Geopolitica.info

FARO ATLANTICO

Emerging & Disruptive Technologies: quale impatto per la NATO?

A cura di *Alessandro Savini e Danilo Mattera*

30 DICEMBRE 2020

- Le tecnologie emergenti e dirompenti rischiano di minare la coesione e l'interoperabilità della NATO.
- Data la loro natura possono costituire un'opportunità per l'Alleanza, solo se riuscirà a promuovere una corretta integrazione col settore privato.
- La creazione di uno strumento di coordinamento atlantico potrà rappresentare un importante passo avanti nell'affrontare opportunità e sfide poste dalle EDT.

DOMINO – Geopolitical Brief n. 14 / dicembre 2020 | Aut. Trib. Roma n. 88 - 6 marzo 2008
Centro Studi Geopolitica.info | www.geopolitica.info | centrostudi@geopolitica.info
Direttore responsabile: Lorenzo Termine

Introduzione

"Il mantenimento del vantaggio tecnologico rappresenta, in ultima analisi, il fondamento su cui si basa la capacità di difesa e di deterrenza della NATO contro potenziali minacce. [Sebbene] le tecnologie emergenti e dirompenti (*Emerging & Disruptive Technologies)* rappresentino una sfida – se sfruttate correttamente – [quest'ultime] possono rappresentare anche un'opportunità per l'Alleanza"[1]. In questo modo vengono considerate le EDT all'interno del report "*NATO2030: United For A New Era*" prodotto dal gruppo di esperti nominati da Jens Stoltenberg – Segretario Generale dell'Alleanza Atlantica – nella cornice dell'omonimo progetto volto a rafforzare l'Alleanza per gli anni a venire. La consapevolezza della crescente complessità dello scenario internazionale, così come della sfida tecnologica portata avanti da attori statali non alleati e della natura dello sviluppo tecnologico (sempre più legato all'attività delle aziende private piuttosto che all'azione propulsiva degli stati) si sono tradotte più volte – in sede di Consiglio Atlantico[2] – in istanze di maggiore attenzione nei confronti di quelle tecnologie foriere di potenziali stravolgimenti tanto nel settore civile quanto in quello militare. Tali istanze si sono tradotte poi – nel luglio del 2018 – in un ag-

1 NATO2030: United for a new Era – Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General p. 29 https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

2 Tra i più rilevanti il Consiglio dei capi di Stato e di Governo tenutosi a Londra nel dicembre 2019: in occasione delle celebrazioni conclusive per il settantesimo anniversario della creazione dell'Alleanza, i delegati degli stati membri affermarono l'impegno dell'Alleanza nel settore tecnologico. https://www.nato.int/cps/en/natohq/official_texts_171584.htm

giornamento della strategia che si propone di sviluppare le competenze tecnologiche della Alleanza, ovvero la *NATO Science & Technology Strategy*[3]. Individuati dalla *NATO Science & Technology Organization* – struttura atlantica dedita alla ricerca scientifica – otto gruppi di tecnologie dirompenti che gli esperti si aspettano possano caratterizzare i prossimi due decenni[4]. A dispetto delle peculiarità e delle possibili applicazioni in campo militari delle otto EDT, un aspetto resta centrale: le nuove sfide tecnologiche determineranno un nuovo adattamento dell'Alleanza; parola di Sir Stuart Peach, *Air Chief Marshall* della *Royal Air Force* e presidente del Comitato Militare dell'Alleanza[5].

Big Data e Advanced Analytics (BDAA)

A partire dagli anni '60 il nostro mondo è diventato sempre più digitale e virtuale e i *Big Data & Advanced Analytics* ne sono l'evoluzione diretta nonché la conseguente necessità di mettere insieme la grande quantità di informazioni che ne derivano. Di cosa si tratta? I *Big Data* descrivono i dati che presentano sfide significative in termini di volume, velocità, varietà, veridicità e visualizzazione. L'aumento della digitalizzazione, la proliferazione di nuovi sensori, le nuove modalità

3 *NATO Science and Technology Strategy: Sustaining Technological Advantage*, luglio 2018, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20181107_180727-ST-strategy-eng.pdf

4 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040: Exploring the S&T Edge*, marzo 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

5 NATO Communications and Information Agency, Nitech: NATO Edge (giugno 2020) p. 21 https://issuu.com/globalmediapartners/docs/nitech_issue_03_june_2020

di comunicazione e la virtualizzazione degli spazi socio-cognitivi (i social media per esempio) hanno contribuito in modo significativo allo sviluppo dei *Big Data*. *Advanced Analytics* invece descrive i metodi analitici avanzati per raccogliere e visualizzare grandi quantità di informazioni[6].

Le caratteristiche delle tecnologie BDAA

I dati disponibili in tutti i futuri spazi di scontro consentiranno all'analitica di fornire previsioni, supporto decisionale in tempo reale e di mettere in evidenza i primi indicatori di successo e gli avvertimenti di crisi. A tal proposito, un maggior uso dell'analitica predittiva e del M&S consentirà ai *decision-makers* di superare i loro limiti cognitivi permettendogli di comprendere al meglio il potenziale impatto delle loro decisioni e di adeguare, di conseguenza, le proprie strategie[7].

I BDAA – composti da quattro elementi essenziali: 1) raccolta (sensori); 2) comunicazione; 3) analisi; 4) *decision-making* – coprono il dominio umano (social media, bioinformatica), fisico (sensori) e informativo (cyber, analisi). In quanto tecnologia cruciale, la comprensione del suo sviluppo sarà un passo importante per il futuro delle altre tecnologie emergenti e dirompenti. Inoltre, secondo il team di esperti della *NATO Science and Technology Organization*, potrà essere abilitata dagli sviluppi di S&T in una varietà di aree che includono: supporto decisionale e supporto alla pianificazione con M&S sul campo di battaglia; aree di missione virtuale, rilevamento di campi elettrici e magnetici, fusione di dati più rapida, telecomunicazioni a banda larga.

6 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040*, p. 42.

7 v. D. Dorner, *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations*, Basic Books, New York, 1997.

Implicazioni per la NATO

La tendenza ad una maggiore digitalizzazione e virtualizzazione potrebbe aumentare nei prossimi anni e avere un effetto dirompente sul contesto operativo e sulle capacità della NATO. In questo senso, molti Stati dell'Alleanza stanno compiendo significativi investimenti nei *Big Data & Advanced Analytics* sia a livello civile sia a livello militare. La NATO, secondo gli scienziati dell'organizzazione, dovrà quindi essere in grado di sfruttare questi investimenti estendendoli, adattandoli ed integrandoli al proprio ambiente decisionale ed operativo. Infatti, l'eccellenza in tale tecnologia ha sicuramente il potenziale per creare un vantaggio decisionale e di conoscenza per l'Alleanza, basato sulla raccolta, l'elaborazione, lo sfruttamento e la fusione di una grande quantità di dati[8]. Secondo il team di esperti le aree suscettibili di ulteriori sviluppi saranno le seguenti:

- ISR;
- Situational Awareness[9];
- Addestramento e prontezza;
- Logistica.

Per quanto riguarda l'ISR, la proliferazione di sensori avanzati e il maggior uso di sistemi autonomi aumenterà sensibilmente le capacità della NATO di rilevamento, classificazione, ricognizione e ingaggio di minacce in tutti i domini operativi. Gli amplificatori di potenza a stato solido e le forme d'onda ottimizzate supporteranno la ricerca simultanea e la capacità di tracciamento per l'interdizione di bersagli ae-

8 NATO Science and Technology Organization, *Science and Technology Trends 2020-2024,* p. 45.

9 Abilità di osservare il contesto operativo, rilevare attacchi e distinguere reali minacce da falsi allarmi.

rei portando la capacità ISR ad essere più veloce e precisa. Inoltre, un maggiore sviluppo del radar passivo[10] permetterà di ridurre la vulnerabilità dei sistemi alla guerra elettronica aumentando la capacità di rilevamento di velivoli *stealth*[11].

Il miglioramento della mappatura delle aree di missione per la pianificazione e preparazione supporterà la programmazione operativa e incrementerà la SA attraverso il potenziamento dei modelli di vita, del territorio e del rilevamento di anomalie. Il progressivo sviluppo della SA, secondo gli esperti, consentirà una maggiore capacità di visualizzazione a bassa potenza per i sistemi dei soldati e un maggiore flusso di informazioni tra il livello tattico e quello di comando. Il sistema di "*geo-tagging*" del soldato – che consente di risalire alla localizzazione geografica di persone od oggetti – sarà fondamentale per generare e fornire informazioni del contesto operativo sempre più precise.

Gli ambienti virtuali e la bioinformatica supporteranno il miglioramento dell'addestramento e la prontezza per le operazioni future. Ad esempio, attraverso il monitoraggio dello stato fisiologico e psicologico si potranno massimizzare le prestazioni e la prontezza generale del soldato potendo evitare o prevenire eventuali danni.

Una maggiore integrazione dei sensori di controllo della condizione dei sistemi d'arma, il monitoraggio in tempo reale dell'inventario e l'utilizzo di gemelli digitali aumenteranno

10 v. Bahman Zouri, *Radar Energy Warfare and the Challenges of Stealth Technology*, Springer Nature, Cham, 2020.

11 v. P. Westwick, *Stealth: The Secret Contest to Invent Invisible Aircraft*, Oxford University Press, Oxford, 2020

significativamente l'efficienza e l'efficacia del sistema logistico dell'Alleanza riducendone i costi del ciclo di vita.

Il team di esperti della NATO ha evidenziato la presenza di sfide di interoperabilità come conseguenza diretta del maggiore sviluppo di tali tecnologie. A tal proposito, serviranno investimenti costanti per mantenere un vantaggio tecnologico e per garantire la resilienza operativa: ciò sfiderà le nazioni dell'Alleanza a mantenere una forza tecnologica comune ed interoperabile. I *big data* sollevano numerose preoccupazioni in materia di sicurezza, privacy e governance e dunque sarà necessario sviluppare politiche sulla raccolta, la conservazione e lo scambio dei dati per consentire ai vari Stati di mantenere la proprietà e il controllo dei dati anche durante la condivisione all'interno dell'Alleanza. Inoltre, l'adozione a livello nazionale di tecnologie BDAA critiche – come per esempio il 5G – può creare un significativo divario digitale a causa delle diverse percezioni delle minacce. Infatti, la mancanza di standard e lo sviluppo di sistemi incompatibili o inaffidabili rischia di limitare la capacità della NATO di condividere C4ISR o altri dati sensibili. Nondimeno, l'eccessivo utilizzo di *Big Data & Advanced Analytics* da parte dell'Alleanza, per quanto riguarda il *decision-making*, aumenterà il rischio e i danni derivanti da attacchi *cyber*. A ciò si potrebbe aggiungere un progressivo sviluppo di nuove tecniche di guerra ibrida.

La NATO e il 5G

Con l'arrivo delle reti 5G, le comunicazioni si trasformeranno in un modello completamente diverso, incentrato su alta densità, grande volume, velocità estremamente elevata, bassa latenza e ritardo nel trasferimento dei dati. Il 5G avrà un

ruolo di abilitatore nella transizione delle comunicazioni da macchina a macchina; ciò supporterà, tra le altre cose, la massiccia condivisione di dati in tempo reale[12].

Secondo Andrea Gilli e Francesco Bechis, sarebbero quattro le ragioni principali legate alle telecomunicazioni che stanno alla base di una progressiva attenzione al 5G. In primo luogo, le telecomunicazioni sono una tecnologia abilitante che può guidare la crescita economica mondiale, non a caso i modelli di previsione hanno stabilito che le reti 5G aggiungeranno bilioni di dollari di valore economico all'economia internazionale. In secondo luogo, nelle telecomunicazioni chi fa la prima mossa ha un vantaggio: i primi operatori possono accumulare un grande vantaggio economico lasciando poco spazio ai concorrenti. In terzo luogo, le telecomunicazioni hanno una dimensione strategica: la velocità, la qualità e la quantità delle informazioni sono cruciali per poter competere nel mondo digitale. Da ultimo, vista la centralità delle informazioni nelle economie moderne, le telecomunicazioni sono considerate un settore strategico: le aziende spesso trasferiscono informazioni private e sensibili e i governi condividono diversi tipi di dati, inclusi materiali classificati.

Un altro motivo per il quale il 5G ha attirato particolare attenzione è che i protagonisti di questa tecnologia non sono aziende occidentali ma aziende con sede in Cina come Huawei e ZTE. Il 5G è anche al centro del dibattito internazionale per lo scontro con gli Stati Uniti, scontro che si è tramutato in sanzioni da parte dell'Amministrazione Trump nei con-

12 A. Gilli e F. Bechis, *NATO and the 5G Challenge*, NATO Review, settembre 2020, https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html

fronti delle *big tech companies* cinesi. Negli ultimi anni tali aziende sono state ripetutamente accusate di aver rubato la proprietà intellettuale e di utilizzare lo spionaggio informatico[13] per accedere ad informazioni riservate.

Nonostante il Segretario Generale della NATO Jens Stoltenberg abbia affermato, durante la riunione dei ministri della Difesa del 25 ottobre 2019, che "le telecomunicazioni di prossima generazione influenzeranno ogni aspetto della società, dai trasporti all'assistenza sanitaria, nonché le nostre operazioni militari", l'Alleanza Atlantica non ha intrapreso un vero e proprio dibattito e non ha preso una reale posizione sul 5G. Attualmente, gli Stati Uniti sono l'unico Stato membro della NATO ad aver adottato misure efficaci per limitare l'accesso alle società cinesi nella propria rete 5G. A tal proposito, la stragrande maggioranza degli alleati non ha bloccato o limitato il ruolo di Huawei o ZTE nelle proprie infrastrutture, fatta eccezione per Grecia, Regno Unito e Repubblica Ceca.

Per il presente e il futuro della NATO sarà fondamentale sfruttare queste nuove opportunità tecnologiche per sviluppare capacità di comando e controllo, di comunicazione e, più in generale, per aumentare l'efficacia delle operazioni alleate. Senza le comunicazioni 5G, sarà difficile sfruttare al massimo i *big data*, l'intelligenza artificiale e il *cloud computing* sul campo di battaglia. Tuttavia, la mancanza di un'unica voce transatlantica sul 5G mette in luce il fatto che la NATO

13 A. Gilli e M. Gilli, *Why China Has Not Caught Up Yet, Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage*, International Security, vol. 43 n. 3, 2019

non è stata progettata per affrontare politiche commerciali e la concorrenza sul mercato nel mondo dell'alta tecnologia[14].

Intelligenza Artificiale (IA)

La disponibilità di una grande quantità di dati ha guidato sia lo sviluppo che la necessità di un maggiore utilizzo dell'intelligenza artificiale. A partire dalla metà degli anni '50, l'IA si è mossa attraverso tre cicli di sviluppo primario, di conseguenza, gli algoritmi di tale tecnologia sono già profondamente radicati da tempo. Tuttavia, nel 2012 c'è stato un progressivo sviluppo della sua applicazione ai problemi pratici grazie al miglioramento degli algoritmi e all'ampia disponibilità di set di formazione disponibile al pubblico.

L'intelligenza artificiale emula aspetti della cognizione umana come la percezione, il ragionamento, la pianificazione e l'apprendimento; non a caso è stata identificata come la più grande sfida tecnologica che l'Alleanza si trova ad affrontare[15]. Si prevede che nei prossimi vent'anni sarà in grado di influenzare, attraverso la sua forza dirompente, lo sfruttamento della crescente digitalizzazione e la conseguente disponibilità di una grande quantità di dati; l'utilizzo di sistemi cyber; il *decision-making* e non solo. L'intelligenza artificiale e i *big data & advanced analytics* sono tecnologie strettamente collegate tra di loro: esistono opportunità di ricerca e sviluppo per l'analisi di grandi insiemi di dati, compresi quelli as-

14 A. Gilli, *NATO and 5G: What Strategic Lessons?,* NDC, Roma, 2020.

15 US Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*, Washington, 2018, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

sociati all'elaborazione dei dati dei sensori e alla fusione. In questo senso, il progressivo aumento dei dati digitalizzati renderà l'uso dell'IA ancora più utile e di fondamentale importanza per i BDAA.

Le applicazioni per l'IA

Stando a quanto riportato dalla RAND[16] nel report del 2019 "*The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations*[17]", è utile distinguere tre grandi tipi di applicazioni per l'IA:

1- *Enterprise IA*: include applicazioni come sistemi di gestione finanziaria o del personale che vengono impiegati in ambienti strettamente controllati dove le implicazioni per guasti tecnici sono basse;

2- *Mission Support IA*: può essere impiegata in missioni ed operazioni, ossia in ambienti meno controllati nei quali le implicazioni per guasti possono essere elevate (software di controllo di sistemi fissi o velivoli a pilotaggio remoto);

3- *Operational IA*: categoria intermedia in termini di controllo dell'ambiente e di implicazioni per guasti che comprende ad esempio la logistica e la manutenzione, o applicazioni legate all'intelligence.

La competizione tra Stati Uniti e Cina si estende all'IA

Negli ultimi anni la competizione tecnologica tra Stati Uniti e Cina si è estesa anche all'IA, tecnologia che però comporta numerose sfide. Come sottolineato dalla DARPA: "Abilitare sistemi di calcolo con un'intelligenza simile a quella umana è ora di fondamentale importanza perché il ritmo delle ope-

16 Think Tank americano fondato nel 1946 e finanziato dal DoD.

17 RAND, *The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations, 2019,* https://www.rand.org/pubs/research_reports/RR4229.html

razioni militari nei domini emergenti supera quello in cui gli esseri umani senza supporto possono orientarsi, capire e agire"[18]. Il Pentagono, per esempio, sta studiando diversi modi per sfruttare tale tecnologia con il fine di ottenere vantaggi come l'autonomia nel campo di battaglia, l'analisi intelligence, la manutenzione predittiva e la medicina militare. L'IA è considerata dal Dipartimento della Difesa americano una tecnologia fondamentale: a riprova di ciò, solo per il 2020, è stato stanziato circa 1 miliardo di dollari per la ricerca e sviluppo. Il *Joint Artificial Intelligence Center* invece vedrà il suo budget raddoppiare fino a superare i 208 milioni di dollari con aumenti significativi anche per i prossimi anni. Inoltre, le forze armate americane sono nella fase di integrazione dell'IA nello sviluppo di sistemi d'arma per migliorare, tra le altre cose, la precisione.

Come già detto, gli Stati Uniti non sono gli unici ad investire in maniera crescente nell'IA. La Cina infatti, secondo il rapporto annuale al Congresso "*Military and Security Developments Involving the People's Republic of China 2020*[19]", sta minacciando il primato di Washington per quanto riguarda tale tecnologia. Pechino, a seguito della pubblicazione del suo piano di sviluppo per l'IA, ha riconosciuto la sua crescente importanza identificandola come priorità strategica. A tal proposito, il Consiglio di Stato cinese ha pianificato un ambizioso piano

18 Defense Advanced Research Project Agency, Department of Defense Fiscal Year (FY) 2020 Budget Estimates, Arlington, 2019, https://www.darpa.mil/attachments/DARPA_FY20_Presidents_Budget_Request.pdf

19 US Department of Defense, *Military and Security Developments Involving the People's Republic of China 2020,* settembre 2020, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF

politico con l'obiettivo di diventare il principale centro di innovazione a livello di IA del mondo entro il 2030[20].

Implicazioni per la NATO

L'intelligenza artificiale, secondo il team di esperti dell'organizzazione della NATO, avrà un impatto significativo sulle capacità militari e sulle forze dell'Alleanza soprattutto attraverso il suo uso incorporato in altre tecnologie come la realtà virtuale o aumentata, il calcolo quantistico, l'autonomia, il M&S, lo spazio, la produzione e la logistica e l'analisi dei *big data*. Gli scienziati concordano sul fatto che nei prossimi 20 anni l'IA avrà un grande impatto su alcune capacità tra le quali:

- C4ISR;
- Sistemi d'arma ed effetti conseguenti;
- UxV;
- CBRN;
- Medicina;
- Logistica;
- Cyberspace.

Relativamente alle capacità di C4ISR, le unità di guerra saranno in grado di impiegare sistemi autonomi abilitati dall'IA in grado di svolgere compiti che vanno oltre a quelli che possono essere considerati pericolosi. Tale tecnologia permetterà di migliorare la fusione, l'analisi e l'elaborazione dei dati nonché un maggiore e preciso supporto alle decisioni per l'identificazione e il *targeting* del bersaglio. Inoltre, l'IA è considerata fondamentale per i sistemi d'arma ed i conse-

20 C. Bidwell e B. MacDonald, *Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security*, Tech. Rep., Federation of American Scientists, 2018, https://fas.org/wp-content/uploads/media/FAS-Emerging-Technologies-Report.pdf

guenti effetti che possono avere: ci si aspettano sviluppi nel *cross-cueing*[21], nella pianificazione della traiettoria, nell'evitare le collisioni, nella selezione delle armi e nella valutazione dei danni da battaglia.

Per i sistemi a pilotaggio remoto, l'IA potrà avere un potenziale impatto nella pianificazione delle traiettorie, nella prevenzione delle collisioni e nell'assistenza all'operatore che, spesso, può controllare più di una piattaforma. L'integrazione di sistemi di *deep learning* in piattaforme mobili migliorerà inoltre le capacità robotiche per la navigazione in determinate situazioni.

La NATO richiede una serie di tecnologie abilitanti ed integrate che forniscano un rapido rilevamento, identificazione e monitoraggio delle minacce CBRN durante qualsiasi missione al fine di informare riguardo alla linea di condotta necessaria per arginare tale minaccia. L'uso dell'IA migliorerà anche la *command situational awareness* e il supporto operativo attraverso nuove capacità di auto-organizzazione.

Le forze militari moderne sono chiamate anche ad intervenire in ambito medico se necessario. In questo senso, l'IA ha il potenziale per assistere nello sviluppo di *best-practices* di trattamento per ridurre la morbilità e la mortalità e mantenere o recuperare funzioni essenziali all'interno di una missione. Nondimeno, fornirà supporto decisionale automatizzato e strumenti di supporto diagnostico per assistere i medici sul campo. I sistemi di IA, specialmente se abbinati a gemelli digitali, avranno il potenziale per ridurre al minimo il

21 Passaggio delle informazioni di rilevamento, geo-localizzazione e puntamento ad un altro sensore senza intervento umano.

tempo di inattività degli equipaggiamenti, minimizzare i guasti del sistema e migliorare la gestione dell'inventario e delle riparazioni.

Per reti autonome resilienti e per la guerra informatica, il sistema di IA sarà in grado di rilevare, valutare e rispondere ben prima che gli esseri umani siano in grado di comprendere la situazione. Tali sistemi avranno la capacità di prendere decisioni indipendenti e di agire in modo rapido lavorando, allo stesso tempo, come parte di un team composto da umani e sistemi di IA.

Anche in questo caso non mancano le sfide. Come per i BDAA, la dipendenza dall'IA aumenterà anche il potenziale impatto degli attacchi cyber e, spesso, tali sistemi sono particolarmente vulnerabili ad attacchi di questo tipo. Secondo il team di esperti, le sfide politiche, legali e di interoperabilità saranno sfide serie per la NATO. Garantire che l'IA sia affidabile, etica e coerente con le *rules of engagement* (ROE) richiederà approcci con una forte enfasi sulla spiegabilità, la fiducia e la collaborazione uomo-IA. Inoltre, sarà necessario, nel contesto delle operazioni dell'Alleanza, definire le procedure per la verifica, convalida e accreditamento di tali sistemi che forniranno da supporto decisionale operativo. Ulteriori sfide sono presenti anche nel settore della R&S dove i sistemi di IA dovranno migliorare soprattutto nel dominio cyber sia in ambito difensivo che in quello offensivo nonché nello sviluppo di contromisure di guerra ibrida.

Autonomia

L'autonomia è la capacità di un sistema di rispondere a situazioni incerte selezionando autonomamente, tra diversi corsi di azione, con il fine di raggiungere obiettivi basati sulla conoscenza e sulla comprensione del mondo, di sé stessi e della situazione[22]. In altre parole, l'autonomia è la capacità di una macchina di eseguire un compito senza l'intervento umano[23] ed è caratterizzata da gradi di comportamento che vanno dal completamente manuale al completamente autonomo.

L'autonomia della piattaforma è uno degli esempi più importanti della robotica rilevante a livello militare e dei sistemi autonomi. Gli UxV, per esempio, chiamati anche sistemi *unmanned,* possono essere pilotati a distanza o possono agire attraverso vari livelli di autonomia nel corso di una missione: vengono utilizzati nel dominio aereo (UAV, UCAV), in quello marittimo (UUV, USV) e in quello terrestre (UGV). Se gli UxV sono diventate tecnologie sempre più comuni ed essenziali per le operazioni militari, l'uso di agenti software virtuali o di bot è oggetto di studio per azioni offensive e difensive nel campo dell'informazione e del cyberspazio. In questo senso, lo sviluppo di agenti software autonomi sicuri, protetti e affidabili fornirà un mezzo per contrastare gli attacchi *malware* su larga scala insieme ad altri eventi di tipo informatico.

22 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040,* p. 59.

23 M.C. Horowitz e P. Scharre, *An Introduction to Autonomy in Weapons Systems*, Center for a New American Security, Washington, febbraio 2015, p. 5.

Scienziati della NATO hanno sottolineato che, nel dominio terrestre, l'impatto dei sistemi autonomi sarà preponderante; cambierà radicalmente il modo in cui l'esercito combatte aumentando la SA, riducendo i carichi di lavoro fisici e cognitivi del soldato, migliorando il supporto decisionale e logistico, facilitando il movimento e la manovra e aumentando la protezione delle forze. I sistemi autonomi però possono essere fondamentali anche all'interno del dominio marittimo, per esempio, per operazioni di lotta antisommergibile, localizzazione e distruzione di mine navali nonché per missioni SIGINT/ELINT. Per le attività della NATO nel settore spaziale e in quello cyber, inoltre, i sistemi autonomi saranno un elemento cruciale del futuro successo operativo – successo che sarà costruito su una progressiva esplorazione delle tecnologie convergenti. A tal proposito, come evidenziato dal documento "*Science and Technology Strategy*[24]" dell'USAF, sciami di sistemi spaziali autonomi a basso costo possono fornire adattabilità e la capacità di assorbire perdite che i sistemi con equipaggio non possono fare.

L'autonomia nei sistemi d'arma

Varie forme di autonomia sono state utilizzate nei sistemi militari da oltre settant'anni. I primi tipi di munizionamento di precisione risalgono alla Seconda Guerra Mondiale mentre sistemi difensivi automatizzati con modalità di controllo umano esistono da decenni e sono utilizzati da molte forze armate. Secondo alcuni studiosi, l'autonomia nei sistemi d'arma è possibile dividerla in tre categorie:

24 United States Air Force, *Science and Technology Strategy: Strengthening USAF Science and Technology for 2030 and Beyond,* aprile 2019, https://www.af.mil/Portals/1/documents/2019%20SAF%20story%20attachments/Air%20Force%20Science%20and%20Technology%20Strategy.pdf

1- *Human "in the loop"*: sistemi d'arma che possono selezionare e colpire determinati bersagli solo attraverso l'intervento umano (munizionamento di precisione);

2- *Human "on the loop":* sistemi d'arma che possono selezionare e colpire determinati bersagli sotto la supervisione di un umano che può annullare in qualsiasi momento l'operazione (sistemi di difesa aerea e missilistica, ad esempio il sistema Aegis degli USA);

3- *Human "out of the loop"*: sistemi d'arma che possono selezionare e colpire determinati bersagli senza l'intervento umano (*loitering munitions*).

Implicazioni per la NATO

UAV di diverse dimensioni e gradi di autonomia sono già utilizzati missioni ISR e di attacco, sfruttando i lunghi tempi di attesa e il posizionamento flessibile vicino a potenziali bersagli. Il tipo di UAV a lunga durata è particolarmente importante per la sorveglianza quando le operazioni vengono condotte per un periodo di giorni. Tuttavia, il maggiore utilizzo di piccoli sciami di droni offre notevoli vantaggi per compiti di ISR, nonché per operazioni offensive e difensive. Il team di esperti della NATO si aspetta che i sistemi autonomi portino notevoli cambiamenti[25]:

- Force structure;
- Contromisure;
- Swarming;
- Logistica;
- Situational Awareness;
- Letalità;

25 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040,* pp. 64-65.

- Sopravvivenza.

Gli UxV e agenti software autonomi sostituiranno gli esseri umani in ambienti di lavoro operativo-tattici come per esempio CBRN, EOD, ricognizione. Un maggiore utilizzo di sistemi autonomi sarà una sfida per lo sviluppo di adeguate competenze militari, strutture organizzative e di addestramento.

Il progressivo uso di droni richiederà maggiori risorse in termini di protezione delle forze con capacità di contro-UxV: si estenderanno a più livelli comprendendo, tra le altre cose, azioni di guerra elettronica, cyber, uccisioni cinetiche, armi ad energia diretta. Sarà dunque necessario difendere gli *asset* critici dagli sciami. Gli sciami UxV consentiranno nuovi paradigmi di rilevamento e di attacco per le forze amiche; si potranno utilizzare come risorse sacrificabili, ad esempio, per penetrare nelle aree nemiche o per proteggere *asset* critici. In questo senso, per il nemico costerà più tempo, energia e risorse difendersi da uno sciame piuttosto che superarlo.

L'autonomia, così come le altre tecnologie, sarà cruciale anche per la logistica: gli UxV potranno trasportare soldati e merci sul campo di battaglia, specialmente nelle quantità relativamente piccole che si applicherebbero in situazioni tattiche. La tecnologia attuale consente di costruire droni a pilotaggio remoto o autonomi che siano in grado di consegnare rifornimenti e munizioni alle truppe sul campo.

Per quanto riguarda la SA, le operazioni di ISR saranno migliorate grazie all'impiego di un'ampia gamma di sensori a bassa potenza (EO, IR, radar). Gli esperti prevedono un maggiore utilizzo in contesti operativi in evoluzione come lo spa-

zio, il cyberspazio e gli ambienti urbani. Per esempio, UAV di diverse dimensioni e gradi di autonomia sono già utilizzati per operazioni di ISR, approfittando del fatto che tali sistemi dispongono di lunghi tempi di sosta e di un elevato tasso di flessibilità di posizionamento. In questo senso, i droni a lunga durata sono particolarmente importanti per le operazioni di lunga durata. Inoltre, cruciale sarà il ruolo degli agenti informatici utilizzati sempre di più per mantenere la SA all'interno degli spazi virtuali a supporto dell'identificazione di minacce o vulnerabilità.

Un gran numero di sistemi a basso costo e una migliore collaborazione uomo-macchina miglioreranno notevolmente la proiezione della forza; ciò porterà alla capacità di raccogliere informazioni costanti e affidabili su vaste aree geografiche. Inoltre, un UAV armato fornirebbe capacità di combattimento aereo senza esporre un pilota a rischi di vario genere e può essere utilizzato per attaccare specifici obiettivi nei vari domini operativi.

Altrettanto importante, si ridurrebbero le perdite in combattimento, verrebbero fornite cure mediche più rapide e una maggiore efficacia operativa. Ci si aspetta anche che gli UAV conducano future missioni di ricerca e salvataggio aumentando ulteriormente le possibilità di sopravvivenza.

La spinta verso sistemi sempre più autonomi incrementerà drasticamente le future capacità della NATO in un ambiente in cui ogni soldato agirà come una squadra. Lo sviluppo di sistemi autonomi è guidato principalmente da esigenze operative come la resistenza ad alta quota (HALE), l'aumento del livello di intelligenza artificiale integrata e il rapporto uomo-

macchina. Gli esperti prevedono che l'integrazione dei sistemi autonomi all'interno dell'Alleanza e degli Stati partner sarà incrementale e che dal 2025 in poi tale tecnologia sarà cruciale per il futuro delle loro operazioni.

Gli investimenti militari in tali tecnologie sono in crescita: si prevede che il mercato globale degli UxV raggiungerà circa 172 miliardi di dollari entro il 2024[26]. Gli Stati Uniti, per esempio, per il budget del 2020 hanno stanziato 3,7 miliardi di dollari di nuovi finanziamenti per sistemi autonomi e 927 milioni di dollari per finanziamenti correlati all'IA[27]. Tutto ciò rappresenterà sicuramente un'opportunità per la NATO ma anche una sfida all'interoperabilità alleata. Inoltre, con la diminuzione dei costi per la produzione dei sistemi autonomi il loro uso ed impiego da parte di attori non statali rischia di aumentare. L'Alleanza dovrà affrontare anche problemi legati alla comunicazione, al controllo e all'integrazione operativa: questi includono, come per l'IA, l'allineamento alle ROE, la condivisione di grandi volumi di dati e la standardizzazione dei protocolli operativi. Affinché la NATO possa maturare un reale e solido vantaggio in termini di sistemi autonomi, gli esperti dell'organizzazione della NATO auspicano miglioramenti e investimenti in alcuni settori chiave della R&S come veicoli e sistemi di nuova generazione a bassa osservabilità, sensori a bassa potenza, armi ad energia diretta, miglioramento della cooperazione uomo-macchina, miniatu-

26 Research and Markets, *Global $172.3 Bn Autonomous Vehicle Markets, 2019-2024: Long Haul Trucking Market Will Grow at a CAGR of Over 60%*, marzo 2019, https://www.prnewswire.com/news-releases/global-172-3-bn-autonomous-vehicle-markets-2019-2024-long-haul-trucking-market-will-grow-at-a-cagr-of-over-60-300818667.html

27 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040,* p. 64.

rizzazione e difesa con armi cinetiche per contrastare gli UAV nemici e per operazioni di *counter-swarm*.

Tecnologie quantistiche (TQ)

Le tecnologie quantistiche di nuova generazione sfruttano la fisica quantistica e i fenomeni associati su scala atomica e subatomica, in particolare *entanglement* e sovrapposizione quantistica. Questi effetti supportano progressi tecnologici significativi principalmente nella crittografia, nel calcolo, nella navigazione e tempistica di precisione, nel rilevamento e nelle comunicazioni.

I sistemi militari moderni si basano sullo sfruttamento della fisica classica, statistica e quantistica. In particolare, la prima rivoluzione quantistica ha posto le basi per i transistor, i chip per i computer, i laser, la risonanza magnetica e le moderne tecnologie di comunicazione. Tuttavia, negli ultimi dieci anni strumenti avanzati e una comprensione più profonda di tali fenomeni hanno fornito opportunità tecnologiche finora inimmaginabili. Così, la seconda generazione di tecnologie quantistiche sta ora emergendo con la possibilità di portare grandi cambiamenti più di quanto successo con la prima. Lo sviluppo delle nuove TQ procede velocemente ma le applicazioni per la difesa e la sicurezza non progrediscono in modo uniforme tra le quattro linee chiave di attività: 1) comunicazione; 2) elaborazione dei dati; 3) posizionamento, navigazione e sincronizzazione; 4) rilevamento. I livelli di investimento nazionali sono in progressivo aumento ma

l'attenzione rimane prevalentemente sulle applicazioni commerciali.

Implicazioni per la NATO

Il team di esperti del *NATO Science and Technology Organization* prevede che le capacità militari dell'Alleanza, abilitate dalle tecnologie quantistiche di nuova generazione, offriranno miglioramenti senza precedenti in settori chiave tra i quali[28]:

- Elaborazione dei dati;
- Rilevamento;
- Comunicazione e crittografia.

I computer quantistici potranno fornire capacità di calcolo migliori per ordini di grandezza, oltre il limite teorico dei computer progettati in modo classico per specifiche classi di problemi analitici (ad esempio ottimizzazione e simulazione). Questo salto computazionale consentirà approcci altamente sofisticati alla crittografia e alla decrittografia dei codici, rendendo obsoleti gli attuali metodi crittografici. M&S sofisticati e rapidi consentiranno processi decisionali operativi e organizzativi complessi, nonché nuovi modi per sviluppare materiali e biotecnologie fino ad ora sconosciuti, nonché IA di nuova generazione.

I sensori quantistici saranno molto più sensibili rispetto ai sistemi attuali. Ciò sosterrà lo sviluppo di radar contro-stealth[29], sensori magnetici, acustici e di gravità con capacità ASW notevolmente aumentate[30]. Altre applicazioni di TQ for-

28 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040,* p. 71.

29 S. Roblin, *Quantum Radars Could Unstealth the F-22, F-35 and J-20 (Or Not),* Maggio 2018, https://nationalinterest.org/blog/the-buzz/quantum-radars-could-unstealth-the-f-22-f-35-j-20-or-not-25772

30 S. Roblin, *No More 'Stealth' Submarines: Could Quantum 'Radar' Make Submarines Easy to Track (And Kill)?*, The National Interest, 2019,

niranno supporto per il rilevamento tattico per tutte le condizioni atmosferiche e per operazioni ISTAR. Inoltre, i sensori quantistici sono potenzialmente più resistenti ad operazioni di *jamming*. Nondimeno, lo sviluppo di un tipo di crittografia che sia indistruttibile e la capacità di decodificare i messaggi usando gli attuali metodi crittografici fornirà sfide significative agli attuali sistemi di C4ISR.

Il calcolo quantistico – la tecnologia quantistica potenzialmente più dirompente di tutte secondo il team di esperti – potrebbe aumentare in modo significativo il processo decisionale e l'efficacia operativa delle forze NATO. Anche in questo caso si riscontrano sfide all'interoperabilità alleata: i diversi tassi di investimento potrebbero portare disparità nelle prestazioni operative tra i membri dell'Alleanza. Inoltre, le potenziali implicazioni per la sicurezza dovute alla perdita di metodi di crittografia utili, la possibile perdita di capacità *stealth* sia nel dominio aereo sia in quello marittimo metteranno a dura prova le future operazioni della NATO. Il team di esperti, in questo senso, ha sottolineato alcune aree di R&S in cui gli alleati dovranno investire per mantenere un certo vantaggio tecnologico nei confronti di potenziali minacce tra le quali il telerilevamento quantistico[31]; posizionamento, navigazione e temporizzazione; comunicazioni quantistiche e calcolo quantistico – tecnologia che, al momento, sembra ancora un miraggio.

https://nationalinterest.org/blog/buzz/no-more-stealth-submarines-could-quantum-radar-make-submarines-easy-track-and-kill-54547

31 Ha il potenziale per rendere obsolete le tecnologie *stealth*.

Tecnologie spaziali

La decisione di riconoscere lo spazio come un nuovo dominio operativo[32] e la volontà di creare un centro dedicato interamente alle attività extra-atmosferiche[33] sono indicative dell'importanza assunta dall'*outer space*[34] nella difesa atlantica. Le infrastrutture spaziali rappresentano un *asset* fondamentale per le forze alleate: supportano le capacità C4ISR, permettono di coordinare meglio le forze alleate sul campo di battaglia e di ampliare le capacità di combattimento delle stesse (ad esempio mediante l'utilizzo di munizionamento di precisione basato su sistemi di posizionamento satellitare)[35]. Secondo quanto sostenuto dal team di esperti della *NATO Science & Technology Organization*, il marcato interesse degli attori privati e il possibile impiego di nuove tecnologie e metodi di produzioni modificheranno in modo sostanziale lo scenario spaziale, con conseguenze rilevanti nel panorama della difesa.

Gli aspetti fondamentali dell'innovazione spaziale

Gli scienziati dell'organizzazione NATO individuano futuri sviluppi tecnologici significativi in tre settori: costruzione

32 La decisione è stata presa dai capi di Stato e di Governo degli stati membri durante il Consiglio Atlantico tenutosi a Londra nel 2019. https://www.nato.int/cps/en/natohq/topics_175419.htm

33 Il centro, promosso dai ministri della Difesa alleati durante il Consiglio Atlantico virtuale dello scorso ottobre, sarà costituto presso il NATO Allied Air Command di Ramstein (Germania) e avrà il compito di coordinare le attività spaziali alleate (es. comunicazioni, immagini satellitari, ampliando altresì la *space situational awareness* delle forze NATO, https://www.nato.int/cps/en/natohq/topics_175419.htm; https://shape.nato.int/about/aco-capabilities2/nato-space-centre

34 Secondo una convenzione internazionale, per spazio si intende quell'ambiente che si estende al di sopra della c.d. "linea di Karman" (ovvero 100 km di altitudine sul livello del mare).

35 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040*, p. 17

delle piattaforme; sensoristica e operazioni. L'avanzamento tecnico nel campo della miniaturizzazione dei carichi (*payload*), così come nel settore della manifattura additiva (*3D printing*), della propulsione e dei materiali, permetterà la costruzione di satelliti dalle dimensioni e dal peso ridotto (cosiddetti *smallsat*, con un peso inferiore ai 500 kg) ma con una capacità operativa simile, se non addirittura migliore, rispetto a quelli già presenti in orbita. La possibilità, inoltre, di lanciare nello spazio un numero ingente di questi nuovi satelliti – al fine di costituire vere e proprie costellazioni artificiali – amplierà la capacità dell'Alleanza di acquisire informazioni, di distribuirle in modo sicuro e di ampliare la capacità di *space situational awareness*[36], ovvero l'abilità di osservare il contesto operativo, rilevare attacchi e distinguere – nel dominio spaziale – reali minacce da falsi allarmi[37]. Gli sviluppi, invece, nel campo della sensoristica consentirà di dotare le nuove infrastrutture orbitanti di strumenti più sensibili, in grado di acquisire una quantità maggiore di dati che saranno utili ai decisori politico-militari per le scelte strategiche ed operative. Quanto detto in precedenza sembrerebbe avvalorare le aspettative di una contestuale crescita del potenziale operativo degli *asset* spaziali.

Implicazioni per la NATO

Lungi dal produrre solo potenziali effetti favorevoli per l'Alleanza, le innovazioni tecnologiche ipotizzate – unite alla democratizzazione dell'accesso allo spazio e alla crescente importanza civile e militare delle infrastrutture satellitari –

36 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040*, p.77.

37 A. Savini e D. Mattera, *La Space Force e il futuro della competizione nello spazio*, febbraio 2020, https://www.geopolitica.info/la-space-force-e-il-futuro-della-competizione-nello-spazio/

rischiano di portare con sé nuove minacce e nuove sfide da affrontare. Lasciando sullo sfondo il possibile affollamento delle orbite connesso ad una maggiore attività privata e al conseguente problema dell'aumento della "spazzatura spaziale", gli *asset* orbitali adoperati dalle forze NATO potrebbero essere considerati come obiettivi prioritari da potenziali avversari: accecare temporaneamente, disabilitare o distruggere tali strumenti inciderebbe in maniera decisiva sulla capacità di risposta delle forze alleate. L'importanza di queste strutture, in sintesi, pone nuove questioni non solo riguardo gli aspetti più strettamente militari o di sicurezza ma anche sulla corretta interpretazione di articoli cardini dell'Alleanza come l'Art.5 e sul possibile rapporto della compagine atlantica con attori privati attivi nel settore spaziale[38].

Tecnologie ipersoniche

Frutto di una ricerca iniziata negli anni '60 del secolo scorso, la tecnologia ipersonica viene considerata da diversi attori internazionali come un potenziale *game-changer* degli affari militari dei prossimi decenni[39]. Quando si fa riferimento alla tecnologia ipersonica in ambito militare si richiamano alla mente vettori in grado di viaggiare a una velocità – almeno – cinque volte superiore a quella del suono[40] e modificare la

38 Per approfondimenti questi temi vedi https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html

39 Stati Uniti, Repubblica Popolare Cinese, India e Federazione Russa – solo per citare gli stati con i budget per la difesa più consistenti – sono impegnati nello sviluppo di programmi ipersonici di varia natura.

40 Nel linguaggio fisico mutuato dal personale aeronautico Mach 5 (dove Mach 1 è la velocità del suono), ovvero circa 6,174 km/h.

propria traiettoria di volo durante il tragitto verso l'obiettivo designato: sebbene, ad – esempio – le testate dei missili balistici rientranti nell'atmosfera siano già in grado di raggiungere tali velocità, queste non riescono a modificare la loro traiettoria durante la fase di volo[41].

I sistemi d'arma ipersonici

Sono tre i sistemi dotati di tale tecnologia su cui si stanno concentrando – con alterne fortune – gli sforzi dei diversi attori internazionali[42]:

1- *Hypersonic Glide Vehicle* (veicolo a planata ipersonica o HGV): dopo esser stati portati alla quota di lancio[43] da un vettore (principalmente di tipo balistico), il mezzo si stacca dal missile e raggiunge l'obiettivo senza una fonte di propulsione propria, sfruttando unicamente l'energia potenziale fornita dal mezzo di supporto. Il particolare profilo aerodinamico del veicolo consente a quest'ultimo di cambiare traiettoria durante la fase di volo e di raggiungere l'obiettivo a velocità ipersonica.

2- *Hypersonic Cruise Missile* (HCM): a differenza dei HGV, la variante ipersonica dei missili cruise si dirige verso l'obiettivo sfruttando una fonte di propulsione propria: tali armi, infatti, sono alimentate da motori – denomi-

41 Da sottolineare, però, la capacità di particolari vettori balitstici (*Terminally Guided Ballistic Missiles*) di modificare – seppur limitatamente – la loro traiettoria nella fase terminale di volo. J. M. Acton, *Silver Bullet? Asking The Right Questions About Conventional Prompt Global Strike*, Carnegie Endowment for International Peace, 2013, p. 36.

42 A causa della mancata possibilità di modificare la loro traiettoria, sono esclusi dalla trattazione i c.d. *hyper-velocity projectiles*, ovvero i proiettili sparati da cannoni elettromagnetici che riescono a superare il muro del regime ipersonico. NATO Science and Technology Organization, *Science and Technology Trends 2020-2040*, p.87.

43 Tale quota può oscillare tra i 40-100 km di altitudine, quindi al di sotto della linea di Karman.

nati *scramjet* – che sfruttano la compressione dell'aria generata dal regime ipersonico per produrre movimento (per questo vengono definiti anche motori *air-breathing*). Poiché questo particolare tipo di motore funziona solo a regimi supersonici, l'HCM deve essere lanciato da un altro vettore – nella maggior parte dei casi un velivolo supersonico – per consentire la corretta combustione all'interno del propulsore[44].

3- *Hypersonic Aircraft:* velivoli o droni – impiegati per missioni ISR – in grado di volare a una velocità prossima o superiore a quella di Mach 5[45].

Implicazioni per la NATO

Il possibile schieramento di questi nuovi armamenti da parte della NATO potrebbe avere risvolti in più scenari operativi, dalle missioni ISR alle attività più strettamente collegate a un potenziale conflitto ad alta intensità: tali armi risulterebbero utili sia per penetrare spazi concepiti per ostacolare la proiezione delle forze nemiche (A2/AD), sia per colpire navi o bersagli terrestri. Da non sottovalutare, inoltre, il potenziale di HGV e HCM in ambito nucleare: oltre alla possibilità di dotare HGV e HCM di testate nucleari, le particolari caratteristiche di questi sistemi d'arma le rendono ideali per condurre attacchi convenzionali contro strutture C2 nemiche (c.d *decapitation strikes*)[46].

Le potenziali capacità dei sistemi ipersonici, però, rappresentano solo una faccia della medaglia: le caratteristiche peculiari di queste armi potrebbero porre non pochi problemi

44 Ibidem.
45 Ibidem.
46 Ivi, p.90.

ai decisori politico-militari dell'Alleanza. Al di là della probabilità di un loro potenziale utilizzo in combattimento, la sola esistenza di queste armi e la mancanza – almeno nel medio periodo – di sistemi d'arma in grado di intercettarle[47] pongono delle questioni rilevanti riguardo la compressione temporale del processo decisionale conseguente alla notizia di un imminente attacco missilistico.

Bio and Human Enhancement Technologies

Soldati dotati di esoscheletri in grado di trasportare pesanti armamenti o capaci di guardare a centinaia di metri di distanza grazie a elmetti futuristici: quelli che all'apparenza potrebbero essere considerati da alcuni come elementi tipici di storie e film fantascientifici, potrebbero in realtà rappresentare possibili applicazioni militari delle più moderne ricerche scientifiche nel campo delle biotecnologie.

Le quattro aree critiche delle biotecnologie

Secondo quanto sostenuto dal team di scienziati della NATO, gli avanzamenti nel capo delle c.d. *Bio & Human Enhancement Technologies* – ovvero in quell'insieme di tecnologie che consentono di utilizzare componenti derivanti da esseri viventi su altre componenti viventi e/o di accrescere le capacità degli esseri umani mediante interventi biomedici – potrebbero cambiare radicalmente il mondo delle forze armate[48]. Sebbe-

47 La particolare altitudine a cui operano le armi ipersoniche e la loro capacità di cambiare traiettoria riducono l'efficacia dei sistemi antimissilistici attualmente adoperati dai principali attori internazionali. Hypersonic Weapons: Background and Issues for Congress (fas.org) p.2.

48 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040*, p. 21.

ne l'arco temporale di applicazione di queste nuove tecnologie sia di medio-lungo periodo – circa vent'anni – gli esperti della NATO avrebbero già individuato quattro aree di potenziale interesse per l'Organizzazione militare del Patto Atlantico[49]:

- Bioinformatics & Bionsensors;
- Human Augmentation;
- Medical Countermeasures & Bio-medical technologies;
- Synthetic Biology.

Per *Bioinformatics* si intende la capacità di raccogliere, organizzare e analizzare dati biologici, in particolar modo quelli generati dalle attività umane. Tali dati possono essere raccolti mediante biosensori, ovvero strumenti in grado di "monitorare e convertire processi biologici o biochimici in imput elettrici"[50]: rientrano nel campo dei biosensori, ad esempio, gli *smartwatch* che riescono a misurare la frequenza cardiaca[51]. In ambito militare, l'utilizzo di biosensori unita alla possibilità di usare soluzioni collegate alla *Bioinformatics*, consentirebbe di avere una maggiore comprensione della salute dei soldati, di migliorare i programmi di addestramento e – in caso di minacce CBRN – di misurare l'esposizione delle forze armate a potenziali agenti letali[52].

La *Human Augmentation*[53] – come si diceva in precedenza – si lega alla possibilità di accrescere le capacità umane, nello specifico quelle che possono essere più rilevanti in un ipote-

49 Ibidem.
50 Ivi, p.95.
51 https://stanmed.stanford.edu/2017winter/what-wearable-biosensors-including-a-smart-watch-can-tell-you-about-your-health.html
52 NATO Science and Technology Organization, *Science and Technology Trends 2020-2040*, p.96.
53 Ibidem.

tico campo di battaglia. Al centro dell'interesse degli apparati militari i progetti che si propongono di aumentare le capacità visive e udite, così come quelle che mirano al miglioramento delle capacità cognitive: il perfezionamento di tali capacità migliorerebbe, ad esempio, la capacità di acquisire bersagli e di combinare più efficacemente l'elemento umano con quello artificiale (c.d *Human-Machine Teaming*). Ricompresi nel settore della *Human Augmentation* i progetti che prevedono lo sviluppo della c.d realtà aumentata e degli esoscheletri: se nel primo caso, uno o più *device* consentono l'integrazione di elementi reali ed elementi virtuali, nell'altro gli elementi meccanici si integrano con quelli biologici. Al netto dei possibili utilizzi in combattimento, gli esoscheletri potrebbero essere utilizzati anche per migliorare le condizioni di vita di quei militari vittime di gravi traumi durante le operazioni.

Lo sviluppo nel campo nel settore *Bioinformatics & Bionsensors* concorre nel generare effetti anche in un altro ambito di ricerca considerato dagli esperti di primaria importanza, ovvero quello delle *Medical Countermeasures & Bio-medical technologies*[54]. La possibilità di disporre di una mole consistente di dati su valori vitali e stato di salute degli individui potrebbe consentire – ad esempio – lo sviluppo di "terapie su misura" che tengano conto delle particolari peculiarità del singolo soggetto trattato. In ambito militare queste tecnologie potrebbero ridurre la mortalità dovuta alle attività di combattimento e migliorare i processi riabilitativi.[55]

54 Ivi, pp. 98-99.
55 Ibidem.

La manipolazione di determinati geni e l'ingegnerizzazione di organismi rappresentano, invece, alcuni degli aspetti cruciali della *Synthetic biology*.[56] Basata su più campi di ricerca – biologia molecolare e ingegneria, solo per citarne alcuni – la *Synthetic biology* mira alla creazione di strutture biologiche dotate di particolari capacità non riscontrabili in natura (es. bio-robot). Sebbene ancora in fase iniziale, sarebbe proprio questo l'ambito tecnologico che gli esperti considerano possa avere i maggiori effetti dirompenti in questo particolare settore.

I possibili rischi per la NATO

In questo scenario, le potenziali minacce per la NATO potrebbero derivare sia da fattori di natura esterna sia fattori interni, riconducibili – quindi – alla stessa compagine alleata. Al possibile impiego di "super-soldati" o allo sviluppo di nuovi agenti patogeni da parte di attori statali o non statali avversi[57], infatti, si potrebbero unire differenze di vedute tra gli alleati riguardo l'impiego di tecnologie che inevitabilmente finiscono col sollevare diverse questioni etiche, politiche e legali. La mancata condivisione tra gli alleati di una cornice etica e legale all'interno della quale inserire lo sviluppo di queste innovazioni potrebbe minare la solidità politico-militare dell'Alleanza, finendo con l'esporre la stessa all'azione di attori che potrebbero non essere affetti dagli stessi dilemmi etici.

56 Ibidem.
57 Ivi, p. 100.

Novel Materials & Manufacturing

Potenziali effetti dirompenti negli affari militari potrebbero essere determinati anche dall'utilizzo di nuovi materiali e mezzi di produzione. Gli esperti della NATO ipotizzano un notevole sviluppo nel campo della produzione dei c.d. *Advanced materials*, ovvero di nuovi materiali dotati di particolari capacità chimico-fisiche (es. resistenza alla tradizione, conducibilità elettrica, resistenza alle alte temperature, leggerezza, flessibilità...) prodotti attraverso tecniche tratte dalle nanotecnologie o dalla *Synthetic biology*. L'utilizzo, inoltre, di metodi di produzione come il *3D printing* (o *Additive manufacturing*) permette lo sviluppo di design difficilmente ottenibili mediante l'utilizzo della tradizionale manifattura sottrattiva. Interessante, nel settore della produzione, anche il c.d. *4D printing*: tale tecnica fonde l'*Additive manufacturing* con nuovi materiali in grado di essere programmati al fine di modificare la propria forma in ragione del cambiamento delle condizioni esterne[58].

Implicazioni per la NATO

Portare tali innovazioni sul campo di battaglia potrebbe: ridurre il peso degli equipaggiamenti dei singoli soldati senza però comprometterne la loro sicurezza (si ipotizzano protezioni costruite in materie ceramiche e grafene, ovvero un sottile strato bidimensionale di atomi di carbonio caratterizzato da una notevole leggerezza e da una resistenza 200 volte maggiore rispetto a quella dell'acciaio)[59]; ridurre l'osserva-

58 Ivi, p.107.

59 https://www.enea.it/it/seguici/pubblicazioni/EAI/anno-2011/indice-world-view-3-2011/il-grafene-proprieta-tecniche-di-preparazione-ed-applicazioni

bilità di mezzi terrestri, navali e aerei mediante la creazione di polimeri in grado di assorbire le onde radar; migliorare la resistenza operativa dei sistemi *unmanned* mediante l'utilizzo di batterie sempre più avanzate; ridurre le spese collegate allo sviluppo di piattaforme e alla loro manutenzione mediante l'utilizzo del *3D printing*.

In questo caso, i principali rischi per le forze NATO potrebbero legarsi alla potenziale democratizzazione dell'accesso a queste ritrovati tecnologici: il rapido sviluppo di queste tecnologie da parte di aziende private potrebbe consentire a una molteplicità di attori (statali e non statali) di acquisire capacità che potrebbero – ad esempio – mettere in discussione le capacità di proiezione delle forze atlantiche.

Conclusioni

La preservazione del vantaggio tecnologico è uno dei fondamenti su cui si basa la capacità della NATO di dissuadere e difendersi da potenziali minacce. Le EDT rappresentano una sfida importante per l'Alleanza e, se sfruttate in maniera adeguata, potranno essere un'assoluta opportunità. Secondo gli esperti, infatti, le tecnologie emergenti e dirompenti rischiano di minare la coesione politica e militare della NATO compromettendo anche l'interoperabilità alleata ma, allo stesso tempo, offrono un'opportunità storica per ampliare il proprio vantaggio strategico: dalla gestione di nuovi tipi di conflitti alla condivisione e all'analisi dei dati ad un livello sempre più veloce e preciso. Tuttavia, l'Alleanza Atlantica deve aumentare maggiormente la propria attenzione su que-

sto settore se davvero vuole contrastare le minacce e sfruttare il vantaggio che possono portare le EDT[60]. In che modo?

Come primo passo per gli alleati della NATO sarà necessario implementare una vera e propria strategia – in modo da poter avere un approccio unico e comune – basata su valutazioni e analisi delle possibili minacce ed opportunità che scaturiscono dall'integrazione delle EDT nei propri sistemi. Inoltre, il team di esperti designati dal Segretario Generale Jens Stoltenberg auspica la creazione di uno strumento di coordinamento transatlantico per una maggiore condivisione di informazioni ed una crescente cooperazione alleata[61].

Sarà poi necessario che l'Alleanza incorpori le EDT all'interno del proprio *defence planning progress* (NDPP) per garantire che tutti gli alleati modernizzino in maniera adeguata le loro forze e che il processo di l'adattamento tecnologico sia incluso nella valutazione di un equo *burden sharing*. In questo senso, l'NDPP dovrà riflettere le capacità della NATO di rispondere alle minacce delle EDT. Nondimeno, la riflessione NATO 2030 lanciata da Stoltenberg ha comportato una maggiore comprensione della crescente minaccia cinese. A tal proposito, gli esperti concordano sul fatto che l'Alleanza dovrà sviluppare una strategia a lungo termine per contrastare la *Military-Civil Fusion*[62] attuata da Pechino in Europa, grazie alla quale la Cina acquisisce proprietà intellettuale e progressi in

60 *NATO 2030: United for a New Era,* novembre 2020, p. 29 https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

61 Ibidem.

62 US Department of State, *Military-Civil Fusion and the People's Republic of China*, https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf

ambito tecnologico per implementare i propri obiettivi militari.

In definitiva, la NATO da sempre si è contraddistinta per la sua capacità di adattamento[63] al contesto strategico circostante, capacità che le ha permesso di superare il collasso dell'Unione Sovietica, gli attacchi terroristici dell'11 settembre nonché la crescente assertività russa a seguito dei fatti in Ucraina. Non è da escludere che tale fenomeno possa accadere nuovamente, anche per quanto riguarda le EDT. [i]

63 v. S.A.Johnston, *How NATO Adapts: Strategy and Organization in the Atlantic Alliance Since 1950*, John Hopkins University Press, Baltimore 2017.

Sigle e acronimi

A2/AD – Anti-Access and Area Denial
ASW – Anti–Submarine Warfare
BDA – Battle Damage Assessment
BDAA – Big Data Advanced Analytics
C2 – Command & Control
C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CBRN – Chemical Biological Radiological Nuclear
DARPA – Defense Advanced Research Projects Agency
EDT – Emerging and/or Disruptive Technologies
ELINT – Electronic Intelligence
EO – Electro-optical
EOD – Explosive Ordnance Disposal
HALE – High Altitude, Long Endurance
HCM – Hypersonic Cruise Missile
HGV – Hypersonic Glide Vehicle
IA – Intelligenza Artificiale
IR – Infrarossi
ISR – Intelligence Surveillance Reconnaissance
ISTAR – Intelligence Surveillance Target Acquisition Reconnaissance
M&S – Modeling & Simulation
NATO – North Atlantic Treaty Organization
PNT – Positioning, Navigation and Timing
R&S – Ricerca e Sviluppo
ROE – Rules of Engagement
S&T – Science & Technology
SA – Situational Awareness
SIGINT – Signals Intelligence
TQ – Tecnologie Quantistiche
UAV – Unmanned Aerial Vehicle
UCAV – Unmanned Combat Aerial Vehicle
UGV – Unmanned Ground Vehicle
USV – Unmanned Surface Vehicle
UUV – Unmanned Underwater Vehicle

Geopolitica.info

Alessandro Savini

Studente del corso di laurea magistrale in Relazioni Internazionali presso l'Università degli Studi Roma Tre e Research Fellow del Centro Studi Geopolitica.info per il quale coordina le attività dell'area Stati Uniti e Nord America e cura "Faro Atlantico: Osservatorio sulla Difesa Euro-Atlantica". I suoi interessi includono la politica estera e di difesa americana, l'evoluzione della NATO dalla fine della Guerra Fredda e gli studi strategici, in particolare le tecnologie emergenti negli affari militari.

Danilo Mattera

Studente del corso di laurea magistrale in Relazioni Internazionali presso l'Università degli Studi Roma Tre. Collaboratore del Centro Studi Geopolitica.info e dell'Istituto Analisi Relazioni Internazionali, cura "Faro Atlantico: Osservatorio sulla Difesa Euro-Atlantica". Autore ed aspirante ricercatore riguardo i temi della difesa e della sicurezza, si occupa principalmente di Alleanza Atlantica e NATO, innovazione tecnologica e studi strategici.

Il Centro Studi

Il Centro Studi Geopolitica.info nasce nel 2004 con l'obiettivo di offrire un contributo al dibattito sulla politica estera, la geopolitica e le relazioni internazionali dalla prospettiva dell'Italia. Le attività del Centro Studi si articolano in tre filoni principali: la pubblicazione della Rivista online *Geopolitica.info* e la ricerca in materia di politica internazionale; la formazione attraverso i corsi in presenza e online sulla piattaforma www.onlineducation.it; l'organizzazione di momenti di dibattito pubblico sui temi dell'agenda politica italiana relativi alle relazioni internazionali. Tutte le attività sono consultabili sul sito web www.geopolitica.info.

Centro Studi Geopolitica.info

www.geopolitica.info | centrostudi@geopolitica.info