Per garantire, infatti, la sicurezza è sempre importante definire un processo di valutazione sia dell'intero sistema (e, conseguentemente, di certificazione nazionale ovvero internazionale per i contesti inter operativi), sia dei suoi singoli componenti.

➤ **Simulazione**

La possibilità di simulare sistemi complicati e complessi (fino a strutture subatomiche), attraverso algoritmi dedicati supportati dalla potenza di calcolo dei computer quantistici (o ibridi), potrà portare, come già sopra accennato, alla vera e propria costruzione di nuovi materiali concepiti *ad hoc* per specifici impieghi (es. per la costruzione di nuovi trasduttori acustici per impieghi *underwater*) e/o farmaci mirati alle specifiche caratteristiche genetiche di un singolo individuo.

➤ **Contesto “Verde”**

La disponibilità di ampie capacità di calcolo e sensoristica avanzata condurrà sia alla costruzione di modelli climatici più affidabili ad ampia scala (megaregioni o planetaria), sia alla realizzazione di modelli fisici a scala atomica per ingegnerizzare processi finalizzati all'aumento dell'efficienza di dispositivi per la produzione di energia e/o per il suo stoccaggio. Non va inoltre dimenticato che il costo energetico degli attuali dispositivi quantistici è estremamente elevato e non è certamente ancora costo-efficacia in un contesto di sostenibilità.

Capitolo 7

BIOTECNOLOGIE

7.1 CAMPI DI APPLICAZIONE DELLE BIOTECNOLOGIE

Le Biotecnologie trovano applicazione in settori molto diversi tra loro, con in comune la caratteristica di avere come prodotti materiale organico od organismi biologici, in ambito sanitario (es. sviluppo di anticorpi monoclonali), agricolo e zootecnico (es. produzione di transgenici in animali e piante), alimentare (es. nuovi enzimi), chimico (es. tessuti vegetali), energetico ed ambientale.

I progressi della bioingegneria nel settore dell'agricoltura, dell'allevamento degli animali e della medicina, hanno sicuramente rinnovato l'interesse militare nel campo delle armi biologiche: la velocità con cui nascono e vengono manipolati nuovi agenti, unita alla facilità di reperirli sul mercato ed utilizzarli a scopo malevolo da un nemico non identificabile, alimenta indubbiamente una grande preoccupazione a livello mondiale.

La bioinformatica e i biosensori avanzati miglioreranno il monitoraggio e la consapevolezza bio-situazionale attraverso l'applicazione della raccolta dati avanzata e dell'analisi predittiva. Sfruttare tali tecniche sosterrà le condizioni di salute, la prontezza operativa e la formazione, attraverso risposte predittive e preventive a questioni ambientali o individuali.

Gli studi sul potenziamento e sul miglioramento umano attualmente sono più mirati su applicazioni di tipo meccanico, *in primis* gli esoscheletri, che, seppur ad oggi limitati a causa del loro costo elevato e considerando i molteplici campi di applicazione (ad esempio logistica e edilizia), saranno in futuro impiegati a livello massivo. Differiscono invece i processi di potenziamento umano di tipo

fisiologico/prestazionale e cognitivo che, a causa di barriere etiche, morali e legali, sono attualmente a livello embrionale.

Lo sviluppo di nuove contromisure mediche e, più in generale, delle tecnologie biomediche riunisce e applica sviluppi paralleli in bioinformatica, biosensori, potenziamento umano e biologia sintetica.



La ricerca applicata nella cura degli infortuni e nelle interfacce neurali, ad esempio, aiuterà a supportare la medicina basata sulle evidenze, la prontezza operativa, la previsione e l'individuazione di malattie, la medicina incentrata sul paziente, il rapido sviluppo di contromisure CBRN (Chimico, Biologico, Radiologico, Nucleare), nonché a migliorare la riabilitazione attraverso nuove interfacce neurali.

In ambito civile, il settore delle Biotecnologie risulta in forte fermento con un chiaro indirizzo strategico: promuovere l'integrazione tra aziende biotecnologiche, aziende farmaceutiche, istituzioni finanziarie e istituti di ricerca e porre le basi per realizzare in Italia quello che potrà divenire uno dei principali *cluster* biotecnologici europei³⁹.

Attualmente in Italia non esistono chiare linee guida di indirizzo strategico e politico militare nel campo delle Biotecnologie applicate alla Difesa; esistono piuttosto alcuni interessamenti e partecipazioni a progetti di ricerca per il settore CBRN e *Human Factor* seguiti dall'EDA (*European Defence Agency*), inerenti database di virus e agenti patogeni⁴⁰.

Secondo le stime dell'OCSE⁴¹, le Biotecnologie nel 2030 avranno un peso enorme nell'economia mondiale: saranno *biotech* l'80% dei prodotti farmaceutici, il 50% dei prodotti agricoli e il 35% dei prodotti chimici e industriali, incidendo nel complesso per il 2,7% del PIL globale. Sempre entro il 2030 si stima che la popolazione mondiale crescerà del 28%, dai 6,5 miliardi del 2005 a 8,3 miliardi, e il reddito medio annuo globale pro-capite subirà un incremento del 57%, dai 5900 dollari del 2005 a 8600 dollari. Una popolazione mondiale più numerosa e ricca farà, quindi, crescere la domanda globale di servizi sanitari che aumentino la qualità e la durata della vita, al pari della domanda di risorse naturali essenziali come cibo, mangimi per animali, fibre per abbigliamento e arredamento, acqua pulita ed energia.

Le Biotecnologie offrono, dunque, le soluzioni tecnologiche per affrontare in modo efficace queste sfide, rappresentando già oggi lo strumento per il raggiungimento di traguardi totalmente inimmaginabili, fino a qualche anno fa, in diversi settori: dalle scienze della vita alla sicurezza alimentare, dall'agricoltura all'industria, fino in generale alla Bioeconomia.

³⁹ Secondo il Rapporto 2020 della FEDERCHIMICA sulle imprese di biotecnologie in Italia, si conferma il primato delle imprese che operano nel settore delle biotecnologie mediche, che sono 344 circa la metà delle imprese *biotech* italiane (49%). Il comparto genera una quota importante del fatturato, corrispondente a oltre 9 miliardi (75% del totale) e determina la maggior parte degli investimenti complessivi in R&S (91%) e occupa oltre il 75% degli addetti alla Ricerca & Sviluppo *biotech* in Italia.

⁴⁰ Analizzando i progetti di ricerca e sviluppo finanziati a breve termine dalla Difesa, sono da menzionare i programmi EMARIS e GRANADA, che hanno l'obiettivo di sviluppare rispettivamente un nuovo sistema di esoscheletro e un nuovo modello di standardizzazione per la generazione di tessuti umani individuo-specifici vascolarizzati e preservati dall'immuno-rigetto, attraverso la manipolazione di cellule staminali. - PNRM 2019/20 di SEGREDIFESA.

⁴¹ BIOTECH, il futuro migliore – FEDERCHIMICA 2020.

7.2 BIOINFORMATICA, BIOSENSORI E BIOELETTRONICA

La Bioinformatica è al centro della moderna biologia molecolare dove vengono sviluppati e utilizzati metodi computazionali per trasformare i dati biologici in conoscenza e tradurli in applicazioni biomediche. Tra i vari metodi computazionali utilizzati, l'apprendimento automatico, una branca dell'Intelligenza Artificiale caratterizzata dalla costruzione di modelli basata sui dati, è stato la tecnologia di calcolo abilitante principale per questo specifico campo della scienza. La bioinformatica è attualmente fortemente correlata al sequenziamento del DNA, poiché la genetica è di estrema importanza per la pratica medica in quanto fornisce una diagnosi per molte malattie clinicamente eterogenee.

Anche il campo dei Biosensori – definiti come dispositivi analitici compatti che incorporano un elemento di rilevamento biologico o di derivazione biologica (come un enzima, un anticorpo, un microbo o un DNA) integrato all'interno o intimamente associato a un trasduttore fisico-chimico – ha ricevuto di recente una spinta notevole per quanto riguarda l'utilizzo di tali tecnologie per il rilevamento del nuovo Coronavirus. Possono, infatti, rappresentare una valida alternativa come adeguati strumenti di rilevamento essenziali per contribuire ad arrestare o diminuire la diffusione di un virus prima che le conseguenze umane ed economiche diventino devastanti. L'applicazione dei biosensori in ambito militare è, pertanto, focalizzata sul monitoraggio dello stato fisiologico in tempo reale, in cui l'impiego di dispositivi indossabili (*wearable*) potrebbe fornire diverse applicazioni operative e tattiche, tra le quali:

- miglioramento delle prestazioni, tramite un supporto tecnologico al fine di ottimizzare la distribuzione del carico di lavoro e una migliore percezione / consapevolezza della situazione del *team*;
- rilevamento di imminente degradazione del soldato a causa del carico di stress (fisico, psicologico e ambientale);
- rilevamento immediato dell'esposizione ad agenti tali da costituire una fonte di rischio;
- individuazione delle vittime, del triage e della gestione clinica precoce;
- ottimizzazione della salute individuale e delle abitudini in termini di preparazione fisica;
- monitoraggio e dosimetria dell'esposizione associata al rischio per la salute a lungo termine.

La Bioelettronica offre notevoli potenzialità per la difesa biologica, in particolare per gli obiettivi di biosorveglianza e preallarme, analisi forense microbica, valutazione del rischio e *delivery* di contromisure mediche (MCM).

Tale tecnologia può trasformare la medicina militare, fornendo ai medici informazioni preziose per migliorare le cure sul campo di battaglia nonché ad assicurare cure prolungate. Ad esempio, i sensori bioelettronici che misurano una molteplicità di segnali, tra cui il battito cardiaco e la secrezione di metaboliti nel sudore, possono fornire il monitoraggio remoto dello stato di salute dei combattenti

durante le operazioni. La bioelettronica di nuova generazione può essere somministrata mediante impianto o può essere ingerita in modo da fornire farmaci terapeutici.

Vasto è il campo di utilizzo, che copre anche un'ampia gamma di possibili future applicazioni militari sulla base di:

- sensori che rilevano e valutano l'evoluzione di una ferita mentre si tiene traccia di come il corpo reagisce agli interventi o al trattamento;
- attuatori ispirati a principi biologici, con applicazioni sperimentali nella robotica;
- apprendimento adattivo che analizzerà tutti i dati per determinare gli interventi necessari.

7.3 POTENZIAMENTO UMANO

Il potenziamento umano si riferisce a tecnologie che migliorano la produttività o le capacità umane o che, in qualche modo, si aggiungono al corpo o alla mente umana, rispetto alle tre principali categorie di miglioramento fisiologico e cognitivo:

- sensi potenziati, ottenuti interpretando le informazioni multisensoriali disponibili e presentando il contenuto soggetto attraverso i sensi umani selezionati (es. vista aumentata, udito, sensazione tattile, olfatto e gusto);
- cognizione avanzata, ottenuta rilevando lo stato cognitivo umano, utilizzando strumenti analitici per farne una corretta interpretazione ed adattando la risposta del computer alle esigenze attuali e predittive dell'utente (es. fornendo informazioni memorizzate o registrate durante l'interazione naturale);
- azione aumentata, ottenuta rilevando le azioni umane e mappandole ad azioni in ambienti locali, remoti o virtuali (es. aumento del motore, forza amplificata e movimento, *input* vocale, controlli basati sullo sguardo, teleoperazione, presenza remota e altri).

➤ Potenziamento meccanico

Gli Esoscheletri sono dispositivi elettro-meccanici essenzialmente finalizzati ad aumentare le caratteristiche strutturali del corpo umano potenziandone la resistenza, l'agilità e/o la forza ovvero finalizzati a compensare una disabilità o aumentare meccanicamente le capacità dell'essere umano (in quest'ambito rientrano anche i dispositivi protesici finalizzati al recupero delle funzionalità di uno o più arti perduti a causa di una patologia o perché amputati). Il concetto di esoscheleto può essere esteso agli “esoscheletri virtuali” in cui un robot (droni/avatar), posto in una posizione remota, si muove in sincronia con i movimenti dell'utente, che potrebbe essere collegato con una tecnologia di Realtà Virtuale che gli permetta di “osservare” il punto di vista del robot.

Questo tipo di interazione uomo-robot potrebbe dimostrarsi particolarmente utile in ambienti operativi pericolosi o non permissivi (es. in ambienti contaminati o in ambito aerospaziale). Allo stato attuale si stanno sviluppando tecnologie capaci di aumentare l'autonomia di queste apparecchiature, riducendone peso e dimensioni e con una capacità di interazione tramite segnali mioelettrici, ossia mediante sensori sulla pelle, idonei a rilevare direttamente le tensioni associate ai segnali cerebrali inviati ai muscoli (*Brain Computer Interface*, BCI).

Inizialmente, la ricerca e lo sviluppo di esoscheletri in campo militare erano focalizzati alla realizzazione di protesi che restituissero la funzionalità di arti persi in azione o con l'obiettivo di migliorare le



capacità dei soldati sul campo di battaglia, rivolgendosi essenzialmente a strutture robotiche indossabili capaci di amplificare la forza e la resistenza di chi le indossa, o aumentarne l'agilità consentendo loro di avanzare su terreni particolarmente accidentati ed impervi.

Gli esoscheletri hanno il potenziale per migliorare le attuali capacità fisiche di un combattente, permettendogli di correre più velocemente, sollevare oggetti più pesanti e alleviare lo sforzo fisico durante operazioni impegnative.

L'obiettivo futuro è lo sviluppo della tecnologia degli esoscheletri per ottimizzarne l'efficacia operativa in teatro d'operazione. Le applicazioni più ampie di esoscheletri, robotica e sistemi autonomi si hanno attualmente nell'ambito della catena logistica (ad esempio, attraverso mezzi di rifornimento aereo o di supporto a squadre per alleviare il carico dei lavoratori, migliorare l'efficienza e ridurre gli infortuni), nell'aumento delle risorse operative e dell'efficacia dei sistemi d'arma (ad esempio, trasporto e caricamento di munizioni) o ancora per l'addestramento di medici e fisioterapisti, l'assistenza ai disabili o come aiuto nel recupero e nel salvataggio di emergenza sul campo di battaglia.

➤ **Potenziamento Neurologico**

Il potenziamento neurologico si riferisce all'estensione delle capacità cognitive in soggetti sani. La neurotecnologia si rivolge a metodi e strumenti che consentono una connessione diretta di dispositivi con il sistema nervoso (*Brain Computer Interface*) che hanno lo scopo di registrare i segnali dal cervello e di "tradurli" in comandi di controllo tecnico o di manipolare l'attività cerebrale tramite stimoli elettrici, magnetici o ottici.

Le neuroprotesi rappresentano l'applicazione più evidente dell'impatto delle neurotecnicologie applicate all'uomo: ne sono esempi gli impianti quali apparecchi acustici collegati direttamente al nervo uditivo ripristinando l'udito in taluni casi, gli impianti retinici per i non vedenti e gli impianti motori per i diversamente abili, oggetto di ricerche sempre più innovative. Sono tutti esempi di neuroprotesi, tecnologie che si interfacciano direttamente con il cervello: alcuni dispositivi sono invasivi e richiedono un impianto chirurgico, mentre altri sono indossabili e non invasivi; alcuni stimolano il cervello, mentre altri ne leggono solo l'attività; altre soluzioni cercano di integrare le due capacità.

Accanto alle protesi sensoriali o motorie, il campo emergente è quello inherente la neuroprotesica cognitiva, tecnologia che mira ad aumentare direttamente fattori come la creatività, la memoria di lavoro e l'intelligenza emotiva. Le funzioni cognitive come la comunicazione, la memoria, il processo decisionale, l'attenzione, la consapevolezza della situazione, le interazioni sociali, la risoluzione di problemi complessi, sono specificamente rilevanti nel contesto militare sia durante gli scenari offensivi e difensivi all'interno di un teatro operativo, sia durante gli esercizi di addestramento sul campo di battaglia per essere meglio preparati per tali scenari.

Quindi, le neurotecnicologie possono trovare adeguato ed efficace impiego nei seguenti settori:

- supporto alle decisioni nel contesto interazione Uomo-Macchina;
- sistemi di controllo diretto nel contesto interazione Uomo-Macchina;
- gestione e comunicazioni nell'interazione interumana;
- monitoraggio delle prestazioni;
- incremento delle prestazioni cognitive e fisiche;
- addestramento.

➤ **Implicazioni etiche del potenziamento umano**

Tutti gli sviluppi e possibili impegni in ambito militare non potranno esimersi dall'affrontare le necessarie implicazioni etiche correlate. Il potenziale di alterare le capacità cognitive, emotive, comportamentali e/o fisiche del personale militare solleva una serie di questioni e problemi etico-legali e sociali, per quanto riguarda il benessere, la considerazione e il trattamento di individui, così come le implicazioni e gli effetti internazionali dell'utilizzo di tali mezzi. Si prevede che il personale militare, dove un vantaggio rispetto all'avversario sposta il piano

dalla questione etica a quella della necessità strategica, avrà esigenze “uniche” che differiranno in modo specifico dalla popolazione generale: in quest’ottica andranno considerati i diversi tipi di scienza e tecnologie emergenti ed i correlati risvolti etici.

Una delle principali preoccupazioni nel contesto militare è quindi la sicurezza e il bilanciamento del rischio: il rischio, per un soldato, di sottoporsi ad un trattamento deve trovare un concreto bilanciamento rispetto alla minaccia operativa che il medesimo trattamento elimina, mitiga o contiene. I miglioramenti che potrebbero potenzialmente salvare le vite dei soldati dovrebbero essere presi seriamente in considerazione. Il contesto militare è, quindi, da considerarsi un ambito “speciale” o “eccezionale” di indagine etica, che può essere in contrasto con un approccio umanitario universalista al consenso informato e in cui i principi della bioetica medica possono dover essere applicati in modo diverso

7.4 BIOLOGIA SINTETICA

La biologia sintetica è una branca interdisciplinare della biologia e dell'ingegneria che combina varie discipline, come la biotecnologia, l'ingegneria genetica, la biologia molecolare, l'ingegneria molecolare, la biologia dei sistemi, la biofisica, l'ingegneria evolutiva, l'ingegneria informatica, l'ingegneria elettrica e l'ingegneria di controllo. Le biotecnologie trovano applicazione in settori diversi, con in comune la caratteristica di avere come prodotti finali o intermedi materiale organico od organismi biologici.

La biologia sintetica è molto promettente nella scoperta e nello sviluppo di farmaci con il potenziale utilizzo di sistemi biologici sintetici per i test antidroga e la capacità di creare nuovi percorsi biochimici per correggere i difetti genetici.

L'elemento che distingue la biologia sintetica dalla biologia molecolare e cellulare tradizionale è l'attenzione alla progettazione e alla costruzione di componenti fondamentali (ad esempio, parti di enzimi, circuiti genetici, percorsi metabolici) che possono essere modellati, compresi e adattati per soddisfare specifici criteri di prestazione e assemblaggio di queste parti e dispositivi più piccoli in sistemi integrati più grandi per risolvere problemi specifici.

I principali settori della biologia sintetica possono essere considerati:

- sintesi genica, che comprende metodi di sintesi artificiale di geni o di stampa del DNA in laboratorio o in contesti di ricerca;
- *Genome Engineering and Editing*, che comprende diversi metodi biotecnologici per la manipolazione di sequenze di acidi nucleici per applicazioni in biologia sintetica;
- tecnologie di clonazione e sequenziamento degli acidi nucleici;
- metodi di mutagenesi diretta al sito per introdurre cambiamenti mirati all'interno dei geni.

La guerra biologica è stata usata come arma nei conflitti per secoli, con effetti di vasta portata e spesso imprevisti e incontrollati sulle popolazioni militari e civili. La biologia sintetica potrebbe essere utilizzata per potenziare patogeni esistenti o creare di nuovi, quindi è importante considerare come questa possa abbassare le barriere relative alla produzione, alla stabilizzazione, al test e alla *delivery* di bioagenti o se i progressi in aree biotecnologiche diverse dalla biologia sintetica possano avere un impatto sul potenziale utilizzo come arma.

Oltre all'ovvio attacco biologico da uno Stato nemico, la Difesa ha un interesse nel prevenire, rilevare e trattare le minacce biologiche per garantire la disponibilità del personale militare e nel fornire assistenza nelle circostanze di crisi sanitarie e umanitarie. La biologia sintetica potrebbe creare materiale resistente alla corrosione, sensori ambientali o medici, ovvero altri materiali con applicazioni relative alla Difesa. La produzione biologica di materiali, farmaci o sensori potrebbe essere più economica, più rapida o più efficace della produzione tradizionale e tali prodotti potrebbero essere di qualità superiore o innovativa.

Le potenziali applicazioni della biologia sintetica in ambito Difesa possono essere riassunte come segue:

- materie prime: materiali più economici per tessuti e altri prodotti; carburanti più economici e lubrificanti ad alte prestazioni;
- materiali speciali: materiali attivi per sensori; polimeri ad alta resistenza per armature; materiali invisibili; rivestimenti resistenti alla corrosione; informatica biologica; archiviazione dei dati e materiali crittografici;
- rilevamento: *tag* distribuiti, sistemi di tracciamento ed inseguimento; sensori clandestini persistenti;
- aspetti medici e prestazioni umane: applicazione profilattica di batteri sulla pelle finalizzata a prevenire infezioni e ad accelerare la guarigione di ferite; probiotici che mitigano gli effetti dello stress e migliorano le prestazioni mentali;
- minacce biologiche e chimiche e le connesse misure difensive: sviluppo di nuovi agenti per il contrasto alla minaccia; trattamenti per armi biologiche e chimiche tradizionali e innovative.

7.5 CONTROMISURE MEDICHE E TECNOLOGIE BIOMEDICHE

Le contromisure mediche e le tecnologie biomediche di supporto assicurano un approccio integrato e sistematico allo sviluppo dei vaccini, farmaci, terapie e strumenti diagnostici necessari per le emergenze di sanità pubblica imputabili ad incidenti, eventi pandemici e malattie infettive emergenti.

Le contromisure mediche, o MCM, possono essere utilizzate per diagnosticare, prevenire, proteggere o trattare condizioni associate a malattie infettive emergenti, disastri naturali o minacce chimiche, biologiche, radiologiche, nucleari (CBRN).

Esempi di tali contromisure mediche includono antivirali, vaccini di nuova generazione, antibiotici e antitossine.

Le tecnologie biomediche costituiscono un campo recente e in rapido sviluppo, i cui assi più importanti sono le tecniche di riabilitazione (es. sistemi di apprendimento per persone disabili, *software* per la formazione), i biosegnali (elaborazione del segnale di *pacemaker*, defibrillatori intracardiaci e impianti per la diagnosi), il telemonitoraggio (monitoraggio a distanza dello stato di salute, monitoraggio domiciliare) e, infine, telemedicina.

L'ingegneria biomedica è l'applicazione di principi di ingegneria e concetti di progettazione alla medicina e alla biologia per scopi sanitari (diagnostici o terapeutici). Questo campo cerca di colmare il *gap* tra ingegneria e medicina, combinando le capacità di progettazione e risoluzione dei problemi dell'ingegneria con le scienze biologiche mediche per far registrare progressi nei trattamenti sanitari, compresa la diagnosi, il monitoraggio e la terapia. Nell'ambito delle attività di un ingegnere biomedico è inclusa anche la gestione delle apparecchiature mediche all'interno degli ospedali nel rispetto degli standard di settore pertinenti. Importanti applicazioni di ingegneria biomedica includono lo sviluppo di protesi biocompatibili, vari dispositivi medici diagnostici e terapeutici che vanno dalle apparecchiature cliniche ai microimpianti, apparecchiature di *imaging* comuni come MRI (*Magnetic Resonance Imaging*) ed ECG/EKG (*Electrocardiogram*), crescita di tessuti rigenerativi, farmaci e farmaci biologici terapeutici.



I biomarcatori forniscono informazioni oggettive sullo stato di salute del soggetto e sono indicatori dei normali processi biologici o delle risposte farmacologiche ad un intervento terapeutico. Si riferiscono a varie proteine, metaboliti, altri composti, geni o eventi biologici che sono indicativi di una rilevante condizione biologica (ad esempio, predisposizione a una malattia o progressione della stessa).

La medicina personalizzata è l'adattamento del trattamento medico alle caratteristiche individuali del paziente, aumentando la capacità di prevedere quali trattamenti medici possano essere sicuri ed efficaci. Le tecnologie mediche personalizzate sono promettenti in termini di previsione, prevenzione e trattamento della malattia mirato alle esigenze individuali.

Le contromisure CBRN sono iniziative e prodotti regolamentati anche a livello internazionale che possono essere utilizzati in caso di potenziale emergenza sanitaria pubblica, generata da un attacco con materiale chimico, biologico, radiologico o nucleare. Tali contromisure possono essere utilizzate per rilevare, diagnosticare, prevenire, proteggere o trattare condizioni associate a minacce del tipo CBRN. Le tecnologie di rilevamento CBRN possono essere segmentate in rilevamento, attrezzatura e tipo di minaccia ed in sistemi *standoff* e *stand alone*, rilevatori di radiazioni, veicoli da ricognizione, sistemi di emergenza e di primo intervento, tute ignifughe e indumenti protettivi, simulatori di addestramento e veicoli senza pilota.

7.6 IMPLICAZIONI SULLA DIFESA E SULLA SICUREZZA

La moderna biotecnologia offre un enorme vantaggio militare. Come ha insegnato la pandemia di COVID-19, le minacce biologiche - che siano di origine naturale, accidentale o intenzionale - sono tra le minacce più gravi per la comunità internazionale. Focolai naturali o accidentali, così come attacchi deliberati, possono avere origine in un Paese e diffondersi a molti altri, con conseguenze internazionali potenzialmente di vasta portata. I progressi della scienza promettono cure migliori

e più rapide, ma comportano anche nuovi rischi per la sicurezza. In questo panorama in rapida evoluzione, la comunità internazionale deve essere preparata a



gestire i rischi posti da focolai naturali di malattie, incidenti con agenti patogeni ad alto rischio o avversari che desiderano fare danni con agenti biologici. L'urbanizzazione, l'invasione dell'habitat e l'incremento della mobilità globale insieme a sistemi sanitari deboli, accrescono la capacità delle malattie infettive di diffondersi rapidamente in tutto il mondo.

L'uso di armi biologiche o la loro proliferazione da parte di attori statali o non statali rappresenta una sfida significativa per la nostra sicurezza nazionale, la nostra agricoltura e l'ambiente. Molteplici nazioni hanno perseguito programmi clandestini di armi biologiche e numerosi gruppi terroristici hanno cercato di acquisire armi biologiche. In generale, si potrebbe dire che due tipi principali di gruppi/individui sono in grado di applicare le tecniche avanzate della biotecnologia ai fini del bioterrorismo. La prima categoria potrebbe essere rappresentata dalle

organizzazioni terroristiche internazionali sponsorizzate da Stati, ossia con l'assistenza dello Stato *sponsor* in possesso di un programma segreto sulle armi biologiche. Il secondo tipo potrebbe essere costituito da scienziati interni ad un laboratorio di microbiologia clinica o in un laboratorio accademico, coinvolti in alcuni aspetti della ricerca microbiologica. È probabile che la biotecnologia determini profondi cambiamenti nel campo militare.

La natura a “duplice uso” della biotecnologia nel campo civile e militare caratterizza un’evoluzione inarrestabile nel campo della ricerca e delle applicazioni, registrando progressi con uno sviluppo esponenziale. Nel breve termine, le biotecnologie potrebbero essere utilizzate direttamente come mezzo di difesa e attacco, generando nuove tipologie di armamenti in grado di produrre danni non letali e reversibili, capaci di alterare le caratteristiche biologiche dei corpi umani. Processi come l’automazione del sequenziamento nei progetti genomici, la bioinformatica e i progressi nella chimica combinatoria e lo *screening* ad alto rendimento dei composti sono in prima linea in questo campo. Di particolare interesse è la convergenza delle biotecnologie con altre tecnologie emergenti, in particolare la manifattura additiva (spesso indicata anche come stampa 3D), l’Intelligenza Artificiale e la robotica, sottolineando che l’intersezione di queste tecnologie è destinata ad avere un impatto sul panorama del rischio biologico e della biosicurezza sollevando un insieme comune di rischi e sfide. Dopotutto, queste tecnologie aumentano l’esposizione dei dati biologici digitalizzati agli attacchi informatici e sono difficili da controllare a causa del loro carattere *dual-use* e del fatto che sono sviluppate principalmente per scopi civili dal settore privato.

Infine, dal punto di vista della biosicurezza, lo sviluppo e la produzione di vaccini hanno un grande valore strategico.

Riassumendo in maniera schematica, di seguito le implicazioni favorevoli (pro) e sfavorevoli (contro) per la Difesa:

➤ **Pro**

- prontezza – l’uso di biomarcatori (fenotipici e genetici) per la diagnostica predittiva consentirà l’identificazione preliminare di problemi medici o debolezze (ad esempio muscolo-scheletriche, psicologiche, immunologiche, fisiologiche o nutrizionali) e un monitoraggio dello stato umano in tempo reale;
- operazioni – i sistemi biomedici indossabili che forniscono la capacità di monitorare continuamente la salute dei militari potrebbero fornire la conoscenza dello stato di salute dei soldati sul campo di battaglia assicurando benefici nel garantire le informazioni essenziali necessarie per la valutazione dello stato delle forze. Queste ultime, sfruttando la bioinformatica, i sensori e le tecnologie di miglioramento, dovrebbero essere in grado di operare in gruppi più piccoli, con implicazioni sull’accessibilità economica (cioè un numero inferiore di soldati, marinai o aviatori può ottenere risultati simili). La realtà virtuale e, in ultima analisi, le interfacce neurali supporteranno

miglioramenti significativi nella consapevolezza situazionale e nelle operazioni dei sistemi autonomi;

- contromisure mediche e assistenza – l'uso di biomarcatori, biosensori e *microarray* (dispositivi micro-fluidici che integrano *chip* informatici con cellule viventi e tessuti) consentirà una diagnosi e una risposta rapida (pre-sintomatiche) ad agenti patogeni naturali, sostanze chimiche, nonché il monitoraggio in tempo reale delle opzioni di trattamento;
- prestazioni – l'ottimizzazione delle prestazioni di ogni individuo nei domini cognitivi, fisici o di resilienza, oltre a migliorare la coesione e l'efficacia del *team*, consentirà di prendere decisioni migliori più velocemente e di produrre azioni meglio sintonizzate sulle esigenze della situazione. I progressi attuali e futuri nel monitoraggio dello stato fisiologico e psicologico massimizzeranno le prestazioni umane complessive e la prontezza, attraverso applicazioni di algoritmi di Intelligenza Artificiale.

➤ **Contro**

Le minacce derivanti dalle biotecnologie aumenteranno in misura non trascurabile a causa della rapida diffusione e il facile accesso delle tecnologie a basso costo. L'aspetto più preoccupante sarà il loro utilizzo da parte di attori non individuabili e senza vincoli etici, in particolare, nei seguenti settori:

- biologia sintetica – l'impatto di nuovi agenti patogeni, nuovi agenti biologici o agenti chimici, con effetti esplicitamente progettati e mirati, metterà in discussione la capacità dei sistemi medici e logistici di farvi fronte, mentre le contromisure stesse potrebbero presentare sfide significative per la salute e la sicurezza;
- design dei farmaci – i criminali e non *state-actor* avranno sempre più capacità di sviluppare agenti farmacologici mirati a basso costo che potrebbero essere usati per interrompere operazioni militari o destabilizzare le società, attraverso effetti psicosociali mirati;
- super-soldati – le biotecnologie, con particolare aspetto alle tecniche per il potenziamento umano, abiliteranno avversari potenziati farmacologicamente, neurologicamente e fisiologicamente;
- interoperabilità – sarà messa a dura prova da diversi standard legali, politici, di formazione, di efficacia operativa ed etici tra le nazioni. Lo sviluppo di standard per i biosensori personali, la gestione dei bio-dati, la condivisione di contromisure mediche, le interfacce uomo-macchina (comprese quelle neurologiche) e i sistemi biomeccanici saranno fattori abilitanti critici, necessari per condurre in maniera efficace le prossime operazioni militari.

CONCLUSIONI

LE TECNOLOGIE EMERGENTI E DIROMPENTI NEL NUOVO CONTESTO MULTIDOMINIO

L'analisi degli scenari futuri (2040⁺) indica un ruolo sempre più determinante e pervasivo delle tecnologie emergenti e dirompenti che modificheranno in maniera sostanziale la società, l'economia, la politica e la dimensione della sicurezza e della difesa nazionale ed internazionale. Lo sviluppo tecnologico, caratterizzato da un andamento esponenziale, procede così rapidamente da non dare l'opportunità di comprenderne il cambiamento, tantomeno le conseguenze correlate. Si rende, quindi, necessario un approccio proattivo e condiviso tra attori istituzionali, ambiente accademico, mondo industriale e della ricerca per colmare la contrapposizione fra il ciclo di vita delle tecnologie e le tempistiche di sviluppo e di approvvigionamento. La capacità di sviluppare ed implementare tali tecnologie pone poi l'attenzione sulle questioni di "sovranità tecnologica" come componente essenziale dell'indipendenza di uno Stato e fondamentale strumento a sostegno del proprio livello di ambizione strategica rispetto ai principali *competitors*.

In tale quadro la Difesa dovrà essere caratterizzata da una spinta capacità di adattamento per affrontare gli scenari operativi futuri caratterizzati da un sistema di relazioni internazionali basato sulla persistente instabilità (*continuum of competition*), al fine di indirizzare le esigenze di trasformazione ed innovazione dello Strumento Militare in ottica Multidominio, in considerazione dell'espansione della competizione a nuova spazi di confronto quali i domini *Cyber* e Spazio, così come agli ulteriori ambienti elettromagnetico ed informativo. Lo sviluppo e l'implementazione di nuove soluzioni tecnologiche rappresentano quindi elementi abilitanti per la condotta delle Operazioni Multidominio. La spregiudicatezza con cui alcuni attori adottano nuove soluzioni tecnologiche per conseguire i propri precipui interessi sfruttando le lacune



normative del diritto internazionale (c.d. *lawfare*) contribuisce ad acuire il possibile divario tecnologico a sfavore dei Paesi occidentali. Per invertire tale tendenza risulta necessario avviare un processo di forte accelerazione dell’innovazione tecnologica, anche in ambito nazionale, attraverso lo sviluppo di nuovi modelli che possano consentire forme di collaborazione pubblico-privato più snelle, attraverso le quali sviluppare e implementare nuove soluzioni tecnologiche sulle quali modellare, qualora necessario, anche l’evoluzione del quadro normativo. Più in generale, si rende necessario promuovere una “Cultura dell’Innovazione” che permetta a tutti i livelli organizzativi e decisionali di cogliere appieno le sfide, ma soprattutto le opportunità offerte dalle tecnologie emergenti e dirompenti.

I principali *trends* di sviluppo delle tecnologie emergenti e dirompenti hanno messo in luce che:

- Il volume, la varietà e la velocità di generazione dei **Dati** (o più correttamente dei “*Big Data*”) rendono indispensabile l’implementazione di processi di *Data Governance* per l’intero ciclo di vita degli stessi (*Data Life Cycle*) mediante capacità di raccolta, memorizzazione e trattazione (es. *Defence Cloud*), disponibilità di sistemi di analisi e predizione in supporto al processo decisionale (c.d *Data Analytics*), applicazione di adeguate forme di protezione che ne impediscano l’uso indiscriminato, definizione di nuove regole etico-giuridiche che bilancino esigenze di *privacy* e disponibilità delle informazioni.
- La trasversalità dell’**Intelligenza Artificiale** quale tecnologia abilitante pone l’attenzione su quale dovrà essere il rapporto uomo-macchina (*Human Autonomy Teaming*) che dall’attuale relazione *master-slave* evolverà ineluttabilmente verso quella di *pear to pear*. Pur essendo ancora radicata la volontà di mantenere la centralità dell’essere umano (*man in/on the loop*), tuttavia la sempre maggiore velocità dei processi decisionali ci costringerà a un’evoluzione delle organizzazioni, sia in termini strutturali che sociali, ponendo maggiori deleghe verso le macchine. Tale evoluzione solleva però importanti questioni in merito ad aspetti di carattere etico (quale *corpus* etico-valoriale per l’elaborazione degli algoritmi), giuridico (perimetro normativo nel quale l’IA deve muoversi ed operare) e di *trust* (la tendenza a “fidarsi” del risultato dell’IA in un processo di analisi).
- Strettamente legati all’IA, i **Sistemi Autonomi** si differenziano in diversi livelli di *reasoning*, ovvero in base alla complessità e criticità dell’azione da compiere, e rappresentano la principale applicazione tecnologica che potrà controbilanciare da una parte la necessità di razionalizzare le risorse e dall’altra di massimizzare le *performance* dello Strumento Militare. In tale quadro saremo quindi di fronte ad un *reshaping* del campo di battaglia in cui saranno impiegati sempre più sistemi autonomi e, come già detto, ad una ridefinizione del ruolo dell’uomo che dovrà considerare tali sistemi come una costante strutturata della propria vita.

- La cosiddetta “democratizzazione dello spazio” conseguente all’abbassamento delle barriere di accesso alle **Tecnologie Spaziali** sta consentendo l’ingresso di nuovi attori (non governativi e commerciali) nella corsa allo sfruttamento del dominio Spazio, cambiandone i tradizionali paradigmi del passato, da logiche prettamente governative e di affermazione politica a quelle prevalentemente commerciali (c.d. “*new space economy*”). Questo nuovo scenario pone sul tavolo molteplici criticità e vulnerabilità quali l’incremento del rischio di *escalation* legato ad una “*weaponizzazione*” dello spazio, la necessità di superare l’attuale quadro regolatore verso un *corpus normativo* che possa garantire la tutela degli interessi nazionali in relazione ai nuovi attori e alle loro ambizioni ed, in ultimo, la forte dipendenza delle Operazioni Multidominio alla disponibilità dei servizi spaziali (es. osservazione della Terra, comunicazioni satellitari, posizionamento e navigazione, *Recognized Space Picture*, ecc.).
- Le **Tecnologie Ipersoniche**, grazie alle loro caratteristiche tecniche (velocità, traiettoria ed imprevedibilità), permettono di superare le tradizionali barriere di difesa missilistica mettendo in crisi le attuali strategie di *Anti-Access/Area-Denial* (A2/AD), proiettando il confronto verso l’*hyperwar*, in cui l’attacco è imprevedibile ed i tempi di reazione risultano minimi od azzerati generando così, un’*escalation* rapida ed imprevedibile. La nuova minaccia evidenzia per il momento la necessità di definire, da un lato una protezione in profondità, intesa come integrazione di molteplici attività svolte da diversi attori a diversi livelli e, dall’altra, la disponibilità di un sistema di Comando e Controllo agile a livello strategico che, nel *counter-hyersonic*, abbia un profilo interministeriale, inter agenzia e multinazionale.
- Le **Tecnologie Quantistiche** offrono ora nuovi e più sofisticati strumenti per i quali diversi attori hanno avviato programmi di finanziamento e sviluppo al fine di raggiungere la c.d. “autonomia quantistica” per goderne dei vantaggi tecnologici e sfruttare una specifica fetta di mercato che muove enormi interessi economico-finanziari, con l’inevitabile ridefinizione degli equilibri geopolitici. Le applicazioni di tali tecnologie avranno un impatto dirompente soprattutto sulla sensoristica, sul calcolo computazionale che supererà quello dei super computer, sulle comunicazioni in termini di crittografia e sulla simulazione di contesti complessi.
- Le **Biotecnologie**, infine, trovano applicazione in diversi settori caratterizzati da prodotti finali volti al potenziamento ovvero al depotenziamento dell’essere umano dal punto di vista biologico. Da qui i “pro” di queste tecnologie quali i biomarcatori per la diagnosi predittiva o le neuroprotesi per l’estensione delle capacità cognitive, ed i “contro” quali nuovi agenti patogeni e biologici contro la salute pubblica o i super soldati avversari potenziati farmacologicamente, neurologicamente e fisiologicamente.

NUOVO MODELLO DI INNOVAZIONE

Lo sviluppo dello Strumento Militare – quale insieme strutturato di personale, mezzi e processi - è un cammino lungo e complesso che deve traghettare quello che sarà l’ambiente operativo futuro. Volatilità, incertezza, ambiguità e mutevolezza caratterizzano la complessità del cambiamento a cui deve rispondere la Difesa attraverso una Cultura dell’Innovazione aperta al mondo esterno (c.d. *Open Innovation*), che potenzi la capacità di comprendere i fenomeni e sia in grado di elaborare risposte rapide ed efficaci per affrontare le nuove sfide e le potenziali minacce per la Sicurezza nazionale. Il ritmo accelerato dell’innovazione e dello sviluppo tecnologico è contraddistinto da un marcato coinvolgimento del settore privato e rende, pertanto, indispensabile la creazione di un nuovo approccio teso a cogliere le opportunità di questa complessità.

L’identificazione dei principali *trends* di sviluppo e delle correlate implicazioni, non emerge da un processo lineare di causa-effetto, bensì da un percorso articolato (c.d. modello *Innovation Journey*) che cogliendo le opportunità, fronteggi le sfide di questa evoluzione e che sia in grado di prevedere le minacce con tempestiche e capacità reattive adeguate alla crescente e continua competizione internazionale.

Un percorso che consenta l’esplorazione dei futuri in un contesto Multidominio dinamico ed interconnesso dove le tecnologie rappresentano un elemento determinante e discriminante negli equilibri in essere per cercare di giungere a conclusioni che delineino non solo i futuri preferibili, frutto delle influenze dell’oggi, ma cerchino di tratteggiare futuri probabili e plausibili.



Partendo quindi dall’analisi delle tendenze di lungo periodo (*strategic foresight*), identificando i *capability gaps & shortfalls*, definendo i problemi militari di livello strategico, sviluppando soluzioni concettuali innovative e tracciando le traiettorie di sviluppo delle tecnologie di potenziale interesse si elaborerà il “**Pensiero Strategico Innovativo**” della Difesa.

Il “viaggio” dell’innovazione, sulla scorta delle scelte strategiche adottate, procede attraverso la fase di *testing* in cui, avvalendosi anche di processi di *red teaming* e tecniche di *alternative analysys*, si verificano validità e solidità delle soluzioni concettuali identificate per dare impulso all’innovazione secondo lo schema del *Technology Readiness Level* (TRL)⁴² che parte dalla ricerca di base (osservazione dei principi e formulazione dei concetti sulle tecnologie - TRL1/2) propedeutica alla ricerca applicata (verifica analitica e sperimentale del concetto tecnologico con l’elaborazione del *Proof of Concept* - TRL3). Un *iter* che possa, con adeguati finanziamenti, essere il vero e proprio motore che spinge e sostiene lo sviluppo tecnologico per il mantenimento del vantaggio strategico della Difesa colmando quel *gap* fra identificazione del problema e la sua soluzione (anche sotto il profilo del *procurement*) ottimizzando tempi e risorse impiegate.

Appare evidente che gli sforzi per intercettare lo sviluppo tecnologico in chiave predittiva devono essere coadiuvati da un atteggiamento “nuovo” che prenda in considerazione altri fattori in gioco come la formazione e la componente legale. La *leadership*, e non solo, deve maturare la consapevolezza di cambiare il proprio approccio (*mindset*) in termini di gestione della complessità. Accettare di investire su molteplici progetti che pur se valutati promettenti soltanto pochi di essi daranno il risultato voluto. Stabilire quindi un processo di selezione che fa emergere soltanto le idee più performanti. Inoltre, va posta l’attenzione sulla componente legale che sta pian piano diventando una vera e propria leva moltiplicatrice, o addirittura uno strumento attivo, nella ridefinizione degli equilibri anche in tema tecnologico. Nell’ambito del confronto con i maggiori *competitors*, non va sottovalutato che la controparte potrebbe utilizzare il *corpus* etico-legale, che caratterizza le società occidentali, a proprio vantaggio ed in maniera malevola (relativizzazione del diritto e dell’etica) al fine di sfruttarne le vulnerabilità (c.d. *lawfare*).

Nel prossimo futuro risulterà vincente un modello di *leadership* caratterizzato da un approccio flessibile e orientato a gestire, promuovere e guidare il cambiamento contrassegnato da sfide sempre più complesse e dalla velocità dei processi decisionali. Il connubio di questi due fattori segnerà il volano per un nuovo paradigma caratterizzato da un *e-leader* con sempre meno competenze tecniche (senza azzerarle) e sempre più competenze trasversali (“*soft skills*”) che siano propensi a sperimentare mettendo da parte i “*bias*” cognitivi.

⁴² *Technology Readiness Level* (TRL), metrica di valutazione del grado di maturità tecnologica di un prodotto o processo, basata su una scala di valori da 1 a 9, dove 1 è il più basso (ricerca di base) e 9 il più alto (prima produzione).

Allegato

METODOLOGIA DI LAVORO E BIBLIOGRAFIA

Abbracciando il paradigma dell'*Open Innovation* attraverso il coinvolgimento del *network INNOV@DIFESA* costituito da esperti militari ed esperti civili provenienti dal mondo accademico, industriale e della ricerca, sono state analizzate sotto la guida dell’Ufficio Generale Innovazione Difesa le principali tecnologie emergenti e dirompenti, cercando di identificarne le traiettorie di sviluppo e le principali implicazioni per la Difesa e la Sicurezza nazionale.

Di seguito l’elenco degli esperti che hanno fornito continuo ed estensivo supporto allo sviluppo del Concetto, ai quali lo Stato Maggiore della Difesa esprime il proprio riconoscimento, e le citazioni bibliografiche.

ESPERTI

Area Industria

- Ing. BECO Stefano – *Innovation and Technological Governance Head of Technology, IPR and Product Policy*;
- Ing. CALDERARO Lucrezia – *Chief Technology & Innovation Office - Leonardo Labs Governance*;
- Dott. CIOLLI Luigi – *Chief Technology Officer Customer Support & Service Solutions*;
- Dott. DISPENZA Massimiliano - *Head of Quantum Technology Leonardo Labs*;
- Gen.Brig. (R). FRISTACHI Pino - *Senior Advisor - Atlantic Organization for Security (AOS)*;
- Dott. LABRUTO Roberto - *Project Manager di Advanced Research Leonardo Divisione Velivoli*;
- Ing. MACCAPANI Andrea – *Unmanned Systems Engineering Architect – Leonardo*;
- Ing. PROIETTI Paolo - *Chief Technology & Innovation Office (CTIO) - Leonardo*;
- Dott. LADETTO Quentin - *Head of Technology Foresight - Arma Suisse*;
- Ing. SCIANNELLI Maria - *Unmanned Systems Engineering Architect*;
- Ing. SCOLARI Franco - Direttore Generale Polo tecnologico Alto Adriatico CEO;
- Dott. SCOTTI DI UCCIO Gustavo - Presidente e Direttore Generale (PDG) *Atlantic Organization for Security (AOS)*;
- Avv. STRIPPOLI LANTERNINI Andrea - Avvocato, Consigliere qualificato DIU- Analista specializzato in Sicurezza e Difesa;

- Dott. TRANCHERO Bruno - *Innovation & Research - Head of Program Management Military Projects* - Leonardo Divisione Velivoli;
- Ing. ZACCHEI Alessandro - Coordinatore del Comitato Tecnico Scientifico del CESMA (Centro Studi Militari Aeronautici) – Ricercatore CEMISS (Centro Militare Studi Strategici) – CTO di *Eurolink Systems*;
- Dott. PEDETTI Luca - *Blockchain Technology Director* – Expertlab.

Area Accademia

- Dott. MATTERA Danilo - Laureando in Relazioni Internazionali presso l'Università degli Studi Roma Tre – Collaboratore esterno Centro Studi Geopolitica;
- Dott.ssa STERZI Francesca – Consulente *freelance*, esperta di Sicurezza, Difesa e formazione di personale internazionale nell'ambito di istituzioni civili e militari- Ufficiale della Riserva Selezionata dell'Esercito.

Area Ricerca

- Dott. CARNIEL Sandro - Direttore della divisione di Ricerca NATO STO CMRE;
- Dott. MILAN Francesco - *Contemporary Security Challenges* presso il *Defence Studies Department, King's College London, al Joint Services Command and Staff College, UK Defence Academy (Shrivenham)*, e presso il *Royal College of Defence Studies (RCDS)* di Londra;
- Dott. VOLPI Angelo - Ricercatore Senior Associato - Consiglio Nazionale delle Ricerche (CNR);
- Dott. GERI Maurizio - *Assistant Integrated Business Support Unit-NATO Center for Maritime Research and Experimentation (CMRE)*.

BIBLIOGRAFIA

Pubblicazioni Nazionali

- STATO MAGGIORE DIFESA, Il Concetto Strategico del Capo di Stato Maggiore della Difesa “Efficienza sistematica, rilevanza complessiva” (2020).
- STATO MAGGIORE DIFESA, Concetto Scenari Futuri (2021).
- STATO MAGGIORE DELLA DIFESA, “Approccio della Difesa alle Operazioni Multidominio” (2021).
- STATO MAGGIORE ESERCITO, Strategia di sviluppo e impiego di Robotic and Autonomous Systems dell'Esercito Italiano. Ed. 2019
- STATO MAGGIORE ESERCITO, Sperimentazione Concettuale dell'Esercito – Linee guida per lo svolgimento dell'esperimento sui Sistemi Robotici ed Autonomi (RAS) – 2020/2021.

Pubblicazioni NATO

- *NATO Science & Technology Trends 2020-2040.*
- *NATO Industrial Advisory Group, Study Group 252. (2021). Emerging and disruptive technologies in the context of emerging powers. Annex I: Bio and Human Enhancement Technologies (BHET).*
- *NATO Industrial Advisory Group, Study Group 253. (2021). Assessment of Human Augmentation Technologies for Exploitation in Battlefield. Annex E: Neurotechnologies.*

Articoli accademici e sitografia

- *Williams, A. P. & Scharre, P. D. (eds.) Autonomous Systems - Issues for Defence Policy Makers (NATO Allied Command Transformation, Norfolk, VA, 2015).* <http://www.act.nato.int/images/stories/media/capdev/capdev>.
- *Zacharias, G. Autonomous horizons: the way forward (Air University Press; Curtis E. LeMay Center for Doctrine Development and Education, Maxwell Air Force Base, Alabama, 2019).*
- *Endsley, M. R. Autonomous Horizons: Autonomy in the Air Force—A Path to the Future. Vol. 1, Human Autonomy "Teaming. Air Force Science and Technology AF/ST TR 15-01, US Air Force, Washington, D.C. (2015).*
- "Potential for Army Integration of Autonomous Systems by Warfighting Function" <https://www.armyupress.army.mil/Journals/MilitaryReview/English-Edition-Archives/September-October-2019/Mittal-Autonomous-Systems/>.
- *Final Report NIAG Sub-Group 259 "Testing, evaluating, verifying and validating (TEVV) of systems embedded autonomous functions (SAF) for future military operations (26 February 2021).*
- *THE NATIONAL ACADEMIES PRESS, Avoiding Surprise in an Era of Global Technology Advances.*
- *Etica & Politica / Ethics & Politics XVI, 2014, 2 di Salvatore Amato.*
- *National DEFENSE, Military to Leverage New Biotech Fields to Gain an Edge by Mandy Mayfield.*
- *Biotechnology, Weapons and Humanity, Croce Rossa (ICRC), 2016.*
- *Innovation in Biotechnology, DARPA, www.darpa.mil.*
- *Strategic Technologies for the Military, By Ajey Lele, 2018.*
- *Breaking Defense, DoD On Biotech: Build Sound Defenses First,* <https://breakingdefense.com/2019/09/biotech-build-defenses-first/>.
- *CRS Report R46458, Emerging Military Technologies: Background and Issues for Congress, by Kelley M. Sayler.*
- *CRS Report R44824, Advanced Gene Editing: CRISPR-Cas9, by Marcy E. Gallo*
- *Biotechnology in Europe, The Tax, finance and regulatory framework and global policy comparison by European Commissioner for Research, Innovation and Science.*
- *Piano programmatico Biotech – il futuro migliore, FEDERCHIMICA 2020.*
- *BioInItaly Report 2020, FEDERCHIMICA.*

- http://theory.caltech.edu/~preskill/talks/Q2B_2017_Keynote_Preskill.pdf.
- *The white book of quantum Computing*, Fujitsu, 2020.
- “Quantum computing: near- and far-term opportunities” by Ewan Munro.
- https://medium.com/@quantum_wa/quantum-computing-near-and-far-term-opportunities-f8ffa83cc0c9.
- *Breakthrough in Secure Quantum Communications Networks led by Bristol University in the UK: “A trusted node-free eight-user metropolitan quantum communication network”*<https://advances.sciencemag.org/content/6/36/eaba095>;
- A new scheme for satellite-based quantum-secure time transfer <https://phys.org/news/2020-05-schemesatellite-based-quantum-secure.html>.
- S. H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, “Quantum illumination with Gaussian states,” *Phys. Rev. Lett.*, vol. 101, p. 253601, 2008 .
- D. Luong, S. Rajan, and B. Balaji, “Quantum two-mode squeezing radar and noise radar: Correlation coefficients for target detection, ”, 2019.
- S. Barzanjeh, S. Pirandola, D. Vitali, and J. M. Fink, “Microwave quantum illumination using a digital receiver, ” *Sci. Adv.*, vol. 6, no. 19, 2020.
- Z. Zhang, S. Mouradian, F. N. C. Wong, and J. H. Shapiro, “Entanglement-enhanced sensing in a lossy and noisy environment,” *Phys. Rev. Lett.*, vol. 114, p. 110506, 2015.
- E. D. Lopaeva, I. Ruo Berchera, I. P. De Giovanni, S. Olivares, G. Brida, and M. Genovese, “Experimental realization of quantum illumination,” *Phys. Rev. Lett.*, vol. 110, p. 153603, 2013.
- Sorelli, Giacomo & Treps, Nicolas & Grosshans, Frédéric & Boust, Fabrice “Detecting a target with quantum entanglement” (2020) - <https://arxiv.org/abs/2005.07116>.
- *Technology Quarterly: Quantum Devices, Here, there and everywhere,’ The Economist, March 11, 2017.*
- “Two-photon entanglement-based terahertz wave imaging device”, Univ. Northwestern, China, 2012.
- “High-resolution imaging via quantum remote sensing,” February 26, 2016, <http://spie.org/newsroom/6298-high-resolution-imaging-via-quantum-remote-sensing>.
- “Development of a squid-based airborne full tensor gradiometers for geophysical exploration,” SEG Technical Program Expanded Abstracts 2016.
- Williams, A. P. & Scharre, P. D. (eds.) Autonomous Systems - Issues for Defence Policy Makers (NATO Allied Command Transformation, Norfolk, VA,2015).<http://www.act.nato.int/images/stories/media/capdev/capdev>.
- Zacharias, G. *Autonomous horizons: the way forward* (Air University Press; Curtis E. LeMay Center for Doctrine Development and Education, Maxwell Air Force Base, Alabama, 2019).

- Endsley, M. R. *Autonomous Horizons: Autonomy in the Air Force—A Path to the Future*. Vol. 1, *Human Autonomy"Teaming. Air Force Science and Technology AF/ST TR 15-01*, US Air Force, Washington, D.C. (2015).
- “Potential for Army Integration of Autonomous Systems by Warfighting Function”.<https://www.armyupress.army.mil/Journals/MilitaryReview/English-Edition-Archives/September-October-2019/Mittal-Autonomous-Systems/>
- Final Report NIAG Sub-Group 259 “Testing, evaluating, verifying and validating (TEVV) of systems embedded autonomous functions (SAF) for future military operations (26 February 2021.



