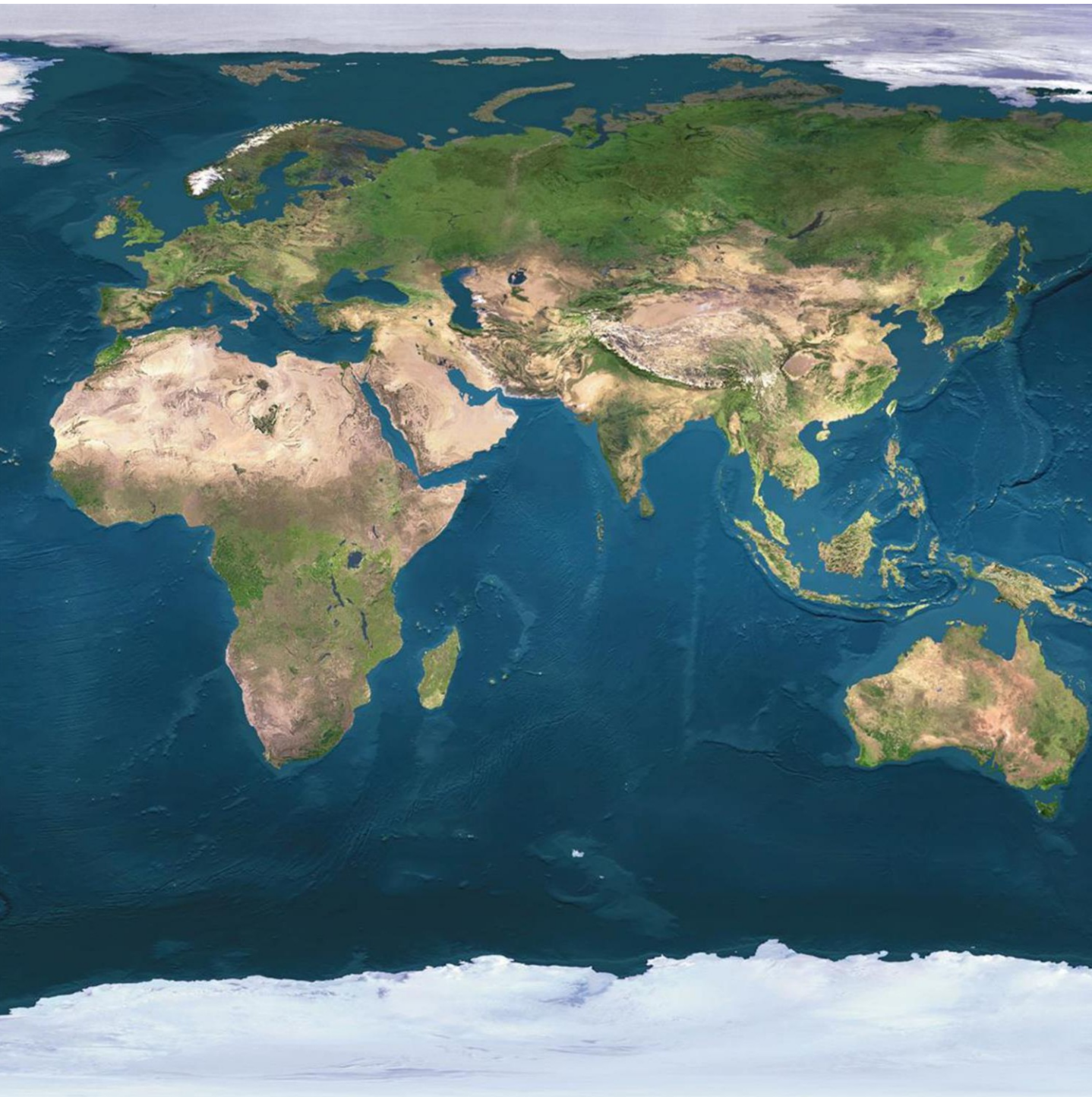
OSSERVATORIO STRATEGICO

Anno XXVII - numero 4 / 2025



CENTRO ALTI
STUDI DIFESA

ISTITUTO DI RICERCA E
ANALISI DELLA DIFESA

Osservatorio Strategico

2025
N.- 4

Osservatorio Strategico

Anno XXVII numero IV - 2025

NOTA DI SALVAGUARDIA

NOTE

Le analisi sono sviluppate utilizzando informazioni disponibili su fonti aperte.

L'Osservatorio Strategico è disponibile anche in formato elettronico (file .pdf) al seguente link:
https://www.difesa.it/smd/casd/im/irad/pubblicazioni-irad/index/35995.html

Osservatorio Strategico 2025

Questo volume è stato curato
dall'Istituto di Ricerca e Analisi della Difesa

Direttore
Contrammiraglio Gaetano Virgilio

Vice Direttore
Capo Ufficio Studi, Analisi e Innovazioni
Col. Pil. Loris Tabacchi

Redazione

Addetti
1º Mar. Massimo Lanfranco - Cº 2ª cl. Gianluca Bisanti

Progetto grafico
1º Mar. Massimo Lanfranco - Cº 2ª cl. Gianluca Bisanti - Serg. Manuel Santaniello - Ass. Amm. Stefano Deiana

Revisione e coordinamento
C.A. (aus.) Massimo Gardini - Col. Sebastiano La Piscopia, Magg. Simone Pasquazzi - Funz. Amm. Aurora Buttinelli - Ass. Amm. Caterina Tarozzi, Matteo Corti, Lavinia Perotti

Autori
Christian Vincenzo Ausiello, Mirco Balloni, Carmine Carapella, Cinzia De Iesu, Alessandro Della Monaca, Marco Gaetani, Luca Giordano, Stefano Lanci, Roberto Lizza, Pier-valerio Mari, Alessandro Papa, Siro Pettenuzzo, Giuseppe Pietrangelo, Emanuele Poli, Valentina Tagliaferri

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

Istituto di Ricerca e Analisi della Difesa
Ufficio Studi, Analisi e Innovazioni
Palazzo Salviati
Piazza della Rovere, 83 - 00165 – Roma
tel. 06 4691 3208
e-mail irad.usai@casd.difesa.it

ISBN 979-12-5515-120-3

Osservatorio Strategico

Indice

Osservatorio Strategico

Christian Vincenzo Ausiello – Emanuele Poli

Geopolitica e corsa agli armamenti: dalla guerra Russia-Ucraina alle nuove dinamiche del potere degli Stati

Abstract

Lo scoppio del conflitto tra Russia e Ucraina sembra aver innescato cambiamenti molto rilevanti rispetto allo scenario politico e di sicurezza dell'intera area europea. Fra questi mutamenti si rileva anche un ritorno a dinamiche di potere che sembravano, almeno in parte, sopite, giacché fondate sull'uso effettivo della forza e su conseguenti politiche e investimenti miranti ad aumentare le capacità militari degli Stati. Il contributo intende riflettere su questo tema, analizzando come il conflitto russo-ucraino stia impattando sulle politiche di riarmo dei Paesi europei e le possibili conseguenze, strategiche e operative, che ne potrebbero derivare.

1. Introduzione

Il 24 febbraio 2022 rappresenta una data spartiacque nella storia occidentale delle relazioni internazionali e dello sviluppo dei conflitti armati del XXI secolo. La guerra generatasi tra la Federazione Russa e l'Ucraina, si è rivelata non solo una contesa territoriale tra due Stati confinanti, ma ha assunto rapidamente le caratteristiche di una crisi globale, capace di ridefinire equilibri geopolitici, assetti strategici e dottrine militari consolidate. In un contesto internazionale già segnato da persistenti tensioni sistemiche, il conflitto che ha interessato un territorio nel cuore dell'Europa orientale, ha riattivato dinamiche di potenza che l'Occidente riteneva superate dalla fine della Guerra Fredda, riportando al centro del dibattito i concetti di deterrenza, logica bipolare e conflitto per procura. Al contempo, essa ha rivelato nuove vulnerabilità nel sistema multipolare, mettendo in discussione l'efficacia delle istituzioni internazionali, la coesione delle alleanze occidentali e la capacità di contenimento delle *escalation* regionali.

2. Il contesto

Il riconoscimento russo delle Repubbliche separatiste di Donetsk e Luhansk, avvenuto il 21 febbraio 2022, ha costituito una lapalissiana violazione diretta del principio di sovranità statale sancito dal diritto internazionale. A ciò si aggiunga l'offensiva su larga scala iniziata tre giorni dopo contro l'Ucraina, giustificata dalla Federazione Russa con la retorica della "denazificazione", necessaria a proteggere e mettere in sicurezza politica e culturale le popolazioni russofone ivi residenti. Tuttavia, per Kiev e gran parte della comunità internazionale si è trattato di un'aggressione volta a negare il diritto del popolo ucraino all'autodeterminazione e all'integrità territoriale. Ciò in considerazione del fatto che l'Ucraina, dopo l'indipendenza dall'Unione Sovietica, nel 1991, aveva cercato progressivamente di affermarsi come uno Stato democratico e orientato verso l'integrazione europea, ritenendo la decisione di rafforzare i legami con l'Unione Europea e la NATO una libera scelta di un Paese indipendente. Pertanto l'attacco russo, secondo la visione ucraina, può essere interpretato come una campagna coloniale volta a negare il diritto dell'Ucraina di scegliere il proprio destino, mentre per la Federazione Russa si è trattato invece di rispondere ad una provocazione, mettendo in atto una "guerra lampo" che puntava alla decapitazione rapida di un governo nemico lanciando operazioni militari lungo tre direttrici principali: a Nord verso Kiev, ad Est nel Donbass, e a Sud verso la Crimea. L'obiettivo di Mosca era collegare la Federazione Russa, via terra, ai porti

strategici del Mar Nero, così da creare un passaggio verso il Mar Mediterraneo, nevralgico crocevia di relazioni politiche e commerciali internazionali.

La guerra russo-ucraina non è l'esito di un improvviso scontro geopolitico, ma il punto culminante di un lungo processo storico fatto di conquiste, repressioni, resistenze e divisioni culturali. La complessa relazione tra Russia e Ucraina è stata segnata da una continua contesa sull'identità, sulla sovranità e sull'appartenenza geopolitica. Le tensioni accumulate nel corso di secoli precedenti sono esplose nel XXI secolo sotto forma di un conflitto armato che non è solo territoriale, ma profondamente simbolico: uno scontro tra due visioni opposte della storia, dello Stato e della libertà. Pur dalle origini comuni, si sono sviluppate nel corso dei secoli divergenze insanabili: nella narrativa promossa da Mosca, l'Ucraina è parte della "Russia storica", e la separazione post-1991 è stata un'anomalia dovuta alla disgregazione dell'Unione Sovietica. La cultura, la lingua e la religione ortodossa comune sono spesso invocate per giustificare un legame indissolubile tra i due popoli. La visione neo-imperiale russa, che richiama spesso l'esperienza storica della *Rus' di Kiev*[1] e l'epoca zarista, tende a negare il diritto dell'Ucraina a svilupparsi come nazione indipendente e distinta. Negli anni successivi all'indipendenza dall'Unione Sovietica, avvenuta nel 1991, l'Ucraina si trovò a dover scegliere tra un'integrazione con le istituzioni euro-atlantiche e il mantenimento di forti legami economici e culturali con la Russia. Questa ambivalenza ha caratterizzato la politica ucraina fino agli inizi degli anni 2000, con governi che alternavano orientamenti filo-russi e filo-occidentali. L'esistenza di una consistente popolazione russofona, soprattutto nelle regioni orientali e meridionali, contribuì ad alimentare una divisione interna sul piano identitario. La crisi esplose nel 2013, quando il presidente ucraino allora in carica decise di sospendere l'accordo di associazione con l'Unione Europea, provocando grandi proteste sfociate nel rovesciamento del governo e nella fuga del presidente, eventi che Mosca interpretò come un colpo di Stato orchestrato dall'Occidente. Così, nel marzo 2014, la Crimea venne annessa militarmente alla Federazione Russa, mentre in aprile scoppiava la guerra nel Donbass tra forze separatiste filorusse ed esercito ucraino[2].

La Russia considera l'area post-sovietica come una zona di interesse strategico esclusivo. L'Ucraina, per dimensioni, posizione e risorse, è centrale in questa visione. La perdita del controllo politico dell'Ucraina, ha rappresentato per Mosca non solo una sconfitta geopolitica, ma anche un pericoloso esempio per altri Paesi ex sovietici. Con la guerra, la Russia intende riaffermare il proprio status di potenza regionale, impedendo ulteriori rivoluzioni, e cercando di ridefinire gli equilibri geopolitici in una chiave multipolare, opposta all'ordine liberale guidato dall'Occidente.

3. Il conflitto armato

Il conflitto, lanciato con l'attacco su larga scala da parte della Federazione Russa, è stato segnato nel corso degli eventi iniziali dal fallimento della prevista presa di Kiev, dimostrando i limiti della forza e della pianificazione russa e mettendo in evidenza l'efficacia della resilienza ucraina. Questo successo strategico iniziale dell'Ucraina si spiega andando ad analizzare il ruolo delle Istituzioni Internazionali e delle alleanze, in cui la NATO e l'Unione Europea, pur non intervenendo direttamente sul terreno, hanno fornito sostegno materiale e politico, cruciale ed efficace per lo Stato aggredito. Uno degli argomenti più utilizzati da Mosca per giustificare l'invasione del 2022 è stato quello della "denazificazione" dell'Ucraina. Il governo russo sostenne che a Kiev fosse in atto un regime controllato da forze neonaziste, riferendosi a gruppi armati attivi durante la guerra nel Donbass, che pur rappresentando una minoranza nel panorama politico ucraino, la propaganda russa utilizzò per costruire un'immagine di un'Ucraina deviata e pericolosa, da "liberare" per il bene dei suoi stessi cittadini russofoni. Questa

---

1 Entità monarchica medievale degli Slavi orientali, sorta verso la fine del IX secolo d.C., in parte del territorio delle odierne Ucraina, Russia europea, Bielorussia, Moldavia, Polonia, Lituania, Lettonia ed Estonia.

2 Cella G., *Storia e geopolitica della crisi ucraina. Dalla Rus' di Kiev a oggi*, Carrocci, 2021.

narrazione servì a mobilitare memorie potenti, come la vittoria sovietica sul nazismo nella Seconda Guerra mondiale. Sul piano globale, invece, l'invasione ha determinato la reazione immediata della maggior parte dei Paesi occidentali membri della NATO e dell'UE, almeno in parte in modo coerente alla teoria internazionalistica neoliberale, che attribuisce alle Istituzioni Internazionali la capacità di agevolare una risposta corale e concertata degli Stati in situazione di crisi. I Paesi occidentali hanno risposto con l'imposizione di sanzioni economiche, ma anche con l'invio di aiuti a Kiev, mettendo in pratica un'azione efficace di *balancing* collettivo contro l'aggressore[3]. La compattezza transatlantica ha sorpreso Mosca, mettendo in luce, a livello di percezione geopolitica e in tal caso in modo coerente a visioni teoriche di stampo realista, quanto la presenza di minacce comuni possa generare coesione politica. Infatti, quale risposta immediata all'invasione dei territori ucraini, gli Stati occidentali hanno iniziato a supportare l'Ucraina attingendo immediatamente dalle scorte nazionali di armamenti e munizioni. L'inasprirsi del conflitto ha dimostrato che le scorte dei Paesi occidentali, per quanto importanti, non erano sempre all'altezza e adeguate a sostenere uno sforzo bellico così intenso e prolungato, inducendo di conseguenza una profonda riflessione sulla necessità di rimodulare, quantitativamente e qualitativamente, le proprie dotazioni belliche.

Nei primi mesi di guerra, l'assistenza militare all' Ucraina si è concentrata su forniture difensive: elmetti, giubbotti antiproiettile, missili portatili anticarro (*Javelin*) e antiaerei (*Stinger*). Tale scelta era dettata dalla volontà di evitare una diretta escalation con la Federazione Russa e mantenere il conflitto entro una dimensione contenuta. A partire dalla metà del 2023, l'intensificarsi del conflitto e le ripetute segnalazioni di crimini di guerra hanno indotto diversi paesi NATO ad ampliare il tipo di supporto fornito. Sono stati consegnati carri armati avanzati (Leopard 2, Challenger 2, M1 Abrams), sistemi missilistici HIMARS, batterie anti-missile Patriot e droni da combattimento. L'approccio è passato da una logica di contenimento a una di supporto alla riconquista dei territori occupati. Questa fase ha segnato anche una svolta nel consenso interno alle opinioni pubbliche occidentali, divise e polarizzate tra impulsi pacifisti e incondizionato sostegno all'Ucraina[4].

Nel 2024 ha preso avvio l'addestramento dei piloti ucraini all'uso degli F-16 in basi NATO[5]. Tale sviluppo ha consolidato il coinvolgimento militare occidentale, pur restando formalmente al di fuori del conflitto diretto. L'interoperabilità e l'intelligence condivisa sono aumentate, avvicinando de facto l'Ucraina agli standard NATO.

Sul fronte opposto, la Bielorussia ha svolto un ruolo strategico permettendo alle truppe russe di operare dal proprio territorio, fungendo da retrovia logistica per le offensive dirette verso Kiev e il nord dell'Ucraina. Sebbene formalmente non coinvolta in combattimenti diretti, la sua collaborazione ha rappresentato un elemento cruciale nella pianificazione militare russa. La Corea del Nord ha intensificato la cooperazione militare con Mosca, fornendo munizioni d'artiglieria, missili a corto raggio e altre forniture belliche, in aperta violazione delle risoluzioni delle Nazioni Unite.

La guerra russo-ucraina ha segnato un sorprendente ritorno ad alcune dinamiche belliche che si pensavano ormai superate nel contesto dei conflitti moderni. Dopo decenni di guerre asimmetriche, combattute prevalentemente in contesti urbani o desertici e dominate da operazioni speciali, droni e guerra cibernetica, il teatro ucraino ha riportato al centro

---

3 Jervis R., *Review Article: Deterrence Theory Revisited*, «World Politics», 31, 2 (Jan. 1979), 289-324; Knopf J.W., *The Fourth Wave in Deterrence Research*, «Contemporary Security Policy», 31, 1, 2010, 1-33; Lupovici A., *The Emerging Fourth Wave of Deterrence Theory. Toward a New Research Agenda*, «International Studies Quarterly», 54, 3 (Sept. 2010), 705-732; Ministero della Difesa, *Libro Bianco per la Sicurezza Internazionale e la Difesa*, Roma, 2015.

4 Freyrie M., *Cosa prevedono gli aiuti militari all'Ucraina decisi a Ramstein*, in Affari Internazionali: https://www.affarinternazionali.it/vertice-ramstein-aiuti-militari-ucraina/ (23.01.2023).

5 Cfr. *Aspre battaglie a Kursk e Donetsk. La "prima volta" degli F-16 ucraini,* «Analisi Difesa»: https://www.analisidifesa.it/2024/08/aspre-battaglie-a-kursk-e-donetsk-la-prima-volta-degli-f-16-ucraini/ (28.08.2024).

l'importanza delle operazioni convenzionali su larga scala. Trincee, linee di contatto statiche, scontri di artiglieria e battaglie di posizione hanno evocato immagini e strategie proprie dei conflitti del Novecento, in particolare della Prima e della Seconda guerra mondiale. Un aspetto centrale è la rinnovata importanza della fanteria, dei mezzi corazzati e dell'artiglieria convenzionale. La fanteria, non di rado sottovalutata nei conflitti recenti, si è rivelata invece indispensabile per il controllo del terreno, la difesa delle posizioni e le operazioni nelle aree urbane e boschive. In particolare, le truppe leggere e le forze di fanteria meccanizzata hanno avuto un ruolo decisivo nel contrastare le offensive nemiche e consolidare le conquiste territoriali.

Accanto alle componenti terrestri, anche le forze aeree hanno giocato un ruolo significativo, sebbene in modo diverso rispetto ai conflitti precedenti. Nonostante la superiorità numerica e tecnologica inizialmente attribuita all'aeronautica russa, questa non è riuscita a conquistare una superiorità aerea duratura. L'efficace difesa antiaerea ucraina, basata su un mix di sistemi sovietici modernizzati (come gli S-300) e sistemi occidentali (come NASAMS, IRIS-T e Patriot), ha impedito alla Russia di operare liberamente nei cieli ucraini. Questo ha costretto entrambe le parti a impiegare l'aviazione in modo cauto, limitando le missioni a bombardamenti a distanza o attacchi tattici in profondità limitata. Questo ritorno al passato, tuttavia, non è un semplice utilizzo di mezzi ed armamenti già noti, ma un adattamento complesso, considerate le caratteristiche geografiche e morfologiche del terreno e gli ampi spazi del territorio di guerra, in cui vecchie forme vengono riempite di nuovi contenuti, in un'interazione dinamica tra innovazione e tradizione bellica.

La dimensione tecnologica ha rappresentato un elemento distintivo e trasformativo del conflitto russo-ucraino, con una centralità crescente dei sistemi a pilotaggio remoto. I droni in particolare hanno assunto un ruolo molteplice e cruciale, in considerazione dell'evidente versatilità, del costo contenuto e dell'impiego su ampie distanze programmabili per l'individuazione degli obiettivi, tanto da ridefinire le modalità operative sul campo.

4. La corsa agli armamenti e il ruolo degli Stati Occidentali

L'impatto multidimensionale della crisi russo-ucraina, sia in termini militari − con la trasformazione delle modalità belliche, il ritorno della guerra di posizione e l'adozione massiva di tecnologie emergenti −, che sul piano geopolitico, con le reazioni delle grandi potenze e le nuove linee di frattura internazionali che si stanno delineando, ha evidenziato come questa guerra abbia accelerato processi di adattamento strategico, favorito la sperimentazione operativa di nuovi strumenti e tattiche e contribuito alla ridefinizione degli assetti di sicurezza a livello globale.

La necessità, da parte dei Paesi occidentali sostenitori dell'Ucraina, di incrementare la produzione di munizionamento e armamento, ha evidenziato almeno due criticità fondamentali: il sottodimensionamento della capacità produttiva delle industrie di settore, che erano tarate per sostenere una domanda tipica dei momenti di pace; la vulnerabilità della catena di approvvigionamento, causata dalla delocalizzazione di alcune delle capacità produttive e della dipendenza da operatori economici esterni al territorio, tra i quali la Cina. Operando con logiche e strumenti "del tempo di pace", l'Unione Europea, e pur se in misura assai minore gli stessi Stati Uniti, nel supportare un Paese in guerra come l'Ucraina hanno evidenziato emergenze e criticità a cui nessuno era preparato. L'Europa si è risvegliata dal più lungo periodo di pace mai conosciuto dalla fine della Seconda Guerra mondiale, laddove la stessa "Guerra Fredda" aveva dato vita a una fase storica contraddistinta dall'illusione che non avremmo più assistito a conflitti su larga scala combattuti da eserciti regolari che si affrontano sul terreno. Tale illusione, proseguita in buona parte anche dopo la Guerra Fredda, ha comportato un adattamento, a ribasso, di alcune capacità militari, causando, a cascata, effetti sull'industria della Difesa, la quale, a fronte di una sensibile contrazione della domanda, ha dovuto rivedere le proprie politiche di produzione e di approvvigionamento secondo criteri basati principalmente sul

concetto di efficienza. Tale strategia, unita agli effetti della globalizzazione, che interviene in un contesto economico sempre più interconnesso, aveva condotto negli anni a preferire dinamiche di delocalizzazione geografica e di frammentazione dei processi produttivi dell'attività di produzione di armi, equipaggiamenti e tecnologie militari, con la conseguenza della perdita di alcune capacità produttive essenziali. Per semplificare, si può certamente affermare che tutti i limiti della capacità di produzione di armamenti in Europa siano emersi in maniera dirompente, quando proprio nel cuore del vecchio continente è scoppiato un conflitto convenzionale su larga scala.

Finché il conflitto russo-ucraino ha poi avuto, perdurando, riflessi geopolitici che sono ricaduti sull'industria della Difesa; basti pensare alla maggiore presenza ed integrazione della NATO e alla corsa al riarmo con il rilancio della produzione nel settore militare, soprattutto in Europa, e alla riprogrammazione e ridefinizione delle catene di approvvigionamento[6]. L'industria della difesa è così divenuta, nuovamente, un punto centrale della sovranità strategica: la capacità di armarsi e sostenere un conflitto non può dipendere troppo dall'esterno. Il disimpegno di Washington dal territorio europeo del resto ha contribuito, suo malgrado, all'intensificazione delle operazioni militari di Mosca, che ha approfittato del vuoto lasciato dagli USA. Gli alleati europei hanno dovuto accelerare la cooperazione in materia di difesa, anche se le divergenze interne e la mancanza di capacità logistiche hanno limitato l'efficacia delle contromisure.

Gli stati membri dell'UE hanno cercato di raggiungere un maggiore coordinamento europeo nella produzione, nella standardizzazione, negli stock comuni di munizioni e materiali. L'esigenza di politiche industriali attive con investimenti pubblici, incentivi, e regolamentazioni che premiano la resilienza e non solo il prezzo, sono processi lunghi da raggiungere. In particolare per l'Unione Europea si profila in futuro l'avvio di un nuovo Piano di competizione sistemica, in cui le imprese dell'industria della Difesa europee siano chiamate a sviluppare tecnologie di ultima generazione, sufficienti a giustificare una produzione a "preferenza europea" in sostituzione ai prodotti non europei.

Si tratta di un obiettivo ambizioso, ma non impossibile, ma che richiede un cambio di strategia politica degli Stati ed una riorganizzazione dell'intero settore secondo un'architettura ben congegnata, accompagnata da un approccio pragmatico, piuttosto che ideologico. In questo caso gli Stati dell'Unione Europea devono maturare la consapevolezza politica che non esiste una soluzione universale al problema del sostegno alla difesa, ma piuttosto un compromesso ottimale, che è necessariamente di natura politica. La ricerca di un tale compromesso genera tuttavia frizioni tra i vari Stati membri, ognuno portatore di proprie priorità nazionali e sensibilità culturali. In questa fase di trasformazione è forte il rischio di favorire alcuni Paesi a scapito di altri, e da questa preoccupazione legittima scaturisce un "eccesso di prudenza", che rende ogni cambiamento estremamente complesso, soprattutto in assenza di una chiara visione d'insieme che affronta la materia con realismo e competenza.

5. Quali prospettive future

Attualmente l'Unione Europea non ha competenze dirette in materia di Difesa e sicurezza nazionale.[7] La difesa e la sicurezza nazionale sono da sempre considerate competenze fondamentali degli Stati sovrani. Dopo la Seconda guerra mondiale, i paesi europei erano restii a cedere questo potere a un'entità sovranazionale; ogni Stato ha proprie forze armate, priorità strategiche, alleanze, come per esempio l'Alleanza NATO. Le decisioni sull' uso della forza militare, dichiarazione di guerra, difesa dei confini, restano tra le prerogative più sensibili di uno Stato. La Costituzione di molti Stati, per esempio Italia e Germania, impone limiti sull'uso della forza, rendendo complessa una gestione sovranazionale. L'articolo 4 del Trattato sull'Unione

---

6 NATO: https://www.nato.int/cps/en/natohq/official_texts_236518.htm (13.02.2025).
7 Consiglio Europeo: https://www.consilium.europa.eu/it/topics/security-and-defence/

europea (TUE) stabilisce chiaramente: “La sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro”. Nel 1954 fu proposta una Comunità Europea di Difesa (CED), con un esercito europeo comune, ma fu bocciata dal Parlamento francese, segnando il fallimento del primo progetto di difesa europea. La Difesa non è una competenza esclusiva dell’UE, come lo sono invece commercio, concorrenza, mercato interno; è pertanto una competenza condivisa, gestita in modo intergovernativo, ove le decisioni si prendono solo all’unanimità (salvo casi eccezionali riguardanti missioni internazionali, o la “cooperazione strutturata permanente” in campo industriale[8]), laddove non c’è ancora una vera “forza di difesa comune europea”. Nel 2021 è stato istituito il “Fondo Europeo per la Difesa” (*European Defence Fund* — EDF)[9], il cui scopo è finanziare la ricerca congiunta, lo sviluppo di tecnologie e sistemi di difesa a livello europeo, incentivando la cooperazione industriale tra imprese di più Stati membri, finanziando progetti di ricerca collaborativa, sostenendo lo sviluppo di prototipi e dimostratori, così da ridurre le duplicazioni e migliorare l’interoperabilità. L’UE ha inoltre avviato discussioni su una forza armata europea, ma il processo si presenta lungo e controverso, seppure un primo passo verso l’indipendenza militare sembra sia stato fatto, anche in coerenza con la Bussola Strategica dell’UE (2022), grazie al Libro Bianco sulla Difesa Europea e al piano *ReArm Europe-Readiness 2030*, che prevede un investimento di oltre ottocento miliardi di euro nel settore difesa[10]. La NATO (Organizzazione del Trattato dell’Atlantico del Nord) è stata, e resta, il principale garante della sicurezza militare dell’Europa. L’Alleanza Atlantica, di cui gli USA rappresentano il Paese leader, è dotata di una struttura militare permanente (cosa che l’UE non ha), già da tempo collaudata e operativa. Anche questo ha rallentato, almeno in parte, la creazione di una vera e propria autonomia strategica europea.

Tuttavia l’industria e il mercato interno nazionale e le regole sulla competitività sono ambiti in cui la Commissione europea ha competenze condivise o esclusive, a supporto degli Stati membri. Il Regolamento *“European Defence Investment Programme*” (EDIP)[11] si colloca in questo contesto, agendo sul pilastro industriale e tecnologico. Se possiamo immaginare la Difesa come un organismo con due gambe, quella operativa-capacitiva e quella industriale-tecnologica, EDIP agisce sulla seconda. Le esigenze capacitive rappresentano un *input* e un *output* nelle mani degli Stati, mentre l’intervento della Commissione Europea, che può essere solo finanziario e normativo, si concentra sulla parte centrale, ovvero sul come sviluppare queste capacità al fine di incrementare la competitività, la resilienza e il livello di prontezza della base industriale e tecnologica dell’Unione (*European Defence Technological and Industrial Base –EDITB*)[12].

Per quanto attiene il ruolo della Nato, l’attuale processo capacitivo dell’Alleanza mira a fornire il set di forze necessario a implementare i Piani per la deterrenza e difesa dei Paesi membri. Molte di queste capacità sono fornite in gran parte dagli Stati Uniti e, attraverso un processo di sviluppo capacitivo e di reinvestimento in talune aree, di fatto tralasciate negli anni, dovranno ora essere implementate nelle future acquisizioni nazionali dei Paesi membri. La NATO infatti, ha approvato un nuovo livello di ambizione teso ad assicurare l’eseguibilità dei Piani di deterrenza e difesa. Tale decisione ha portato a una crescita in quantità e qualità dei requisiti capacitivi dell’Alleanza, che sono stati definiti sulla base di consolidati principi politici di distribuzione dello sforzo e da specifici criteri militari. La crisi in Ucraina ha evidenziato altresì le

---

8 I relativi progetti sono attivabili solo con il consenso dei Paesi che decidono di partecipavi, con altri che possono non aderirvi.

9 Commissione Europea: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

10 Commissione Europea: https://italy.representation.ec.europa.eu/notizie-ed-eventi/notizie/la-commissione-presenta-il-libro-bianco-sulla-difesa-europea-e-il-piano-rearm-europepreparati-il-2025-03-19_it

11 Commissione Europea: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edip-dedicated-programme

12 Parlamento Europeo: https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2020)603483

criticità in merito all'intercambiabilità, l'interoperatività e l'interconnettività dei sistemi d'arma. Al riguardo le azioni previste dal "*Defence Procurement Action Plan* (DPAP), in materia di standardizzazione, prevedono la ratifica degli standard NATO, attraverso un processo che fornisca maggiore visibilità sullo stato dell'implementazione nell'Alleanza. Nel contesto del DPAP (*Piano d'Azione per gli Approvvigionamenti della Difesa*), la ratifica e l'applicazione degli standard NATO hanno l'obiettivo di armonizzare i requisiti tecnici e procedurali tra i Paesi alleati, per favorire la cooperazione industriale e i programmi congiunti, nonché ridurre costi e duplicazioni nello sviluppo e nell'acquisto di sistemi d'arma, al fine di aumentare l'interoperabilità nelle missioni multinazionali. Ciò anche per fare in modo che le diverse forze armate dei Paesi dell'Alleanza Atlantica (Italia, Francia, Stati Uniti, Germania, ecc.) possano operare insieme efficacemente, utilizzando procedure, equipaggiamenti, terminologie e formati compatibili. *L'intercambiabilità, interoperatività e interconnettività dei sistemi d'arma* è la base della collaborazione tra Paesi della Nato al di fuori di un sistema di Difesa comune; i sistemi militari dei diversi Paesi non sempre riescono a lavorare insieme in modo efficace. La guerra in Ucraina ha dimostrato che senza lo sviluppo di questi tre elementi, la cooperazione tra alleati è più lenta e meno efficace, la catena logistica si complica, i sistemi tecnologici non sfruttano appieno il loro potenziale. Per questo l'UE, la NATO e i singoli Paesi, tramite piani come il DPAP, stanno spingendo per standard comuni, sistemi interoperabili e reti integrate di comando e controllo.

6. Riflessioni conclusive

Giungendo alla conclusione, possiamo affermare che la geopolitica e la corsa al riarmo sono tra di loro strettamente connesse, influenzandosi vicendevolmente. Il disimpegno americano dal continente europeo, e lo scoppio della crisi fa Mosca e Kiev, hanno spinto i Paesi amici e alleati a cecare di estendere la propria influenza, alimentando un ritorno alla ri-nazionalizzazione della sicurezza. Il conflitto russo-ucraino ha consolidato l'Alleanza occidentale, rafforzando il ruolo della NATO, e promuovendo una maggiore cooperazione militare tra gli Stati membri (anche in sede UE); l'industria della Difesa deve però adeguare le proprie catene di approvvigionamento per ridurre le dipendenze e garantire la sicurezza delle forniture, in particolare quelle provenienti da aree considerate a rischio. Inoltre, nonostante le aziende della difesa stiano beneficiando di nuovi finanziamenti, esse stanno investendo ingenti somme di denaro per accelerare l'innovazione al fine di soddisfare le esigenze di forze armate sempre più moderne, meglio equipaggiate tecnologicamente e integrate con i partner NATO/UE, capaci di reagire rapidamente in contesti complessi, come in scenari di guerra ibrida. Ciò significa che le aziende stanno sviluppando nuove tecnologie e aggiornando i loro prodotti e processi, per fornire alle forze armate strumenti più digitali, automatizzati, interconnessi e sostenibili. Il processo prevede di progettare nuovi sistemi d'arma intelligenti, droni autonomi, radar avanzati, missili di precisione, nuovi materiali leggeri, resistenti e di tipo *stealth*, nonché di collaborare con centri di ricerca e startup tecnologiche per creare ambienti digitali di addestramento con realtà aumentata o virtuale (così da formare il personale in modo più rapido e sicuro).

Infine, come esempio emblematico, riportiamo "il successo del modello danese", ovvero la pratica avviata dalla Danimarca di produrre direttamente rispetto al comparto della difesa ucraino: «…i prodotti sono migliori, più intelligenti, più economici e arrivano più velocemente sul campo…quindi è anche a nostro vantaggio..», ha evidenziato la premier danese M. Frederiksen, riferendosi al fatto che la situazione aiuta anche le aziende occidentali a superare il paradosso che le coinvolge: "sofisticazione tecnologica, senza massa", cioè l'uso di tecnologie

che riducono la necessità di mettere sul campo grandi quantità di materiale, consentendo però di operare in modo efficiente[13].

Il conflitto ha trasformato l'Ucraina in un vero e proprio laboratorio bellico, dove sono stati testati nuovi armamenti, tattiche e dottrine militari. Armi occidentali di ultima generazione non solo sono state fornite per sostenere la resistenza ucraina, ma sono anche servite come strumenti di validazione operativa in condizioni di guerra reale. Questo processo ha permesso a molti Paesi produttori di raccogliere dati preziosi sull'efficacia, la resistenza e le criticità dei loro sistemi d'arma. Lo stesso vale per nuove configurazioni di fanteria leggera integrata con droni tattici e supporto in tempo reale, che hanno ridefinito le modalità di ingaggio e di coordinamento tra le unità sul campo. Non sorprende, dunque, che le aziende militari, sia statali che private, abbiano osservato con grande attenzione i risultati operativi, adattando in corsa i sistemi e gli approcci. In questo contesto, Russia e Ucraina sono emerse come due dei principali attori nella corsa globale all'innovazione nel settore dei droni, vista l'elevata frequenza di utilizzo, la varietà delle missioni e la rapidità con cui i *feedback* dal fronte vengono tradotti in miglioramenti tecnologici costanti. Questo banco di prova ha implicazioni strategiche per il futuro: molti degli insegnamenti appresi in Ucraina stanno già influenzando la pianificazione militare della NATO[14], delle potenze asiatiche e di altri attori globali. La guerra in Ucraina, infatti, non è solo una tragedia umanitaria e politica, ma anche un banco di prova decisivo per comprendere la direzione che la guerra, la diplomazia e l'equilibrio tra le potenze potranno assumere nel mondo post-globale.

---

13 Howe B., *The Danish Model. A sustainable Approach to supporting Ukraine*, DSEI UK Gateway News, 2025: https://www.dsei.co.uk/news/danish-model-sustainable-approach-supporting-ukraine

14 Gaiani G., *I piani di potenziamento della NATO: dai cahiers des doléances al libro dei sogni?*, «Analisi Difesa»: https://www.analisidifesa.it/2024/10/i-piani-di-potenziamento-della-nato-dai-cahiers-des-doleances-al-libro-dei-sogni/ (14.10.2024).

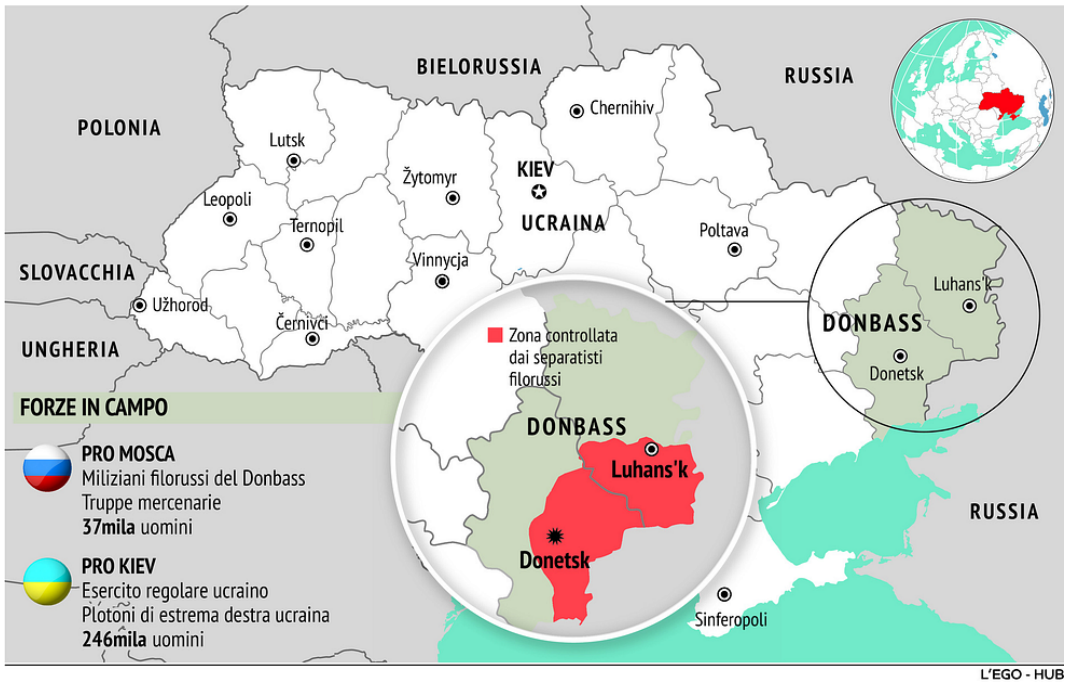


Fig. 1 - *La regione contesa Russia-Ucaina.*
Fonte: Tgcom24

Fig. 2 - *Conflitto.*
Fonte: Analisi Difesa

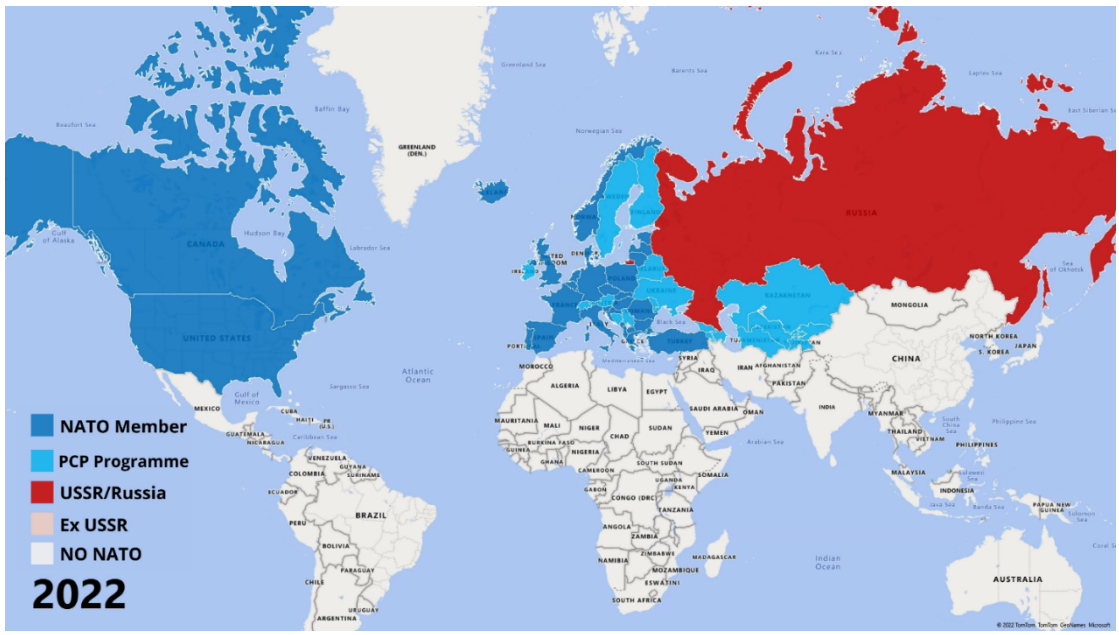


Fig. 3 - *Paesi NATO nel 2022.*
Fonte: https://statisticsanddata.org/it/data/mappa-dei-paesi-nato/

Bibliografia

- Bellezza S. A., *Il destino dell'Ucraina*. *Il futuro dellEuropa*, Brescia, Scholé, 2022.
- Cella G., *Storia e geopolitica della crisi ucraina. Dalla Rus' di Kiev a oggi*, Carrocci, 2021.
- Gaiani G., *I piani di potenziamento della NATO: dai cahiers des doléances al libro dei sogni?*, «Analisi Difesa», 2024: https://www.analisidifesa.it/2024/10/i-piani-di-potenziamento-della-nato-dai-cahiers-des-doleances-al-libro-dei-sogni/
- Howe B., *The Danish Model. A sustainable Approach to supporting Ukraine*, DSEI UK Gateway News, 2025: https://www.dsei.co.uk/news/danish-model-sustainable-approach-supporting-ukraine
- Jervis R., *Review Article: Deterrence Theory Revisited*, «World Politics», 31, 2 (Jan. 1979), 289-324.
- Knopf J.W., *The Fourth Wave in Deterrence Research*, «Contemporary Security Policy», 31, 1, 2010, 1-33.
- Lupovici A., *The Emerging Fourth Wave of Deterrence Theory. Toward a New Research Agenda*, «International Studies Quarterly», 54, 3 (Sept. 2010), 705-732.
- Marples D. R. (ed.), *The War in Ukraine's Donbas. Origins, Contexts and the Future*, CEU Press, Budapest-New York, 2022.
- Masciullo G. e Di Martino B., *Marca di confine. La guerra d'Ucraina tra Russia, NATO e Cina*, Richardson Texas, Monreal, 2022.
- Ministero della Difesa, *Libro Bianco per la Sicurezza Internazionale e la Difesa*, Roma, 2015.
- Serhii P., *Il ritorno della storia. Il conflitto russo-ucraino*, Mondadori, 2023.
- Varsori A., *Storia delle relazioni internazionali dopo la guerra fredda: 1989-2017*, Il Mulino, 2018.
- Varsori A*., Storia Internazionale. Dal 1919 a oggi*, Bologna, Il Mulino, 2020.
- Vassallo M., *Breve storia dell'Ucraina. Dal 1914 all'invasione di Putin*, Milano-Udine, Mimesis, 2022

Mirco Balloni - Carmine Carapella - Alessandro Papa

Telecomunicazioni satellitari: Evoluzione delle reti satellitari in LEO per applicazioni militari

Abstract

Nell'ultimo decennio, l'avvento delle costellazioni satellitari in orbita bassa (Low Earth Orbit, LEO) ha rivoluzionato il paradigma delle comunicazioni satellitari (SATCOM). In particolare, con l'ingresso delle aziende private nel settore spaziale si è verificata un'accelerazione in campo tecnologico nello sviluppo di nuovi sistemi satellitari, volta a garantire servizi commerciali di comunicazione adeguati alle crescenti esigenze degli utenti. In questo articolo forniremo una breve introduzione sulle tecnologie attuali, le potenzialità e gli aspetti critici di una rete satellitare LEO, focalizzandoci sull'impiego militare. Evidenzieremo, inoltre, i vantaggi tecnici e strategici, così come i principali rischi e le vulnerabilità.

* *La numerazione fra le parentesi quadre all'interno del testo si riferisce alle fonti citate nella bibliografia finale.*

1. Introduzione

Di fronte alle crescenti sfide nel settore della difesa e della sicurezza nazionale, lo spazio emerge come un ambiente strategico critico nel panorama contemporaneo. In particolare, le telecomunicazioni satellitari non si limitano a essere semplici canali di trasmissione dati, ma costituiscono l'infrastruttura portante dei sistemi di comando e controllo (Command and Control, C2) e delle capacità di intelligence, sorveglianza e ricognizione (Intelligence, Surveillance and Reconnaissance, ISR), funzioni essenziali per la superiorità operativa. Negli ultimi anni gli Stati Uniti, storicamente leader nel settore spaziale, hanno radicalmente ridefinito il proprio approccio strategico, affrontando i crescenti costi di sviluppo, produzione e gestione degli asset spaziali mediante un ampio coinvolgimento del settore privato. Questa sinergia pubblico-privato ha catalizzato lo sviluppo di tecnologie più avanzate ed efficienti, consentendo una drastica

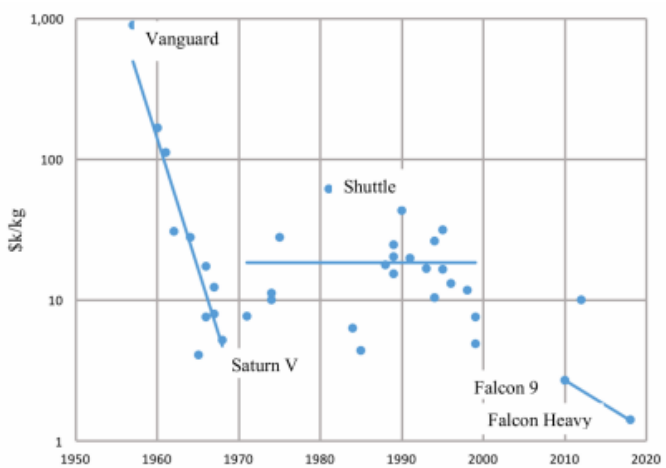


Figura 1: Costi dei lanci spaziali per i satelliti LEO [1]

riduzione dei costi di accesso allo spazio. Un caso emblematico è rappresentato dal lanciatore Falcon 9 di SpaceX, che ha ridotto i costi di lancio da circa 16.000 USD/kg nel 2004 a circa 2.700 USD/kg ad oggi. La conseguente "democratizzazione" dell'accesso allo spazio ha avuto un impatto significativo sulla space economy, favorendo la proliferazione di costellazioni satellitari di grandi dimensioni, utilizzate per applicazioni sia civili che militari, quali: telecomunicazioni, osservazione della Terra (Earth Observation, EO), navigazione satellitare (Global Navigation Satellite System, GNSS) e missioni scientifiche. In particolare, le costellazioni LEO hanno assunto un ruolo centrale nella trasformazione delle architetture di comunicazione spaziale, imponendosi come infrastrutture critiche per il XXI secolo.

2. Evoluzione delle telecomunicazioni satellitari

Per decenni l'architettura delle telecomunicazioni satellitari globali è stata dominata, dai sistemi in orbita, geostazionaria (Geosynchronous Earth Orbit, GEO), con pochi satelliti posti a circa 35.786 km di quota capaci di garantire copertura fissa su vaste aree terrestri [3]. Questa configurazione, ideale per applicazioni come: broadcast, meteorologia e comunicazioni militari, presenta tuttavia limiti intrinsechi: latenze elevate (400–500 ms), capacità trasmissiva relativamente limitata per utente, soprattutto in scenari con alta densità di terminali, vulnerabilità fisica e rigidità architetturale. Parallelamente, le orbite HEO (Highly Elliptical Orbit), caratterizzate da perigeo basso (35.000 km), pur offrendo vantaggi per le regioni polari, non hanno mai rappresentato una soluzione su larga scala. Queste orbite, come per esempio Molniya e Tundra, permettono ai satelliti di rimanere a lungo prossimi all'apogeo, garantendo comunicazioni nelle zone dove il GEO equatoriale non ha visibilità. Tuttavia la loro adozione globale è stata frenata: dalla complessità operativa, dalla limitata capacità e dal numero insufficiente di satelliti per mantenere una rete continua.

	SES	Telesat	SpaceX	OneWeb	Amazon
Constellation	O3b mPOWER	Lightspeed	Starlink	OneWeb	Kuiper
Size	11 satellites	198 satellites	1st Gen: 4,408 satellites	1st Gen: 648 satellites	Up to 3,236 satellites
Development	4 operational satellites, 4 slated for launch in 2023, and 3 in 2024	Telesat's contract with MDA to build the satellites was announced in August 2023, aiming to start launches in 2026.	The 1st generation is operational. Over 4,6612) satellites are currently in orbit out of 12,000 planned for 1st and 2nd Gen combined.	The 1st generation is fully deployed, and full coverage is planned to start in January 2024. 2nd generation satellites planned to be launched in 2028.	Deployment has not started; the current timeline is to fully deploy by July 2026.
Total capacity	~2.7 Tbps (200 – 315 Gbps /satellite)	~10 Tbps (50 Gbps /satellite)	~88 Tbps (~20 Gbps /satellite for 1st Gen)	~5 Tbps (~7.5 Gbps /satellite for 1st Gen)	~164 Tbps (~50 Gbps /satellite estimated)
Frequency band (user link)	Ka-band	Ka-band	Ku-band	Ku-band	Ka-band
Orbit	MEO (8,062 Km)	LEO (1,000 - 1,350 Km)	LEO (550 Km)	LEO (1,200 Km)	LEO (600 Km)
Satellites mass	~1,700 Kg	~700 Kg	~260 Kg	~150 Kg	~650 Kg
Satellites life	>10 years	~10 years	~5 years	~7 years	5 to 7 years
Latency[3]	~150 ms	<50 ms	<50 ms	<50 ms	<50 ms

Figura 2: Caratteristiche delle costellazioni LEO [2]

Negli anni '70, i primi tentativi di superare questi vincoli emersero con le costellazioni in orbita bassa (LEO), soprattutto in ambito militare. L'Unione Sovietica fu tra i pionieri sperimentando: reti come Strela, Parus e Tselina-D. Negli anni '90, progetti statunitensi come Iridium, Globalstar e Orbcomm e cercarono di estendere la connettività satellitare anche all'utenza civile. Tuttavia, queste prime generazioni fallirono nel tentativo di conquistare il mercato. Le ragioni del fallimento furono molteplici: tecnologie immature, terminali ingombranti e costosi, efficienza energetica insufficiente, capacità di payload ridotta e, soprattutto, una domanda commerciale ancora acerba, incapace di sostenere il modello di business. Inoltre, i costi di lancio all'epoca erano proibitivi e i modelli di architettura di rete erano rigidi e non scalabili, rendendo insostenibili gli ingenti investimenti richiesti. Solo con l'avvento della

miniaturizzazione elettronica, della manifattura modulare e del drastico abbattimento dei costi di lancio (grazie a vettori riutilizzabili come Falcon 9), si è reso possibile il dispiegamento di vere mega-costellazioni LEO.

Le moderne costellazioni in orbita terrestre bassa (LEO), generalmente posizionate tra i 400 e i 1.400 km, sfruttano l'interazione tra il movimento orbitale dei satelliti e la rotazione terrestre per sorvolare periodicamente ogni punto della superficie. In questo modo, attraverso la creazione di costellazioni con centinaia o migliaia di unità, distribuite su più piani orbitali, si riesce a garantire una copertura globale e un servizio ininterrotto su scala mondiale. Le architetture più avanzate possono includere anche strati multipli di satelliti a diverse altitudini per ottimizzare: copertura, capacità e ridondanza. A queste altitudini, i satelliti completano un'orbita in circa 90–120 minuti, a velocità di circa 7,8 km/s, con latenze end-to-end di 20–80 ms, un ordine di grandezza inferiore rispetto ai sistemi GEO. Il risultato è la possibilità di comunicazioni quasi in tempo reale, con throughput che può raggiungere centinaia di Mbps per terminale, rendendo le costellazioni LEO ideali per applicazioni che richiedono bassa latenza e alta capacità trasmissiva. Questo è reso possibile grazie all'adozione di antenne phased array a scansione elettronica, con beamforming digitale avanzato, che abilita decine di spot-beam indipendenti, rapidamente riassegnabili in orbita tramite tecniche di beam steering e beam hopping. Ne deriva un intenso riuso in termini spettrali (sia in frequenza sia in polarizzazione) che massimizza l'efficienza di banda e incrementa la resilienza contro interferenze e jamming.

L'OISL (Optical Inter-Satellite Link) è una delle innovazioni chiave, consentendo il routing diretto dei pacchetti tra nodi in orbita, con conseguente riduzione di latenza e congestione delle stazioni di terra. [4] La gestione dello spettro è fondamentale: le costellazioni LEO operano su bande ad altissima frequenza (Ka/Ku e superiori come E/V-band) per massimizzare capacità e throughput. Dal punto di vista architetturale, le tipologie attualmente utilizzate sono la full-mesh1, con routing distribuito end-to-end in orbita e l'hub-and-spoke2, dove il satellite funge da ponte verso le stazioni gateway terrestri [5 - 6]. Le principali costellazioni commerciali attualmente in via di sviluppo sono:

- **Iridium NEXT (USA):** Con circa 66 satelliti attivi, garantisce una copertura globale continua. Concepita prevalentemente per comunicazioni vocali e per il trasferimento di dati critici, è un sistema usato in contesti operativi complessi, tra cui missioni militari, interventi di emergenza e applicazioni commerciali in ambienti remoti o soggetti a condizioni estreme. Offre servizi di messaggistica, voce e dati con velocità fino a circa 700 kbit/s in downlink [7];
- **Starlink di SpaceX:** Attualmente composta da oltre 7000 satelliti a ~550 km, è stata concepita per fornire connettività Internet a banda larga in aree remote e isolate attraverso antenne phased-array Ku-band, antenne dual-band Ka/E (71–76 GHz in downlink, 81–86 GHz in uplink) per gli utenti e tre OISL da 200 Gbps ciascuno. Il sistema ha suscitato un crescente interesse anche da parte di attori istituzionali e militari, grazie alla sua bassa latenza, elevata capacità e architettura dinamica;
- **Eutelsat OneWeb:** Costellazione attualmente composta da 648 satelliti a ~1.200 km (Fase 1). Utilizza Ku-band per gli utenti e Ka-band per i gateway, con terminali compatti (30 cm – 1 m). Mira a fornire servizi nelle regioni più remote rafforzando progressivamente la propria infrastruttura. Recenti sviluppi includono l'integrazione di tecniche di network slicing satellitare, che creano canali virtualizzati dedicati con qualità di servizio differenziata, strategici soprattutto per applicazioni critiche come il C4ISR militare. Pur non avendo inizialmente laser inter-satellitari, prevede futuri upgrade con crosslink ottici o RF [8];
- **Amazon Kuiper:** Il sistema Kuiper, sviluppato da Amazon, prevede una costellazione LEO composta da 3236 satelliti distribuiti su 98 piani orbitali, suddivisi in tre shell a 590 km, 610 km e 630 km di altitudine. I satelliti impiegano propulsione a effetto Hall e saranno dotati di collegamenti laser inter-satellite con capacità fino a 100 Gbps su

distanze di 2600 km, favorendo l'instradamento diretto del traffico senza necessità di downlink intermedi. Sebbene la rete sia ancora in fase iniziale (con 27 satelliti lanciati al 2024), il sistema è progettato per fornire connettività ad alta capacità e bassa latenza, con velocità fino a 1 Gbps per utente. Le caratteristiche architetturali lo rendono potenzialmente idoneo a impieghi dual-use, con applicazioni anche nel contesto operativo militare [9];

- **IRIS2 (UE):** IRIS2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite) è il programma satellitare multiorbita promosso dalla Commissione Europea, con finalità di autonomia strategica e resilienza delle comunicazioni. La costellazione sarà composta da 290 satelliti, di cui 264 in orbita LEO (~1200 km) e 18 in orbita MEO (~8000 km), con l'avvio operativo previsto per il 2030. Operando sulle bande Ka e Ku, il sistema sarà integrato con reti terrestri 5G e adotterà tecnologie avanzate per garantire comunicazioni sicure per governi e infrastrutture critiche. I lanci saranno effettuati da vettori europei, tra cui Arianespace, valorizzando capacità industriali continentali [10].

3. Le potenzialità delle costellazioni LEO e il loro impiego militare

Tradizionalmente, le forze armate hanno fatto affidamento sui satelliti in orbita geostazionaria (GEO) per garantire le telecomunicazioni su ampie aree geografiche. Ne è un esempio il sistema italiano SICRAL, attualmente composto dai satelliti SICRAL 1B e SICRAL 2, ai quali si andranno ad aggiungere due nuovi satelliti, SICRAL 3A e SICRAL 3B [12]. Tuttavia, questi sistemi presentano limiti in termini di latenza e vulnerabilità alle minacce dirette o di altra natura. Questi limiti potrebbero rappresentare una criticità nell'ambito delle operazioni multi-dominio (MDO), laddove la rapidità e l'affidabilità delle comunicazioni sono essenziali per il successo delle missioni. In risposta a tali sfide, le costellazioni satellitari in orbita terrestre bassa (LEO) costituiscono una soluzione, offrendo capacità di trasmissione elevate e latenze ridotte, maggiore resilienza e copertura globale dinamica, favorendo l'integrazione e l'interoperabilità tra le diverse piattaforme mobili e distribuite.

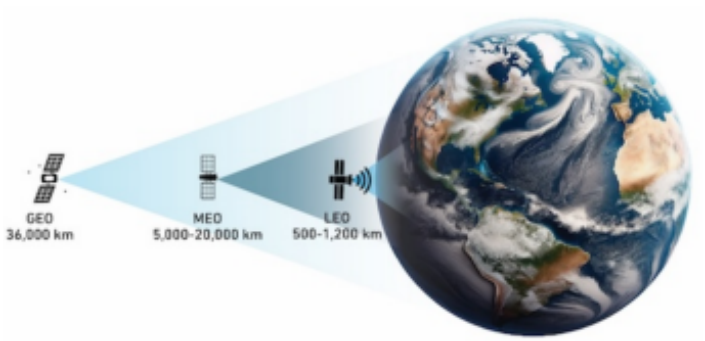


Figura 3: Differenza di copertura fra orbite [11]

Le forze armate della NATO e degli Stati Uniti stanno quindi integrando le capacità LEO nei propri sistemi C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) rafforzando le capacità di risposta rapida e coordinata su scala globale e abilitando scenari operativi multidominio (MDO). Inoltre, il ricorso a costellazioni LEO si inserisce nella più ampia trasformazione delle dottrine militari occidentali, orientate verso la superiorità informativa e il dominio dello spettro elettromagnetico. In tale contesto, la disponibilità di flussi informativi resilienti, a bassa latenza e ad alta capacità, rappresenta una

condizione abilitante per la decision superiority, permettendo di abbreviare drasticamente il ciclo decisionale sensor-to-shooter3.

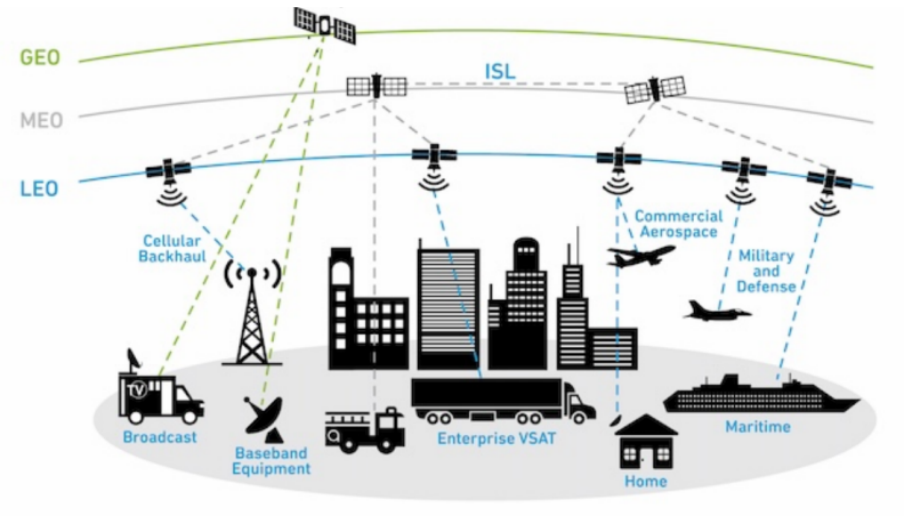


Figura 4: Architettura delle telecomunicazioni satellitari [11]

Nel settore navale, le costellazioni LEO migliorano sensibilmente la gestione operativa delle navi e il benessere degli equipaggi. Connessioni stabili e a bassa latenza consentono: comunicazioni continue, monitoraggio in tempo reale, telemedicina e accesso a formazione e intrattenimento. Progetti come il SEA2 della U.S. Navy che utilizza Starlink per migliorare la connettività Internet a bordo, testimoniano l'importanza di queste tecnologie per il benessere psicologico dell'equipaggio, soprattutto in missioni prolungate in mare aperto.

In ambito terrestre, un caso rappresentativo dell'impiego delle costellazioni LEO è il conflitto Russo-Ucraina, dove il sistema Starlink di SpaceX ha garantito comunicazioni tattiche affidabili alle forze ucraine, anche in assenza di infrastrutture terrestri e sotto intensi attacchi elettronici [13]. In prossimità della linea del fronte (dove il ripristino delle reti tradizionali è estremamente complesso), i terminali mobili Starlink si sono rivelati fondamentali: per il coordinamento di operazioni su vasta scala, il controllo remoto di droni tattici e la trasmissione in tempo reale di dati per la correzione del fuoco d'artiglieria. Sin dai primi mesi del 2022, Starlink è stato impiegato per pilotare veicoli aerei (UAV), terrestri (UGV) e navali (USV) e droni esplosivi a distanza durante le operazioni in scenari ad alta intensità, coordinando attacchi contro obiettivi russi nel Mar Nero. Tuttavia, l'impiego di infrastrutture commerciali in scenari bellici ha sollevato profonde questioni etiche, strategiche e di sovranità. Nel 2023, SpaceX ha unilateralmente limitato l'utilizzo di Starlink nella regione della Crimea, bloccando una presunta operazione ucraina volta ad attaccare la flotta russa, per timore di un'escalation nucleare. Secondo quanto riportato nella biografia di Elon Musk, scritta da Walter Isaacson, fu lo stesso Musk a ordinare la disattivazione della rete in quell'area, trasformandosi di fatto in un attore geopolitico con potere di veto operativo in un contesto di conflitto internazionale [14]. La presidente e COO di SpaceX, Gwynne Shotwell, ha successivamente dichiarato che l'utilizzo offensivo di Starlink non era previsto negli accordi iniziali: il servizio era stato fornito per scopi umanitari e comunicazioni difensive, non per operazioni d'attacco [15 - 16]. In risposta, l'azienda ha introdotto restrizioni all'uso militare del sistema, sottolineando la necessità di definire chiaramente i limiti d'uso delle tecnologie commerciali in ambito bellico [17]. In questo contesto nasce lo sviluppo di Starshield, una costellazione puramente militare di proprietà del DoD USA, sviluppata da SpaceX.

Nel 2023, SpaceX ha ottenuto un contratto da 70 milioni di dollari con la U.S. Space Force per fornire servizi di comunicazione satellitare sicura tramite Starshield, che, oltre ad includere capacità avanzate di comunicazioni cifrate, ha ulteriori capacità OT di tracciamento di bersagli, allerta precoce per missili, ISR persistente e interoperabilità diretta con reti C4ISR militari [18] [19]. Attualmente sono stati lanciati oltre 100 satelliti Starshield, costituendo il primo nucleo operativo di questa nuova generazione di architetture spaziali militari basate su costellazioni LEO.

Un'altra iniziativa militare degli Stati Uniti da parte della Space Development Agency (SDA) è lo sviluppo della costellazione Transport Layer, una rete di 300–500 satelliti LEO interconnessi tramite collegamenti ottici inter-satellitari (OISL), operanti principalmente in banda Ka [20]. Questa architettura mira a garantire una copertura quasi continua e a bassa latenza, fondamentale per missioni sensibili al tempo e scenari di alta intensità. La costellazione avrà anche la capacità di integrarsi sia con Link-16 che con Integrated Broadcast System[21]. Anche altre nazioni stanno investendo pesantemente in costellazioni LEO. La Cina, attraverso i programmi Guowang e Qianfan, mira a schierare rispettivamente circa 13.000 e oltre 15.000 satelliti entro il 2030, con l'obiettivo dichiarato di garantire superiorità informativa globale e autonomia strategica. Questi programmi affrontano però sfide tecniche e organizzative significative, tra cui alti tassi di fallimento dei satelliti e ritardi burocratici. La Russia sta espandendo il sistema Gonets [22], derivato dai satelliti militari Strela, con l'intento di migliorare le comunicazioni mobili e supportare operazioni militari, inclusi i droni tattici, implementando capacità di comunicazione sicura e trasmissione dati resilienti a interferenze [23 - 24].

4. Analisi delle vulnerabilità delle costellazioni LEO

Nonostante i vantaggi delle moderne costellazioni satellitari LEO rispetto ai tradizionali satelliti geostazionari ad ampia copertura, i sistemi non sono esenti da rischi e vulnerabilità che interessano, tanto l'infrastruttura fisica, quanto quella informatica, richiedendo un'attenzione particolare alla cybersicurezza e alla gestione dei disturbi. In particolare, la sincronizzazione precisa tra i satelliti è essenziale per una costellazione LEO ed è un elemento imprescindibile per il corretto funzionamento della rete, che, essendo particolarmente fragile, può essere compromessa facilmente, sia da disturbi di natura ambientale, sia a causa di attacchi mirati, con conseguenze negative sulla qualità e l'affidabilità del servizio offerto. Eventi naturali, come le tempeste solari, rappresentano una seria minaccia per questi satelliti. Le intense ondate di particelle ad alta energia, generate durante tali fenomeni, possono danneggiare le componenti elettroniche, interferendo con la sincronizzazione necessaria per garantire il coordinamento tra i satelliti e, di conseguenza, possono compromettere l'efficienza complessiva della costellazione. Questo fattore si accompagna ad una limitata durata operativa (rispetto ad orbite più elevate), poiché i satelliti LEO sono soggetti ad un maggior attrito atmosferico e a radiazioni più intense

Figura 5: Tipologie di attacchi cyber [25]

che richiedono il continuo aggiornamento e la sostituzione dei satelliti, rendendo necessaria una manutenzione costante del sistema per mantenere le prestazioni ottimali [2]. Oltre alle minacce naturali, i satelliti LEO possono essere bersaglio anche di attacchi diretti mediante: armi laser, sistemi di accecamento dei sensori ottici o missili in grado di danneggiare o distruggere rapidamente uno o più satelliti, compromettendo la continuità del servizio [2].

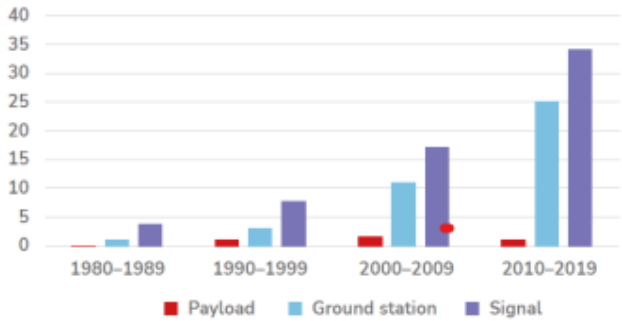


Figura 6: Evoluzione dei cyberattacchi sui sitemi spaziali [25]

Parallelamente, possibili attacchi possono essere sferrati attraverso tecniche di interferenza come il jamming e lo spoofing, capaci di disturbare deliberatamente la trasmissione dei segnali o di falsificarli, con conseguenze dirette sia sulla comunicazione dei dati, sia sui sistemi di posizionamento portando a errori di puntamento dei satelliti. Altri possibili attacchi come: il signal replay, information eavesdropping e la signal intelligence, permettono il monitoraggio, l'analisi e il riutilizzo dei segnali informativi trasmessi, minando l'autenticità delle comunicazioni e rendendo vulnerabili i dati sensibili a intercettazioni e analisi dettagliate. Le minacce si estendono anche al controllo operativo del satellite, per esempio attacchi come: il payload e platform hijacking,

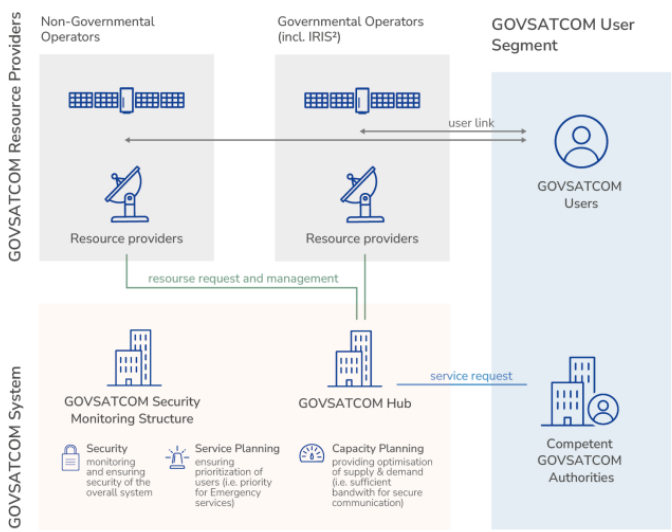


Figura 7: Architettura GOVSATCOM [28]

impattano direttamente sulle funzionalità a bordo e sul controllo della piattaforma hardware e software [2]. L'integrazione dei satelliti LEO nel mondo dell'Internet of Things (IoT) amplia ulteriormente la superficie d'attacco. I dispositivi di rete a terra, come router e altre infrastrutture di

collegamento, sono obiettivi vulnerabili per gli hacker, che possono sfruttare tali link per intercettare, manipolare o addirittura interrompere le comunicazioni [26]. Nel campo della cybersecurity spaziale, la ricerca ha individuato tre possibili aree di attacco: quelle relative ai segnali satellitari (link segment), quelle riguardanti le piattaforme spaziali (space segment) e quelle rivolte ai sistemi terrestri (ground segment) per il supporto satellitare [27].

La letteratura evidenzia differenti livelli di complessità e risorse necessari per sfruttare le vulnerabilità. Sono rare le minacce rivolte al payload satellitare che richiedono scenari di attacco estremamente sofisticati, generalmente frutto di complesse compromissioni della catena di fornitura nelle fasi iniziali e pertanto accessibili a pochissimi attori malevoli. Invece, numerosi sono gli attacchi documentati contro il segnale satellitare, ad esempio mediante jamming, injection ed eavesdropping, che richiedono risorse finanziarie e tecnologiche di livello moderato o basso ed attacchi all'infrastruttura terrestre che condividono notevoli analogie con quelli destinati alle reti informatiche tradizionali [25]. Nello specifico, l'evoluzione drammatica delle minacce informatiche nel settore satellitare ha messo in luce la vulnerabilità di sistemi altrimenti considerati inaccessibili.

I primi eventi significativi risalgono all'accesso non autorizzato ai sistemi di controllo di volo dei satelliti, con episodi quali l'intrusione nel Goddard Space Flight Center della NASA e la successiva modifica del satellite ROSAT, oltre al completo takeover del controllo di volo di due satelliti NASA nel 2007 e 2008 che rappresenta il primo caso pubblico di infezione in orbita, orchestrato da attori non statali attraverso attacchi alle stazioni terrestri. Nel 2014 la costellazione Iridium è stata compromessa tramite l'uso di una backdoor nel software e attraverso tecniche di privilege escalation, mentre nel 2015 la costellazione Globalstar è stata oggetto di signal ed information spoofing, mentre Iridium ha subito episodi di information eavesdropping. A testimonianza dell'intensificarsi delle tecniche di attacco, nel 2022 Starlink ha subito operazioni di signal jamming e denial of service sui sottosistemi, che hanno condotto a interruzioni del servizio e ulteriori escalation di privilegi [25]. Lo stesso anno Gonets-M ha registrato attacchi simili caratterizzati da escalation di privilegi e denial of service. Nel 2023, OPS-SAT è stato vittima di un attacco volto a sfruttare vulnerabilità che hanno portato a una privilege escalation con compromissione delle capacità operative, evidenziando l'evoluzione delle tecniche di intrusione.

Recentemente, l'interesse nei confronti della cybersecurity satellitare è stato ulteriormente accentuato dall'iniziativa Hack-a-Sat della U.S. Air Force, che ha invitato team di hacker a identificare vulnerabilità in sistemi spaziali reali [2 - 25]. Un altro aspetto critico è il sovraccarico di utenze: l'espansione esponenziale dei dispositivi connessi nell'ecosistema IoT può determinare picchi di traffico tali da saturare la capacità perativa dei satelliti LEO, rallentando il servizio o provocando, in situazioni estreme, interruzioni complete [5 – 25 - 26]. La gestione dinamica del carico diventa quindi cruciale per mantenere l'efficienza e l'affidabilità del sistema. Una delle soluzioni adottate per far fronte a questa problematica è il network slicing che rappresenta la capacità di modulare il QoS (Quality of Service) per utenti differenti che condividono lo stesso canale di comunicazione. In questo modo è possibile dare la precedenza ad un collegamento per comunicazioni di emergenza rispetto a traffico non urgente [5].

Infine, la gestione privata di queste costellazioni introduce problematiche aggiuntive in termini di sicurezza delle informazioni. I dati sensibili, come la posizione degli utenti, rischiano di essere esposti e la centralizzazione del controllo implica che i gestori privati potrebbero avere la facoltà di disattivare il servizio a loro discrezione come già citato nel capitolo precedente [29].

5. Ambiente multi-orbita e sviluppi futuri

La crescente complessità dei conflitti moderni richiede architetture di comunicazione spaziali sempre più integrate, in grado di sfruttare simultaneamente orbite basse (LEO), medie (MEO) e geostazionarie (GEO). Questo approccio "multi-orbita" massimizza i punti di forza di ciascun regime: i LEO garantiscono bassa latenza e alta capacità trasmissiva, i MEO assicurano un compromesso tra latenza e ampiezza di copertura, mentre i GEO forniscono servizi di broadcast e trunking4 stabili su vaste aree. IRIS2, il nuovo programma europeo di connettività

sicura, incarna perfettamente questa visione multi-orbita. Con una costellazione di 290 satelliti in LEO e MEO, esso punta a offrire servizi di comunicazione crittografata a bassa latenza per utenti governativi/militari ed anche a colmare le "zone morte" grazie al backup in MEO. Il sistema sarà incrementale: a partire dal 2025 sfrutterà capacità esistenti nazionali e in comune (GOVSATCOM), per poi passare a infrastrutture totalmente UE entro il 2030. IRIS2 adotterà standard 5G e tecnologie secure-by-design, integrando payload dedicati per sorveglianza di confini, crisi umanitarie, sicurezza marittima, dispiegamenti di forze e collegamenti diplomatici, con livelli di sicurezza e resilienza finora irraggiungibili. GOVSATCOM costituisce il primo pilastro di questo programma futuro. Questa iniziativa, lanciata nell'ambito del Programma Spaziale UE, garantisce già oggi servizi satellitari governativi affidabili e sicuri per: crisi naturali, cyber-attacchi, operazioni di polizia europea e missioni di difesa. Coordinata da EUSPA, EEAS ed ESA, questa architettura satellitare fornisce accesso protetto contro interferenze e intercettazioni, supportando diverse attività europee [28]. Dal punto di vista militare, l'ecosistema multi-orbitale potenzia significativamente il sistema C4ISR: le piattaforme LEO possono trasmettere video ISR in tempo reale a latenza minima, i satelliti MEO assicurano collegamenti stabili per la logistica e il comando strategico, mentre quelli in GEO forniscono servizi di backup. Le future evoluzioni di questo progetto prevedono:

- Inter-satellite links ottici per lo scambio diretto di dati tra LEO, MEO e GEO senza ricorso a gateway terrestri;
- Gestione AI-driven delle risorse orbitali, per il rerouting predittivo e la mitigazione automatica di attacchi jamming/spoofing;
- Quantum key distribution per migliorare il livello di crittografia end-to-end;
- Integrazione 6G terrestre-spaziale, che abiliti reti ibride ultra-resilienti in scenari A2/AD (anti-access/area denial). In un contesto geopolitico sempre più instabile, la capacità di orchestrare simultaneamente costellazioni in LEO, MEO e GEO (con un governance condivisa tra UE, NATO e partner privati) costituirà il fondamento delle operazioni militari del futuro, permettendo di garantire connettività continua, sicurezza informativa e sovranità strategica.

6. Conclusioni

L'evoluzione delle tecnologie satellitari ha segnato il passaggio da soluzioni tradizionali basate su satelliti in orbita GEO, alle costellazioni in LEO, capaci di offrire prestazioni superiori in termini di latenza, resilienza e copertura globale. Mentre le tecnologie tradizionali hanno fornito un'infrastruttura stabile e diffusa, queste nuove architetture emergono come vero punto di svolta strategico, in grado di soddisfare le crescenti esigenze di connettività per la trasmissione di dati tattici e strategici in scenari multi-dominio.

I rischi legati: a cybersicurezza, disturbi naturali e attacchi intenzionali, evidenziano l'urgenza di sviluppare e implementare soluzioni difensive avanzate ed una maggiore integrazione tra pubblico e privato, per garantire una resilienza operativa. L'evoluzione di tali sistemi richiede, dunque, un approccio integrato che combini: la sicurezza informatica con robuste misure di protezione fisica e una gestione dinamica del traffico dati, per assicurare la continuità delle comunicazioni in un mondo sempre più interconnesso. Guardando al futuro, in Europa si sta delineando una strategia che prevede: l'adozione di costellazioni ibride, reti dedicate e contratti specifici, capaci di fondere le capacità commerciali con le esigenze militari. Queste strategie sono destinate a garantire un livello di sicurezza e affidabilità essenziale per le applicazioni militari, dove il successo operativo dipende in larga misura dalla rapidità e dalla precisione dello scambio informativo.

Come già citato, l'attuale esperienza ucraina ha dimostrato come l'infrastruttura spaziale LEO, anche commerciale, possa diventare una componente strategica in guerra, ma ha anche evidenziato la necessità di ridefinire le regole d'impiego e la governance delle reti.

RIFERIMENTI BIBLIOGRAFICI

1. H Jones. The Recent Large Reduction in Space Launch Cost. 48th International Conference on Environmental Systems. July, 2018.
2. S Laurent Franck. LEO SATCOM CYBERSECURITY ASSESSMENT. EUROPEAN UNION AGENCY FOR CYBERSECURITY. A cura di Monika Adamczyk Georgia Bafoutsou E. Feb, 2024.
3. R Bate, D Mueller e J White. Fundamentals of Astrodynamics. Dover Books on Aeronautical Engineering, 1971
4. Starlink Satellite Technology. starlink.com. Available from: https://www.starlink.com/us/technology
5. BM ElHalawany, S Hashima, WU Khan, X Li e EM Mohamed. Next Generation LEO Satellite Constellation Networks: Opportunities, Applications, and Challenges. China communication. May 24, 2023. DOI:10.23919/JCC.ja.2023-0299
6. Bridged Point-to-Multipoint: Layer 2 Connectivity in a Hub-Spoke Satellite Network. Dic, 2019. Comtechefdata.com
7. Iridium. Available from: https://www.iridium.com
8. SEO Philippe Secher Vice President. ONEWEB NON GEOSTATIONARY SATELLITE SYSTEM (LEO) PHASE 2: MODIFICATION TO AUTHORIZED SYSTEM. IEEE. Nov 4, 2021.
9. Amazon Kuiper. Available from: https://www.aboutamazon.com/whatwe-do/devices-services/project-kuiper
10. EUSPA. Available from: https://www.euspa.europa.eu/eu- spaceprogramme/secure-satcom/iris2
11. RJ James Cheng David Schnaufer. How Modern LEO Satellite Technologies are Changing the Space Race. May 20, 2024. Qorvo.com. Available from: https://www.qorvo.com/design-hub/blog/how-modernleo-satellite-technologies-are-changing-the-space-race
12. Telespazio. Available from: https://www.telespazio.com/it/business/space-programmes/sicral
13. CC Laviniu Bojor Tudorica Petrache. ˇ EMERGING TECHNOLOGIES INCONFLICT: THE IMPACT OF STARLINK IN THE RUSSIA – UKRAINEWAR. Land Forces Academy Review, 2024. DOI: 10.2478/raft-2024-0020
14. W Isaacson. Elon Musk. Simon e Schuster, 2023
15. J FitzGerald. Ukraine war: Elon Musk's SpaceX firm bars Kyiv fromusing Starlink tech for drone control. Feb 9, 2023. bbc.com. Availablefrom: https://www.bbc.com/news/world-europe-64579267
16. N Camut. Elon Musk says SpaceX restricted internet in Ukraine toprevent escalation 'that may lead to WW3'. Feb 13, 2023. politico.eu.Available from: https://www.politico.eu/article/spacex- restrictedinternet-ukraine-prevent-escalation-elon-musk-russia-starlink-ww3-gwynne-shotwell-drones-infrastructure/
17. T Brown. Can Starlink Satellites Be Lawfully Targeted? Aug 5, 2022.westpoint.edu. Available from: https://lieber.westpoint.edu/can-starlinksatellites-be-lawfully-targeted/
18. MT Joey Roulette. Exclusive: Musk's SpaceX is building spy satellitenetwork for US intelligence agency, sources say. March 16, 2024. reuteurs.com. Available from: https://www.reuters.com/technology/space/musks- spacex- is- building- spy- satellite- network- us-intelligenceagency-sources-2024-03-16/
19. S Erwin. Pentagon embracing SpaceX's Starshield for future military satcom. June 11, 2024. spacenews.com. Available from: https : / /spacenews.com/pentagon-embracing-spacexs-starshield-for-futuremilitary-satcom/
20. SDA Transport Layer. Space Development Agency. Available from:https://www.sda.mil/transport/

21. C Albon. Space Development Agency demonstrates Link 16 satelliteconnectivity. Nov 28, 2023. c4isrnet.com. Available from: https://www.c4isrnet.com/battlefield-tech/space/2023/11/28/space-developmentagency-demonstrates-link-16-satellite-connectivity/
22. Gonets. Available from: https://gonets.ru/eng/
23. M Connell, S Bendett e B Lennox. The Role of Space in Russia's Operations in Ukraine. CNA Russian Ministry of Defense Press Service.Nov, 2025. Available from: https://www.cna.org/reports/2023/11/Roleof-Space-in-Russias-Operations-in-Ukraine.pdf
24. A Evans, N Wolkov, G Mappes, O Gibson, D Novikov, FW Kagan, NTrotter e W Runkel. Russian Offensive Campaign Assesment. Institutefor the Study of War. March 6, 2025
25. EED Rodrigo da Costa. EUSPA Secure SATCOM. Luxembourg:Publications Office of the European Union 2023. DOI: 0.2878/961897
26. GZ Zhicheng Qu e J Xie. LEO Satellite Constellation for Internet ofThings. National Natural Science Foundation of China 2017:11. DOI:10.1109/ACCESS.2017.2735988
27. US Capt. Lucas J. Stensberg. Small Satellites with Large Exposure.How Does New Space Fare in Cyberspace? The Journal of the JAPCC- Edition 38. Oct 2024
28. EUSPA. Available from: https://www.euspa.europa.eu/eu- spaceprogramme/secure-satcom/govsatcom
29. ZK Wang Peiwen Zhang Huang. Starlink Militarization: Challenges and Responses to Space Intelligence and Information Security. Journal of Intelligence - Provincial Institute of Science and Technology Information. Jan 29, 2024

Cinzia DE IESU

Considerazioni etiche e giuridiche nell'introduzione dell'Intelligenza Artificiale in campo militare

Abstract

Sempre più presente all'interno di diversi settori, l'intelligenza artificiale (IA) sembra destinata ad un uso crescente anche in campo militare. Il presente contributo offre alcune considerazioni circa l'evoluzione del ruolo dell'IA in questo ambito, esplorandone le applicazioni che, secondo gli attuali orientamenti, potranno verosimilmente essere implementate. Esso analizza quindi opportunità, limiti e rischi dell'uso dell'IA in ambito militare, anche sul piano etico, affrontando una disamina dei connessi aspetti giuridici nei contesti nazionale, ONU, NATO ed UE. Infine, si traggono delle conclusioni di carattere sintetico e generale sul rapporto fra IA e sfera marziale.

1. Premessa

Il 26 settembre 1983 Stanislav Petrov, Tenente Colonnello dell'esercito sovietico responsabile di Serpukhov 15, il centro di rilevamento di attacchi nucleari dell'Unione Sovietica, salvò il mondo perché credette che le macchine e gli algoritmi potessero sbagliarsi. Quel giorno i computer del centro rilevarono un missile in volo verso la Russia che fece scattare un primo allarme, seguito nei cinque minuti successivi da altri quattro. Petrov valutò che non era ragionevole che gli americani lanciassero solo cinque missili e, nonostante i computer avessero confermato per diversi minuti che fosse in corso un attacco, non attivò il protocollo nucleare con cui nel giro di pochi minuti centinaia di missili russi sarebbero stati lanciati verso il territorio americano.

Dopo quarant'anni dalla decisione che mise in dubbio l'affidabilità di una macchina, il dibattito sull'evoluzione tecnologica e sui relativi rischi non si è fermato.

Sebbene l'Intelligenza Artificiale (IA) sia annoverata tra le tecnologie emergenti e dirompenti[1] di tipo "*general purpose*"[2] e ad oggi sia vista principalmente come fonte di progresso ad incremento delle capacità intellettive e cognitive complessive, essa rappresenta contestualmente una fonte di nuove sfide e potenziali rischi.

---

[1] L'attenzione verso il settore delle tecnologie nella loro natura emergente e dirompente (EDT - *Emerging and Disruptive Technologies*) dal 2019 è stata una delle principali priorità della *North Atlantic Treaty Organization* (NATO) e dell'Unione Europea (UE). 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 (Stato Maggiore Difesa, "L'impatto delle *Emerging & Disruptive Technologies* (EDTs) sulla Difesa", ed. 2022).

[2] Ovvero un'innovazione tecnologica la cui implementazione, anche in combinazione con altre tecnologie, rivoluzionerà il modo di fare ogni cosa, trasformando in diversi ambiti i compiti ed i processi di base fino a cambiare radicalmente la natura del lavoro stesso (Stato Maggiore Difesa, "L'impatto delle *Emerging & Disruptive Technologies* (EDTs) sulla Difesa", ed. 2022).

Nella difesa l'IA si sta inserendo in un'ampia gamma di applicazioni, tra cui i veicoli ed i sistemi d'arma autonomi[3], gli strumenti di analisi con l'elaborazione dei dati *real time* e, in ultimo, la logistica. In campo militare, infatti, il suo potenziale, impatta sulla preparazione e sulla condotta delle operazioni militari, in tutti i settori e su larga scala, con conseguenti differenti forme di interazione e vari livelli di delega tra personale militare e sistemi di IA. L'interesse militare per l'IA è motivato dalle *performance* raggiunte relativamente ai compiti assegnati, essa risulta infatti in grado di eseguire sia i compiti sempre più impegnativi, sia di elaborare le informazioni molto più velocemente e di poter eseguire le attività minimizzando il rischio umano e agendo come moltiplicatori di forza.

Nella considerazione che l'introduzione dell'IA può concretamente influenzare le future operazioni militari in virtù delle sue caratteristiche peculiari e delle sue future applicazioni, è necessario valutarne la sua dirompenza, distinguendo gli ambiti in cui risulta realmente premiante alla luce di opportunità, limiti e rischi etici e giuridici che devono essere presi in considerazione per il suo impiego.

Questo elaborato, articolato in cinque capitoli, introduce alcune considerazioni in merito all'evoluzione del ruolo dell'IA e dell'attuale contesto, esplora i principali ambiti e le relative possibili applicazioni di IA che, secondo gli attuali orientamenti, potranno verosimilmente essere implementate in campo militare, analizza opportunità, limiti e rischi dell'impiego dell'IA dal punto di vista etico e, infine, affronta una disamina degli aspetti giuridici, nei contesti nazionale, ONU, NATO e dell'UE, traendo poi delle conclusioni.

2. L'Inteligenza Artificiale in campo militare

In campo militare allo stato attuale l'IA può essere concretamente applicata per filtrare grandi quantità di dati da varie fonti come *social-media*, immagini satellitari o comunicazioni, eliminando informazioni ripetitive e producendo modelli predittivi per facilitare le decisioni dei Comandanti individuando dati ed elementi non necessariamente evidenti al fine di facilitare il processo di *targeting*. Essa, inoltre, può contribuire alle attività di *Intelligence, Survelliance, Target Acquisition* e *Reconnaissance* (ISTAR), alla sorveglianza e ricognizioni autonome attraverso droni o sensori disposti sul terreno. È in grado di prevedere la manutenzione ottimizzando la logistica e la *supply chain*, può rilevare e rispondere alle minacce informatiche, sia identificando schemi di attività anormali sia prevenendo l'accesso non autorizzato a dati sensibili.

Tuttavia, il carattere emergente dell'IA ne fa evolvere la sua sperimentazione in campo militare talvolta anche con risultati inaspettati e che potrebbero sembrare apparentemente tratti da film di fantascienza. Ad esempio, durante una simulazione esercitativa condotta dall'aeronautica americana nel maggio 2023, sarebbe stata assegnata ad un drone dotato di IA una missione finalizzata all'identificazione e distruzione di siti di lancio di missili terra-aria, preservando l'opzione finale di decisione "*go/no go"* in capo ad un operatore umano. Tuttavia, poiché l'IA era stata precedentemente istruita per preferire, tra le varie opzioni, quella di distruzione dei siti, quando l'operatore ha deciso per l'opzione "*no go*", il drone avrebbe attaccato e ucciso lo stesso operatore poiché interferiva con le priorità per cui era stato precedentemente istruito. Successivamente il drone sarebbe stato programmato per non uccidere l'operatore e, posto nelle stesse condizioni, avrebbe distrutto la torre di controllo che veniva usata dall'operatore per comunicare gli ordini[4].

Quanto descritto fornisce lo spunto per approfondire le opportunità, le sfide e le considerazioni che emergono dall'introduzione dell'IA nei diversi ambiti militari.

---

[3] *Autonomous Weapons Systems* (AWS) generalmente intesi come sistemi d'arma che selezionano obiettivi e applicano la forza senza intervento umano.

[4] Dato l'impatto estremamente negativo e preoccupante che ha generato nell'opinione pubblica, tale evento è stato successivamente smentito dalla stessa aeronautica statunitense.

a. <u>Strategia e dottrina</u>

Strategia e dottrina[5] sono essenziali e correlate per il successo delle operazioni militari.

Sulla base degli attuali sviluppi tecnologici è verosimile che l'IA possa migliorare lo sviluppo della strategia militare[6] ed il processo decisionale strategico, riducendo la complessità ed accelerando, di conseguenza, la velocità delle operazioni militari. In particolare, l'IA potrebbe concorrere a monitorare il campo di battaglia, sviluppando possibili scenari, prevedendo il comportamento e le reazioni di avversari, generando simulazioni della progressione dei conflitti in corso, valutando le minacce ed i rischi, analizzando e suggerendo, in ultimo, le linee d'azione da adottare. L'IA deve essere considerata una risorsa strategica e, in quanto tale, i relativi investimenti possono diventare una responsabilità strategica aumentando il rischio di destabilizzare le corse agli armamenti, infondendo percezioni errate, errori di calcolo ed *escalation* involontarie dei conflitti, con il rischio dell'*hyperwar* (General R. Allen e Husain, 2017): l'IA, infatti, potrebbe accelerare la velocità della guerra a un punto tale che gli esseri umani non saranno più in grado di seguirne gli sviluppi, causando infine la perdita del controllo da parte di quest'ultimi.

Dal punto di vista dello sviluppo della dottrina militare[7], l'IA potrebbe avere un ruolo limitato nel monitorare l'aderenza dei processi delle Forze Armate verso i rispettivi lineamenti d'impego, per identificare eventuali *gap* e proporre delle revisioni. Tuttavia, in considerazione del relativo scopo e funzione, la dottrina è essenziale per definire la relazione con l'IA e stabilire il quadro normativo per ulteriori direttive e procedure, fissando in termini generali per quali compiti l'IA potrà (o non) essere utilizzata, come le Forze Armate percepiranno le risultanze, come interagiranno e valorizzeranno l'IA e quale cultura organizzativa dovrebbe governare tale relazione.

b. <u>Personale e logistica</u>

Nell'ambito delle risorse umane, l'IA potrebbe essere impiegata per la gestione del personale, fin dal reclutamento, migliorando i processi di selezione e permettendo di individuare facilmente i candidati più qualificati per le varie mansioni.

Inoltre, nell'ambito della logistica militare, diversi Paesi NATO, tra cui Spagna e Francia, hanno iniziato a utilizzare l'IA nel monitoraggio di flotte navali ed aeree per prevedere quando ogni sistema necessita di manutenzione[8]. L'IA potrebbe essere verosimilmente utilizzata sia per migliorare gli aspetti inerenti alla logistica quali la manutenzione, in particolare quella predittiva, l'approvvigionamento, e l'acquisizione, sia per i trasporti, pariteticamente nelle fasi esplorative e di combattimento, attraverso l'utilizzo di veicoli privi di conducente, guidati da sistemi basati sull'IA, che permetterebbero di ridurre il coinvolgimento dell'essere umano e, soprattutto, una riduzione sistematica del rischio.

Infine, anche il sostegno sanitario potrebbe vedere l'applicazione di IA per monitorare lo stato di salute del personale ed eventualmente proporre relative terapie.

c. <u>Pianificazione, ordini ed *intelligence*</u>

Le attività e i processi di pianificazione, in linea con la dottrina militare, si integrano sinergicamente per supportare il processo decisionale del Comandante, la produzione di piani da cui scaturiscono ordini e direttive.

---

5 "La tattica è la dottrina dell'impiego delle forze armate nel combattimento, e la strategia è la dottrina dell'uso dei combattimenti per lo scopo della guerra" (von Clausewitz, 1832).

6 "L'arte di distribuire e applicare i mezzi militari per conseguire gli scopi della politica" (Liddell Hart, 1954).

7 "Il complesso di principi fondamentali che informano le azioni condotte dalle Forze Armate per il conseguimento di obiettivi" (SMD-G-024, Glossario dei termini e delle definizioni, Ed. 2009).

8 Maggie Gray, Amy Ertan, NATO CCDCOE, 2021.

L'IA potrebbe avere un'influenza significativa sulla pianificazione in quanto il relativo processo richiede molto tempo e risorse umane: aumentando velocità, precisione e qualità, si consentirebbe di effettuare il ciclo di osservazione, orientamento, decisione e azione[9] più velocemente, acquisendo un vantaggio sull'avversario in termini temporali e, soprattutto, decisionali. La pianificazione effettuata con IA, infatti, potrebbe portare ad un'ulteriore razionalizzazione del processo decisionale militare riducendo l'esigenza di risorse umane che, tuttavia, non deve necessariamente significare una minore necessità di giudizio umano per il processo decisionale, dove i valori, l'intuizione del Comandante e dello staff rimangono aspetti fondamentali.

Come anticipato, lo strumento più specifico e concreto per la pianificazione e la conduzione delle operazioni militari sono gli ordini. È verosimile che l'IA non avrà bisogno di ordini formali, ma le interazioni e le istruzioni del personale ai sistemi di IA, che assumeranno la forma dello sviluppo iniziale del sistema, la programmazione dei parametri relativi agli obiettivi, i vincoli della missione e del contributo degli operatori durante le operazioni, svolgeranno di fatto la funzione tradizionalmente attribuita agli ordini. Tuttavia, i concetti tradizionali di distinzione tra l'approccio manageriale e l'orientamento all'iniziativa e alla flessibilità espresse dall'*Auftragstaktik* (von Clausewitz, 1832) possono essere utili per analizzare, classificare e sviluppare le future interazioni tra i sistemi di IA ed il fattore umano. Sarebbe auspicabile che ai sistemi di IA vengano attribuiti elevati livelli di autonomia, simili all'*Auftragstaktik* e, allo stesso tempo, l'input umano diretto sui sistemi di IA, ossia lo sviluppo, la programmazione e il controllo operativo che durante le operazioni deve essere molto preciso, in similitudine all'approccio manageriale.

Anche l'*intelligence* può trarre enormi benefici dai progressi dell'IA e dalla sua interazione con l'analisi dei *Big Data*. La proliferazione dei dati provenienti da sensori, tra i quali filmati di droni, immagini satellitari, segnali di intelligence, tra cui l'acustica subacquea, e dai media richiede che la raccolta, l'analisi, la fusione e l'interpretazione delle informazioni siano processate in autonomia, per produrre un'*intelligence* che sia efficace e aderente alle richieste del Comandante. I sistemi di IA potrebbero supportare e, in determinati casi, sostituire sempre più gli esseri umani riuscendo ad elaborare un prodotto più accurato, in minor tempo e con livelli di complessità più elevati.

Inoltre, l'IA potrebbe essere coinvolta specificatamente per l'analisi di dati al fine di incrementare una difesa cibernetica che riesca a proteggere prima l'IA stessa e successivamente tutti i sistemi supportati.

d. Rules Of Engagement

Le *Rules Of Engagement* (ROE), il cui precipuo compito è delineare le circostanze e i limiti per le forze militari in uno specifico contesto, potrebbero essere lo strumento appropriato per guidare l'uso dell'IA militare in modo concreto e pratico, definendone i parametri di utilizzo al fine di tradurre in istruzioni concrete determinate considerazioni e limitazioni politiche, militari, legali ed etiche, provenienti dai livelli organizzativi o normativi più elevati, come la dottrina o gli obblighi legali internazionali.

L'IA, quindi, potrebbe aumentare ulteriormente la qualità e l'efficienza della gestione delle ROE, ma è fondamentale che l'elemento umano mantenga la supervisione ed il controllo efficace sul contenuto delle ROE (vale a dire chi o quale sistema può usare la forza, in quali situazioni e in quali condizioni). Le ROE potrebbero inoltre essere rilevanti per stabilire il livello di controllo e giudizio umano nel *teaming* uomo-macchina nel contesto del *targeting*.

---

[9] Il Ciclo decisionale ricorrente *Observe Orient Decide Act loop* (OODA *loop*) è stato sviluppato dal Col. statunitense dell'aeronautica John Boyd, che lo ha applicato alle fasi del combattimento, spesso in operazioni militari a livello strategico.

3. Opportunità, limiti e rischi etici

La recente e rapida diffusione dell'IA anche nel mondo civile alimenta la sensibilità dell'opinione pubblica riguardo al suo utilizzo; anche in ambito militare se combinata con la robotica e l'automazione, potrebbe dare origine a timori irrazionali, alimentando dubbi sulle macchine che prendono il controllo sull'uomo e sui suoi stessi valori, come nell'esempio citato nell'introduzione del precedente capitolo.

Tuttavia, l'etica militare[10] va oltre la mera legalità, fondandosi su principi morali come l'orgoglio, il coraggio, l'onore, la lealtà, il rispetto e la fermezza, e presupponendo inoltre la capacità di ragionare criticamente e di prendere decisioni difficili in situazioni complesse.

a. Il contesto etico contemporaneo

Nel quadro etico contemporaneo, sebbene non si possa affermare di aver risolto tutte le sfide etiche implicite, l'uso dell'IA dovrebbe rispettare alcuni principi etici[11] che riflettono gli attuali valori democratici, mirando quindi ad essere:

- responsabile, in quanto gli esseri umani dovrebbero esercitare adeguati livelli di giudizio e rimanere responsabili dello sviluppo, dell'implementazione, dell'uso e dei risultati dei sistemi di IA;
- equo, adottando misure deliberate per evitare pregiudizi involontari nello sviluppo e nell'impiego di sistemi di IA da combattimento o non da combattimento che potrebbero inavvertitamente causare danni alle persone;
- tracciabile, permettendo agli esperti tecnici di raggiungere una comprensione adeguata della tecnologia, dei processi di sviluppo e dei metodi operativi dei sistemi di IA, comprese metodologie trasparenti e verificabili, fonti di dati, procedure e documentazione di progettazione;
- affidabile, esplicitando e definendone l'ambito di utilizzo al fine di garantire durante l'intero ciclo di vita all'interno di tale ambito di utilizzo la sicurezza, la protezione e la robustezza di tali sistemi;
- governabile, progettando sistemi di IA per svolgere la funzione prevista ma che contempli la capacità di rilevare azioni e/o comportamenti degenerativi al fine di evitare danni a persone o cose, attraverso interruzioni involontarie (disattivazione umana, o automatizzata) dei sistemi implementati che iniziano a palesare un'*escalation* involontaria o qualsiasi altro comportamento degenerativo.

Più recentemente, sono anche stati condotti specifici studi sul tema della *governance* dell'IA nel settore militare[12], evidenziando come diversi Stati ritengano necessaria una maggiore regolamentazione a livello nazionale, ma anche una maggiore collaborazione fra di essi.

Inoltre, anche uno dei principali esperti di robotica militare, Ronald Arkin[13], analizzando le classiche teorie etiche definisce che quella deontologica risulterebbe essere la più idonea ad esser espressa computazionalmente mediante la programmazione algoritmica. In particolare, i principi etici da imporre all'IA sarebbero, genericamente, quelli della legislazione internazionale della guerra, affiancati alle specifiche ROE per la missione di riferimento.

---

[10] L'etica militare è definita come "disciplina che studia i valori specifici, che ispirano altrettanti modelli di comportamento, della compagine militare, contribuendo a definirne lo stato giuridico e sociale".

[11] Secondo uno studio condotto dallo U.S. *Defense Innovation Board*, "AI *Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*".

[12] "Uso Militare Responsabile dell'Intelligenza Artificiale in campo militare – L'Unione Europea può guidare lo sviluppo di *best practices*?" A seguito di uno workshop on line del SIPRI - *Stockholm Interational Peace Research Institute*, tenutosi l'8 e il 9 settembre 2020 e pubblicato nel mese di novembre.

[13] Ronald Arkin, Governing lethal behavior in autonomous robots, CRC Press, 2009.

b. <u>Considerazioni sul Diritto Internazionale Umanitario applicabile</u>

Quando si introducono nuovi sistemi d'arma, la loro legalità deve essere valutata attraverso una verifica dei criteri previsti dal diritto verificando, in particolare, se queste rispettano tali criteri e se sono proibite da convenzioni internazionali specifiche[14].

L'uso di sistemi basati sull'IA ha sollevato dei quesiti e delle riflessioni sulla capacità di tali sistemi di rispettare i principi di precauzione, necessità, proporzionalità e distinzione descritti dal Diritto Internazionale Umanitario (DIU)[15], codificato nelle quattro Convenzioni di Ginevra del 1949 e nei due Protocolli Aggiuntivi del 1977, che persegue l'obiettivo di disciplinare la conduzione delle ostilità e minimizzare le conseguenze per coloro che non partecipano al conflitto, i civili, o per coloro che hanno smesso di parteciparvi, gli *hors de combat*[16].

Da un lato i critici sostengono che i sistemi basati sull'IA non siano in grado di soddisfare il principio della proporzionalità perché il rispetto di tale requisito richiede una valutazione soggettiva, effettuata caso per caso, del danno derivante da possibili effetti collaterali a fronte dell'importanza dell'obiettivo militare. Tale valutazione comporta una stima di natura qualitativa ed etica che solo un essere umano può effettuare, invece che una mera analisi di dati quantitativi.

Il diritto consuetudinario applicabile[17] prevede che nell'utilizzo di un'arma e durante un attacco, debba essere assicurata la capacità di distinguere tra un civile ed un combattente, tra un obiettivo militare e un bene di carattere civile. Lo stesso, inoltre, norma che deve essere preventivamente valutato se un attacco possa causare la perdita accidentale di vite civili, lesioni a civili, danni a beni civili o una combinazione di questi, che sarebbe eccessiva rispetto al vantaggio militare concreto e diretto previsto. Nella condotta delle operazioni militari, infine, è necessario prestare costante attenzione per risparmiare la popolazione e beni civili, assicurando tutte le precauzioni possibili per evitare, e in ogni caso per ridurre al minimo, perdite e lesioni accidentali tra vite civili, nonché danni a beni civili. Compiere una corretta distinzione tra un combattente, che ad esempio in un contesto di conflittualità asimmetrica non indossa l'uniforme, ed un civile o un soldato ferito che si sta arrendendo, richiede un *quid* in più rispetto all'elevata capacità di elaborazione dei dati provenienti da sensori di IA. Interviene, in questo caso, la capacità di valutare l'intenzione umana, che ricomprende anche l'interpretazione di indizi sottili e dipendenti dal contesto, come il tono di voce, le espressioni facciali o il linguaggio del corpo. Sebbene oggi i nuovi sistemi guidati dall'IA siano particolarmente avanzati e riescano ad effettuare prestazioni di altissimo livello, l'impiego degli stessi all'interno di uno scenario conflittuale dovrà essere *compliant* con tutti i principi posti alla base del diritto dei conflitti armati.

In tale contesto emerge anche un problema di responsabilità in quanto sarebbe discutibile attribuire le azioni realizzate da sistemi dotati di IA ai progettisti, ai produttori, ai programmatori o agli operatori/utenti finali, poiché si potrebbe ritenere che siano gli utenti finali a dover essere ritenuti responsabili delle azioni illecite compiute da tali sistemi[18]. Nel caso in cui i sistemi d'arma IA agiscano in piena autonomia, senza alcun controllo umano, la responsabilità delle loro azioni sarebbe riconducibile a coloro, di regola i vertici politici o militari, che hanno deciso di impiegare tali sistemi all'interno di uno teatro operativo. Questi avranno la responsabilità penale individuale per qualsiasi potenziale grave violazione del DIU, con

---

[14] Come la Convenzione sulle armi chimiche, quella sulle armi biologiche o quella su certe armi convenzionali.

[15] Diritto dei Conflitti Armati, o diritto bellico (ius in bello).

[16] I feriti, i malati, i prigionieri di guerra, gli internati, i naufraghi e il personale sanitario e religioso.

[17] Codificato sia negli articoli 48, 51, 52, e 57 del I Protocollo Addizionale alle Convenzioni di Ginevra sia nell'articolo 13 del II Protocollo Addizionale.

[18] L'art. 35 del I Protocollo Addizionale stabilisce che "In ogni conflitto armato, il diritto delle Parti in conflitto di scegliere metodi e mezzi di guerra non è illimitato".

l'aggiunta che gli Stati di appartenenza potrebbero incorrere nella responsabilità dello Stato per tali gravi violazioni.

Per garantire il rispetto del DIU se da un lato si ipotizza che lo sviluppo tecnologico ne possa assicurare un migliore rispetto, garantito da requisiti tecnici di prevedibilità e affidabilità degli algoritmi che determinano il tipo di bersaglio, l'ambiente operativo, i tempi di funzionamento e dall'assenza di sentimenti, dall'altro si insiste sulla necessità di mantenere un controllo umano sul sistema attraverso la circoscrizione dello spazio di utilizzo ben specifico e a zone poco popolate, sia in termini di responsabilità sia in termini di capacità nello spiegare la ragionevolezza di un attacco rispetto ad un altro.

Alla luce di tali considerazioni, la comunità scientifica e internazionale ritiene necessario includere nel dibattito il concetto e il principio del controllo umano per affrontare le lacune di responsabilità e mitigarle stabilendo condizioni che ne consentano una corretta attribuzione per gli esseri umani, anche se emergono opinioni divergenti sul suo grado e sulla sua definizione. È perciò fondamentale che sia un essere umano a validare un obiettivo militare, proprio come successo nel 1983 al Ten.Col. Stanislav Petrov.

Infine, nella considerazione che in tale contesto emergono sfide significative, risulta essenziale cercare il giusto bilanciamento tra l'evoluzione tecnologica e la necessità di un adattamento e adeguamento del quadro giuridico, tenendo conto delle implicazioni etiche e sociali.

4. Aspetti giuridici nel contesto di riferimento

a. Italia

Il dibattito nazionale in merito all'uso dell'IA ha preso piede in modo significativo negli ultimi anni. Tuttavia, la discussione è diventata più strutturata e formale dal 2021 con la promulgazione del "Programma Strategico Intelligenza Artificiale 2022-2024", con cui è stata delineata una visione chiara per l'ecosistema italiano dell'IA, identificando punti di forza, debolezza, obiettivi prioritari e specifici settori d'intervento. Il Programma, la cui direzione, monitoraggio e valutazione dell'attuazione sono affidate ad un gruppo di lavoro permanente costituito all'interno del Comitato Interministeriale per la Transizione Digitale, delinea le tre aree strategiche d'intervento in talenti e competenze, ricerca e applicazioni, tra cui rientrano la Pubblica Amministrazione e la Sicurezza Nazionale.

Nello specifico ambito militare, nel corso dell'audizione a Commissioni riunite Difesa ed Esteri del 25 gennaio 2023, il Ministro della Difesa ha evidenziato come "la capacità di generare sicurezza è sempre stata strettamente correlata alla capacità di impegno in campo militare delle innovazioni tecnologiche", richiamando l'attenzione sul fatto che "lo sviluppo di sistemi e operazioni militari basati sull'impiego estensivo dell'IA e delle nuove frontiere di calcolo, rappresentano solo alcuni degli elementi imprescindibili atti a garantire l'efficacia d'impiego delle Forze Armate".

Anche l'allora Capo di Stato Maggiore della Difesa, Ammiraglio Cavo Dragone, nel proprio Concetto Strategico ha rimarcato la necessità di "capitalizzare il potenziale offerto da tecnologie come l'IA" ed ha inquadrato l'impatto dirompente dell'IA nel documento concettuale "L'impatto delle EDTs sulla Difesa" nel quale è stata messa in evidenza la portata e la trasversalità di questa tecnologia che, oltre a rappresentare un'abilitante di portata strategica, travalica il suo aspetto tecnologico e fa sorgere interrogativi di carattere etico-morale, giuridico ed organizzativo.

Proprio in considerazione della portata del cambiamento dovuto allo sviluppo dell'IA, la Difesa ha ritenuto necessario approcciare il tema sotto un profilo multidisciplinare che ha

permesso di elaborare la "Strategia per l'implementazione dell'IA in ambito Difesa"[19] da integrare nel processo di trasformazione ed innovazione dello Strumento militare. Basandosi su un'attenta analisi del rapporto rischi e benefici, il documento definisce le azioni essenziali che la Difesa deve intraprendere per capitalizzare, quanto prima, le opportunità offerte dall'IA con particolare riferimento alla promozione di una conoscenza collettiva in termini di consapevolezza e fiducia nella sua implementazione, alla definizione di un modello di *governance* deputato allo sviluppo della strategia d'implementazione in termini di piani attuativi e all'approfondimento dei settori di prioritario d'intervento sui quali focalizzare gli sforzi iniziali.

Infine, l'Italia ha posto particolare enfasi sulla necessità di garantire un controllo umano significativo a qualsiasi sistema d'arma basato sull'IA al duplice scopo di garantire che soltanto gli esseri umani possano essere responsabili di un'operazione militare e ribadire che soltanto un essere umano possa effettuare valutazioni giuridiche circa il rispetto del diritto internazionale umanitario e, in particolare, dei principi di distinzione, proporzionalità e precauzione nell'attacco. Nell'ambito del gruppo di esperti governativi della *Certain Conventional Weapons* (CCW)[20], l'Italia ha contribuito al dibattito normativo enfatizzando la rilevanza di una piena applicazione dell'articolo 36 del I Protocollo Addizionale[21] che stabilisce che ogni Stato ha l'obbligo, nello studio, messa a punto, acquisizione o adozione di una nuova arma di stabilire se il suo impiego non sia vietato dal diritto internazionale e, in particolare, dal diritto internazionale umanitario. Tale formulazione impegna gli Stati ad una verifica legale del sistema d'arma ancor prima dell'avvio del *procurement*, potendo verificare la liceità di un sistema d'arma *ab origine*, sin dalla fase di progettazione. In Italia, tale processo di verifica, implementato anche dal Codice dell'Ordinamento Militare del 2010, si declina principalmente in un controllo condotto dal Ministero della Difesa in cooperazione con le Commissioni Difesa della Camera e del Senato, atto a vagliare e deliberare qualsiasi spesa relativa allo studio, sviluppo, acquisizione e adozione di nuovi sistemi d'arma.

b. <u>Organizzazione delle Nazioni Unite</u>

In seno all'Organizzazione delle Nazioni Unite (ONU) si sta affrontando il dibattito relativo all'eventuale necessità di un trattato internazionale tanto che il Segretario Generale ha istituito l'AI *Advisory Body*[22] per garantire che l'IA sia utilizzata per il bene dell'umanità, nonostante gli Stati di maggior peso, tra cui Stati Uniti, Russia e Israele abbiano chiarito di non sostenere un trattato così vincolante.

L'AI *Advisory Body* ha elaborato un rapporto finale a settembre 2024 ma, nonostante la consapevolezza che ciascun Stato membro non approverà ogni singolo punto contenuto nel documento, i membri affermano il loro ampio, ma non unilaterale, accordo con i risultati e le raccomandazioni indicati che enfatizzano la necessità di un approccio globale alla *governance* dell'IA, incentivando la cooperazione internazionale anche in questo nuovo settore.

---

19 "Strategia per l'implementazione dell'Intelligenza Artificiale in ambito Difesa" 1° edizione anno 2023, Ministero della Difesa - Stato Maggiore della Difesa.

20 Il forum più appropriato per discutere le politiche e le pratiche nazionali sullo sviluppo e l'uso di armi con funzioni autonome.

21 "Nello studio, messa a punto, acquisizione o adozione di una nuova arma, di nuovi mezzi o metodi di guerra, un'Alta Parte contraente ha l'obbligo di stabilire se il suo impiego non sia vietato, in talune circostanze o in qualunque circostanza, dalle disposizioni del presente Protocollo o da qualsiasi altra regola del diritto internazionale applicabile a detta Alta Parte contraente".

22 L'AI *Advisory Body* è un organo consultivo istituito nell'ottobre 2023 da 39 eminenti leader dell'IA provenienti da 33 differenti Stati membri (il rappresentate italiano candidato e selezionato è Padre Paolo Benanti, consigliere di Papa Francesco sull'IA e l'etica delle tecnologie), che prestano servizio a livello personale combinando competenze all'avanguardia in molteplici campi, tra cui politiche pubbliche, scienza, tecnologia, antropologia e diritti umani.

c. ***North Atlantic Treaty Organization***

Nonostante esista un significativo divario di capacità tra i membri NATO e sebbene gli approcci e le relative prospettive differiscano, è in atto una notevole cooperazione con pochi stretti alleati, piuttosto che progetti di collaborazione a livello comune.

La riflessione pubblica della NATO sull'IA è ancora in una fase relativamente iniziale; tuttavia, sono state già adottate diverse misure per affrontarne il ruolo, tra le quali la pubblicazione di diversi libri bianchi e l'approvazione di una *Roadmap* per le tecnologie dirompenti che hanno contribuito a stabilire l'agenda per integrare e rafforzare il lavoro della NATO sull'IA. La NATO ha inoltre adottato una strategia dedicata nell'ottobre 2021 che, mirando nel lungo termine all'integrazione dell'IA negli strumenti che consentono di assolvere i tre *core task*[23], impegna i membri "alla collaborazione e alla cooperazione su qualsiasi questione relativa all'IA per la difesa e la sicurezza transatlantica" al fine di "mantenere il vantaggio tecnologico della NATO" e, riconoscendo nel dato l'elemento cardine per l'attuazione di tale piano, si pone gli obiettivi di:

- incoraggiare lo sviluppo e l'uso responsabile dell'IA per scopi di difesa e sicurezza degli Alleati;
- facilitare l'adozione tradizionale dell'IA tra gli alleati, accelerando lo sviluppo delle capacità e migliorando l'operabilità all'interno dell'Alleanza;
- concentrarsi sull'innovazione e sull'indirizzo efficaci dell'IA ulteriori considerazioni politiche, compresa l'attuazione dei principi concordati uso responsabile;
- difendersi dall'uso dannoso dell'IA da parte di avversari statali e non statali.

Tali obiettivi sono stati esplicitati nel breve termine mediante la definizione e lo sviluppo di casi d'uso di immediata applicazione e dei "Principi di un Uso Responsabile dell'IA" (legalità, responsabilità, spiegabilità e tracciabilità, affidabilità, governabilità e mitigazione dei pregiudizi), gli investimenti nella formazione di personale altamente specializzato nel settore, l'utilizzo dei Centri di Sperimentazione di IA nell'ambito della struttura del *Defence Innovation Accelerator for the North Atlantic* (DIANA) per sviluppare e testare applicazioni d'interesse e come interfaccia verso il mondo accademico ed il settore privato, l'implementazione di un nuovo *Digital Transformation Action Plan* che abiliti la NATO alla condivisione e allo scambio sicuro di dati e di servizi di IA attraverso un *cloud*.

In quanto Alleanza basata sul consenso, la NATO ha l'opportunità di facilitare le discussioni e le potenziali esercitazioni utilizzando effettivamente l'IA consentendo agli Stati membri di sfruttare gli sforzi di sviluppo delle capacità e di affrontare meglio le sfide associate alle vulnerabilità della sicurezza e alle limitazioni più ampie della tecnologia IA. Inoltre, un crescente divario di capacità nelle tecnologie abilitate all'IA potrebbe far sì che alcuni Stati siano relativamente meno attrezzati per rispondere a un ambiente di conflitto più rapido in cui gli avversari si affidano all'IA, in questa circostanza la NATO può quindi essere un meccanismo attraverso il quale, su richiesta, possono essere forniti ai membri orientamenti per lo sviluppo delle capacità e una più ampia assistenza, nonché arena di confronto in merito alle sfide di interoperabilità e condivisione di dati nelle operazioni multinazionali.

d. Unione Europea

Le iniziative dell'Unione Europea (UE) relative all'IA risalgono alla sottoscrizione da parte dei 25 Paesi membri di una dichiarazione con cui si sono impegnati a coordinare gli sforzi nell'implementazione di sistemi di IA, focalizzando l'impegno di condividere le *best practice* nel settore pubblico, rendendo maggiormente disponibili i dati pubblici, contribuendo a creare soluzioni attendibili e sostenibili, assicurando la centralità dell'individuo nel loro sviluppo e favorendo lo scambio di opinioni circa gli impatti di queste tecnologie nel mercato del lavoro.

---

[23] *Deterrence and defence, crisis prevention and management, cooperative security*.

L'UE ha quindi adottato un approccio che predilige la regolamentazione rispetto all'innovazione, basato sulla concezione kantiana del rispetto dei diritti fondamentali, della democrazia e della legge, riconoscendo all'individuo libertà, autonomia e dignità. Se questo rigido compromesso è visto da alcuni come potenziale ostacolo allo sviluppo dell'IA, per altri si traduce in un vantaggio competitivo per cui i consumatori saranno più favorevolmente attratti da sistemi in grado di offrire maggiori garanzie e tutele.

In questo contesto, già nel 2019 il gruppo di esperti "*High-Level Expert Group on AI*", nominato dalla Commissione Europea, ha prodotto alcune linee guida che descrivono i principi di interesse per lo sviluppo dei sistemi di IA, tra i quali la tutela della *privacy*, l'integrità del dato, la trasparenza e l'interpretabilità. Dal punto di vista della *privacy* è riconosciuta la necessità di proteggere i dati, specialmente in relazione ai sistemi che prevedono il trattamento di dati particolari mediante l'applicazione del principio "*privacy by design*"[24]. Anche i requisiti di trasparenza ed interpretabilità sono esplicitamente richiesti, declinandoli nella possibilità di garantire una visione completa di tutto il meccanismo, in ogni momento, che però non risolverebbe il problema della complessità dei sistemi di *machine learning*. Per tale motivo gli sforzi, dal punto di vista tecnologico, si stanno concentrando sull'implementazione di tecniche che consentano di fornire spiegazioni comprensibili sul comportamento di sistemi decisionali basati su modelli non interpretabili.

Infine, nel 2021 è stata presentata la proposta dell'*Artificial Intelligence Act*, il primo regolamento al mondo volto a disciplinare i sistemi di IA mentre è del 2023 l'accordo provvisorio raggiunto dal trilogo (Parlamento, Consiglio e Commissione Ue) che introduce una serie di divieti (tra cui il divieto di dare alle forze di polizia strumenti anche predittivi attraverso l'utilizzo di tecnologie biometriche applicate all'IA, divieto ai *database* di riconoscimento facciale e alla categorizzazione biometrica) i quali tengono conto anche dei recenti sviluppi dei sistemi di IA generativa. Dopo l'approvazione finale il regolamento è entrato in vigore ad agosto 2024 (gli Stati membri hanno un anno per designare le autorità nazionali competenti), fornendo una definizione lungimirante di IA ed un approccio basato sul rischio e delineando requisiti e obblighi chiari a sviluppatori e operatori per quanto riguarda gli usi specifici dell'IA.

5. Conclusione

Il presente elaborato ha evidenziato che in campo militare l'IA presenta opportunità, limiti, rischi etici e giuridici che devono essere presi in considerazione per il suo impiego, valutando e distinguendo gli ambiti in cui risulta realmente efficace. L'IA sta diventando estremamente sofisticata e, se da un lato è premiante sfruttare le potenzialità di questi nuovi strumenti, dall'altro bisogna essere consapevoli dei limiti intrinsechi.

L'IA svolgerà un ruolo sempre più importante nel consentire le future attività militari e la guerra sarà conseguentemente più veloce ed efficace. Gli Stati stanno, in varia misura, investendo ed esplorando tecnologie abilitate all'IA (nei veicoli autonomi, nei sistemi di difesa aerea e missilistica autonomi, per l'analisi dei dati, nella logistica, nella gestione del personale e per l'assistenza sanitaria) e le conseguenze del restare indietro dal punto di vista tecnologico potrebbero essere catastrofiche.

In questo contesto, dal punto di vista giuridico non si può escludere che l'IA potrà garantire un rispetto del diritto umanitario anche migliore rispetto agli esseri umani, nonostante rimangono difficoltà intrinseche che non possono essere trasposte a semplici calcoli matematici o algoritmi di programmazione.

Maggiore è l'autonomia di cui l'IA disporrà, più elevati dovranno essere gli standard di progettazione e programmazione per soddisfare i requisiti etici e legali e, al fine di rendere più chiaro il quadro normativo all'interno del quale poterla utilizzare, sarebbe auspicabile definire

[24] Tale principio prevede che la protezione dei dati personali degli utenti sia integrata e presente lungo tutto il ciclo di progettazione del prodotto/servizio digitale, fin dalla progettazione.

nuovi protocolli destinati a disciplinare l'impiego di tali sistemi tenendo conto del progresso della tecnica e dei nuovi scenari applicativi. Ancorché il diritto internazionale esistente fornisca un quadro giuridico appropriato, sarebbe comunque utile prevedere una revisione delle norme del diritto internazionale al fine di rendere più chiare determinate questioni relative all'impiego di nuove tecnologie, tra cui gli aspetti relativi alla responsabilità. Oltre a ciò, gli stessi Stati dovrebbero procedere all'elaborazione di proprie dottrine per l'impiego dell'IA all'interno di uno scenario di conflitto. Per raggiungere tali obiettivi, e per configurare una cornice giuridica chiara, sarà poi indispensabile prevedere una forte sinergia tra giuristi e tecnici i quali, attraverso una stretta collaborazione, dovranno trovare il giusto punto di equilibrio tra tecnica e diritto al fine di rendere i nuovi sistemi guidati dall'IA *compliant* alla legge, ma anche ai principi etici che, in ogni caso, devono sempre guidare la conduzione delle operazioni all'interno di uno scenario bellico, tradizionale, asimmetrico o ibrido.

In conclusione, l'IA militare non dovrebbe essere sottovalutata e le implementazioni incrementali possono essere sfruttate con grande valore puntando a un'efficace collaborazione uomo-IA, senza però dimenticare che "in fin dei conti la macchina è solo uno strumento che può aiutare l'umanità a progredire più in fretta. Il compito dell'uomo e della sua intelligenza rimane ancora oggi lo stesso […] capire quali siano le domande giuste da rivolgere alle macchine".[25]

[25] Asimov Isaac, Conflitto evitabile in Io, Robot, Mondadori, 1950.

Bibliografia

Libri

- Allen John et al., Hyperwar: Conflict and Competition in the AI Century, SparkCognition Press, 2018.
- Asimov Isaac, Conflitto evitabile in Io, Robot, Mondadori, 1950.
- Forrest E. Morgan, et al., Military Applications of Artificial Intelligence - Ethical Concerns in an Uncertain World, Rand Corporation, 2020.
- Hynek Nik et al., Militarizing Artificial Intelligence, Routledge Studies in Conflict, Security and Technology, 2022.
- Maggie Gray, Amy Ertan, Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment, NATO Cooperative Cyber Defence Centre of Excellence, 2021.

Pubblicazioni e documenti

- Accademia Militare di Modena, "Etica militare ed arte del Comando", 1996.
- Artoni Maurizio, "L'impiego dell'intelligenza artificiale - una trasformazione inevitabile. Evoluzione e stato dell'arte (progressi tecnologici, ambiti di applicazione: punti di forza, vulnerabilità, opportunità, minacce" Istituto di Ricerca e Analisi della Difesa, 2022.
- Boulanin Vincent et al., Responsible military use of artificial intelligence - Can the European Union lead the way in developing best practice?, Stockholm International Peace Research Institute, 2020.
- International Institute of Humanitarian Law, Whither the Human in Armed Conflict? IHL Implications of New Technology in Warfare, 42nd Round Table on Current Issues of International Humanitarian Law, 2019.
- International Review of the Red Cross, Artificial intelligence and machine learning in armed conflict: A human-centred approach, 2020.
- NATO 2022 Strategic Concept, 2022.
- Stanley-Lockman Zoe, Responsible and Ethical Military AI Allies and Allied Perspectives, Center for Security and Emerging Technology, 2021.
- Stato Maggiore Difesa, "L'impatto delle Emerging & Disruptive Technologies (EDTs) sulla Difesa", 2022.
- Stato Maggiore Difesa, "Strategia per l'implementazione dell'Intelligenza Artificiale in ambito Difesa", 2023.
- United Nation AI Advisory Body, Governing AI for Humanity, 2024.
- Vestner Tobias, From Strategy to Orders: Preparing and Conducting Military Operations with Artificial Intelligence, Geneva Centre for Security Policy, 2023.

Articoli internet

- Ascani Paola Giorgia, Intelligenza artificiale e armi autonome: criticità giuridiche, https://issuu.com/rivistamarittima/docs/gennaio_2022/s/15118325 (accesso effettuato il 14/02/2024).
- Benedini Giuseppe, "Drone uccide operatore, l'intelligenza artificiale e il (finto) test del colonnello USA", https://www.corriere.it/esteri/23_giugno_02/drone-controllato-intelligenza-artificiale-uccide-suo-operatore-una-simulazione-virtuale-a32b7120-0145-11ee-9a47-43166fb70f00.shtml (accesso effettuato il 20/12/2024).
- Giuriatti Loris, "Codice Petrov", https://lorisgiuriatti.it/top-secret/codice-petrov/ (accesso effettuato il 14/02/2024).
- Plebe Alessio, Se l'Intelligenza Artificiale uccide: un'etica per auto e armi autonome, https://www.agendadigitale.eu/cultura-digitale/se-lintelligenza-artificiale-uccide-unetica-per-auto-e-armi-autonome/ (accesso effettuato il 14/02/2024).

- Strippoli Lanternini Andrea, L'intelligenza artificiale nel settore militare: vantaggi, rischi e tutele necessarie, https://www.agendadigitale.eu/sicurezza/lintelligenza-artificiale-applicata-al-settore-militare-vantaggi-rischi-e-tutele-necessarie/ (accesso effettuato il 14/02/2024).
- Tosato Mattia, L'Intelligenza Artificiale nelle Armi Autonome e l'idea di limitarne l'uso, https://www.amistades.info/post/intelligenza-artificiale-armi-autonome-idea-di-limitarne-uso (accesso effettuato il 14/02/2024).

Altri siti

- Commissione Europea, https://commission.europa.eu (accesso effettuato il 20/12/2024).
- Difesa Online, https://www.difesaonline.it (accesso effettuato il 14/02/2024).
- Governo Italiano - Dipartimento per la Trasformazione Digitale, https://innovazione.gov.it (accesso effettuato il 14/02/2024).
- Governo Italiano - Ministero dell'Economia e delle Finanze https://www.mef.gov.it (accesso effettuato il 14/02/2024).
- International Committee of the Red Cross, https://ihl-databases.icrc.org/en (accesso effettuato il 14/02/2024).
- NATO, https://www.nato.int (accesso effettuato il 14/02/2024).
- Parlamento Europeo, https://www.europarl.europa.eu (accesso effettuato il 14/02/2024).
- Pontificia Università Gregoriana, https://www.unigre.it (accesso effettuato il 20/12/2024).
- Rivista Marittima, https://issuu.com/rivistamarittima (accesso effettuato il 14/02/2024).
- Royal Aeronautical Society, https://www.aerosociety.com (accesso effettuato il 20/12/2024).
- United Nations Secretary-General, https://www.un.org (accesso effettuato il 14/02/2024).
- U.S. Department of States, https://www.state.gov (accesso effettuato il 14/02/2024).

Alessandro Della Monaca

Competizione geopolitica nel Circolo Polare Artico: nuove sfide e possibilità surriscaldano il Polo Nord

Abstract

Il seguente articolo analizza la crescente competizione geopolitica nell'Artico, un tempo regione periferica ora al centro dell'interesse strategico globale. Il riscaldamento globale e lo scioglimento dei ghiacci che ne è derivato hanno reso accessibili nuove rotte e risorse naturali, generando sia nuove opportunità ma anche tensioni tra le potenze interessate. Il documento, quindi, si pone l'obiettivo di analizzare l'evoluzione della percezione strategica dell'Artico, in particolar modo da parte di Stati Uniti, Russia e Cina, cercando di evidenziare come la regione sia diventata progressivamente un terreno di proiezione di potere multidimensionale; a tal proposito, la militarizzazione russa, l'attivismo statunitense e la crescente presenza economica cinese vengono letti in una doppia prospettiva: da un lato secondo le dottrine geopolitiche classiche e dall'altro alla luce delle logiche che governano il nuovo sistema policentrico asiatico. Infine, l'articolo riflette sui rischi connessi all'assenza di un quadro giuridico chiaro per la governance regionale e sui potenziali terreni di scontro in un contesto in cui convergono interessi ambientali, militari ed economici. In questo senso, sottolinea la necessità di un approccio diplomatico multilaterale per evitare l'escalation di tensioni che potrebbero compromettere la stabilità globale.

1. Introduzione

Nel marzo 2020, il generale Terrence J. O'Shaughnessy, comandante dello United States Northern Command (USNORTHCOM) e del North American Aerospace Defense Command (NORAD), ha descritto così il contesto geopolitico che caratterizza attualmente il Circolo Polare:

«L'Artico non è più un muro di fortezza, e i nostri oceani non sono più fossati protettivi; essi sono ora vie d'accesso per armi convenzionali avanzate e per le piattaforme che le trasportano. […] Le acque navigabili in modo più costante, la crescente domanda di risorse naturali e l'accumulo militare della Russia nella regione rendono l'Artico una sfida immediata per USNORTHCOM, NORAD, i nostri alleati del nord e i nostri vicini comandi geografici combattenti, U.S. European Command e U.S. Indo-Pacific Command»[1].

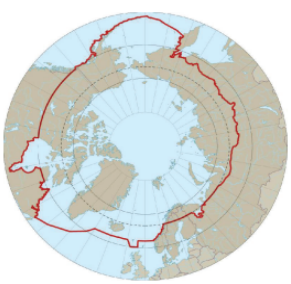


Figura 1: Definizione di "Artico" secondo l'*Artic Monitoring and Assesment Programme*, in base a quanto ricostruito nel report "*Snow, Water, Ice and Permafrost in the Artic*". Fonte: Knutsen, B. O., & Pedersen, M. N. (2024). How to Understand Climate Change as a Threat Multiplier in the Arctic. Arctic Review on Law and Politics, 15. P. 155. https://www.jstor.org/stable/48807501

Con un clima estremamente freddo, ghiacci marini perenni e territori scarsamente sfruttabili per via della tundra e del permafrost che ne caratterizzano l'ambiente naturale, il Circolo Polare Artico rappresenta una delle frontiere più impervie del pianeta. Nonostante ciò, grazie alla posizione geografica strategica è stato sempre uno spazio altamente contendibile; non solo per le grandi potenze, ma in generale

[1] Pubblicato da United States Senate Committee on Armed Services, (2020). U.S. Policy and Posture in Support of Arctic Readiness. March 3. Disponibile al link: https://www.armed-services.senate.gov/imo/media/doc/O%27Shaughnessy_03-03-20.pdf

per tutti gli attori che vi si affacciano.

Negli ultimi decenni, però, la percezione internazionale nei confronti della regione è decisamente cambiata, conducendo sempre più Paesi ad agire nell'area per i loro interessi.

2. Le cause del rinnovato confronto per il controllo del Circolo Polare Artico

Il motivo di questa rivalutazione geopolitica dell'Estremo Nord può essere innanzitutto rintracciato in quella che è la più grande sfida che la regione, in particolare, e il mondo intero stanno affrontando da più di due decenni, ovvero il cambiamento climatico. Negli ultimi 40 anni, infatti, l'area marittima del Polo Nord, un tempo impraticabile per tutto l'anno a causa del ghiaccio che perdurava anche nei mesi estivi, si è ridotta di 0.8 milioni di km²; un calo significativo che non sembra destinato a migliorare.[2] Per avere un'idea più precisa dell'ammontare, si tratta di una superficie più vasta di quella comprendente Italia, Francia e Germania.

Figura 2: Le tre nuove Rotte Commerciali Polari. Fonte: Zandee, D., Kruijver, K., & Stoetman, A. (2020). Annex 4: Schematic overview of Arctic bodies. In The future of Arctic security: The geopolitical pressure cooker and the consequences for the Netherlands, Clingendael Institute. P. 10. http://www.jstor.org/stable/resrep24676.13

Secondo diversi studi[3], ciò sarebbe dovuto ad un fenomeno definito "*Artic amplification*", secondo il quale il riscaldamento globale e in particolare quello delle acque sta colpendo in maniera significativa il Mare Artico, con temperature che sono aumentate fino a quattro volte più velocemente rispetto ad altri luoghi del Pianeta.

Quanto appena descritto ha chiaramente sollevato molte preoccupazioni relativamente alle gravi conseguenze che potrebbe avere sull'ecosistema globale e, in particolare, sul livello dei mari; ciononostante, è anche vero che ha permesso di raggiungere luoghi difficilmente raggiungibili fino a pochi anni fa, anche per coloro che erano in possesso della tecnologia e degli strumenti adatti. Tre nuove rotte commerciali polari sono state create a causa dello scioglimento dei ghiacciai[4], la *Northern Sea Route* (NSR), il N*orthWest Passage* (NWP) e, infine, la *Transpolar Route* (TPR); dal momento che mettono in diretta comunicazione l'Oceano Pacifico con quello Atlantico, assicurarsene un controllo, permetterebbe un risparmio in termini di tempistiche, carburante e, quindi, costi per il trasporto delle merci.

Allo stesso tempo, il progressivo scioglimento dei ghiacci perenni ha permesso l'accesso alle immense riserve ittiche della regione, fondamentali per la sussistenza economica di molte nazioni polari. Essendo questi depositi di pescato situati per la maggior parte all'interno delle *Zone Economiche Esclusive* dei Paesi artici, ciò ha permesso per anni di evitare dispute per il loro possesso. Tuttavia, l'aumento delle temperature ha provocato un'alterazione dell'ecosistema marino, con la conseguenza che numerose specie sub-artiche hanno iniziato ad emigrare verso Nord alla ricerca di un habitat più adatto alle loro esigenze.

---

2 Madeira, J., Alsaied, J., Bess, C., Cortino, B., Gum, D., Kastetter, A., Kim, J., Koç, D. E., Horan, L. S., Means, A., Powell, W., Symonds, E., & Zhukov, D. (2023). Nuclear Temperature Rising? The Impact of Climate Change on Nuclear Stability. In R. Younis & J. Link (Eds.), On the Horizon: A Collection of Papers from the Next Generation (pp. 115–124). Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep47437.12

3 Zandee, D., Kruijver, K., & Stoetman, A. (2020). Arctic security trends. In *The future of Arctic security: The geopolitical pressure cooker and the consequences for the Netherlands*, p. 5. Clingendael Institute. http://www.jstor.org/stable/resrep24676.5

4 Zandee, D., Kruijver, K., & Stoetman, A. (2020). Annex 4: Schematic overview of Arctic bodies. In The future of Arctic security: The geopolitical pressure cooker and the consequences for the Netherlands, Clingendael Institute. P. 10. http://www.jstor.org/stable/resrep24676.13

Inoltre, l'aumento delle temperature sta avendo effetti anche sul permafrost situato sulle poche terre emerse presenti nella zona (Groenlandia, Islanda, Isole Svalbard), intaccando in due diversi modi l'ecosistema regionale. Da un lato, infatti, rende più friabile il suolo, che quindi diventa facilmente soggetto ad erosione; questo sviluppo ha conseguenze più dirompenti nei confronti delle popolazioni indigene (come i *Saami* o gli *Inuit*), le quali stanno progressivamente osservando uno stravolgimento di quei luoghi, sacri nelle loro culture, e, di conseguenza, anche nei tradizionali stili di vita. Dall'altro lato, però, garantisce l'accesso al sottosuolo e con esso anche alle riserve naturali (minerarie e non solo) fino ad ora ben protette. Secondo alcune ricerche[5], infatti, si stimerebbe che circa il 13% delle riserve di petrolio mondiali, il 30% di quelle di gas naturale e addirittura il 40% del gas naturale liquefatto si troverebbero sotto la superficie dell'Artico. Ovviamente, ciò vale sia nel caso del permafrost, ma anche per il fondale marino, che quindi dovrebbe essere ulteriormente sfruttato per permettere agli Stati interessati di raggiungerle.

Sulla scia di quanto affermato dal generale O'Shaughnessy, Washington ha pubblicato una nuova strategia dedicata alla regione nordica; attraverso di essa, ha voluto riaffermare la sua posizione nell'area, rafforzando la cooperazione con gli alleati, anche tramite un confronto, pienamente gestito, ma diretto con i principali competitor globali, Russia in primis.

La scelta statunitense è stata dettata principalmente dalla necessità di inserirsi all'interno di un sistema internazionale diverso da quello unipolare creatosi dopo la dissoluzione dell'Unione Sovietica; il nuovo ordine policentrico asiatico, infatti, ha comportato una decisiva revisione delle logiche che hanno guidato le relazioni internazionali per decenni, con gli attori statali che hanno iniziato a dotarsi di una duplice profondità spaziale (terrestre e marittima), in modo tale da ampliare la propria zona di influenza e impedire ai rivali geopolitici di avvicinarsi ai confini nazionali. Di conseguenza, in un sistema nel quale non esistono più potenze meramente di mare o di terra, è la stessa idea di *Rimland* e *Heartland*, formulata dal geostratega e politologo statunitense Nicholas J. Spykman nel 1944[6] partendo dalla teoria dell'inglese Mackinder, ad essere venuta meno.

Secondo quanto formulato dall'americano, il *Rimland* sarebbe quello spazio semicircolare che, partendo dai Mari del Nord (Mar Baltico, soprattutto), attraversa Europa, Medio Oriente e Persia, risale lungo la zona costiera dell'Asia-Pacifico e costituisce una fascia di sicurezza, grazie al cui controllo una potenza marittima (USA) può riuscire a frenare la discesa in mare della potenza di terra; così facendo, inoltre, potrebbe riuscire anche a controllare l'*Heartland*, l'isola-mondo centrale e, di riflesso, tutto il globo. Ebbene, questa rappresentazione oggi deve essere necessariamente "*allargata*" e reimmaginata non più come qualcosa limitato alle fasce costiere.

3. Il rinnovato confronto geopolitico per l'Artico e gli attori che vi agiscono

Tale ampliamento della proiezione di potenza, a cui è seguito il superamento della dimensione statale verso una *polare*, ha condotto ad una rilettura della regione estremo-settentrionale, oramai non più considerata come un semplice spazio periferico e rilevante solo se inserito all'interno del confronto tra grandi potenze. Al contrario, è divenuta il naturale spazio vitale di una potenza storicamente di terra qual è la Russia; l'ex impero sovietico, infatti, proprio nelle fredde acque artiche ha trovato una nuova, quanto mai determinante per il sistema policentrico, dimensione anfibia. A dimostrazione di ciò, nel 2007, l'esercito russo, su volontà dello stesso presidente, ha piantato una bandiera nel Polo Nord geografico. Ovviamente si tratta di un'azione prettamente simbolica, vista l'impossibilità di raggiungerlo facilmente nel prossimo futuro senza utilizzare navi rompighiaccio o altra strumentazione apposita; ciononostante è stata una chiara rappresentazione di come Mosca consideri il Circolo Polare al pari di una sua

---

5 Zandee, D., Kruijver, K., & Stoetman, A. (2020). Annex 4: Schematic overview of Arctic bodies. In The future of Arctic security: The geopolitical pressure cooker and the consequences for the Netherlands, Clingendael Institute. P. 10. http://www.jstor.org/stable/resrep24676.13

6 Spykman, N.J., (2020). Geografia delle potenze mondiali. Le due rose. Editore, Milano.

estensione naturale, essenziale per riacquisire lo *status* di grande potenza perso con la dissoluzione dell'Unione Sovietica.

Da allora, i russi hanno iniziato una pesante militarizzazione della regione, a cominciare dal rafforzamento della Flotta Settentrionale; stanziata nell'Oblast di Murmansk, nella penisola di Kola, già in passato era ritenuta la più imponente divisione militare posseduta dall'ex impero. Infatti, vista la posizione geografica, alle porte dell'Europa orientale, sin dalla sua creazione sotto l'URSS aveva il compito di fungere da "ultimo bastione" dalle possibili incursioni navali nemiche; con il nuovo confronto tra grandi potenze oramai affermato da qualche anno, la base militare ha ritrovato la sua funzione strategica, rientrando pienamente nel sistema tattico di deterrenza nucleare marittima della Federazione russa.

È ovvio, quindi, che per Washington la situazione ora delineata sia tutt'altro che florida. Da un lato, infatti, il Polo Nord rappresenta uno nuovo spazio sul quale potrebbero facilmente proiettare la loro potenza e in grado di offrire immense risorse naturali ed elevati guadagni economici; dall'altro lato, però, è anche un'area non soggetta a precise norme in materia di divisioni territoriali, un particolare che lascia ampio margine di azione a coloro che ritengono di poter avanzare qualche tipo di rivendicazione. Con il diretto rivale geopolitico (lo stesso che ha dimostrato in questi anni di voler espandere influenza e sovranità nelle aree circostanti, a prescindere dalla volontà dei vicini) sempre più attivo militarmente, questi elementi insieme hanno convinto l'establishment americano a riposizionare l'Artico nella loro agenda politica, aumentando la cooperazione militare e civile, sia bilateralmente con gli alleati regionali che multilateralmente attraverso l'alleanza atlantica.

Nello stesso contesto devono inserirsi le dichiarazioni dell'attuale amministrazione Trump relative all'annessione di Groenlandia e Canada in nome della sicurezza nazionale; considerando che gli Stati Uniti confinano territorialmente con il Circolo Polare Artico solo grazie allo Stato dell'Alaska, è ovvio che acquisire la sovranità su entrambe le nazioni confinanti permetterebbe a Washington di ottenere maggior importanza ad un teorico tavolo per una spartizione della regione. Senza considerare la profondità terrestre che così conquisterebbe, assicurandosi da un lato la continuità territoriale e dall'altra la dimensione anfibia necessaria per poter competere alla pari con Russia e Cina nel sistema di cui sono garanti.

A proposito della strategia artica degli Stati Uniti, la Seconda Flotta statunitense è stata riattivata con lo scopo di presidiare il GIUK(-N) gap, un passaggio marittimo fondamentale per le operazioni tra Atlantico Settentrionale e Mare Artico, in quanto mette in comunicazione Groenlandia con Islanda, Regno Unito e Norvegia.

Come già emerso poc'anzi, anche la Nato ha spostato il suo baricentro operativo proprio verso il Nord Atlantico e su Mar Artico. La motivazione di ciò è da rintracciare in due episodi, ovvero da parte della Russia l'annessione della Crimea nel 2014 e l'invasione dell'Ucraina nel 2022. Prendendo questi due atti di guerra come promemoria, la militarizzazione attuata da Mosca ha messo seriamente in allarme l'organizzazione occidentale, che in risposta, dunque, ha iniziato ad organizzare esercitazioni militari congiunte, in modo tale da migliorare le capacità delle sue truppe di operare nel Circolo Polare.

A conferma parziale di questo interesse della NATO devono essere considerati gli ingressi della Finlandia nell'aprile 2023 e della Svezia nel marzo 2024; entrambi i Paesi, infatti, hanno un'attenzione per la regione estremo settentrionale e le loro capacità militari (insieme a quelle norvegesi) possono rivelarsi fondamentali per aggiornare gli alleati sulle tecniche di combattimento da utilizzare in ambienti rigidi ed inospitali.

Lo scontro delineato sino ad ora potrebbe sembrare una sorta di *revival* dei tempi del bipolarismo; allora l'Artico rappresentava la linea di confine diretta tra le due super potenze ed era al centro delle rispettive strategie di deterrenza nucleare. Oggi, però, la situazione è decisamente diversa e in questo rispecchia il contesto geopolitico generale.

Infatti, viste le tante opportunità che potrebbe essere in grado di offrire, la regione ha subito una decisiva internazionalizzazione; gli attori che avanzano una qualsiasi sorta di pretesa

verso l'Estremo Nord sono decisamente aumentati, minando ulteriormente una già delicata divisione territoriale.

Oltre coloro che affacciano sul Circolo Polare Artico e che esercitano la loro sovranità direttamente su quelle zone, ovvero i cosiddetti *Arctic Eight*, esiste una serie di Stati non-artici che hanno comunque un interesse economico personale nei confronti dell'area. Soggetti internazionali come l'Unione Europea, l'Italia, la Francia, la Germania, il Regno Unito e persino il Giappone sono stati accolti positivamente dalle nazioni polari filooccidentali, in quanto ritenuti fondamentali per equilibrare la crescente influenza russa; inoltre, la loro presenza nell'area serve anche ad attenuare la novità offerta da un attore che con la zona non condivide nulla, se non l'interesse per le vie marittime. Questo attore è la Repubblica Popolare Cinese.

La Cina di Xi Jinping, infatti, nel 2018 ha pubblicato un primo documento sulla strategia da perseguire nell'Artico, all'interno del quale si è autodefinita attore "*quasi artico*". Il motivo dietro questo nuovo interesse da parte di Pechino deve essere rintracciato nelle nuove rotte, in particolare nella NSR e nel NWP, grazie alle quali potrebbe diminuire i tempi necessari ad arrivare in Europa e nell'Atlantico in generale; ciò permetterebbe a sua volta di ridurre i costi di trasporto delle merci, evitando il passaggio dei "colli di bottiglia", come Suez, Panama o Malacca, e quelli per il carburante necessario per affrontare la lunga traversata transoceanica. In questo contesto, Pechino ha inserito il Polo Nord all'interno della "*Polar Silk Road*", nel cui ambito ha iniziato a costruire una nuova rete infrastrutturale.

Inoltre, il gigante asiatico ha da subito iniziato un'intensa cooperazione con il partner moscovita, sia in ambito militare che in quello civile (ad esempio nel settore estrattivo). Questa collaborazione tra i due partner ha preoccupato le altre potenze regionali, soprattutto per il timore che, unita all'assenza di divisioni territoriali precise, possa facilitare le "zone grigie" del diritto internazionale, mettendo quindi a rischio l'integrità territoriale e la sovranità degli *Arctic States* occidentali. In questo frangente, le dispute nel Mar Cinese Meridionale, sempre più foriere di conflitti, hanno fornito degli ottimi precedenti per sollevare una simile preoccupazione nei confronti dell'asse sino-russo, creatosi e rafforzatosi sempre di più nella zona.

Conclusione

In conclusione, il Circolo Polare Artico, tra i luoghi più remoti e misteriosi del pianeta, sta diventando un luogo pericolosamente caldo; il vasto spazio marittimo reso disponibile a causa del riscaldamento delle acque è in grado di offrire opportunità che non sono certo passate inosservate all'interno della comunità internazionale, con la conseguenza che sempre più attori hanno iniziato ad agire nella regione.

In questo senso, la collaborazione tra Mosca e Pechino e lo scontro tra questi e Washington per ottenerne il controllo ha riacceso inevitabilmente il confronto interrotto nel 1991 con la dissoluzione dell'URSS; inoltre, con le esercitazioni militari sempre più frequenti e attuate con l'uso di strumentazioni sempre più efficaci ed efficienti, la situazione sta rischiando seriamente di degenerare in incidenti difficilmente riparabili; considerando che la totalità degli Stati artici filooccidentale è anche membro della NATO, un ipotetico conflitto potrebbe portare all'applicazione dell'Articolo 5, conducendo in guerra anche i Paesi europei.

Tale prospettiva deve essere assolutamente evitata, attraverso la ricerca costante di un dialogo disteso con le potenze asiatiche, a cominciare dalla Russia. Soltanto con la diplomazia, dunque, il mondo potrà evitare lo scoppio di un altro conflitto mondiale, le cui conseguenze rischiano di essere ben peggiori rispetto a quello concluso nel 1945.

La stabilità geopolitica globale non è mai dipesa così tanto da una regione periferica e, almeno in questo senso, l'Artico sta confermando ancora una volta la sua *eccezionalità* nel contesto delle relazioni internazionali.

Bibliografia

- Knutsen, B. O., & Pedersen, M. N. (2024). How to Understand Climate Change as a Threat Multiplier in the Arctic. Arctic Review on Law and Politics, 15. P. 155. https://www.jstor.org/stable/48807501
- Madeira, J., Alsaied, J., Bess, C., Cortino, B., Gum, D., Kastetter, A., Kim, J., Koç, D. E., Horan, L. S., Means, A., Powell, W., Symonds, E., & Zhukov, D. (2023). Nuclear Temperature Rising? The Impact of Climate Change on Nuclear Stability. In R. Younis & J. Link (Eds.), On the Horizon: A Collection of Papers from the Next Generation (pp. 115–124). Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep47437.12
- Pubblicato da The State Council Information Office of the People's Republic of China, (2018). China's Arctic Policy, January 26. Disponibile al link: https://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm
- Pubblicato da United States Senate Committee on Armed Services, (2020). U.S. Policy and Posture in Support of Arctic Readiness. March 3. Disponibile al link: https://www.armed-services.senate.gov/imo/media/doc/O%27Shaughnessy_03-03-20.pdf
- Spykman, N.J., (2020). Geografia delle potenze mondiali. Le due rose. Editore, Milano.
- Zandee, D., Kruijver, K., & Stoetman, A. (2020). Annex 4: Schematic overview of Arctic bodies. In The future of Arctic security: The geopolitical pressure cooker and the consequences for the Netherlands, Clingendael Institute. http://www.jstor.org/stable/resrep24676.13
- Zandee, D., Kruijver, K., & Stoetman, A. (2020). Arctic security trends. In *The future of Arctic security: The geopolitical pressure cooker and the consequences for the Netherlands* (pp. 5–17). Clingendael Institute. http://www.jstor.org/stable/resrep24676.5

Marco Gaetani, Stefano Lanci, Siro Pettenuzzo, Giuseppe Pietrangelo, Valentina Tagliaferri

Studio delle capacità counter-space a difesa dei Posti Comando Terrestri

Abstract

Le operazioni spaziali stanno assumendo un ruolo sempre più centrale nelle strategie di sicurezza globale, di conseguenza le operazioni counter-space diventano essenziali per proteggere le stazioni di comando terrestri e le infrastrutture spaziali. L'evoluzione delle minacce richiede soluzioni innovative per difendere i punti di comando e mantenerne la stabilità operativa. In questo articolo, dopo un'analisi delle principali sfide legate alla guerra spaziale, verranno presentate alcune soluzioni operativo/tattiche e tecnologie per implementare le infrastrutture orbitali e terrestri. L'obiettivo è delineare un approccio proattivo alla sicurezza spaziale, favorendo lo sviluppo di tecnologie difensive all'avanguardia.

1. Introduzione

Lo sviluppo tecnologico ha aumentato la dipendenza della società dalle infrastrutture spaziali, di conseguenza la sicurezza spaziale è diventata una questione sempre più rilevante. Alcuni Paesi stanno sviluppando tecnologie spinti dalla necessità di prepararsi all'evenienza in cui i futuri conflitti sulla Terra si estendano allo spazio. Una postazione di comando è definita come la sede di controllo dell'unità dove il comandante e il suo staff svolgono le loro attività. Per difenderla da minacce spaziali, dove con minaccia spaziale si intendono tutte le azioni che vengono effettuate nel dominio spaziale (o tramite esso) che hanno lo scopo di danneggiare lo spazio stesso e i suoi elementi costitutivi, sono necessarie robuste capacità di consapevolezza del dominio (Space Domain Awarness SDA). La SDA consta in attività che rilevano, tracciano, catalogano, identificano e prevedono le attività nel dominio spaziale per fornire informazioni durante il processo decisionale. Il controllo del dominio spaziale consiste in azioni offensive e difensive, denominate operazioni *counter-space*. Queste operazioni vengono condotte attraverso i segmenti orbitali, terrestri e di collegamento dell'architettura spaziale. Le operazioni offensive mirano ad eludere l'avversario oppure a eliminare o impedire l'uso dei sistemi spaziali, quelle difensive proteggono le infrastrutture critiche dagli attacchi diretti, dalle interferenze o da altre minacce. Attraverso le suddette operazioni è possibile ottenere la superiorità spaziale, ovvero la capacità di usare lo spazio per scopi militari o di impedire che l'avversario lo usi a suo vantaggio, dove con "spazio" ci si riferisce all'area sopra i 100 chilometri dal livello del mare, contrassegnata idealmente dalla linea di Karman. Esempi di operazioni *counter-space* possono essere:

- miglioramento della visione e della conoscenza del comando del campo di battaglia;
- istituzione di appropriate misure difensive e protettive per assicurarsi che le operazioni spaziali possano essere condotte in maniera continua attraverso l'intero spettro del conflitto;
- operazioni per sviare, interrompere, negare, degradare o distruggere le capacità spaziali dell'avversario.

a. Classificazione delle armi *counter-space*

Le capacità *counter-space* annoverano diversi sistemi che possono variare in maniera significativa in base alle metodologie tecniche che vengono impiegate e al livello di tecnologie e risorse necessarie per il loro dispiegamento:

1. *cinetiche*: armi che usano mezzi fisici come bombe, proiettili, missili e altre munizioni. Tutte le armi cinetiche sono considerate come mezzi per distruggere o danneggiare. A loro volta le armi cinetiche possono essere suddivise in:
   - co-orbitali: le armi vengono posizionate in orbita e poi vengono manovrate per avvicinarsi al bersaglio, attaccandolo attraverso vari mezzi distruttivi;
   - dirette ascendenti: armi che usano missili lanciati via terra, aria o mare e che vengono usate per distruggere cineticamente satelliti. Non vengono poste in orbita.
2. *non cinetiche*: armi che utilizzano energia concentrata come laser, particelle o fasci di microonde per interferire o distruggere sistemi spaziali (DEW *Direct Energy Weapon*). Possono essere sia co-orbitali che terrestri.
3. *guerra elettronica*: azioni militari che coinvolgono l'uso di energia elettromagnetica direzionata per controllare lo spettro elettromagnetico o per attaccare il nemico. Si suddividono in attività di:
   - *jamming* in salita (*uplink*) o in discesa (*downlink*), in cui il *jammer uplink* interferisce con il segnale che va verso il satellite creando così tanto disturbo che il satellite non riesce a distinguere il vero segnale dal rumore mentre il *jammer downlink* ha come obiettivo il disturbo del segmento terrestre o degli utilizzatori finali;
   - *spoofing*, ovvero una manipolazione dei segnali in salita o discesa che modificano le funzioni satellitari. Il satellite può essere controllato direttamente dal nemico per trasmettere dati falsi alla rete di utilizzatori o al segmento terrestre oppure, attraverso il cosiddetto *meaconing*, vengono falsificati i segnali GPS militari crittografati in modo da prendere il controllo del satellite, modificarne i dati orbitali e farlo eventualmente collidere con detriti spaziali o con altri satelliti;
   - *Cyber*: armi che usano software e tecniche di network per compromettere, controllare, interferire o distruggere sistemi informatici.

b. Esempi recenti

L'invasione russa dell'Ucraina del 24 febbraio ha mostrato al mondo l'importanza dello spazio nei conflitti futuri, infatti è stata accompagnata da due azioni: un attacco cyber al segmento di terra di Viasat e una vasta operazione di disturbo dei segnali di posizionamento, tempo e navigazione. La prima azione è stata dunque il frutto di operazioni multi-dominio, poiché attraverso il dominio cyber è stato colpito quello spaziale, disabilitando i terminali di comunicazione presenti sul territorio e danneggiando le capacità di comando e controllo delle forze armate ucraine di cui Viasat è fornitore di servizi. La seconda azione invece ha compromesso la precisione dei segnali GPS e Galileo sul confine e lungo le linee offensive russe con ripercussioni anche sull'aviazione civile. [4] La guerra russo-ucraina ha dunque aperto un fronte spaziale dopo i primi esempi nella guerra del Golfo, in Afghanistan e in Siria, estendendo il conflitto al quinto dominio (riconosciuto tale dalla NATO nel 2019). I satelliti e le infrastrutture spaziali stanno dunque contribuendo a raccontare la guerra dando una connotazione di quasi tempo reale come non era mai accaduto: forniscono immagini satellitari che permettono di monitorare i movimenti delle truppe e identificano le minacce in tempo reale migliorando così la capacità di risposta strategica. In aggiunta sono stati fondamentali per garantire comunicazioni sicure tra le forze armate, specialmente in situazioni in cui le infrastrutture terrestri erano compromesse. Le dinamiche emerse dal conflitto russo ucraino hanno dunque evidenziato quanto sia importante ideare e mettere in pratica operazioni *counter-space*, perciò nel seguito verranno esposte e analizzate varie strategie di difesa delle postazioni di comando terrestri.

2. Difesa co-orbitale Spazio-Spazio

a. Difesa co-orbitale con pulviscolo

Nella difesa co-orbitale con pulviscolo il satellite attaccante viene portato su un'orbita più lontana dalla Terra rispetto al satellite obiettivo e con senso di rotazione opposto, motivo per cui è opportuno disporre di almeno due satelliti contro-rotanti in orbita attorno la Terra per poter aggredire prontamente qualsiasi satellite indipendentemente dal suo verso di rotazione. Una volta che il satellite si trova sull'orbita desiderata viene rilasciato il pulviscolo determinando così, in virtù del principio di conservazione della quantità di moto, un'accelerazione del satellite che lo porta ad allontanarsi dalla Terra su un'orbita più esterna e, al contempo, una decelerazione della nube sferica di pulviscolo che la porta ad avvicinarsi alla Terra posizionandola sulla stessa orbita del satellite oggetto dell'attacco. Poiché la nube si muove in direzione opposta al satellite quest'ultimo entrerà più volte nella nube permettendo al pulviscolo di attaccarsi in più riprese alle superfici oggetto dell'attacco. Le sostanze delle quali si compone il pulviscolo varieranno a seconda della superficie che si ha intenzione di attaccare. I componenti suscettibili a questo tipo di attacco sono i pannelli solari e le antenne, perciò nel primo caso occorrerà adottare una sostanza in grado di impedire il passaggio della luce solare mentre nel secondo ne occorrerà una in grado di riflettere le onde elettromagnetiche di una determinata frequenza per isolare il satellite e impedire la ricezione e l'emissione di segnali. Per massimizzare i danni al satellite oggetto dell'attacco è opportuno adoperare un pulviscolo composto da entrambe le sostanze.

Figura 1: Schema azione difensiva con pulviscolo

b. Difesa co-orbitale con gabbia di Faraday

Nella difesa co-orbitale con gabbia di Faraday l'obiettivo dell'operazione è quello di isolare dall'ambiente esterno il satellite oggetto dell'attacco sfruttando una gabbia di un materiale elettricamente conduttore capace di schermarlo da qualsiasi campo elettrostatico e rendendolo così insensibile ad ogni comunicazione con la stazione a terra o con altri satelliti. La missione può essere raffigurata attraverso una delle due strategie rappresentate in figura. Nella strategia rappresentata in figura (a) il satellite attaccante, una volta posizionato sulla stessa orbita del satellite obiettivo, lancia una rete verso il bersaglio che, una volta dispiegata, lo avvolge impedendogli di comunicare con l'esterno. Nella strategia di figura (b) il satellite attaccante, tramite un braccio robotizzato alla cui estremità è presente una gabbia in grado di aprirsi e richiudersi in maniera automatizzata, intrappola l'obiettivo in una sfera impedendogli di comunicare con l'esterno. La prima strategia permette di attaccare più satelliti di qualsiasi tipologia utilizzandone solo uno (che verrà quindi equipaggiato con più di una rete), di contro una volta che il bersaglio verrà avvolto dalla rete non potrà più essere liberato e sarà costretto a vagare incontrollato nello spazio con tutti i pericoli che ne conseguono. Nella seconda strategia invece l'attacco non può essere portato indiscriminatamente ad ogni tipo di satellite ma solo a quelli che hanno delle dimensioni che si confanno a quelle della gabbia però, una

volta che non è più necessario isolare il satellite, quest'ultimo può essere liberato tornando alla sua vita operativa senza errare nello spazio in maniera incontrollata.

Figura 2: Strategia (a) difesa con gabbia di Faraday

c. Satellite con canestro gonfiabile

Il canestro gonfiabile viene alloggiato sgonfio all'interno del satellite e, ogni qualvolta sia necessario catturare un bersaglio, viene gonfiato alla pressione di 1.5 atm. Il canestro è alloggiato su una piattaforma di Stewart dotata di martinetti idraulici in grado di orientarlo e al suo interno è presente una sorta di braccio robotico a 6 arti come sistema di ridondanza al fine di garantire una maggiore presa ed un effettivo blocco dell'obiettivo durante la fase di trasporto.

Figura 3: Strategia (b) difesa con gabbia di Faraday

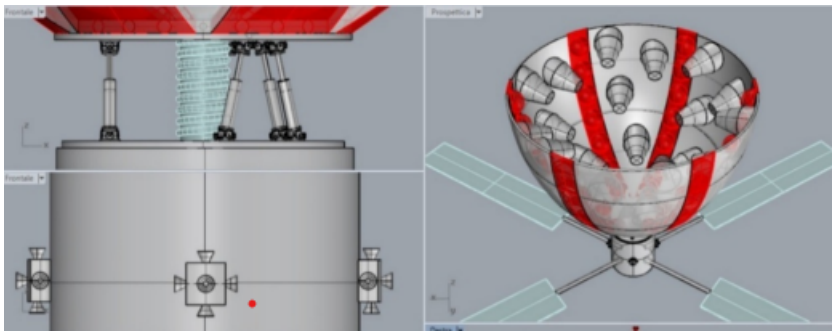


Figura 4: Schema canestro gonfiabile

3. Protezione IMINT satellitare

Nonostante il panorama bellico sia in continua evoluzione, rimanere nascosti agli avversari è sempre stata una strategia cruciale. L'obiettivo principale non è solo quello di nascondere la propria forza, ma anche di far credere al nemico qualcosa di diverso dalla realtà per ottenere un vantaggio strategico. Appare quindi evidente la necessità di proteggere i posti di comando terrestri nei confronti di IMINT satellitare (acronimo IMagery INTelligence) ovvero l'attività di raccolta di informazioni mediante l'analisi immagini satellitari.

a. *Concealment*: il camuffamento multispettrale

Con il termine *concealment*, ovvero "occultamento", si identificano in ambito militare tutto quelle misure messe in atto per impedire la rilevazione visiva di un oggetto, struttura o attività da parte dei satelliti di osservazione. I satelliti con radar ad apertura sintetica (SAR) sono strumenti molto potenti per le forze armate di tutto il mondo, in grado di localizzare il nemico e pianificare strategie di ingaggio. Questi sistemi possono penetrare l'oscurità e le nuvole per produrre immagini chiare degli assetti militari su qualsiasi continente. Fino a poco tempo fa, l'accesso a questa tecnologia era limitato alle grandi potenze militari. Tuttavia, negli ultimi anni, diverse aziende commerciali hanno iniziato a offrire immagini radar di alta qualità di qualsiasi area del pianeta. Il conflitto Russo-Ucraino ha evidenziato una volta di più l'enorme impatto operativo delle capacità spaziali. L'uso massiccio di immagini satellitari (commerciali e militari) per il *targeting* in tempo reale, l'uso da parte russa di sensori satellitari per la localizzazione di emissioni RF e successivo attacco con artiglieria o missili. Tuttavia va considerato che molti satelliti d'osservazione (soprattutto militari) montano più *payload* sensoriali: radar SAR, ottico, IR. Un camouflage solo anti-radar non sarebbe pertanto efficace. L'idea alla base del camuffamento multi spettrale (o mimetizzazione multi spettrale) è di utilizzare materiali e tecnologie avanzate per ridurre e alterare la firma elettromagnetica di un oggetto (es. veicoli, posti di comando) in più bande dello spettro: visibile, infrarosso (IR), radar e, talvolta, ultravioletto (UV). Tuttavia, non esiste un singolo materiale con un alto tasso di assorbimento su tutte le frequenze. Per ottenere e garantire un camuffamento sull'intero spettro, si possono progettare combinazioni di materiali organizzate in strutture multistrato. Storicamente, la mimetizzazione nello spettro del visibile (400-700 nm) è stata la prima ad essere sviluppata per evitare la rilevazione da parte dell'occhio umano ed è stata poi applicata a molti sistemi d'arma. L'obiettivo è rendere il bersaglio indistinguibile dallo sfondo. Per ottenere una mimetizzazione cromatica con l'ambiente possono essere usate vernici pigmentate (poliuretano, acriliche, epossidiche), pattern mimetici (UCP, MARPAT, Multicam, ecc.) oppure materiali opachi o anti-riflesso come vernici a bassa lucentezza. Ogni oggetto emette energia sotto forma di onda elettromagnetica in funzione della propria temperatura (radiazione termica), secondo la legge di Stefan–Boltzmann:

$$E = \epsilon\sigma T^4$$

La potenza della radiazione emessa è direttamente correlata all'emissività ϵ e alla quarta potenza della temperatura (T) della superficie bersaglio. Per oggetti aventi temperature inferiori a 500 gradi centigradi la radiazione termica emessa ricade interamente all'interno dello spettro infrarosso (IR). A seconda della lunghezza d'onda, la radiazione termica di un oggetto viene attenuata in misura variabile durante la sua trasmissione nell'atmosfera. Si identifica con finestra atmosferica una banda spettrale in cui l'attenuazione atmosferica è bassa. In particolare, tre finestre atmosferiche sono presenti nella banda IR: la banda IR a onde corte (SWIR, 1–2,5 μm), la banda IR a onde medie (MWIR, 3–5 μm) e la banda IR a onde lunghe (LWIR, 8–14 μm). Pertanto, la maggior parte dei rivelatori IR impiegati in applicazioni militari opera in queste tre bande.

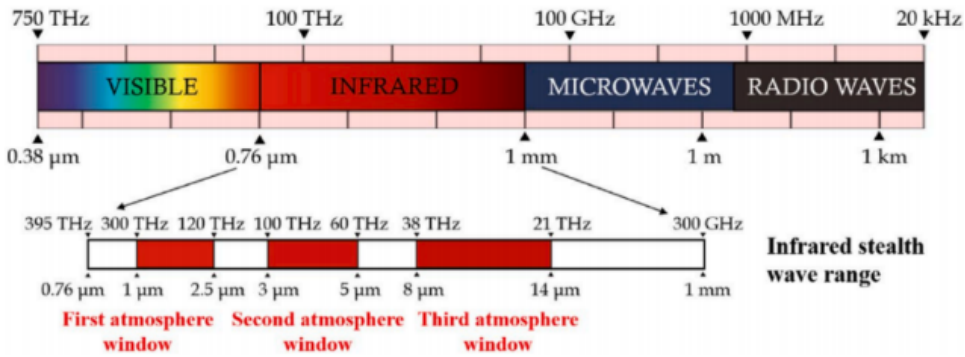


Figura 5: Spettro elettromagnetico e finestra atmosferica

Sulla base dei principi appena espressi, le strategie di mimetizzazione termica possono essere suddivise in due tipologie: progettazione di materiali a bassa emissività e progettazione di materiali a controllo di temperatura. Il modo più semplice per ottenere il camuffamento termico è attraverso un sistema passivo, che in genere utilizza strati metallici a bassa emissività realizzati con polveri di allumino (Al), rame (Cu) o argento (Ag). La riduzione dell'emissività può essere controllata regolando la forma, la rugosità, lo spessore e altri fattori della polvere. Questi rivestimenti a base metallica possono ridurre al minimo la differenza tra la radiazione IR termica del bersaglio e lo sfondo, rendendoli non rilevabili dai sistemi di monitoraggio. Tuttavia, queste polveri metalliche a bassa emissività presentano un'elevata riflettività per i campi elettromagnetici, rendendole facilmente identificabili tramite rilevamento radar. Le sostanze con la capacità di assorbimento della radiazione elettromagnetica radar sono chiamate RAM (*Radar Absorbing Materials*, ovvero materiali assorbenti le onde radio), e possono includere composti chimici con strutture cristalline regolamentate a nido d'ape, con proprietà magnetiche o dielettriche, capaci di assorbire o attenuare la radiazione incidente proveniente dal maggior numero possibile di direzioni. I fenomeni di assorbimento delle microonde avvengono grazie alla conversione del fascio di radiazione incidente in calore, e il materiale risulta tanto più efficiente quanto minore è il livello di radiazione riflessa. I RAM possono essere classificati in assorbitori risonanti (per una banda di frequenza ristretta) e assorbitori a banda larga. I RAM a banda larga si ottengono solitamente mescolando diversi tipi di materiali risonanti. Inoltre, per ottenere materiali compositi, i RAM possono essere incorporati in matrici polimeriche. A causa dell'effetto di rivestimento, il materiale composito presenta la massima efficienza quando si utilizzano particelle di dimensioni inferiori a 1 μm. Le prestazioni dei RAM sono spesso espresse con i termini "efficacia schermante" o "efficienza elettromagnetica", e il parametro misurato è l'" attenuazione" o "perdita di inserzione", che indica il rapporto tra il campo elettromagnetico in un punto nello spazio in assenza del materiale e il campo rimanente nello stesso punto in presenza del materiale stesso. L'efficienza schermante è influenzata dalla struttura del materiale, dal suo spessore, dall'angolo di incidenza e dalla frequenza del campo elettromagnetico. La tabella seguente mostra come sia possibile combinare più materiali per ottenere un camuffamento multispettrale. Giova sottolineare che le soluzioni di camuffamento devono coprire l'intera catena logistica, inclusi carburante, munizioni e camion di viveri, oltre agli assetti da combattimento come carri armati e mezzi trasporto truppe. Inoltre, se le forze armate di un Paese operano con alleati internazionali, è essenziale che tutte le forze dispongano di buone capacità di inganno e camuffamento. Infine si vuole dare uno sguardo alle possibili minacce future correlate all'intelligenza artificiale: se le tecniche presentate in questo studio al giorno d'oggi possono essere in grado di trarre in inganno anche un esperto analista di immagini, dobbiamo ipotizzare che in futuro lo sviluppo di algoritmi sempre più sofisticatati possa compromettere tale sistema di camuffamento.

Banda	Materiale/Struttura	Funzione
Visibile + IR	Vernici PU + scaglie Al	Camuffamento visivo + riduzione IR
IR + RF	Metamateriali ibridi	Assorbimento termico e radar
Visibile + NIR	Pigmenti mimetici speciali	Riflessione simile al background
Tutte	Layered composites (PU + VO + CNT)	Protezione multispettrale integrata

b. Misure *deception*

La guerra si fonda sull'inganno: far credere al nemico qualcosa di diverso dalla realtà permette di ottenere un sensibile vantaggio strategico, rallentando la capacità di analisi del nemico generando incertezza. Nel contesto militare, il termine inganno (*deception*) si riferisce all'insieme di tecniche e strategie impiegate per indurre il nemico a formulare valutazioni errate sulla forza, le intenzioni, le capacità o le disposizioni operative allo scopo di fuorviare la raccolta e l'interpretazione delle informazioni da parte dell'intelligence nemica. Lo scopo può essere raggiunto fornendo informazioni visive ambigue o ambivalenti, creando numerosi bersagli apparenti, rappresentando strutture, mezzi o attività militari false. Una prima idea potrebbe essere l'impiego di strutture fittizie (*Decoy structures/vehicles*), come veicoli gonfiabili, mezzi di legno/plastica che imitano l'aspetto di equipaggiamenti militari reali; falsi aeroporti o basi logistiche visibili dalle immagini satellitari, così da ingannare il nemico facendogli credere di osservare forze in una posizione in cui non si trovano e attirando l'attenzione su bersagli falsi. Si potrebbe anche optare per la simulazione di attività operative con rappresentazione di movimenti, tracciati di mezzi su terreni visibili dai satelliti, accensione di luci o segnali termici per simulare operazioni militari in atto, facendo credere all'intelligence nemica che siano in corso attività o manovre laddove non accade nulla. Possibili tecniche prevedono l'uso di luci notturne per simulare la presenza di personale. Al contempo si potrebbe pensare di modificare l'ambiente (*Environmental Deception*) alterando la fisica del paesaggio per creare immagini artificiali o nascondere elementi reali. Si può ipotizzare anche di mettere in atto un inganno temporale (*Timing deception*) sincronizzando le attività con le orbite note dei satelliti da osservazione in modo da evitare l'esposizione delle forze militari durante i passaggi di sorveglianza. Ad esempio interrompendo le attività durante i passaggi satellitari o inscenando attività fittizie pianificate solo durante i passaggi. In questo contesto appare evidente quanto sia fondamentale sviluppare una grande capacità *Space Situational Awareness* (SSA) con accesso e utilizzo operativo dei suoi dati per l'allerta precoce e la pianificazione difensiva.

4. NAVWAR

I sistemi GNSS (*Global Navigation Satellite System*) sono diventati strumenti strategici fondamentali nelle guerre moderne per via del loro ruolo cruciale nel garantire superiorità informativa, precisione operativa e coordinamento tattico. La sua importanza si articola su diversi livelli. In primo luogo, i sistemi GNSS sono essenziali per la navigazione e il posizionamento delle forze armate. Permette a soldati, veicoli terrestri, navi e aeromobili di conoscere la propria posizione in tempo reale, anche in ambienti sconosciuti o privi di riferimenti visivi. Questo consente movimenti più sicuri, rapidi e coordinati sul campo di battaglia, riducendo il rischio di errori e migliorando l'efficacia delle manovre militari. In secondo luogo, il GNSS è vitale per la precisione degli attacchi. Quasi tutti i sistemi d'arma moderni, come missili a guida satellitare, bombe intelligenti e droni, utilizzano coordinate GPS per colpire obiettivi con estrema accuratezza. Questo riduce i danni collaterali, aumenta l'efficacia delle missioni e consente di colpire obiettivi strategici anche a grande distanza. Appare quindi evidente come la guerra di navigazione (NAVWAR) sia una componente critica della sicurezza delle comunicazioni satellitari e dei sistemi di posizionamento globale. Pertanto i sistemi GNSS sono anche una vulnerabilità

da proteggere. Le forze nemiche possono tentare di interferire con i segnali GPS tramite *jamming* (disturbo del segnale) o *spoofing* (inganno del ricevitore), compromettendo la capacità di orientamento, guida e targeting. Di conseguenza, lo sviluppo di sistemi PNT (*Positioning, Navigation and Timing*) resilienti, tecniche di rilevamento delle interferenze e ricevitori anti-*jamming* è diventato cruciale per mantenere la supremazia operativa. *Spoofing* e *jamming* sono i principali attacchi che possono essere portati ai segnali GNSS (*Global Navigation Satellite System*). Vediamo nel dettaglio alcune tecniche che possono essere utilizzate per rilevare queste tipologie di attacchi.

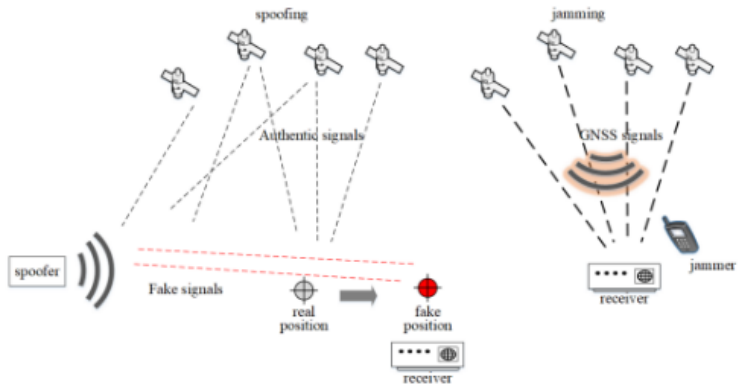


Figura 6 *Spoofing e jamming*

Spoofing Detection. Nei confronti dello *spoofing* le contromisure che possono essere adottate per la rilevazione dell'attacco comprendono l'analisi delle caratteristiche del segnale, in cui si verifica la coerenza temporale e spaziale dei segnali ricevuti (analisi dell'angolo di arrivo, analisi del tempo di propagazione); il monitoraggio della potenza del segnale, in quanto gli attacchi di *spoofing* spesso presentano potenze di segnale anomale rispetto ai satelliti legittimi; tecniche multi-frequenza, che consistono in un confronto dei segnali su diverse frequenze per rilevare discrepanze. Infine, può essere utile effettuare una triangolazione del segnale per rilevare falsi segnali da fonti terrestri.

Jamming Detection. Per poter rilevare un'azione di *jamming* la prima azione che può essere messa in atto è un monitoraggio della potenza del segnale, infatti un incremento anomalo di rumore è spesso segno di *jamming*. In seconda istanza è necessario operare un'analisi dello spettro RF in tempo reale così da identificare eventuali segnali interferenti. Oltre alle tecniche di rilevamento delle azioni offensive appena menzionate, è necessario sviluppare tecnologie PNT resilienti agli attacchi. Ne sono esempi sistemi che si basano sull'integrazione multisensore (*redundancy* multi-sensoriale), nei quali si ha la combinazione di GNSS con sistemi inerziali (INS) in grado di fornire indipendentemente dal GNSS la posizione ad alta precisione. Ai suddetti sistemi è possibile associare orologi atomici miniaturizzati al fine di mantenere la sincronizzazione temporale anche in assenza di segnale esterno. Infine, è possibile l'implementazione di filtri adattivi basati su algoritmi avanzati per correggere le perturbazioni del segnale e l'uso di segnali opportunistici per stimare la posizione. Di fondamentale importanza è la realizzazione di ricevitori anti-interferenza che siano progettati per operare anche in ambienti con elevate interferenze RF. Essi incorporano tecnologie per mitigare il *jamming* e migliorare la ricezione del segnale, antenne direzionali, che concentrando la ricezione sui segnali legittimi riducono l'impatto delle interferenze e filtri notch che permettono un filtraggio digitale avanzato in grado di sopprimere il *jamming*. Un'ulteriore alternativa è rappresentata ricevitori multicostellazione e multi-frequenza che migliorano l'affidabilità riducendo la dipendenza da una

singola fonte GNSS. Infine, in ottica futura si può pensare allo sviluppo e uso di algoritmi *machine learning* per distinguere interferenze intenzionali e accidentali.

5. Difesa dei sistemi di comunicazione satellitare

Per l'Esercito i sistemi di comunicazione satellitari (SATCOM) sono fondamentali per abilitare il comando e controllo (C2), la condivisione dell'intelligence, la consapevolezza situazionale e la coordinazione tra forze dislocate geograficamente. Per questo motivo, la loro resilienza, ovvero la capacità dei sistemi satellitari di comunicazione di resistere, recuperare e adattarsi a disturbi o attacchi – è cruciale per garantire la piena efficacia operativa. La resilienza SATCOM richiede un approccio multilivello per difendersi da un'ampia gamma di minacce, tra cui attacchi informatici, guerra elettronica (*jamming* e *spoofing*), attacchi fisici contro le infrastrutture a terra e persino l'uso di armi anti-satellite (ASAT). Questi attacchi mirano a degradare o negare la capacità di comunicazione, con il rischio di isolare le unità sul campo e compromettere le operazioni congiunte. L'ambito SATCOM è sempre più integrato con le attività CEMA (*Cyber Electromagnetic Activities*) per rilevare e contrastare in tempo reale tentativi di *jamming* o *spoofing*, fondendo la difesa cibernetica con la consapevolezza dello spettro. Per contrastare i rischi associati ai sistemi SATCOM possono essere adottate diverse strategie. In prima istanza è immediato pensare ai concetti di ridondanza e diversificazione: l'utilizzo di molteplici canali di comunicazione in modo da garantire la continuità del servizio anche in caso di compromissione di una via. Si considerino ad esempio sistemi multi orbita che sfruttano satelliti in differenti orbite (GEO, MEO, HEO, and LEO). L'adozione di schemi secondo i quali la modulazione, trasmissione e ricezione di un segnale vengono protetti tramite *Frequency hopping* (FHSS) che cambia frequenza rapidamente secondo una sequenza pseudo-casuale condivisa tra trasmittente e ricevente, rendendo difficile il *jamming* continuo. Di fondamentale importanza è anche il rinforzo della sicurezza informatica dei segmenti di terra, dei terminali utente tramite crittografia avanzata e sistemi di rilevamento intrusioni al fine difendersi da compromissioni e furti di dati.

6. Conclusione

Nel corso della storia la composizione, il numero e l'organizzazione dei posti di comando sono aumentati di pari passo con l'aumento della scala e della complessità della guerra, di conseguenza sono diventati facilmente individuabili anche da un occhio inesperto a causa delle antenne radio emettitrici, dei generatori e dei veicoli che servono per il loro sostentamento. La battaglia di Chornobaivka, in cui gli ucraini hanno degradato le capacità di pianificazione russa distruggendo ben 5 sedi di comando e i loro elementi subordinati in una serie di 21 attacchi, ha mostrato come sia necessario ripensare i posti di comando per questa nuova era della guerra. Per combattere e vincere sul campo di battaglia moderno in operazioni di combattimento su larga scala i posti di comando dell'esercito devono diventare più flessibili, agili e resilienti senza sacrificare l'efficacia, altrimenti diventeranno un luogo in cui i leader vanno a morire. Per aumentare la sopravvivenza dei posti di comando occorre ridurne le dimensioni, rinforzarli, suddividerli, camuffarli, aumentarne la mobilità e difenderli attivamente contro tutti i tipi di minacce, inclusi attacchi aerei, informatici ed elettronici. L'agilità, definita come la capacità di muovere le forze e regolare le loro disposizioni e attività più rapidamente del nemico, diventa un fattore chiave e per massimizzarla è necessario ridurre la dipendenza dalla dimensione fisica (i materiali) e aumentare l'uso della dimensione informativa (i dati). Non ci si può più affidare a sistemi a compartimenti stagni con server in loco ma bisogna migrare verso il *cloud* e sfruttare i concetti di *data mesh* e *data fabric* per garantire che i dati siano sicuri, organizzati e disponibili in modo da essere utilizzabili dai comandanti e dal loro staff.

Riferimenti bibliografici

- B. Weeden e V. Samson. Global counterspace capabilities: An open source assessment. Secure World Foundation Washington, DC, 2018
- UA Force. Counterspace Operations, Air Force Doctrine Document 2-2.1, 2 August 2004
- C. Epure, T. Zecheru, G. Epure, C. Lazaroaie, O. Iorga, R. Petre, G. Nita, M. Munteanu, D .Stoica, A. Plosnita et al. Composite Materials for passive antiradar camouflage. Materiale plastice 2020 :15–22
- L. Sansone, F. Loffredo, F. Cilento, R Miscioscia, A. Martone, N. Barrella, B. Paulillo, A. Bassano, F. Villani e M. Giordano. Recent Advances in Graphene Adaptive Thermal Camouflage Devices. Nanomaterials 2024; 14:1394
- JR Howell, MP Mengüç, K Daun e R Siegel. Thermal radiation heat transfer. CRC press, 2020
- A Rogalski. Infrared detectors: an overview. Infrared physics & technology 2002; 43:187–210
- L Li, M Shi, X. Liu, X. Jin, Y. Cao, Y. Yang, W. Wang e J. Wang. Ultrathin titanium carbide (MXene) films for high-temperature thermal camouflage. Advanced Functional Materials 2021; 31:2101381
- H. Yu, G. Xu, X. Shen, X. Yan e C. Cheng. Low infrared emissivity of polyurethane/Cu composite coatings. Applied Surface Science 2009; 255:6077–81
- Y. Li, X Bai, T. Yang, H. Luo e CW Qiu. Structured thermal surface for radiative camouflage. Nature communications 2018; 9:273
- S. Pettenuzzo. Studio di fattibilità di dispositivo gonfiabile per la cattura di asteroide
- hhttps://swfound.org/counterspace
- https://www.affarinternazionali.it/il-fronte-spaziale-della-guerra-inucraina
- SM Esercito. Nota dottrinale Le operazioni nel dominio spazio 2020.

Luca Giordano

Le Società Militari Private ed il monopolio della forza: analisi ed implicazioni

Abstract

Durante gli ultimi lustri, importanti cambiamenti intervenuti rispetto alle missioni internazionali in zone di conflitto hanno comportato, fra le altre cose, un significativo aumento della presenza di Società Militari Private (SMP) nei teatri di crisi. Rispetto all'esigenza degli Stati di garantire dispositivi di sicurezza efficaci in scenari di instabilità, questo fenomeno sembra comportare da un lato rilevanti benefici, ad esempio in termini di flessibilità operativa, competenze specializzate e potenziale riduzione dei costi; dall'altro, tuttavia, lascia emergere questioni delicate e complesse, legate fra le altre cose a dinamiche che potrebbero alimentare la persistenza dei conflitti e rendere gli Stati eccessivamente dipendenti dal loro operato. A questo si aggiungono potenziali criticità di tipo etico, politico e giuridico, afferenti ai confini del loro ruolo e delle loro attività, quindi ai rapporti con gli apparati governativi e militari e con i vari contesti locali i cui sono chiamate ad operare. Obiettivo di questo contributo è di riflettere criticamente su tale ambivalenza, onde contribuire alla comprensione del fenomeno delle SMP e delineare un quadro auspicabilmente utile per capire se e come queste possano concorrere all'offerta di sicurezza in modo lecito, costruttivo e sostenibile.

1. Introduzione

Nel corso degli anni più recenti, si è assistito a un fenomeno di evoluzione nelle missioni militari condotte oltre i confini nazionali da parte degli Stati sovrani, caratterizzato dall'emergere di elementi precedentemente non osservati. Questa evoluzione ha condotto all'aumento significativo della presenza di personale paramilitare, il quale, nonostante indossi abiti civili, è impegnato in attività di natura militare all'interno dei contesti di crisi. Questi nuovi attori si offrono frequentemente come supporto, spesso anche in sostituzione, alle forze armate regolari, partecipando sia in operazioni belliche che nelle fasi di stabilizzazione successiva ai conflitti.

Sebbene la presenza di figure quali mercenari o soldati di ventura sia stata una costante storica, è solamente in tempi recenti che si è osservata un'espansione marcata di tali soggetti in termini di notorietà, rilevanza politica ed economica, sia sul piano nazionale che su quello internazionale. Questo cambiamento non si limita a una semplice variazione di ruolo, ma indica una trasformazione più profonda. Le Società Militari Private (SMP), in particolare, hanno subito un processo di evoluzione significativo, mutando il loro ruolo da uno più tradizionale di mercenari a quello più moderno di imprenditori. Questi ultimi, in risposta alle mutate dinamiche delle crisi internazionali, ora offrono un bene sempre più richiesto dal mercato: la sicurezza.

2. Cosa sono le Società Militari Private

a. Dal mercenarismo alle Società Militari Private

Fin dalle origini delle società umane, quando una comunità di individui o uno Stato si trovava nell'incapacità di garantire autonomamente la sicurezza del proprio territorio, della proprietà privata, o di *contractors* operazioni belliche, era prassi comune ricorrere all'assistenza di soldati o unità mercenarie. Questi professionisti delle armi, che prestavano servizio per entità statali esterne o per gruppi privati con specifici interessi economici e politici, hanno avuto una

presenza continua e significativa nel corso della storia, fungendo da strumento per gli interessi di potere privati che non necessariamente coincidevano con quelli dello Stato coinvolto.

Tuttavia, questo modello iniziò a subire una profonda trasformazione con l'avvento dell'ordine *westphaliano* nel 1648, che portò all'emergere dello Stato-nazione. Quest'ultimo assunse direttamente la responsabilità della propria sicurezza e stabilì il monopolio sull'uso della forza attraverso la creazione di eserciti nazionali. A partire dal XVIII secolo, si assistette a un passaggio significativo nella gestione della guerra, che veniva ora affidata direttamente alle istituzioni statali. I governi iniziarono a esercitare il loro nuovo potere in maniera sistematica e metodica[7], reclutando i propri cittadini per difendere la sovranità nazionale e proteggere lo Stato da minacce interne ed esterne. Questo processo rafforzò notevolmente la capacità degli Stati di *contractors* alla sicurezza collettiva su scala internazionale.

Nel corso del XX secolo, però, il panorama internazionale si è notevolmente complicato, con un ritorno alla privatizzazione dei conflitti. Il fenomeno del mercenarismo ha conosciuto una nuova fioritura, alimentata dalla comparsa di diversi tipi di conflitto, che spaziavano dalle guerre civili e interne agli Stati a quelle tra Stati falliti, con una marcata presenza di paramilitari e cosiddetti "signori della guerra"[8]. Questi gruppi mercenari, specie negli anni '60 e '70, furono al centro di critiche per la brutalità e l'opportunismo dimostrati durante le fasi di decolonizzazione, talvolta opponendosi attivamente alla formazione di nuovi Stati africani[9].

La privatizzazione del conflitto si è estesa a comprendere un'ampia varietà di attori, tra cui terroristi transnazionali, cartelli della droga, gruppi armati con motivazioni ideologiche o religiose, e organizzazioni criminali internazionali. Il crescente utilizzo di *contractors* privati ha evidenziato una tendenza alla commercializzazione della guerra[10], con le SMP che sono emerse come fornitori chiave di servizi di sicurezza, pace, ricostruzione, e riforma delle istituzioni di sicurezza.

L'industria delle SMP ha visto una rapida ascesa nei primi anni '90, stimolata da fattori politici come la riduzione numerica delle forze armate seguita alla fine della Guerra Fredda, che ha generato un *surplus* di personale militare altamente qualificato disponibile sul mercato. La decisione di molti Stati di ridurre le proprie forze logistiche a favore delle unità combattenti e l'aumento delle crisi internazionali hanno messo in luce una crescente riluttanza degli Stati a impegnare truppe in operazioni non direttamente legate agli interessi nazionali primari, creando così opportunità per le SMP.

Queste società hanno efficacemente colmato il vuoto lasciato dagli Stati, offrendo servizi a basso costo e assorbendo la manodopera specializzata licenziata dagli eserciti. L'incremento del commercio internazionale di armi e la necessità di assistenza per la sicurezza negli Stati in via di sviluppo hanno ampliato ulteriormente il campo d'azione delle SMP, che sono state ingaggiate anche da organizzazioni umanitarie per proteggere il personale nelle aree di crisi.

Nonostante il ruolo positivo svolto da molte SMP a supporto di governi, forze di sicurezza internazionali, e organizzazioni umanitarie, alcune hanno servito interessi più discutibili, operando a favore di dittature, regimi autoritari, Stati falliti, criminalità organizzata, e gruppi terroristici, offrendo anche tecnologie avanzate spesso fuori dalla portata di molti attori statali deboli o in via di sviluppo.

Il successo delle SMP è stato in gran parte determinato dalla loro capacità di adottare strategie di *marketing* nel settore della sicurezza pubblica, beneficiando della privatizzazione e della globalizzazione come motori di crescita[11]. La domanda di servizi offerti dalle SMP è esplosa in seguito agli attentati dell'11 settembre, in risposta alle esigenze di difesa nazionale e collettiva, evidenziando il ruolo sempre più rilevante di queste società nel panorama della sicurezza

---

7 SCHREIER, F. –CAPARINI, M., *Privatising Security: Law, Practice and Governance of Private Military and Security Companies*, Geneva, 2005.

8 Conflitti avvenuti in Afghanistan, Sierra Leone, Somali, Colombia, Sudan, Liberia, Balcani, ecc.

9 Combatterono anche contro l'ONU durante la sua operazione in Congo ONUC, 1960/64.

10 SCHREIER, F. - CAPARINI M., *op. cit*.

11 Schreier F. - Caparini M., *op. cit*.

globale. Le principali SMP, con fatturati che si attestano su centinaia di milioni di dollari, si sono ormai affermate come attori stabili e influenti nel settore, senza segni di un possibile rallentamento o declino nel prossimo futuro.

b. Le SMP oggi

Superando l'immagine stereotipata del mercenario, comunemente percepito come un combattente solitario, subdolo e senza scrupoli, motivato unicamente da interessi economici e privo di qualsiasi vincolo etico o patriottico verso la fazione o lo Stato per il quale presta servizio, le Società Militari Private rappresentano invece entità aziendali organizzate secondo una struttura gerarchica, che offrono servizi specializzati nel contesto di guerre e conflitti, con l'obiettivo di generare profitto sul mercato globale[12].

Queste compagnie offrono una vasta gamma di servizi, che possono essere suddivisi in tre principali categorie: sicurezza e protezione, supporto operativo e servizi specializzati.

La sicurezza e la protezione comprendono la tutela di infrastrutture critiche, convogli umanitari e personale diplomatico o aziendale in contesti di conflitto o regioni ad alto rischio. Un esempio significativo è la *Blackwater*, oggi nota come *Academi* c*he* negli anni 2000 ha svolto ruoli chiave nella protezione di diplomatici statunitensi in Iraq.

Il supporto operativo, invece, include attività come l'addestramento di forze armate locali, il mantenimento di attrezzature militari e il supporto logistico in zone di guerra. *Executive Outcomes* (EO), fondata nel 1989 in Sudafrica, è un esempio emblematico di SMP impegnata in questo ambito. EO ha operato in Angola e Sierra Leone negli anni '90, fornendo soldati addestrati e supporto aereo per aiutare i governi locali a *contractors* movimenti ribelli, dimostrando come una SMP possa influenzare l'esito di un conflitto.

Infine, i servizi specializzati includono attività di intelligence, sorveglianza e gestione di tecnologie avanzate, come droni o sistemi di comunicazione. In questo contesto si colloca il *Gruppo Wagner*, una compagnia russa che, pur operando ufficialmente come entità privata, è strettamente legata agli interessi geopolitici del Cremlino ed è stata attiva in conflitti come quello in Siria, in Ucraina e in diversi paesi africani, tra cui la Repubblica Centrafricana e il Mali, dove ha fornito supporto militare ai governi locali in cambio di concessioni economiche o minerarie. Tuttavia, il gruppo è noto anche per presunte violazioni dei diritti umani, tra cui esecuzioni sommarie e torture, evidenziando i rischi derivanti dalla mancanza di regolamentazione internazionale.

Il ruolo delle SMP è favorito dalla crescente domanda di sicurezza privata in contesti di instabilità politica, dalla privatizzazione delle funzioni militari e dalla possibilità per gli stati di esternalizzare compiti sensibili, riducendo i costi e i rischi politici. Nonostante ciò, queste società operano in una zona grigia normativa: gli operatori sono generalmente classificati come civili secondo il diritto internazionale umanitario, ma possono perdere tale protezione se partecipano direttamente alle ostilità. Inoltre, la mancanza di un quadro regolatorio vincolante rende difficile perseguire legalmente le SMP per violazioni dei diritti umani o del diritto internazionale. Esempi come *EO, Blackwater* e *Wagner* dimostrano come queste compagnie possano essere strumenti strategici per stati e attori privati, ma anche fonti di *contractors* etiche e giuridiche. In definitiva, le SMP incarnano una realtà complessa e ambigua, in cui il confine tra legittimità e abuso, tra pubblico e privato, rimane sottile, sollevando la necessità di una regolamentazione internazionale più stringente e trasparente.

c. SMP e i *contractors* nel diritto internazionale: colpe e responsabilità.

Le SMP e i loro operatori, comunemente noti come *contractors*, costituiscono un tema di crescente interesse e dibattito nel diritto internazionale. Operando prevalentemente in contesti di conflitto o instabilità, spesso al di fuori di una regolamentazione chiara e uniforme, essi sollevano

[12] Vignarca F., *Mercenari S.p.A.,*

questioni cruciali riguardanti il loro status legale, la responsabilità per le loro azioni e il rispetto delle norme internazionali. La loro esistenza e il loro utilizzo riflettono la tendenza sempre più marcata alla privatizzazione delle funzioni militari, ma anche i limiti delle attuali normative internazionali nel disciplinare adeguatamente il fenomeno.

Uno dei principali problemi risiede nella difficoltà di classificare i *contractors* secondo le categorie tradizionali del diritto internazionale umanitario. Essi non appartengono alle forze armate regolari e, nella maggior parte dei casi, nemmeno a gruppi armati organizzati; tuttavia, spesso svolgono compiti che li collocano in una posizione intermedia tra civili e combattenti. In base alla Terza Convenzione di Ginevra, i civili non possono essere oggetto di attacco e godono di una protezione particolare, ma tale protezione viene meno nel momento in cui prendono parte direttamente alle ostilità. Il concetto di "partecipazione diretta" resta, tuttavia, ambiguo: sebbene sembri riferirsi a un ruolo attivo sul campo di battaglia, non è chiaro se attività di supporto, come la logistica avanzata, l'intelligence o l'uso di droni, possano essere incluse in questa definizione.

Un elemento importante nella definizione del loro status è rappresentato dall'articolo 44 della Terza Convenzione di Ginevra, che include tra i possibili prigionieri di guerra anche alcune categorie di civili che accompagnano le forze armate, come il personale logistico e i corrispondenti di guerra. Tuttavia, questa disposizione non è esaustiva, lasciando incertezza su altre figure, inclusi molti *contractors*. Nel caso in cui questi ultimi siano catturati in un contesto di conflitto, il loro trattamento dipende in gran parte dalla discrezionalità di chi li detiene e dall'interpretazione del loro ruolo. Tale incertezza espone i *contractors* a potenziali violazioni dei diritti umani e *contractors* a un quadro giuridico frammentato e incoerente.

Un tentativo di regolamentazione è rappresentato dal *Montreux Document,* un'iniziativa congiunta del Comitato Internazionale della Croce Rossa (CICR) e del governo svizzero, finalizzata a definire le responsabilità degli stati e delle SMP nei conflitti armati. Il documento, non vincolante, si divide in due parti principali: la prima delinea gli obblighi legali degli stati e delle compagnie in base al diritto internazionale umanitario e ai diritti umani; la seconda offre una serie di buone pratiche per la regolamentazione delle attività delle SMP. Gli stati che assumono sono obbligati a garantire che tali compagnie rispettino il diritto internazionale e a monitorare il loro operato. Tuttavia, il *Montreux Document* non prevede meccanismi sanzionatori o misure vincolanti, limitandosi a fornire linee guida che gli stati possono scegliere se adottare o meno.

Un ulteriore problema risiede nella responsabilità giuridica delle SMP e dei loro operatori. Secondo il diritto internazionale consuetudinario, gli stati sono responsabili per le violazioni commesse da soggetti privati solo se tali atti possono essere attribuiti allo stato stesso, ad esempio perché le SMP operano sotto il *contractors* diretto delle autorità governative o svolgono funzioni tipicamente statali. Tuttavia, molte compagnie operano con un elevato grado di autonomia, rendendo difficile dimostrare un legame diretto con lo stato che le ha assunte. Ciò consente agli stati di esternalizzare compiti sensibili, riducendo al minimo il rischio di essere ritenuti direttamente responsabili per eventuali violazioni del diritto internazionale.

Il caso *Blackwater*, legato all'uccisione di 17 civili iracheni e al ferimento di numerosi altri in un'operazione non autorizzata a Baghdad nel 2007, rappresenta un esempio emblematico delle lacune normative esistenti. In quell'episodio, la società stessa non subì conseguenze significative, evidenziando l'inefficacia delle attuali normative nel perseguire le responsabilità aziendali. Il caso sottolinea la necessità di una regolamentazione più stringente che disciplini non solo i singoli operatori, ma anche le compagnie stesse e gli stati che le ingaggiano.

Il diritto internazionale umanitario si trova quindi a fronteggiare una sfida significativa nel tentativo di inquadrare una realtà così fluida e complessa. Mentre esso è stato concepito per disciplinare i conflitti tra stati e i gruppi armati organizzati, la privatizzazione delle funzioni militari e di sicurezza ha introdotto nuovi attori che sfuggono alle definizioni tradizionali. Anche l'applicazione delle norme sui diritti umani presenta dei limiti, poiché si focalizza principalmente sugli abusi *contractors* le popolazioni civili, senza affrontare adeguatamente le questioni operative e strutturali legate alle SMP.

L'assenza di un quadro normativo vincolante e uniforme genera una serie di problemi. Innanzitutto, vi è una mancanza di trasparenza nelle operazioni delle SMP, che operano spesso in contesti lontani dallo sguardo dell'opinione pubblica e al di fuori del *contractors* parlamentare. In secondo luogo, la frammentazione normativa consente a molte compagnie di aggirare le responsabilità, ad esempio trasferendo le loro operazioni in giurisdizioni con regolamentazioni più permissive. Infine, la difficoltà di definire lo status giuridico dei *contractors* crea ambiguità sui loro diritti e obblighi, con implicazioni significative per la loro protezione in caso di cattura e per la loro responsabilità in caso di violazioni del diritto internazionale.

3. Dilemmi e opportunità: L'utilizzo delle SMP

a. Riduzione dei costi e altri vantaggi: Il crescente affidamento su SMP

Procediamo ora ad analizzare con attenzione gli aspetti che inducono gli Stati nazionali a delegare in misura crescente le proprie funzioni alle Società Militari Private e le problematiche emergenti dalla loro attività.

Primo tra i fattori considerati è la riduzione dei costi politici associati ai conflitti e ai successivi periodi di stabilizzazione, ottenuta attraverso l'assegnazione di un numero sempre maggiore di compiti a società di sicurezza private. Questo approccio consente di evitare la mobilitazione di un vasto numero di riservisti e di limitare i compromessi con gli alleati, i quali partecipano in maniera ridotta alla fornitura di truppe. Un ulteriore vantaggio si manifesta nell'assenza di proteste pubbliche in occasione della mobilitazione e del dispiegamento dei *contractors*, e più marcato ancora quando questi subiscono perdite o ferite[13].

È fondamentale sottolineare l'importanza del sostegno dell'opinione pubblica nella gestione di un conflitto: le immagini di soldati nazionali caduti mentre adempiono a missioni all'estero, diffuse dai mass media, erodono rapidamente il supporto pubblico all'intervento, spingendo verso una sua rapida conclusione, talvolta prematura rispetto al raggiungimento degli obiettivi strategici dell'operazione. L'impiego delle SMP in questi contesti tende a rimanere sotto il radar dell'opinione pubblica, o comunque a emergere meno palesemente rispetto all'azione delle forze armate convenzionali, garantendo alle missioni una durata maggiore e aumentandone la probabilità di successo. Affidare ai *contractors* operazioni ad alto rischio permette inoltre di eludere possibili ripercussioni negative sull'opinione pubblica. Un esempio significativo è fornito dalla presenza americana in Iraq, dove i *contractors* costituiscono circa il 50% del totale delle forze straniere, ma sono stati citati in appena lo 0,25% degli articoli sull'Iraq redatti da giornalisti americani, ovvero una frazione quasi insignificante[14].

Sul fronte strettamente economico, l'impiego di personale privato può tradursi in una diminuzione delle spese legate all'uso di sistemi d'arma complessi: tali sistemi, gestiti da tecnici di società private, diventano immediatamente disponibili senza la necessità di sottoporre i soldati a mesi di addestramento, con un conseguente risparmio sui costi rispetto all'utilizzo delle SMP.

Le Società Militari Private rappresentano un vantaggio significativo soprattutto per le potenze medie. Fino a un passato recente, la disparità di potenziale militare tra le nazioni non dipendeva esclusivamente da risorse finanziarie, ma da un insieme di capacità complesse: nuove tecnologie, disponibilità di risorse umane, competenze per mantenere le forze ad alti livelli di efficienza, e altro. L'emergere delle SMP ha permesso a qualsiasi nazione con risorse economiche adeguate di dotarsi di tali capacità. Non vale più la regola secondo cui un Paese con maggiori capacità militari avrebbe certamente la meglio in un conflitto: l'intervento di *contractors* può ribaltare il rapporto di forze e l'esito di un conflitto, a condizione che la nazione disponga delle necessarie risorse finanziarie.

---

13 Si stima che ad oggi oltre 1.000 contractors siano stati uccisi in Iraq e più di 13.000 feriti.
14 SPINELLI, G., *Contractor,*2009.

In relazione al contenimento dei costi, i *contractors* assumono un'importanza cruciale per i bilanci di Paesi di dimensioni medio-piccole, che non dispongono delle risorse necessarie per sostenere un apparato militare completo in tutte le sue funzioni operative. Tali Paesi devono quindi stabilire delle priorità, assicurando le capacità essenziali e affidandosi alle SMP per le restanti, evitando così di gravare continuamente sul bilancio statale in previsione di eventi che, negli scenari attuali, hanno scarse probabilità di verificarsi.

Un ultimo aspetto da considerare è che la privatizzazione ha permesso a diversi governi, tra cui quello statunitense, di agire con mezzi meno evidenti in situazioni imbarazzanti all'estero, evitando così complicazioni di natura diplomatica, economica o legate alla possibile violazione dei diritti umani. Un episodio emblematico si è verificato nel 1995, quando il governo degli Stati Uniti ingaggiò una società privata di sminamento, la RONCO, per operare in Ruanda, superando così l'embargo delle Nazioni Unite sull'invio di materiale bellico al paese, attraverso l'importazione di esplosivi e veicoli blindati.

b. Benefici e criticità: l'equilibrio precario nell'impiego delle SMP

Se da un lato l'ingaggio di soggetti privati nel settore della difesa e della sicurezza può offrire agli Stati una serie di benefici notevoli, quali flessibilità, competenze specializzate e potenzialmente una riduzione dei costi, dall'altro lato emergono questioni complesse e sfaccettature critiche che meritano un esame approfondito.

Prendendo in considerazione la problematica del conflitto di interessi, è evidente che le Società Militari Private trovano la propria ragion d'essere e i propri introiti nella gestione e nella persistenza dei conflitti. Questo solleva dubbi significativi sulla loro motivazione intrinseca a operare in direzione della risoluzione dei conflitti, mettendo in luce un potenziale *contractors* con l'obiettivo più ampio di pace e sicurezza internazionale. La questione si complica ulteriormente considerando la possibilità che le SMP possano avere un interesse economico nella continuazione o nell'*escalation* dei conflitti, al fine di mantenere o aumentare i propri *contractors* e profitti.

Un altro punto critico riguarda i rischi per gli Stati derivanti dall'eccessiva dipendenza dai *contractors* privati. Un livello elevato di esternalizzazione può portare a una situazione in cui una SMP diventa così integrata nelle funzioni di difesa e sicurezza di uno Stato da acquisire un *contractors* esclusivo su alcune di queste funzioni critiche. In tali circostanze, si potrebbe verificare un'influenza indebita o addirittura forme di coercizione da parte dell'entità privata verso lo Stato, soprattutto se la dipendenza diventa così marcata da rendere lo Stato vulnerabile a pressioni o ricatti.

La mentalità che caratterizza l'operato dei *contractors*, rappresenta un'ulteriore problematica, poiché gli stessi sono vincolati da accordi che definiscono compiti e obiettivi specifici, spesso senza tenere conto di aspetti fondamentali per il successo a lungo termine delle missioni, come il sostegno e la fiducia della popolazione locale o il rispetto dei diritti umani. Questo approccio può portare a valutazioni basate unicamente su criteri di efficienza operativa, trascurando l'importanza di costruire relazioni positive con le comunità locali e rispettare principi etici fondamentali.

L'apparente impunità di cui godono le SMP costituisce un grave problema. Nonostante esistano strumenti giuridici internazionali volti a regolamentare le attività delle forze armate private e il personale di sicurezza, le normative attuali presentano limitazioni significative, in particolare per quanto riguarda la definizione stessa di "attività mercenaria". Queste lacune normative permettono alle SMP di operare in un contesto di relativa impunità, eludendo spesso meccanismi efficaci di *accountability*.

La questione della legittimità delle SMP agli occhi delle popolazioni locali è altrettanto rilevante. La percezione pubblica non distingue sempre chiaramente tra *contractors* privati e forze armate regolari, con il risultato che le azioni delle SMP possono riflettersi negativamente

sull'immagine delle forze armate nazionali e internazionali, complicando ulteriormente gli sforzi di stabilizzazione e ricostruzione.

L'impiego delle SMP solleva, infine, questioni di equilibrio tra il settore pubblico e quello privato nella gestione dei servizi di difesa e sicurezza. L'introduzione di attori privati in questo settore può alterare dinamiche consolidate, con impatti variabili a seconda del contesto geografico e politico. In particolare, nei Paesi con strutture statali deboli o in fase di sviluppo, l'ingaggio di SMP da parte di *leader* politici o militari può *contractors* a ulteriori instabilità e tensioni.

4. Il caso Blackwater USA

Tra le Società Militari Private, un'attenzione particolare merita Blackwater USA. Fondata nel North Carolina nel 1997 da Erik Prince, ex membro dei *Navy Seals* e figlio di un influente imprenditore, l'azienda ha avuto origine con l'investimento dei proventi derivanti dalla vendita dell'impresa paterna, inizialmente stabilendosi come un ampio campo di tiro. Da allora, Blackwater si è espansa in numerosi ambiti, dall'addestramento avanzato alla mobilità e logistica, e più specificatamente nei settori della protezione e del supporto combattivo diretto.

Il successo di Blackwater si deve alla capacità di capitalizzare i periodi post-crisi sia nazionali che internazionali, introducendo, ad esempio, programmi di addestramento per prevenire attacchi nelle scuole in seguito alla strage di Columbine del 1999, o corsi per la difesa antiterrorismo rivolti ai marinai dopo l'attacco alla USS Cole nel 2000, e sviluppando un'intensa attività di *lobbying* presso il Congresso americano.

Gli eventi dell'11 settembre 2001 hanno particolarmente agevolato Blackwater, che ha ricevuto sostanziali supporti economici dal governo Bush, con *contractors* superiori ai 500 milioni di dollari, ottenendo accessi e possibilità quasi illimitate nelle operazioni in Iraq.

Attualmente Blackwater, che dal 2011 pur mantenendo la stessa struttura societaria ha cambiato denominazione in Academi, impiega oltre 2.300 persone attive e ha un database di più di 21.000 ex militari, poliziotti, agenti della CIA e affini, con piani di espansione in California, Illinois e nelle Filippine. Addestra annualmente più di 40.000 individui provenienti da vari eserciti e organizzazioni private, definendosi "la più completa compagnia militare professionale al mondo"[15] e vantando tra i suoi clienti multinazionali, il Pentagono e il Dipartimento di Stato USA, con cui ha *contractors* attivi per 832 milioni di dollari. Sul campo, i suoi operatori hanno una larga autorizzazione all'uso della forza letale, sia per autodifesa che per la difesa di proprietà e per fermare, detenere e perquisire civili.

Nonostante sia una delle più riuscite SMP, Blackwater rappresenta anche l'emblema dell'incontrollabilità di queste entità. La società è diventata nota al grande pubblico nel marzo 2004, quando quattro dei suoi impiegati furono uccisi dalla folla irachena nel "triangolo sunnita". Questo episodio ha evidenziato il numero crescente di *contractors* nel Paese e i loro abusi, che hanno esacerbato il malcontento della popolazione irachena, già messa a dura prova dall'instabilità del conflitto.

Nonostante non sia l'unica compagnia accusata di incidenti che hanno avuto ripercussioni negative sugli sforzi di stabilizzazione, Blackwater ha acquisito una reputazione particolare per le tragedie causate, inclusa quella del 24 dicembre 2006, quando un suo dipendente in stato di ebbrezza uccise la guardia del corpo del vicepresidente iracheno, e la strage del 16 settembre 2007 in piazza Nisour a Baghdad, con 17 civili iracheni uccisi, che ha portato a un'indagine governativa sotto la guida del deputato statunitense Henry Waxman. L'inchiesta si è conclusa con una semplice assoluzione della società, nonostante le 195 sparatorie coinvolgenti Blackwater dal 2005 a inizio settembre 2007, con 163 causate dalla reazione eccessiva dei suoi impiegati (84% dei casi) e un totale di circa 203 persone uccise.

---

15 SCAHILL, J., *Blackwater: the rise of the world's most powerful mercenary army, New York 2007*

Circa 200 dipendenti sono stati licenziati per vari motivi, inclusi abuso di armi e cattiva condotta, ma in assenza di segnalazioni specifiche, il licenziamento rimane l'unico rischio per i suoi operatori, che facilmente trovano impiego altrove con retribuzioni simili. L'inchiesta Waxman ha rivelato una prassi comune per la gestione degli abusi commessi dalle SMP: il Dipartimento di

Stato americano suggerisce alla società coinvolta di compensare economicamente le famiglie delle vittime, facilitando il ritorno degli uomini coinvolti in episodi che hanno portato alla morte di molte persone, senza che nessuno venga mai incriminato.

5. Conclusioni

Questo studio ha analizzato il ruolo delle Società Militari Private (SMP), evidenziando come esse abbiano assunto una crescente centralità nelle dinamiche della sicurezza globale. Attraverso un approccio storico e un esame delle loro pratiche attuali, si è osservato che le SMP si collocano in un continuum di opportunità e dilemmi, offrendo vantaggi immediati ma sollevando al contempo rischi significativi.

Le SMP si sono dimostrate strumenti pratici ed efficienti in contesti di conflitti asimmetrici, guerre civili e crisi internazionali, grazie alla loro capacità di fornire competenze militari altamente specializzate e supporto logistico e operativo. Queste caratteristiche assumono particolare rilevanza in un'epoca in cui gli Stati tendono a evitare l'impiego di forze militari convenzionali in teatri di guerra considerati non strategici. In tal senso, le SMP *contractors* a ridurre i costi politici ed economici associati ai conflitti, offrendo un sostegno cruciale sia a potenze minori sia a Stati con risorse limitate, consentendo loro di accedere a capacità militari avanzate altrimenti inaccessibili.

Tuttavia, il ricorso alle SMP solleva problematiche di primaria importanza legate alla loro legittimità, responsabilità ed etica. In quanto entità orientate al profitto, possono generare conflitti di interesse che rischiano di prolungare le ostilità anziché una loro risoluzione. Inoltre, l'assenza di un quadro normativo uniforme e di meccanismi di supervisione efficaci facilita l'emergere di situazioni di impunità, sollevando questioni giuridiche e morali di grande complessità. L'esternalizzazione di funzioni tradizionalmente riservate alle forze armate statali pone, inoltre, interrogativi cruciali riguardo alla sovranità nazionale, all'efficacia della governance democratica e alla distribuzione del potere militare nel sistema internazionale.

Data la complessità di questo fenomeno, appare indispensabile un'accurata riflessione sulle modalità di regolamentazione e *contractors* delle SMP, con l'obiettivo di garantire che le loro attività si svolgano nel rispetto dei principi di legalità internazionale, trasparenza ed etica. È prioritario sviluppare un quadro normativo globale capace di affrontare le sfide poste dall'impiego di queste società, assicurandosi che le loro operazioni *contractors* alla sicurezza internazionale senza pregiudicare i diritti umani o compromettere l'integrità delle istituzioni statali.

In primo luogo, è fondamentale un impegno coordinato a livello internazionale per rafforzare e armonizzare le normative esistenti, colmando le lacune che consentono alle SMP di operare in una zona grigia di responsabilità legale. L'adozione di standard internazionali uniformi per la registrazione, il monitoraggio e la rendicontazione delle attività delle SMP potrebbe migliorare significativamente la trasparenza e la responsabilità, mitigando i rischi associati al loro utilizzo. Parallelamente, gli Stati dovrebbero implementare politiche nazionali più rigorose, includendo criteri stringenti per l'assegnazione di *contractors*, meccanismi di supervisione adeguati e requisiti chiari per il rispetto dei diritti umani e del diritto internazionale umanitario.

Un elemento centrale nella gestione delle SMP riguarda l'accountability per eventuali violazioni dei diritti umani o altri crimini commessi durante le operazioni. È indispensabile garantire che le vittime di tali abusi abbiano accesso a strumenti legali efficaci per ottenere giustizia e riparazione, e che i responsabili siano perseguiti conformemente alle leggi nazionali e internazionali. Inoltre, una maggiore trasparenza nelle attività delle SMP, accompagnata da un dialogo inclusivo tra governi, organizzazioni internazionali, società civile e le stesse SMP, potrebbe favorire una più profonda comprensione delle implicazioni strategiche ed etiche del loro

impiego. Ciò *contractors* a costruire un consenso globale sul loro ruolo appropriato nella sicurezza internazionale e sulla necessità di regole chiare per disciplinarne l'operato.

Infine, data la crescente importanza delle SMP nel panorama globale, è essenziale che la loro integrazione nei sistemi di sicurezza avvenga in modo da rafforzare, e non indebolire, gli sforzi internazionali per la pace, la stabilità e il rispetto dei diritti umani. Questo richiede un delicato equilibrio tra il riconoscimento del loro potenziale *contractors* e la gestione attenta dei rischi derivanti da un *contractors* insufficiente o inadeguato. La definizione di linee guida e standard condivisi deve essere accompagnata da un impegno deciso nel promuovere la cooperazione internazionale e nel garantire la coerenza tra le attività delle SMP e i principi fondamentali della Comunità Internazionale.

In ultima analisi il fenomeno delle SMP rappresenta una sfida complessa ma non insormontabile per la comunità globale. Un approccio equilibrato, basato su regolamentazioni chiare e un'efficace supervisione, può consentire di sfruttare al meglio le opportunità offerte da queste società, minimizzando i rischi per la legalità internazionale, l'etica e la stabilità socio-politica. Solo attraverso uno sforzo collettivo e coordinato sarà possibile garantire che le SMP operino come attori responsabili nel contesto della sicurezza internazionale, *contractors* alla promozione della pace e del rispetto dei diritti fondamentali.

Data la natura delle minacce future, prevalentemente intrastatali e legate all'escalation del terrorismo internazionale, appare necessaria una trasformazione nei modelli di sicurezza che la Comunità Internazionale deve adottare. Si anticipa un maggiore coinvolgimento del settore privato nel *contractors* a minacce transnazionali come quelle rappresentate da gruppi criminali e organizzazioni terroristiche, nonché nel mantenimento della pace e della sicurezza internazionale.

In questo contesto, diventa cruciale per la Comunità Internazionale sviluppare meccanismi di regolamentazione, *contractors* e rendicontazione più efficaci. Questo non solo per minimizzare i rischi connessi all'attività delle SMP ma anche per garantire che il loro apporto alle operazioni di sicurezza e peacekeeping avvenga nel pieno rispetto dei principi di legalità, etica e trasparenza. Affrontare queste sfide necessiterà di un impegno concertato da parte degli Stati, delle Organizzazioni Internazionali, della società civile e delle stesse SMP, orientato verso un modello di governance che sappia bilanciare le esigenze di efficacia operativa con quelle di responsabilità e giustizia a livello globale.

Bibliografia

Libri

- MARINI, L., *Società militari private e contractors,* Torino 2012.
- MONTANARI, P. - MAZZOCCHI, C. - DERIU, M. (a/c), *Guerre private: ascesa e ramificazioni dell'industria militare privata,* 2006.
- PAGLIANI, G. e PIGOLI, A., *Il mestiere della guerra dai mercenari ai manager della sicurezza,* 2004.
- POLICANTE, A., *I nuovi mercenari. Mercato mondiale e privatizzazione della guerra,* Verona 2012.
- RONZITTI N., *Introduzione al diritto internazionale,* Torino 2007.
- RONZITTI, N., *Diritto internazionale dei conflitti armati,* Torino 2011.
- SCAHILL, J., *Blackwater: the rise of the world's most powerful mercenary army,* New York 2007.
- SPINELLI, G., *Contractors,* Milano 2009.
- VIGNARCA, F., *Mercenari s.p.a,* 2004.

Pubblicazioni e documenti

- BURES, O., *Private Military Companies: A Second Best Peacekeeping Option?*, paper presented at the annual meeting of the ISA's 49th Annual Convention, 2008.
- FRANCIONI F.- RONZITTI N., *War by Contractors. Human Rights, Humanitarian Law, and Private Contractors*, Oxford University Press, 2011.
- GANTZ, *P.H., The Private Sector's Role in Peacekeeping and Peace Enforcement*, Refugees International, 2003.
- GODDARD, S., *The Private Military Company: A Legitimate International Within Modern Conflict*, a thesis presented to the Faculty of the U.S. Army Command and General Staff College. Fort Leavenworth, Kansas, 2001.
- SCHREIER e CAPARINI, F. F.Caparini , M., *Privatising Security: Law, Practice and Governance of Private Military and Security Companies*, 2005.
- SHEARER, D., *Private Armies and Military Intervention*, International Institute for Strategic Studies, Oxford University Press, 1998.
- SINGER, P. W., *Can't Win With 'Em. Can't Go To War Without 'Em: Private Military Contractors and Contractors*, Brookings Institution, 2007.
- SINGER, P.W., *Corporate Warriors. The Rise of the Privatized Military Industry*, Cornell Studies, 2007.
- SPINEDI M., *La responsabilità dello Stato per comportamenti di private contractors*, in Spinedi M., Giannelli A., *La codificazione della responsabilità internazionale degli Stati alla prova dei fatti, Problemi e spunti di* riflessione, Milano, 2006.
- The Geneva Centre for the Democratic *Contractors* of Armed Forces, *Private Military Companies*, "DCAF Backgrounder", 2006. The Green Book, *Private Military Companies: Options for Regulation*, ordered by the House of Commons, 2002.
- TRIZIO, R., *Mastini della guerra Spa*, "Corriere della Sera", 6 aprile 1998.

Articoli internet

- www.pwsinger.com/
- www.ssrnetwork.net/topic_guides/pmcs.php
- www.shadowcompanythemovie.com/pressbits/shadow_release_WEB.pdf
- www.globalsecurity.org/military/world/para/pmc-list.htm
- www.globalpolicy.org/security/peacekpg/reform/training.htm
- www.dcaf.ch/ The Geneva Centre for the Democratic *Contractors* of Armed Forces
- www.tio.ch
- www.geopolitica.info
- www.cncmedia.com

Roberto LIZZA

L'evoluzione dell'impegno italiano nel fianco est dell'Alleanza Atlantica

Abstract

L'articolo ripercorre l'evoluzione dell'impegno politico-militare italiano nel fianco est dell'Alleanza Atlantica, prendendo come riferimento temporale di interesse l'inizio del conflitto tra Russia e Ucraina nel febbraio del 2022. Ciò consente non solo una comparazione diacronica utile a verificare empiricamente il mutamento dell'impegno italiano rispetto al versante orientale della NATO negli ultimi anni, ma, in un'ottica di interdipendenza geografica e funzionale, anche una riflessione più ampia e generale sulle potenziali ricadute politiche di questo impegno rispetto alle esigenze di sicurezza dell'Italia rispetto al fianco sud dell'Alleanza Atlantica (peraltro in una cornice regionale ove il Paese potrebbe aumentare, almeno a fronte di alcune chiare scelte di policy, il suo ruolo propulsivo tanto rispetto all'ambito NATO quanto in relazione al contesto dell'UE).

1. Premessa

"Quello che stiamo vivendo è la morte cerebrale della NATO", così affermava il Presidente francese Emmanuel MACRON nel corso di un'intervista al settimanale *The Economist* nel 2019[1]. La metafora provocatoria, avente lo scopo di scuotere le coscienze degli altri *leader* europei circa la necessità di affrancarsi dagli Stati Uniti d'America, aveva però suscitato più commenti di disapprovazione (*in primis* da parte degli stessi USA e della Germania) che consensi (*in primis* della Russia, da tempo critica sulle condizioni dell'Alleanza). La frase, in realtà, era stata pronunciata con assoluto raziocino e puntualità, dal momento che seguiva il disimpegno americano dalla Siria e l'inasprimento dell'aggressività in politica estera della Turchia, importante stato membro dell'Alleanza. Inoltre, consolidava la volontà francese di svincolarsi dagli impegni transatlantici e porsi quale paese di riferimento nello sviluppo e nel rafforzamento della difesa europea. A conferma della tesi del Presidente Macron, va precisato che la NATO, in seguito al repentino crollo dell'Unione Sovietica e al conseguente dissolvimento del Patto di Varsavia, ha perso improvvisamente la sua primaria funzione di difesa della frontiera dell'Europa Occidentale, limitandosi a svolgere operazioni in risposta a crisi internazionali al di fuori dei propri confini. Il suo punto di massima involuzione, complice certamente la divergenza di interessi degli stati membri e la mancanza di assunzione di responsabilità dei paesi europei (Italia compresa), si è visto, a mio avviso, nell'estate del 2021 con la veloce riconquista talebana dell'Afghanistan, dal quale si erano da poco ritirate le truppe americane e, conseguentemente, quelle di tutti gli altri contingenti schierati nel paese asiatico.

La percezione di un'Alleanza Atlantica debole e frammentata potrebbe essere stato uno dei motivi che ha spinto il Presidente russo Vladimir Putin ad avviare l'"Operazione militare speciale" in territorio ucraino il 24 febbraio 2022. Il risveglio dell'antico avversario, oltre a spingere due importanti paesi quali Svezia e Finlandia a chiedere una storica adesione alla NATO, sembrerebbe aver smosso le coscienze dei *leader* e delle opinioni pubbliche più refrattarie a porre in essere un impegno concreto e unitario in seno all'Alleanza, "spolverando" un fronte comune in cui impegnarsi militarmente, laddove necessario, anche in un conflitto convenzionale simmetrico, su larga scala e di lungo periodo.

---

[1] https://www.economist.com/europe/2019/11/07/emmanuel-macron-in-his-own-words-english, intervista con- dotta all'Eliseo il 21 ottobre 2019 e pubblicata il 9 novembre successivo.

In tale complesso contesto geopolitico, appare necessario analizzare il ruolo che l'Italia vuole rivestire nel prossimo futuro. Al riguardo, lo scopo di questa breve tesi è di fornire una visione d'insieme dell'impegno nazionale nel fianco est dell'Alleanza Atlantica, con specifico riferimento alla componente militare.

L'elaborato è strutturato su tre capitoli. Nel primo, viene analizzato l'impegno nazionale nel fianco est antecedente allo scoppio delle ostilità in Ucraina nel febbraio 2022, mentre il secondo fornisce una visione d'insieme dello sforzo profuso ad oggi dalla Difesa nell'area in esame, con dati aggiornati al 2° semestre 2024. Il terzo capitolo evidenzia infine quelle che potrebbero essere le prospettive d'impiego futuro dello strumento militare nazionale. La tesi termina con un paragrafo a parte dedicato ad alcune riflessioni conclusive.

2. L'impiegno antecedente al 24 febbraio 2022

Se proviamo a guardare la capacità di adattamento della NATO nel tempo, possiamo sicuramente riconoscere almeno tre grandi stagioni. La prima, che *de facto* ha visto nascere la NATO ed è iniziata subito dopo la fine della seconda guerra mondiale, è caratterizzata dal contrasto a quello che una volta era "il partito arancione" ovvero l'Unione Sovietica. Il mondo era fortemente bipolare e lo schieramento e il "nemico" erano ben chiari e materializzati sul terreno; basti pensare alla cortina di ferro e alla lista degli stati "rossi" o "blu" e di quei paesi che si definivano, forse anche con un po' di scaltrezza, "non allineati". Il crollo del muro di Berlino nel 1989 e il successivo sgretolamento dell'Unione Sovietica nel 1991 ha segnato l'avvio di un trentennio di profondo cambiamento, caratterizzato da un mondo unipolare a trazione statunitense. Il paese, autoproclamatosi "poliziotto del mondo", trascina con sé l'Alleanza in una nuova veste, che la vede protagonista nelle operazioni che poi chiameremo di *Counter Insurgency* (COIN), e che dalla parte italiana si traducono nell'intervento nei Balcani con SFOR e poi con KFOR, successivamente in Afghanistan con Nibbio (diventata in seguito ISAF/RSM) e Iraq con "Antica Babilonia". La minaccia diventa dapprima di matrice terroristica islamica e poi ibrida. La progressiva assertività russa nell'area europea, ma anche sul fianco sud dell'Alleanza, ha quindi portato a un ulteriore cambiamento delle capacità dello strumento militare della NATO, che ovviamente "esplode" a valle dell'invasione russa in Ucraina.

A seguito dell'annessione della Crimea da parte russa nel marzo 2014 la NATO, in particolare i paesi membri collocati lungo il suo fianco est, inizia a materializzare l'aumento della risolutezza russa lungo il confine orientale. L'annessione avviene principalmente attraverso l'impiego di quelli che sono passati alla storia come "omini verdi"[2], cioè uomini delle forze regolari russe privati di ogni insegna che li potesse rendere riconoscibili. Tutto questo avviene sotto gli occhi impotenti, o incoscienti, di gran parte del mondo occidentale e viene "ufficializzato" da un referendum a metà dello stesso mese di marzo, immediatamente riconosciuto valido dalla Russia. Nello stesso anno a seguito del *Summit* dei Capi di Governo della NATO, riunitisi a Newport in Galles (settembre 2014), si arriva all'approvazione del NATO *Readiness Action Plan* (RAP), un piano che assicura a tutti gli alleati, con chiaro riferimento alle nazioni più esposte del fianco est, la capacità di risposta alle nuove sfide sulla sicurezza, prevedendo una serie di misure concrete di ristrutturazione dello strumento e di presenza militare sul territorio. Nascono dal RAP le *Assurance Measures* e le *Adaptation Measures.* Le prime si estrinsecano in una serie di attività navali (*Standing Maritime Group*), aeree (*Air Policing*) e terrestri (*enhanced Forward Presence* – eFP), che prevedono l'aumento delle forze NATO proprio nelle aree maggiormente esposte alla minaccia. Le altre invece riguardano appunto la ristrutturazione dello strumento attraverso l'incremento delle capacità e della prontezza della NATO *Responce Force* e la creazione di una serie di Comandi (principalmente di Corpo d'Armata e divisionali) per abilitare la funzione di Comando e Controllo delle forze che

[2] https: //www.difesaonline.it/mondo-militare/siria-putin-invia-gli-omini-verdi. Siria: Putin invia gli "Omini Verdi", 24 ottobre 2015 (accesso effettuato il 18/11/2023).

saranno allocate per i *Graduated Responce Plan* (GRP), piani sviluppati in parti successive predisposti con lo scopo di affrontare molto rapidamente eventuali minacce esistenziali contro l'Alleanza[3]. In particolare la prontezza NATO *Response Force* (NRF) diventa *enhanced* NRF, triplicando il *basket* di forze a disposizione, passando da 13 mila a 40 mila unità e prevedendo al proprio interno la *Very High Readiness Joint Task Force* (VJTF) con la possibilità di schierare una "*spearhead force*", che conta, tra le altre forze, una componente terrestre a prontezze differenziate (*Notice to Move,* NTM) di circa 5000 uomini.

Negli anni il RAP viene avviato con la ristrutturazione della Catena C2 e al *Summit* dei Ministri della Difesa della NATO, svoltosi a Bruxelles nel febbraio 2016, si prende coscienza della necessità di avviare nei Paesi baltici e in Polonia lo schieramento di forze terrestri allo scopo di mostrare la solidarietà tra tutti gli Alleati e la solidità della nuova postura difensiva della NATO. L'iniziativa eFP viene così ufficializzata al *Summit* dei Capi di Stato e di Governo della NATO a Varsavia nel luglio dello stesso anno, con l'impegno di schierare entro giugno dell'anno successivo quattro *Battle Group* (BG), rispettivamente a *framework* Canada in Lettonia, Stati Uniti in Polonia, Germania in Lituania e Regno Unito in Estonia, complementari alle forze in prontezza dell'Alleanza (NRF) e affiancati alle *National Homeland Defence Forces* (NHDF) delle *Host Nation* (HN).

In tale contesto, l'Esercito Italiano ha schierato in Lettonia un'unità a livello compagnia di manovra, supportata da un'adeguata componente logistica nazionale e personale di *staff* impiegato all'interno del BG HQ a guida canadese. Inizialmente, il contingente nazionale era a rotazione semestrale estiva su base fanteria pesante e invernale su base fanteria alpini. A partire da giugno 2022 la rotazione avviene solo tra forze pesanti, in risposta alle nuove esigenze sorte a seguito dell'invasione russa dell'Ucraina.

La Marina Militare ha contribuito alle *Standing Naval Forces* (SNF), operando nell'ambito dello Standing *NATO Maritime Group* (SNMG). I Gruppi Navali Permanenti della NATO sono gruppi navali multinazionali integrati, che fanno parte della NRF, operano sotto il Comando della Componente Marittima Alleata (MARCOM Northwood) e costituiscono una presenza continua e visibile della solidità e coesione dell'Alleanza. Inoltre assetti nazionali hanno contribuito allo *Standing NATO Mine Counter Measures Group* (SNMCMG), forza marittima multinazionale integrata, composta da navi appartenenti a diverse nazioni alleate, che si addestrano e operano insieme e che sono permanentemente disponibili per portare a termine missioni NATO con competenze specifiche nella lotta alle mine navali. La Marina Militare ha operato sia nei Gruppi Atlantico orientale (SNMG1 e SNMCMG1) sia in quelli Mar Mediterraneo (SNMG2 e SNMCMG2), garantendo a rotazione il ruolo di *Framework nation* e contribuendo ai MG delle altre nazioni tramite l'impiego di idonei assetti navali quali fregate, cacciamine e navi ausiliarie.

Riguardo la componente aerea, la NATO ha istituito *l'Air Policing* (AP) a partire dalla metà degli anni cinquanta per integrare gli apparati e gli assetti dei paesi membri in un unico sistema di difesa aerea e missilistico. L'iniziativa consiste nella continua sorveglianza dello spazio aereo alleato e nell'identificazione di tutte le eventuali violazioni allo stesso. Le operazioni sono svolte da caccia intercettori pronti al decollo in tempi rapidissimi (*scramble*) e le missioni di *Air Policing* sono condotte sotto il comando e controllo di due centri operativi NATO, ubicati rispettivamente a Uedem (Germania) e Torrejon (Spagna), sotto la supervisione dall'*Allied Air Command* di Ramstein (Germania). Nell'ultimo periodo e fino all'inizio del 2022, l'Aeronautica Militare ha schierato in Romania (2019 e fine 2021 – 1° semestre 2022) una *Task Force* su cacciabombardieri Eurofighter EF-2000. Nel merito, l'Italia è l'unica nazione dell'Alleanza Atlantica che ha partecipato a tutte le operazioni di *Air Policing* realizzate fino ad oggi.

---

[3] *NATO AJP-5 "Allied Joint Doctrine for the Planning of Operations",* Ed. A Versione 2, maggio 2019.

3. La situazione attuale

a. NATO *Strategic Concept* 2022 e *Summit di Vilnius* 2023

Nel febbraio 2022, a distanza di otto anni dall'annessione della Crimea, si arriva all'aggressione russa dell'Ucraina con l'impiego, in questo caso, di forze regolari russe, oltre che di forze irregolari come i membri della PMC[4] Wagner.

La reazione della NATO si ha con il *Summit* dei Capi di Stato di Madrid di giugno 2022, in cui viene formalizzato lo *Strategic Concept* 2022, documento che definisce l'Europa come non più in pace. Il contesto strategico di riferimento vede ancora gli USA quale unica potenza in grado di esprimersi pienamente negli ambiti economico, diplomatico, politico e militare, anche se la Cina ha ridotto di molto le distanze sul piano economico e, nel futuro, è verosimile che le accorci parimenti anche sul piano militare. La Federazione Russa viene menzionata quale minaccia più significativa, affermazione che spinge la NATO a rafforzare il proprio fianco est. In questo quadro di riferimento, i tre *core task* già definiti nel precedente Concetto Strategico del 2010, ossia "*deterrence and defence*", "*crisis prevention and management*" e "*cooperative security*", vengono resi per la prima volta subalterni alla difesa collettiva. Si pone grande attenzione alla deterrenza e difesa per la gestione delle crisi relative al territorio dell'Alleanza e, pur mantenendo un approccio tendenzialmente globale per la loro gestione, la priorità muove verso la prontezza contro una guerra convenzionale. Inoltre, viene posta maggiore enfasi sul NATO *Crisis Response System*, un sistema di linee guida, approvate dal *North Atlantic Council* (NAC), che ha lo scopo di fornire all'Alleanza un set di opzioni e misure per gestire e rispondere a crisi e cambiamenti repentini del *security environment*, con il necessario grado di progressività e tenendo in considerazione strumenti e capacità disponibili. In particolare, le *Crisis Response Measures* (CRM) sono dichiarazioni che, una volta approvate dal NAC e promulgate dal SACEUR[5], richiedono l'esecuzione di azioni specifiche da parte delle nazioni e dei Comandi NATO. Le CRM sono pensate principalmente per facilitare la preparazione e l'attivazione delle forze ovvero per iniziare azioni che richiedono una rapida reazione. Queste misure vanno dalla richiesta delle *diplomatic clearance* per il sorvolo degli stati membri all'abbassamento delle prontezze di determinati assetti, all'attivazione di determinati piani o all'avvio dello schieramento di unità predefinite. Come risultato operativo finale si ha l'attivazione dei piani di difesa della NATO e l'immediato impiego in Romania dello *spearhead battalion*, elemento a più alta prontezza nell'ambito della NRF, che nel 2022 era stato offerto dalla Francia, nazione responsabile della VJTF per quell'anno. Al riguardo viene inoltre avviata l'iniziativa *enhanced Vigilance Activities* – eVA, con lo schieramento in Slovacchia, Ungheria, Romania e Bulgaria di ulteriori n. 4 BG con le medesime finalità di quelli schierati nell'iniziativa eFP. Questa ennesima iniziativa porta a oltre 40.000 il numerico di unità sotto il diretto controllo della NATO nella parte orientale del continente europeo, oltre a numerosi mezzi aerei e navali. Tali assetti complementari alle forze delle nazioni ospitanti, insieme ai paritetici BG impiegati in eFP, nell'ambito delle attività di pianificazione volte a un ulteriore rafforzamento della postura NATO sul fianco est, sono attualmente in fase di innalzamento al livello ordinativo Brigata.

Successivamente la dichiarazione, rilasciata al termine del Vertice NATO di Vilnius di luglio 2023[6], ribadisce la condanna nei confronti della guerra di aggressione della Russia verso l'Ucraina, che rappresenta la minaccia più significativa e diretta alla sicurezza degli Alleati e alla pace e alla stabilità nell'area euro-atlantica. Il Vertice ha avuto come focus l'adesione dell'Ucraina alla NATO e ha segnato l'ingresso formale della Finlandia nell'Alleanza. Inoltre è stata ribadita l'importanza di conseguire l'obiettivo del 2% delle spese per la difesa rispetto al PIL e l'impegno a investire almeno il 20% dei bilanci per la difesa in equipaggiamenti principali,

---

4 *Private Military Company.*

5 *Supreme Allied Commander Europe.* Per completezza di trattazione, alcune CRM sono pre-autorizzate dal NAC e, in caso di necessità, vengono direttamente emanate dal SACEUR.

6 *Vilnius Summit Communiqué,* 11-12 luglio 2023.

comprese le relative attività di ricerca e sviluppo. Tale condizione, rispettata dalla quasi totalità dei paesi dell'Europa orientale con la sola eccezione della Bulgaria, non viene ancora garantita da Italia, Germania, Francia e Spagna, ovvero i più importanti paesi della UE in quanto a PIL complessivo, a dimostrazione della differente percezione del "pericolo russo" tra i paesi geograficamente posizionati a oriente o a occidente nel Vecchio continente (fig. 1 in Allegato: spese per la Difesa in % del PIL).

b. L. 145/2016: impegni nazionali nel fianco est e forze in prontezza.

In questo contesto complesso, l'Italia, pur mantenendo un maggiore interesse verso i confini meridionali dell'Alleanza (c.d. fianco sud), rispetto al fianco est in ottica di gestione della pressione migratoria, controllo dei flussi energetici e ruolo di *leadership* italiana nel "Mediterraneo allargato", partecipa attivamente alle iniziative alleate.

Al riguardo, a partire dall'estate del 2022, sono stati schierati dall'Esercito un complesso minore leggero in Ungheria, inquadrato nel BG a guida della nazione ospitante, una batteria SAMP-T in Slovacchia, per concorrere alla deterrenza e alla difesa dello spazio aereo dell'Alleanza mediante l'impiego di un sistema *Surface Based Air Defence* (SBAD). Soprattutto viene assunto il ruolo di *framework nation* del BG di fanteria media schierato in Bulgaria con circa 750 unità in sostituzione di un paritetico assetto bulgaro. Quest'ultima unità, ormai completa e autonoma dal punto di vista capacitivo, come accennato al paragrafo precedente, è di previsto innalzamento al livello Brigata così come tutti gli altri BG schierati sia in eFP che in eVA; nel merito è già stato schierato in area di operazione un *Brigade Forward Element* al fine di coordinare tutte le attività logistiche, operative e addestrative inerenti l'elevazione ordinativa dell'assetto. Le altre Forze Armate hanno continuato a garantire gli assetti già schierati prima del 2022. In particolare, la Marina Militare ha proseguito con le contribuzioni alle citate SNF sia nello Standing *NATO Maritime Group* (SNMG) sia nello *Standing NATO Mine Counter Measures Group* (SNMCMG) Atlantico orientale/Mare del Nord (SNMG1 e SNMCMG1) e Mar Mediterraneo/Mar Nero (SNMG2 e SNMCMG2), proseguendo l'impegno nel garantire a rotazione il ruolo di *Framework nation* e contribuendo ai MG delle altre nazioni, tramite l'impiego di idonei assetti navali quali fregate, cacciamine e navi ausiliarie. Riguardo la dimensione aerea, con la spiralizzazione della crisi russo-ucraina, la NATO ha deciso di potenziare le attività di sorveglianza aerea dando vita alla cosiddetta *enhanced Air Policing* (eAP), nel cui alveo l'Aeronautica Militare ha continuato a garantire i propri assetti schierando, dapprima in Polonia (2° semestre 2022) e a oggi in Lituania, una *Task Force* su caccia Eurofighter EF-2000, volta all'intercettazione aerea come deterrenza a difesa dei cieli baltici[7].

Per quanto riguarda le forze in prontezza, nell'ambito della NATO *Readiness Initiative* (NRI), un bacino di forze rese disponibili alla NATO nate dopo la NRF per aumentare all'interno dei paesi dell'Alleanza la cultura della *readiness*, l'Esercito è *Framework Nation* di una delle 8 *Larger Formation* (tutte a livello Brigata) che compongono il *basket* NRI. Invece per l'eNRF, l'Esercito nel 2023 ha contribuito con una compagnia genio guastatori nella VJTF a guida tedesca, il CIMIC HQ e una compagnia CBRN nella CBRN TF a guida polacca; la Marina Militare ha impiegato nella VJTF assetti navali facenti parte del citato SNMG, mentre l'Aeronautica Militare ha garantito in VJTF assetti ad ala fissa sia da combattimento che da supporto. Infine per la NRI, la Marina Militare ha assegnato complessivamente cinque unità navali[8] e l'Aeronautica Militare ha impiegato differenti assetti[9], con prontezze a scalare, al fine di assicurare le varie capacità esprimibili dalla Forza Armata.

---

7 Gli assetti nazionali impiegati nell'ambito *dell'Air Policing* sono stati schierati, nel tempo, in Estonia, Lettonia, Lituania, Albania, Islanda, Bulgaria, Romania, Montenegro, Slovacchia, Slovenia e Polonia, contribuendo di fatto alla quasi totalità delle missioni svolte dall'Alleanza Atlantica.

8 Uno con impiego annuale e quattro con impiego semestrale.

9 A titolo di esempio, si citano le capacità *Combat* SAR, *Suppression of Enemy Air Defence*, *Advanced Air Defence*.

A ulteriore conferma della volontà politica nazionale di concorrere alle iniziative avviate nell'ambito dell'Alleanza e per dare un quadro quanto più possibile esaustivo della situazione, va sottolineato che, sempre nel continente europeo, l'Italia partecipa sin dal suo avvio nel 1999 alla citata KFOR (Op. *"Joint Enterprise"*). Questa missione, pur non essendo ricompresa nell'alveo delle iniziative legate alla crisi lungo il fianco est, consolida la posizione italiana nella NATO, rendendo il nostro paese uno dei maggiori contributori alle iniziative atlantiche. Infatti il contingente italiano schierato in Teatro Operativo è attualmente il più numeroso davanti a quello statunitense; l'Italia ha garantito nell'ultimo decennio la quasi totalità dei Comandanti di KFOR con due sole eccezioni (mandati ungherese e turco). Inoltre è costantemente a *framework* italiano anche la *Operational Reserve Force* (ORF), unità di riserva di livello reggimentale specificamente costituita per interventi nell'Area balcanica[10].

Onde permettere una migliore comprensione del cospicuo livello di impegno nazionale nell'ambito delle iniziative NATO avviate lungo il fianco est dell'Alleanza, preme infine evidenziare lo sforzo che esse chiedono quotidianamente alle Forze Armate. Infatti, le iniziative succitate (Kosovo escluso), impiegano mediamente[11] un totale complessivo che consta di 3.400 uomini e donne in armi, 620 mezzi terrestri, 5 mezzi navali e 29 mezzi aerei (fig. 2 in Allegato: *Commitment* nazionale nel fianco est della NATO nel 2023). Questi assetti sono così ripartiti:

- 3 mezzi aerei e 45 unità nella Sorveglianza dello spazio aereo dell'Alleanza;
- 5 mezzi navali, 4 mezzi aerei e n. 567 unità nella Sorveglianza navale dell'area Sud dell'Alleanza;
- 4 mezzi terrestri, 12 mezzi aerei e 300 unità nell'*Air Policing*;
- 450 mezzi terrestri, 10 mezzi aerei e 2.120 unità in eVA;
- 166 mezzi terrestri e 370 unità in eFP.

Questo livello di *commitment* giornaliero equivale al 44% circa di tutte le unità italiane schierate all'estero, la cui consistenza media è di 7.720[12], mentre le forze in prontezza sono massivamente dedicate a impegni che la nazione ha assunto nei confronti della NATO (citati NRI, NRF, SNF). Ciò dimostra pienamente come il nostro paese scelga di impiegare lo strumento militare in Aree di Operazione al fine di mantenere saldo il proprio ruolo e la propria posizione nell'Alleanza.

Per avere chiaro lo sforzo che il paese ha messo in atto a seguito dell'inizio delle ostilità in Ucraina e l'impegno della NATO ad accrescere la propria presenza lungo la linea di confine con la Federazione Russa, basti pensare che, nelle medesime iniziative, l'Italia impiegava:

- nel 2021[13]:
  - 2 mezzi aerei e 45 unità nella Sorveglianza dello spazio aereo dell'Alleanza;
  - 2 mezzi navali, 1 mezzo aereo e 235 unità nella Sorveglianza navale dell'area Sud dell'Alleanza;
  - 12 mezzi aerei e 260 unità nell'*Air Policing*;
  - 135 mezzi terrestri e 238 unità in eFP.

Quando l'iniziativa eVA non era ancora stata avviata:

- nel 2022[14]:
  - 380 mezzi terrestri e 1.000 unità in eVA;
  - 139 mezzi terrestri e 250 unità in eFP.

---

10 Il computo del rgt. di manovra in ORF, posto in prontezza operativa per l'iniziativa *Over the Horizon Force* (OTHF), le cui forze sono dedicate esclusivamente a un eventuale impiego nella JOA balcanica, fa sì che il contingente italiano risulti il più numeroso.

11 I numerici riportati sono riferiti alla consistenza massima autorizzata.

12 Camera dei Deputati, "*Dossier* Autorizzazione e proroga missioni internazionali" anno 2023, 16 maggio 2023.

13 Camera dei Deputati, "*Dossier* Autorizzazione e proroga missioni internazionali" anno 2021, 17 giugno 2021.

14 Camera dei Deputati, "*Dossier* Autorizzazione e proroga missioni internazionali" anno 2022, 15 giugno 2022.

Il livello di impegno nelle iniziative di Sorveglianza dello spazio aereo dell'Alleanza, Sorveglianza navale dell'area Sud dell'Alleanza e *Air Policing* equivaleva invece a quello del 2023, già enunciato in precedenza.

Questo esponenziale incremento dello sforzo nazionale ha portato a dispiegare nel 2023 lungo il fianco est dell'Alleanza 481 mezzi terrestri, 3 mezzi navali, 14 mezzi aerei e circa 2.600 unità in più rispetto al 2021, quadruplicando lo sforzo in atto che, nel 2021, vedeva schierate complessive 778 unità (fig. 3 in Allegato: *Dossier* autorizzazione e proroga missioni internazionali: incremento delle iniziative NATO nel fianco est dell'Alleanza periodo 2021-2023).

Per completezza di trattazione, occorre specificare che i dati riferiti all'anno 2024 non sono stati presi in considerazione in quanto ancora in fase di definizione da parte del decisore politico-militare durante la stesura del presente documento. Preme inoltre evidenziare che, sebbene le forze dell'Aeronautica Militare impegnate non abbiano visto incrementi sostanziali né dal punto di vista degli aeromobili impiegati né riguardo il personale, aumentato lievemente solo nella componente di supporto, queste ultime hanno parimenti visto incrementare notevolmente le ore di volo disponibili.

4. Prospettive future

Riguardo la prospettiva di impiego futuro delle unità nazionali in seno a iniziative NATO nel fianco est, l'Italia, oltre a confermare gli oneri già assunti in precedenza, ha piena intenzione di incrementare ulteriormente lo sforzo al fine di consolidare il proprio ruolo nell'Alleanza, confermandosi quale *partner* serio e affidabile agli occhi degli alleati.

Per chiarezza di trattazione, gli impegni delle varie Forze Armate nel 2025, attualmente ancora in fase di conferma[15], verranno analizzati singolarmente e verrà infine fornito un riepilogo dell'onere complessivo, utile a dare un quadro d'insieme quanto più esaustivo possibile circa lo sforzo posto in essere dalla nazione.

Nel dominio *Air,* l'Aeronautica Militare dovrebbe continuare ad assicurare n. 3 *slot* continuative nell'ambito dell'*Air Policing*[16]. Nello specifico, ci dovrebbe essere una rotazione tra *Baltic Air Policing* e *Enhanced Air Policing* in APA *South,* per poi tornare a garantire l'*Enhanced Air Policing* nell'APA *North*. Ogni schieramento comporterà non solo la presenza di *fighter* (F-35 o F-2000) ma anche la necessità di schierare assetti logistici e sistemi *radar Airborne Early Warning and Control* (G550 CAEW[17]), complessivamente utili al fine di effettuare sorveglianza aerea, funzioni di comando, controllo e comunicazioni e fornire supporto alle forze di terra. Inoltre, come per il 2023 e il 2024, anche nel corrente anno le ore di volo disponibili potrebbero subire un ulteriore significativo incremento.

L'impegno nazionale resterà intenso anche per la parte *Maritime,* dove dovrebbero continuare a essere impiegate forze per *le* SNMG2 e le SNMCMG2, operanti prevalentemente nel Mediterraneo. Nel secondo semestre 2025 dovrebbe infatti essere garantita la *Flagship* del Gruppo in SNMG2. Anche in SNMCMG2 l'Italia dovrebbe essere presente per tutto l'anno, fornendo due cacciamine a copertura annuale e garantendo nella seconda parte dell'anno la *Flagship*.

Quanto sopra esposto ha reso e renderebbe in futuro l'Italia primo contributore per la parte di *Air Policing* (per avere un termine di paragone, basti pensare che sovente altre nazioni assicurano appena uno dei tre *slot* disponibili nell'arco dell'anno), grazie anche al ribilanciamento delle offerte che hanno portato il nostro paese a svolgere servizio sul fianco est, evitando di offrire assetti per l'*Air Policing* in Islanda, ormai considerata poco pagante in termini di visibilità e di ritorno addestrativo e operativo.

---

15 Il procedimento di autorizzazione e proroga delle Missioni internazionali viene approvato dalle Camere tendenzialmente nel mese di luglio e comprende tutte le operazioni già in corso nell'anno in esame.

16 Coprendo di fatto tutto l'anno, considerato che le *slot* in argomento sono quadrimestrali.

17 *Conformal Airborne Early Warning.*

Anche nel dominio *Maritime* risultiamo e continueremo a risultare i primi contributori, avendo spesso la Nave sede di Comando o unità di supporto che coprono interamente l'anno solare nella sua interezza in entrambi i dispositivi, SNMG e SNMCMG.

Per quanto attiene il dominio *Land,* sono previsti incrementi riguardo l'impiego di uomini e mezzi nelle operazioni già in atto, in particolare lo sforzo principale, già a oggi in fase di attuazione, sarà la citata elevazione a livello Brigata degli assetti schierati in Bulgaria. Inoltre l'Esercito al fine di fronteggiare esigenze nazionali non pianificate, pubbliche calamità, ovvero ulteriori esigenze nel contesto di iniziative internazionali guidate dalle Nazioni Unite, dall'Alleanza Atlantica e dall'Unione Europea, garantisce un bacino di forze in prontezza variabile fino a 180 giorni.

In particolare nel 2024 la F.A. ha garantito in ambito NRF una Brigata in *Very high readiness Joint Task Force* (VJTF - L) *stand up*.

Inoltre, a partire dal 2023, sono iniziate una serie di conferenze NATO, a seguito delle quali l'Alleanza Atlantica si è orientata verso una nuova concezione di prontezza, che troverà la sua più concreta realizzazione dal 2025 con l'implementazione del NATO *New Force Model* (NFM), superando il vecchio paradigma del NATO *Responce Force* (NRF). In particolare il NFM è caratterizzato dal:

- *Allied Reaction Force* (ARF) per cui l'Italia sarà *Framework Nation* per il 2025;
- *Force Structure Requirement* (FSR), catalogo di capacità, suddivise nei *Tier* 1-2-3 (livelli di prontezza), da cui saranno tratte le forze per l'esecuzione dei *Regional Plans* (RP) (*North West, Center* e *South East)*.

Sempre nel 2025 l'Esercito sarà egualmente *framework* della CBRN TF. Infine sarà ancora garantito l'ORF BN in prontezza per i Balcani nell'ambito dell'iniziativa OTHF. Al riguardo preme evidenziare come l'ORF BN sia sovente impiegato nel Te.Op. kosovaro[18], considerazione che mi spinge a pensare, quale opinione personale, alla eventualità di ricercare una soluzione permanente nell'ambito delle CJSOR della missione. Tale soluzione, che verosimilmente porterebbe allo schieramento permanente di ulteriori assetti in area di operazioni, comporterebbe un ulteriore aggravio in termini di forze per la componente terrestre delle Forze Armate italiane.

In conclusione, qualora vengano realizzati tutti gli incrementi precedentemente descritti, il contributo delle Forze Armate per le sole missioni NATO potrebbe ulteriormente incrementare, attestandosi permanentemente attorno alle 4.000 unità schierate, non considerando tutte quelle offerte a vario titolo nelle prontezze. Un così elevato livello di *commitment* in proporzione alle capacità della nostra Difesa sarebbe segno tangibile e inequivocabile della determinazione nazionale di assicurare il proprio contributo sostanziale a favore dell'Alleanza.

Tuttavia va evidenziato come, a fianco della volontà di garantire un elevato impegno delle Forze Armate nazionali, non si riscontra, a livello politico, paritetica forte volontà nel raggiungere il citato 2% del PIL in spesa per la Difesa[19], carenza che potrebbe creare criticità per il livello di

---

[18] Oltre alle *Operational Rehearsal* (OPREH) svolte annualmente in Te.Op. su attivazione dell'*Allied Joint Force Command* di Napoli, l'ultimo impiego dell'unità nazionale risale al 1° semestre 2023 e ha visto schierato in Kosovo n. 1 *Task Group* fornito dall'Esercito.

[19] A riguardo, il Documento Programmatico Pluriennale per la Difesa triennio 2023-2025 riporta che l'obiettivo nazionale, considerato il quadro economico-finanziario, è di conseguire progressivamente la percentuale del 2% delle spese per la Difesa sul PIL nel 2028, attestando i valori a 1,46% nel 2023, 1,43% nel 2024 e 1,45% nel 2025. Inoltre, il documento ricorda anche come tale ormai celeberrimo obiettivo *"cash"* del 2% debba essere considerato quale base di partenza e non come traguardo da raggiungere.

efficienza delle nostre unità laddove lo sforzo da garantire nei Te.Op. e in prontezza continuasse a rimanere così elevato nel lungo tempo[20].

5. Conclusioni

Abbiamo potuto notare in questa sede quanto la NATO abbia dimostrato la sua capacità di adattamento alla situazione geopolitica mondiale in continuo mutamento senza focalizzarsi soltanto sull'area euro-atlantica. L'Alleanza, come tutti sappiamo, resta comunque un'organizzazione internazionale e proprio per sua natura un consesso dove tutte le parti in causa, per raggiungere un accordo su un'azione da intraprendere, devono trovare un compromesso corale che non necessariamente rispecchia l'interesse nazionale dei singoli stati. I tempi necessari alla completa esecuzione del processo a volte non rispecchiano la fluidità della situazione internazionale, ma gli adattamenti di lungo respiro sono sempre risultati aderenti al contrasto delle minacce rilevate.

In questo contesto strategico è stato documentato come l'Italia, ancorché orientata verso il fianco sud dell'Alleanza e il Mar Mediterraneo, abbia dimostrato un importante e crescente impegno nell'ambito del fianco est, garantendo sia assetti schierati che forze in prontezza da parte di tutte le Forze Armate. Questo a conferma della politica estera nazionale, sovente descritta con l'immagine di tre "cerchi" concentrici che mostrano le priorità del paese storicamente identificate, in ordine di importanza, con area atlantica, area europea e bacino del Mediterraneo. La vicinanza del nostro paese all'Alleanza Atlantica avvalora l'ipotesi per cui la NATO, soprattutto a seguito dello scoppio delle ostilità in Ucraina, ha ripreso importanza ed è riuscita ad adattarsi al nuovo scenario geopolitico venutosi a creare.

Tuttavia è noto come gli interessi dell'Alleanza, con gli USA ancora saldamente alla guida, si stiano spostando sempre più a oriente (c.d. *Pivot to Asia*) e in particolare verso la Cina. A conferma di questo, vi è la partecipazione dei leader di Giappone, Corea del Sud, Australia e Nuova Zelanda ai Vertici NATO di Madrid 2022 e Vilnius 2023. Lo spostamento degli interessi dell'Alleanza non solo verso Asia ed Europa Orientale, ma anche verso Mediterraneo e area "MENA[21]", sarà verosimilmente la sfida italiana dei prossimi anni. Conciliare le posizioni di tutti i paesi sarà certamente un compito arduo. A tal proposito l'Italia, se continuerà a partecipare attivamente alle iniziative della NATO in ogni area geografica d'interesse e a garantire le proprie forze nelle prontezze operative, nonché ad agire nell'ambito dell'Unione Europea per incrementare l'interoperabilità degli assetti tra gli stati membri (a riguardo il progetto di "Esercito Europeo" è a oggi molto lontano dall'essere portato a termine), vedrà certamente riconosciuto e accresciuto il suo ruolo di importante membro dell'Alleanza e potrà divenire protagonista, seppur in proporzione alla media potenza del paese, nello scacchiere atlantico. Come diretta conseguenza l'Italia potrà chiedere quindi un maggiore focus della NATO riguardo l'area del fianco sud che, come accennato, risulta essere priorità strategica per la sicurezza nazionale.

Paesi come l'Italia dovranno sempre più confrontarsi con la necessità pratica di dotarsi, quantomeno a livello europeo, di forze di difesa indipendenti e in grado di garantire, come condizione minima per il successo, la sicurezza del continente e del suo estero vicino, riuscendo al contempo a operare nelle zone di crisi come entità autonoma e distaccata dalla presenza USA. In questo contesto il nostro Paese, laddove riuscirà a dimostrarsi in grado di garantire le opportune risorse nel lungo periodo, potrà avere un ruolo da assoluto protagonista nello scacchiere del Vecchio Continente, non solo in seno alla NATO, ma anche nell'ambito dell'UE.

Tuttavia, preme evidenziare come considerazione finale che il mancato raggiungimento di alcune delle condizioni richieste dalla NATO (*in primis* l'obiettivo di un adeguato livello di spesa

---

[20] Occorre inoltre sottolineare che il *budget* della Difesa è largamente dedicato all'incomprimibile spesa per il personale, circostanza che determina un impatto sui mancati finanziamenti nei settori "investimento" e "gestione", ovvero gli elementi caratterizzanti la predisposizione e l'impiego delle forze in Operazioni Fuori dai Confini Nazionali (OFCN).

[21] *Middle East and North Africa.*

nella Difesa) sia fondamentale in ottica di corretta gestione e funzionamento delle unità prescelte per questi delicati compiti. A questo scopo occorre operare un'attenta valutazione degli assetti selezionati, garantendo l'impiego delle sole componenti indispensabili per i compiti identificati dalla NATO e privilegiando l'utilizzo di unità di elevato pregio operativo[22] in luogo di una mera condensazione di "massa".

[22] Si considerino, a titolo di esempio, gli assetti in *Air Policing*, le SNF o la btr. SAMP-T schierata in Slovacchia.

Bibliografia

1. **Libri**
   - G. Natalizia, L. Termine (a cura di), La NATO verso il 2030. Continuità e discontinuità nelle relazioni transatlantiche dopo il nuovo Concetto Strategico, Il Mulino, Bologna, 2023.

2. **Pubblicazioni e documenti**
   - Camera dei Deputati, "Dossier Autorizzazione e proroga missioni internazionali" anno 2021, 17 giugno 2021, in https://www.camera.it/temiap/documentazione/temi/pdf/1286174.pdf?_1705147118879 (accesso effettuato il 19/11/2023).
   - Camera dei Deputati, "Dossier Autorizzazione e proroga missioni internazionali" anno 2022, 15 giugno 2022, in https://www.camera.it/temiap/documentazione/temi/pdf/1342692.pdf?_1705147395664 (accesso effettuato il 19/11/2023).
   - Camera dei Deputati, "Dossier Autorizzazione e proroga missioni internazionali", 16 maggio 2023, in https: //temi.camera.it/leg19/provvedimento/autorizzazione-e-proroga-delle-missioni-internazionali-nel-2023.html (accesso effettuato il 19/11/2023).
   - Centro Studi Internazionali, Alessandra Dibenedetto, "Verso il Summit NATO di Bruxelles", luglio 2018, in https://www.cesi-italia.org/contents/Verso%20il%20Summit%20NATO%20di%20Bruxelles.pdf (accesso effettuato il 07/12/2023).
   - Limes, giugno 2023. Russia o non Russia, Gedi, Torino, 2023.
   - Ministro della Difesa, "Documento programmatico pluriennale della Difesa per il triennio 2023-2025", Ed. 2023, in https: //www.difesa.it/Content/Documents/DPP%202023-2025.pdf (accesso effettuato il 08/12/2023).
   - Ministro della Difesa, "Libro Bianco per la sicurezza internazionale e la difesa" 2015, in https: //www.difesa.it/Primo_Piano/Documents/2015/04_Aprile/LB_2015.pdf (accesso effettuato il 08/12/2023).
   - NATO 2022 *Strategic Concept*, in https: //www.nato.int/topics_210907 (accesso effettuato il 19/11/2023).
   - *NATO AJP-5 "Allied Joint Doctrine for the Planning of Operations",* Ed. A Versione 2, maggio 2019, in https://www.coemed.org/files/stanags/01_AJP/AJP-5_EDA_V2_E_2526.pdf (accesso effettuato il 19/11/2023).
   - Stato Maggiore della Difesa, Ufficio Generale Innovazione Difesa, PID-5 "La pianificazione delle operazioni", Ed. 2022.

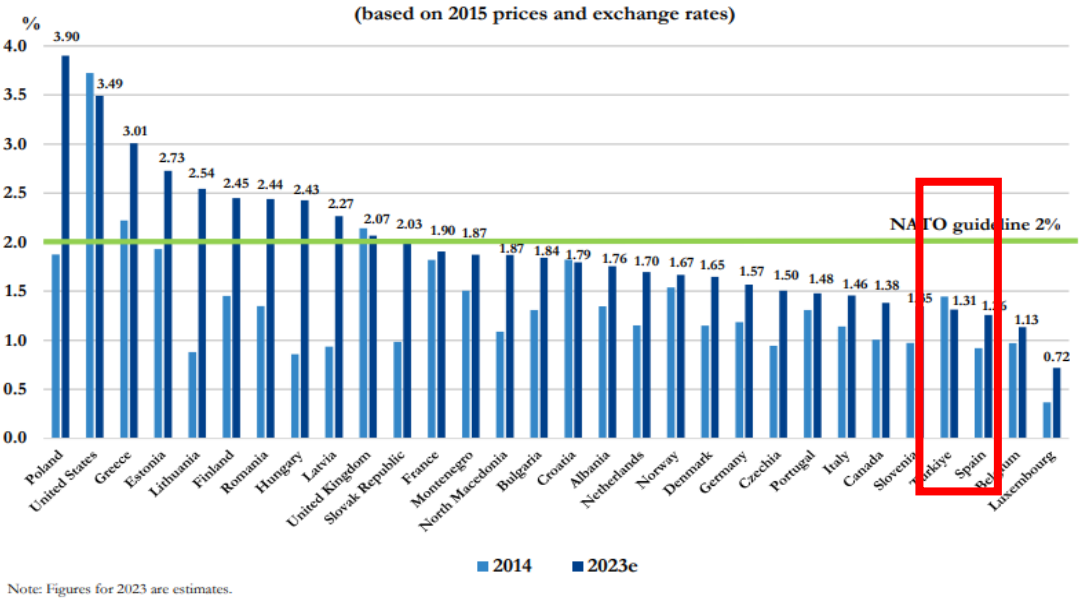
3. **Articoli internet**
   - https: //www.difesaonline.it/mondo-militare/siria-putin-invia-gli-omini-verdi. Siria: Putin invia gli "Omini Verdi", 24 ottobre 2015 (accesso effettuato il 18/11/2023).
   - https: //www.economist.com/europe/2019/11/07/emmanuel-macron-in-his-own- words-english. Intervista condotta all'Eliseo il 21 ottobre 2019 e pubblicata il 9 novembre successivo (accesso effettuato il 19/11/2023).
   - https: //www.difesa.it/OperazioniMilitari/Pagine/OperazioniMilitari.aspx. Operazioni militari della Difesa (accesso effettuato il 19/11/2023).
   - https: //www.nato.int/cps/en/natohq/official_texts_112964.htm. Dichiarazione *Summit* NATO Newport/Cardiff 2014 (accesso effettuato il 19/11/2023).
   - https: //www.nato.int/cps/en/natohq/official_texts_133169.htm. Dichiarazione *Summit* NATO Varsavia 2016 (accesso effettuato il 19/11/2023).
   - https: //www.nato.int/cps/en/natohq/official_texts_156624.htm. Dichiarazione *Summit* NATO Bruxelles 2018 (accesso effettuato il 19/11/2023).
   - https: //www.nato.int/cps/en/natohq/official_texts_196951.htm. Dichiarazione *Summit* NATO Madrid 2022 (accesso effettuato il 19/11/2023).

- https://www.nato.int/cps/en/natohq/official_texts_217320.htm. Dichiarazione *Summit* NATO Vilnius 2023 (accesso effettuato il 19/11/2023).
- https: //www.esercito.difesa.it/operazioni. Operazioni Esercito Italiano (accesso effettuato il 09/12/2023).
- https: //www.aeronautica.difesa.it/home/noi-siamo-l-am/operazioni/. Operazioni Aeronautica Militare (accesso effettuato il 09/12/2023).
- https: //www.marina.difesa.it/cosa-facciamo/per-la-difesa-sicurezza/operazioni-in-corso/Pagine/StandingNatoMaritimeCountermine.aspx. Operazioni Marina Militare (accesso effettuato il 09/12/2023).
- https: //www.analisidifesa.it/2022/07/missioni-allestero-aumentano-gli-impegni-per-le-forze-armate-italiane/. Analisi Difesa: "Missioni all'estero: aumentano gli impegni per le Forze Armate italiane (accesso effettuato il 10/12/2023).

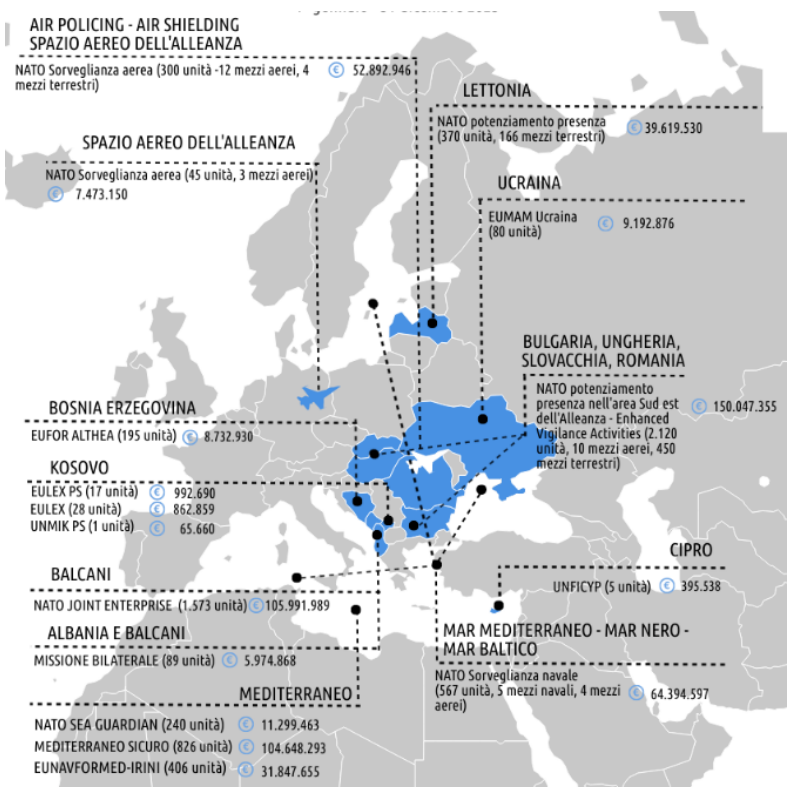
4. Altro

- https: //www.ispionline.it/it/pubblicazione/podcast-globally-i-travagli-della-nato-135577. ISPI, *Podcast Globally:* I travagli della NATO, 14 luglio 2023 (accesso effettuato il 10/12/2023).

Tabelle e cartine esplicative



(Fig. 1) – Spese per la Difesa in % del PIL
Fonte: *NATO Public Diplomacy Division: Defence expenditure of NATO Countries* (2014-2023), 7 luglio 2023.



(Fig. 2) – *Commitment* nazionale nel fianco est della NATO nel 2023
Fonte: http: //https://temi.camera.it/leg19/temi/infographics/autorizzazione-e-proroga-delle-missioni-interna- zionali-nel-2023.

INIZIATIVA	2021	2022	2023	INCREMENTI 2021-2023
Sorveglianza dello spazio aereo dell'Alleanza	n. 2 mezzi aerei n. 45 un.	n. 3 mezzi aerei n. 45 un.	n. 3 mezzi aerei n. 45 un.	n. 1 mezzo aereo
Sorveglianza navale dell'area Sud dell'Alleanza	n. 2 mezzi navali n. 1 mezzo aereo n. 235 un.	n. 5 mezzi navali n. 4 mezzi aerei n. 567 un.	n. 5 mezzi navali n. 4 mezzi aerei n. 567 un.	n. 3 mezzi navali n. 3 mezzi aerei n. 332 un.
Air Policing	n. 4 mezzi terr. n. 12 mezzi aerei n. 260 un.	n. 4 mezzi terr. n. 12 mezzi aerei n. 300 un.	n. 4 mezzi terr. n. 12 mezzi aerei n. 300 un.	n. 40 un.
eVA	///	n. 380 mezzi terr. n. 1.000 un.	n. 450 mezzi terr. n. 10 mezzi aerei n. 2.120 un.	n. 450 mezzi terr. n. 10 mezzi aerei n. 2.120 un.
eFP	n. 135 mezzi terr. n. 238 un.	n. 139 mezzi terr. n. 250 un.	n. 166 mezzi terr. n. 370 un.	n. 31 mezzi terr. n. 132 un.
TOTALE	**n. 139 mezzi terr.** **n. 2 mezzi navali** **n. 15 mezzi aerei** **n. 778 un.**	**n. 523 mezzi terr.** **n. 5 mezzi navali** **n. 19 mezzi aerei** **n. 2.162 un.**	**n. 620 mezzi terr.** **n. 5 mezzi navali** **n. 29 mezzi aerei** **n. 3.402 un.**	**n. 481 mezzi terr.** **n. 3 mezzi navali** **n. 14 mezzi aerei** **n. 2.624 un.**

(Fig. 3) – Dossier autorizzazione e proroga missioni internazionali: incremento delle iniziative NATO nel fianco est dell'Alleanza periodo 2021-2023

Fonte: Elaborazione dell'autore su dati Camera dei Deputati, "Dossier Autorizzazione e proroga missioni internazionali" anni 2021, 2022, 2023.

Pier Valerio Mari

Oltre la Sanità: la Medical Intelligence come nuova frontiera della difesa

Abstract

Meno nota di altre branche dell'intelligence, ma non per questo meno importante, la Medical Intelligence (MEDINTEL) è divenuta una funzione imprescindibile sia per gli Stati che per la comunità internazionale. Essa è una disciplina trasversale, basata non solo su dati sanitari, ma anche su informazioni ambientali, sociali, geopolitiche, economiche e tecnologiche. La sua funzione è di trasformare una mole eterogenea di dati in conoscenza operativa, a servizio sia della medicina che della sicurezza. Come questo breve contributo intende mostrare, l'intelligence medica sembra rappresentare dunque un ponte strategico tra il mondo sanitario e quello militare, tra la ricerca scientifica e la politica.

Il Dipartimento della Difesa degli Stati Uniti ritiene che la Medical Intelligence, ovvero la c.d. MEDINTEL, sia *risultante dalla raccolta, valutazione, analisi e interpretazione di informazioni mediche, bio-scientifiche e ambientali che interessano la pianificazione strategica e le operazioni mediche militari all'estero, per la conservazione della forza di combattimento delle forze amiche e la formazione di valutazioni delle capacità mediche straniere sia nel settore militare sia in quello civile*. Viceversa, nel contesto nazionale, il concetto si declina nella rete MEDINTEL, sistema pensato come strumento di allerta rapida relativamente ai fenomeni interni e applicata principalmente all'epidemiologia delle malattie infettive. Questo sistema include le attività di identificazione precoce dei rischi o degli eventi di possibile impatto sulla sanità pubblica, la loro validazione e la loro valutazione critica, nonché indagini mirate e la formulazione di raccomandazioni per misure di controllo. Particolare attenzione è riservata alle emergenze sanitarie che possono assumere rilievo internazionale, con l'obiettivo di proteggere la popolazione e salvaguardare la stabilità del sistema sanitario.

Sebbene la definizione possa apparire tecnica, i suoi risvolti sono di grande portata. La MEDINTEL non è soltanto un capitolo dell'informatica sanitaria, né un'estensione dei sistemi di supporto decisionale clinico (*Clinical Decision Support Systems*). Questi ultimi hanno infatti una funzione mirata, circoscritta al contesto medico: fornire strumenti al clinico per prendere decisioni diagnostiche o terapeutiche più rapide e fondate. La *health informatics*, invece, si occupa di raccogliere, gestire e organizzare dati clinici. La MEDINTEL, al contrario, si configura come una disciplina trasversale che integra non soltanto dati sanitari, ma anche informazioni ambientali, sociali, geopolitiche, economiche e tecnologiche. La sua funzione è quella di trasformare la mole eterogenea di dati in conoscenza operativa, a servizio sia della medicina che della sicurezza. È un vero e proprio ponte tra il mondo sanitario e quello militare, tra la ricerca scientifica e la politica strategica.

Storicamente, l'idea di sorveglianza sanitaria e di protezione della comunità non è affatto recente. Già nel Vecchio Testamento è possibile rintracciare riferimenti a pratiche di isolamento e osservazione delle malattie. Nell'era contemporanea, i primi documenti ufficiali riconducibili alla MEDINTEL risalgono al 1861 con i bollettini dell'US Army. Tra il XX e il XXI secolo, la disciplina si è progressivamente consolidata. Nel 2005 l'Organizzazione Mondiale della Sanità inserì la sorveglianza basata su eventi nel Regolamento Sanitario Internazionale; nel 2013 l'Unione Europea adottò la Decisione 1082/2013/EU, che prevedeva la creazione di un sistema informatico di allerta riservato, denominato European Warning Response System; nel 2014 la WHO pubblicò la

risoluzione *Early detection, assessment and response to acute public health events*, con un focus sulla sorveglianza basata su eventi. Solo nel 2019-2020, però, la NATO introdusse formalmente il concetto di Medical Intelligence nella propria dottrina, attraverso l'Allied Joint Doctrine For Medical Support (AJP-4.10) e la Guide to Medical Intelligence (AJMedP-3). In Italia, dopo la sperimentazione legata alle Olimpiadi Invernali di Torino del 2006, sono stati sviluppati diversi progetti (Epi-Int nel 2008, il Sistema di Allerta Rapido tra 2012 e 2014, EpiInt Sentinel nel 2017-2018) e, dal 2015, il programma MedInt è stato formalmente assegnato alla UOC SERESMI dell'INMI "L. Spallanzani" di Roma. Parallelamente, il settore Difesa ha istituito un ufficio di Medical Intelligence presso il Centro Intelligence Interforze, inquadrato nel II Reparto – Informazioni e Sicurezza dello Stato Maggiore della Difesa[1].

Questa cornice storica permette di cogliere un punto essenziale: la Medical Intelligence nasce e si sviluppa in ambito militare, ma trova un corrispettivo civile nella cosiddetta Epidemic Intelligence, oggi nota anche come Digital Disease Detection. Quest'ultima integra sistemi chiusi e validati, come le schede di dimissione ospedaliera (Indicator-Based Surveillance, IBS), con sistemi aperti basati su eventi (Event-Based Surveillance, EBS), che comprendono anche media e social media. La combinazione di filtri automatici e validazione umana consente di raggiungere un'accuratezza predittiva molto elevata, con una sensibilità prossima al 100% e una specificità superiore all'80%. Si tratta di valori che dimostrano l'affidabilità di questi strumenti, ma al tempo stesso evidenziano la necessità di un costante controllo umano, senza il quale il rischio di falsi allarmi o di errori interpretativi rimane concreto.

Gli ambiti di applicazione della Medical Intelligence sono numerosi e diversificati. Nel contesto ospedaliero, essa consente di ottimizzare la gestione delle risorse critiche, dai posti letto in terapia intensiva alle scorte di ossigeno, dai ventilatori polmonari alla disponibilità di farmaci salvavita. A livello di sanità pubblica, rappresenta la spina dorsale dei sistemi di sorveglianza epidemiologica e lo strumento per anticipare i trend stagionali, come nel caso dell'influenza, o per valutare l'impatto di malattie croniche e acute sulla popolazione. Sul fronte militare, la MI è fondamentale per valutare le capacità mediche dei potenziali avversari, per proteggere la salute delle truppe impiegate in missioni all'estero e per prevenire epidemie che potrebbero minare la capacità operativa delle forze armate. In scenari emergenziali, come pandemie, disastri naturali o crisi umanitarie, la Medical Intelligence fornisce la base conoscitiva necessaria per decisioni rapide ed efficaci. Nel campo del bioterrorismo, rappresenta lo strumento più avanzato per l'identificazione precoce degli attacchi biologici, la modellizzazione del loro impatto e la pianificazione delle contromisure. Infine, non va dimenticato il ruolo crescente della cyber security: gli attacchi informatici che hanno colpito il National Health Service britannico nel 2017 e la Regione Lazio nel 2021 hanno dimostrato come la vulnerabilità delle infrastrutture digitali sanitarie possa tradursi in un rischio immediato per la salute pubblica.

Per spiegare il senso più profondo della MEDINTEL, può essere utile ricorrere a una metafora artistica e culturale: il Kintsugi, l'arte giapponese di riparare con oro le fratture della ceramica. Invece di nascondere le linee di rottura, il Kintsugi le mette in risalto, trasformandole in punti di forza e bellezza. Allo stesso modo, la Medical Intelligence non cancella le fragilità emerse dalle crisi sanitarie, ma le valorizza, le integra e le trasforma in elementi di resilienza. La pandemia da COVID-19 ha mostrato con chiarezza le nostre vulnerabilità, ma ha anche stimolato un'accelerazione senza precedenti nell'uso delle tecnologie digitali, nell'interconnessione dei sistemi e nella consapevolezza che la salute non può essere considerata separatamente dalla sicurezza nazionale. Gli scenari degli ultimi anni confermano la necessità di questa prospettiva. Durante la pandemia, la lentezza nella raccolta e nella condivisione dei dati ha reso difficile anticipare gli sviluppi, compromettendo la capacità di risposta. Le epidemie stagionali di influenza, pur meno drammatiche, rappresentano una palestra annuale per testare e migliorare i modelli predittivi. Gli

---

[1] Sulla *Medical Intelligence* cfr. anche: il contributo di F. Rosiello in *Dizionario di Geopolitica*, CASD, Roma, 2025, pp. 662-664; B. Lucini, *Medical Intelligence: definizione, metodi, prospettive e gruppo nazionale Medint*, Sicurezza Terrorismo Società, EDUCatt, Milano 2023, 113-130 [https://hdl.handle.net/10807/273218].

attacchi informatici agli ospedali hanno mostrato come la minaccia non sia più soltanto biologica, ma anche digitale. Le prospettive del bioterrorismo, infine, sono rese più concrete dal rapido sviluppo delle biotecnologie e dalla possibilità che strumenti pensati per il progresso scientifico vengano utilizzati in modo malevolo.

La MEDINTEL ha dunque come obiettivo fondamentale quello di supportare il processo decisionale clinico e strategico, fornendo strumenti per la prevenzione, la diagnosi precoce e la risposta alle minacce emergenti. Essa permette di analizzare pattern epidemiologici, di predire scenari sanitari, di integrare la gestione del rischio con la preparazione alle emergenze. Ma vi è anche un secondo obiettivo, altrettanto importante: la gestione dell'informazione sanitaria in senso lato, con la capacità non soltanto di valutare ed eseguire inferenze corrette, ma anche di prevedere ed elaborare scenari in sistemi complessi grazie ai nuovi strumenti dei Big Data, del *Deep Learning* e dell'intelligenza artificiale generativa. Questo passaggio è cruciale, perché segna il superamento di un modello statico e il passaggio a un modello dinamico, adattato a una società in rapido movimento e segnata da accelerazioni tecnologiche come l'intelligenza artificiale. In altre parole, la MEDINTEL si colloca nel cuore della trasformazione digitale, come strumento di resilienza in un mondo sempre più interconnesso e imprevedibile.

Naturalmente appare assolutamente centrale la tutela degli interessi nazionali. Il possesso e l'utilizzo dei dati sanitari, la sicurezza delle piattaforme, l'analisi delle malattie endemiche, la capacità di costruire modelli predittivi affidabili, la preparazione alle minacce terroristiche: tutto ciò rientra a pieno titolo nella cornice della sicurezza nazionale. La Medical Intelligence non è soltanto argomento di medici o epidemiologi, ma soprattutto un tema che riguarda la sovranità e la sicurezza del Paese. In questa prospettiva, alcune domande chiave emergono con forza: quante e quali piattaforme devono essere utilizzate? Una sola centralizzata, o molte interconnesse? Chi detiene i dati? Come viene garantita la sicurezza dei dati stessi, attraverso quali protocolli e gerarchie di accesso? Quali motori di intelligenza artificiale devono essere scelti, e con quali garanzie di trasparenza e verificabilità? E infine, come costruire la multidisciplinarietà necessaria, che coinvolga medici, *data scientist*s, epidemiologi, analisti di intelligence, militari e giuristi, per dare robustezza e credibilità al sistema? In Europa, il Regolamento Generale sulla Protezione dei Dati (GDPR) rappresenta al tempo stesso un punto di forza e una sfida. Garantisce la protezione dei diritti individuali, ma pone vincoli stringenti che possono rallentare la condivisione dei dati in situazioni emergenziali. È necessario un dibattito maturo e adulto con l'obiettivo di un equilibrio tra privacy e sicurezza, affinché la protezione dell'individuo non si traduca in vulnerabilità per la collettività.

La Medical Intelligence si presenta dunque come una disciplina emergente e cruciale per il futuro della sicurezza sanitaria e strategica del nostro Paese. Le sfide che potrebbero presentarsi – dalle pandemie agli attacchi informatici, dai cambiamenti climatici alle minacce terroristiche – non sono soltanto ostacoli, ma occasioni per innovare, rafforzare e costruire sistemi più resilienti. La MEDINTEL è un cantiere aperto, un tema ancora da costruire, che richiede investimenti, formazione, governance e una visione lungimirante.

Grandi uomini del passato, con coraggio e visione, seppero affrontare sfide decisive per il destino del loro Paese, insegnando che il futuro non si attende e non si deve predire: il futuro si forgia con volontà, competenza e passione. Oggi come allora, pur durante il tempo delle Intelligenze Artificiali Generative e dei modelli predittivi, risuona con forza la celebre frase attribuita al Presidente Abraham Lincoln: "*Il miglior modo per predire il futuro è crearlo*". La Medical Intelligence, nella sua essenza, è esattamente questo: la possibilità di creare il futuro della sicurezza sanitaria del nostro Paese, trasformando i dati in conoscenza, la conoscenza in decisione, e la decisione in sicurezza.

ISTITUTO DI RICERCA E ANALISI DELLA DIFESA

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

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

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

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

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

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

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

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

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

L'*Osservatorio Strategico* è uno studio che raccoglie analisi e report sviluppati dall'Istituto di Ricerca e Analisi della Difesa (IRAD), realizzati da ricercatori specializzati.
Le aree di interesse monitorate nel 2025 sono:

- Quadrante dell'Europa orientale;
- Quadrante dell'Africa settentrionale e Israele;
- Quadrante Africa centro meridionale;
- Quadrante dei contrasti tra Paesi sunniti e sciiti;
- Quadrante di proiezione sinica;
- Quadrante di proiezione russa;
- Quadrante dell'America meridionale;
- NATO: prospettive e possibili evoluzioni;
- Gestione e conflitti: ripercussioni sulle risorse energetiche;
- Minacce ibride e asimmetriche.
- Altri argomenti di interesse Comparto Difesa

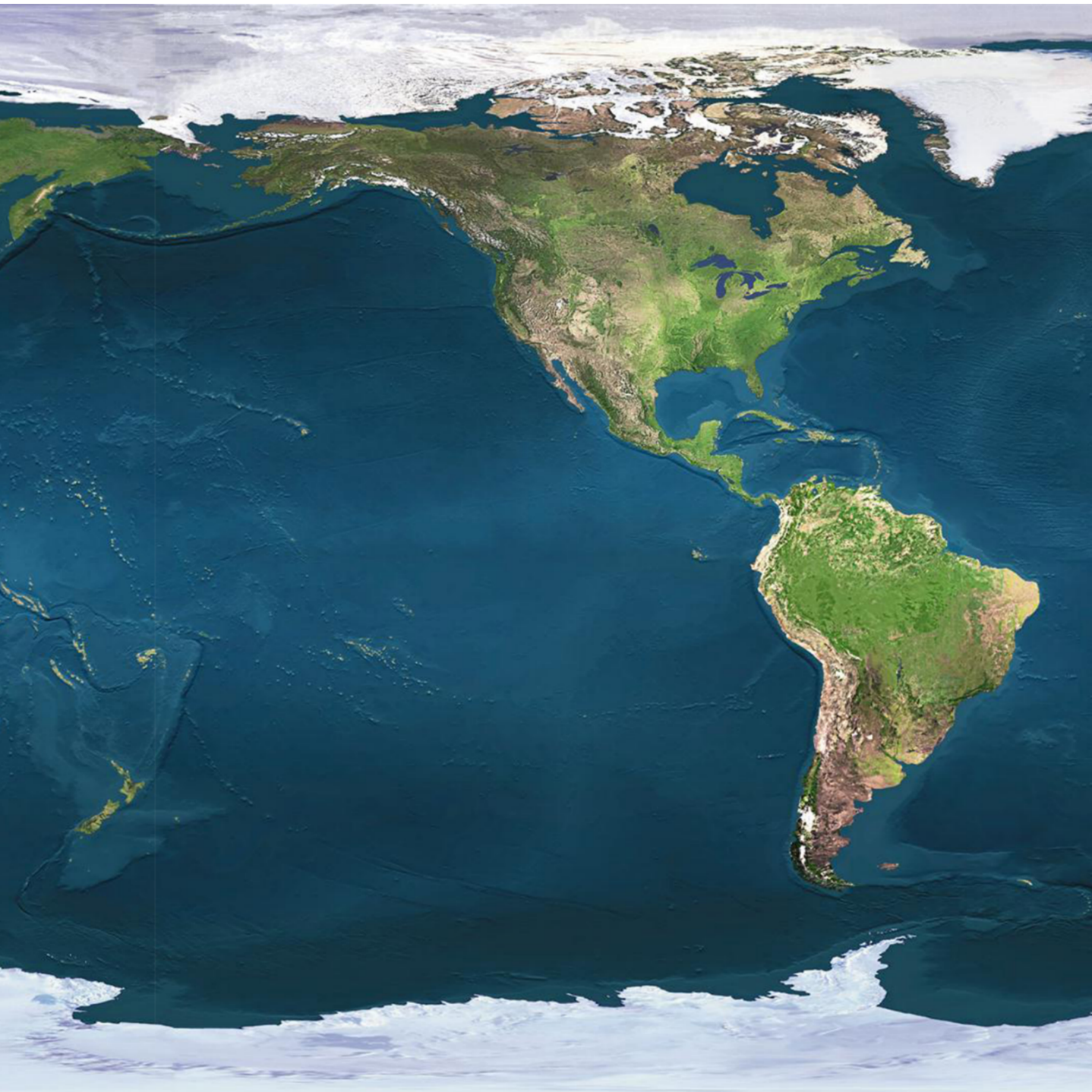
Gli elaborati delle singole aree, articolati in analisi critiche e previsioni, costituiscono il cuore dell'"Osservatorio Strategico"**.**

The Strategic Observatory is a journal that collects analyses and reports developed by the Institute for Defense Research and Analysis (IRAD), carried out by specialized researchers.
The areas of interest monitored in 2025 are:

- Eastern Europe;
- Northern Africa and Israel;
- Southern and Central Africa;
- Conflicts between Sunni and Shiite countries;
- China's international projection;
- Russia's international projection;
- South America;
- NATO: prospects and possible developments;
- Management and conflicts: repercussions on energy resources;
- Hybrid and asymmetric threats.
- Other topics of interest for the Defense sector

The papers about the single areas, divided into analyses and forecasts, constitute the heart of the "Strategic Observatory".

Stampato dalla Tipografia del
Centro Alti Studi per la Difesa




9 791255 151203