Analytica®
ANALISI | STRATEGIA | SCENARI



Policy Brief

La flotta ombra nel Mediterraneo Centrale

Analisi Dottrinale, Implicazioni per lo Spionaggio e Minacce alla Sicurezza Marittima

Autore
Denise Serangelo

analytica-intelligence.com

Il concetto di "Flotta Ombra" (*Shadow Fleet o Dark Fleet*) descrive un fenomeno operativo e strategico caratterizzato dall'impiego di una rete opaca e diversificata di navi mercantili — in prevalenza petroliere per il trasporto di greggio (*Crude Oil Tankers*) e raffinati (*Product Tankers*) — strutturata per eludere i regimi sanzionatori e gli embarghi commerciali internazionali. L'obiettivo primario di tali operazioni è garantire la continuità dell'esportazione di risorse energetiche a sostegno delle economie di Paesi soggetti a restrizioni severe (in particolare la Federazione Russa, l'Iran e il Venezuela), attraverso la sistematica occultazione dell'origine del carico e l'offuscamento dell'effettiva proprietà.

Sotto il profilo analitico e della dottrina strategico-militare, la flotta ombra ha superato la sola dimensione economico-finanziaria e di elusione sanzionatoria per configurarsi come un vero e proprio vettore per operazioni ibride e asimmetriche nella *Grey Zone Warfare*. L'architettura opaca di questi vettori navali, concepita originariamente per aggirare i regimi sanzionatori, mette a disposizione di attori statali avversari un'infrastruttura d'impiego altamente versatile, il cui valore risiede nella sua intrinseca natura a doppio uso: la stessa copertura commerciale utilizzata per il trasporto illecito di risorse energetiche diventa infatti il vettore ideale per la condotta coperta di operazioni d'intelligence, ricognizione e sabotaggio asimmetrico.

Tale assetto consente la proiezione di capacità ISR la condotta di operazioni coperte e la potenziale minaccia verso le infrastrutture marittime critiche quali cavi sottomarini, gasdotti e parchi eolici *offshore*, garantendo al contempo il requisito strategico fondamentale della plausibile denegabilità.

Nel quadro della competizione strategica contemporanea, la *Hybrid Warfare* costituisce il livello concettuale più ampio entro il quale strumenti militari e non militari vengono integrati per perseguire obiettivi strategici attraverso una combinazione di pressione politica, economica, informativa, cibernetica e coercitiva. *La Grey Zone* identifica invece lo spazio operativo nel quale tali strumenti vengono impiegati al di sotto delle soglie che potrebbero determinare una risposta militare diretta, sfruttando ambiguità, gradualità e difficoltà di attribuzione. In questa prospettiva, il riferimento al pensiero strategico di Gerasimov è utile per evidenziare la centralità, nella concezione russa della competizione contemporanea, dell'integrazione tra strumenti militari e non militari e della manipolazione delle soglie del conflitto, pur senza configurare la cosiddetta "dottrina Gerasimov" come una dottrina formalmente codificata.

La Flotta Ombra può essere interpretata come uno degli strumenti attraverso i quali un attore statale o para-statale può operare all'interno di questo spazio di competizione. L'impiego di vettori commerciali formalmente privati, registrati sotto bandiere di comodo e inseriti in strutture proprietarie e gestionali opache consente infatti di sfruttare infrastrutture civili per attività potenzialmente rilevanti sul piano

strategico, mantenendo elevata l'ambiguità sull'effettivo rapporto tra l'operatore e l'eventuale Stato sponsor. Sorveglianza, raccolta informativa, mappatura delle infrastrutture, attività di disturbo o interferenza possono così essere condotte attraverso piattaforme la cui natura commerciale costituisce, al tempo stesso, una copertura operativa e un elemento di complicazione dell'attribuzione.

La rilevanza strategica di tale modello risiede pertanto non soltanto nell'effetto materiale prodotto, ma nella possibilità di separare l'azione dall'eventuale decisore statale attraverso una catena di attribuzione complessa — Stato sponsor, intermediari, società di comodo, armatore, nave ed equipaggio — rendendo più difficile dimostrare un controllo o un mandato diretto. La plausible deniability diviene così una componente funzionale della *Grey Zone*: l'ambiguità non elimina necessariamente la possibilità di attribuzione, ma ne aumenta i costi politici, giuridici e operativi e può ritardare la decisione dello Stato colpito sulla natura e sull'intensità della risposta.

La Flotta Ombra deve pertanto essere considerata non come una manifestazione autonoma della *Hybrid Warfare*, ma come una possibile infrastruttura abilitante della competizione nella *Grey Zone*: uno strumento capace di combinare proiezione commerciale, raccolta informativa, accesso a spazi strategici e potenziale coercitivo, mantenendo l'attività formalmente separata dalle strutture militari dello Stato sponsor.

Il Mediterraneo Centrale rappresenta un baricentro geopolitico e una delle SLOC più vitali ed esposte del pianeta, articolandosi lungo un corridoio marittimo ad alta densità che connette l'Atlantico all'Oceano Indiano attraverso i choke points dello Stretto di Gibilterra, del Canale di Sicilia e del Canale di Suez. La convergenza di questi colli di bottiglia strategici e la costante saturazione del traffico mercantile rendono questo bacino ristretto un teatro operativo ideale per l'impiego asimmetrico della flotta ombra. In questo scenario, l'opacità tattica delle petroliere sanzionate si trasforma in un fattore di destabilizzazione multidimensionale: la massa di navi commerciali in transito offre infatti la copertura perfetta per mimetizzare sia le tecniche di inganno marittimo dirette all'elusione degli embarghi, sia la condotta di operazioni coperte.

La vulnerabilità del bacino supera così la sola dimensione economico-sanzionatoria per investire direttamente la sicurezza delle infrastrutture marittime critiche sottomarine. I fondali del Canale di Sicilia e dei bacini adiacenti custodiscono un'intricata rete di dorsali in fibra ottica intercontinentali e condotte energetiche strategiche, fondamentali per la stabilità finanziaria e l'approvvigionamento del continente europeo. In questo contesto, la presenza sregolata di navi prive di tracciabilità certa o di una chiara attribuzione statale mettono a disposizione degli attori ostili una versatile piattaforma a doppio uso. Tali vettori consentono di abbinare al traffico illecito di risorsa energetica la condotta di attività d'intelligence passiva, il tracciamento dei dispositivi navali della NATO e la potenziale esecuzione di azioni di disturbo o sabotaggio asimmetrico ai danni dei fondali, garantendo allo Stato sponsor la necessaria plausible deniability per eludere ritorsioni formali o risposte militari dirette.

Anatomia e tattiche operative della flotta ombra.

A causa della loro natura intrinsecamente illecita, le unità navali appartenenti alla flotta ombra mettono in atto sofisticate contromisure tattiche per eludere il tracciamento dei centri di controllo del traffico marittimo detti anche VTS e la sorveglianza satellitare. L'obiettivo primario di tali manovre è scongiurare ispezioni, sequestri del carico o procedure di abbordaggio da parte delle autorità navali internazionali. Per raggiungere questo scopo, gli operatori adottano un complesso protocollo di evasione basato su inganni tecnologici e manipolazioni. L'impiego sistematico di queste procedure sregolate non solo compromette l'efficacia del contrasto sanzionatorio, ma mina gravemente la sicurezza della navigazione e la tutela degli ecosistemi marini.

I protocolli operativi di evasione adottati dalle navi ombra si articolano attraverso una complessa integrazione di inganni tecnologici, manipolazioni fisiche e artifizi societari, concepiti per rendere inefficaci i tradizionali sistemi di sorveglianza marittima.

Il primo pilastro strategico risiede nella manipolazione dei dati di posizionamento informatico. Spegnendo deliberatamente il transponder AIS — in palese violazione della Regola 19 del Capitolo V della Convenzione SOLAS — la nave entra in una fase di buio operativo (*going dark*) per effettuare manovre non autorizzate. Per evitare di insospettire gli algoritmi di monitoraggio satellitare con una scomparsa improvvisa, gli operatori ricorrono sempre più spesso all'AIS Spoofing e al disturbo dei segnali GNSS. Mediante *software* dedicati o apparati radio modificati, il transponder trasmette coordinate fittizie che proiettano la nave su rotte teoriche prive di anomalie, mentre la posizione reale si trova a centinaia di miglia di distanza. Un caso emblematico è rappresentato dalle petroliere che risultano formalmente in navigazione circolare nell'Atlantico mentre si trovano all'ormeggio o all'ancora presso terminali petroliferi soggetti a sanzioni, come quelli dell'Iran o del Venezuela, o intente a caricare greggio russo nel Mar Nero.

Il secondo momento critico riguarda le operazioni di trasbordo in alto mare *(Ship-to-Ship - STS*), condotte lontano dalla vista delle autorità costiere per rescindere il legame tracciabile tra il punto di estrazione e la destinazione finale. Queste manovre ad alto rischio avvengono in aree marittime strategiche caratterizzate da giurisdizioni sovrapposte o scarsamente presidiate, come le acque internazionali al largo del Golfo di Laconia in Grecia, le adiacenze del Canale di Suez o lo spazio marittimo antistante l'enclave di Ceuta. Durante il trasferimento del carico da una nave navetta a un vettore a grande capacità si applica spesso la tecnica del blending o miscelazione: il greggio sanzionato viene combinato con idrocarburi di differente estrazione per alterarne la composizione chimica e consentire l'emissione di una polizza di carico contraffatta che attesti una provenienza lecita, ad esempio mediorientale o del Sud-est asiatico.

A livello strutturale e identificativo, la flotta ombra neutralizza i controlli amministrativi attraverso la continua mutazione della propria identità navale e societaria. Questo processo sfrutta il fenomeno del *flag-hopping*, ovvero il cambio compulsivo del registro di bandiera verso Paesi caratterizzati da controlli minimi e scarsa cooperazione internazionale, come Gabon, Eswatini o Palau. Nei casi più estremi si verifica il cosiddetto *ghost flagging*, in cui la nave naviga esibendo documenti di immatricolazione fittizi rilasciati da enti non riconosciuti o registri fraudolenti. Per impedire la verifica visiva o satellitare, gli equipaggi modificano la livrea dipingendo un nome falso sullo scafo e coprendo o alterando il numero IMO, l'identificativo univoco e permanente assegnato dall'Organizzazione Marittima Internazionale che dovrebbe seguire la nave per l'intero ciclo di vita.

Questa opacità tecnica è infine blindata da un'architettura finanziaria basata su catene di società di comodo (*shell companies)* e scatole cinesi con sede in giurisdizioni offshore quali le Isole Marshall, Panama o Dubai. Cambiando continuamente la proprietà formale e l'entità gestrice della nave a intervalli di pochi mesi, la reale proprietà beneficiariarimane del tutto inaccessibile. Ciò rende vani i tentativi di sequestro amministrativo o le azioni legali da parte dei governi occidentali, poiché ogni provvedimento sanzionatorio viene sistematicamente eluso con la liquidazione della società proprietaria e la contestuale intestazione del bene a un nuovo veicolo societario opaco.

Vectoring di spionaggio e rilevamento coperto (ISR/SIGINT)

L'integrazione di vettori mercantili opachi all'interno delle architetture d'intelligence statali segna l'evoluzione strategica della flotta ombra da semplice strumento di elusione sanzionatoria a vera e propria piattaforma navale per operazioni coperte e raccolta informativa (*Maritime Intelligence Operations*). Tale assetto asimmetrico non sostituisce, ma affianca e potenzia l'attività delle navi ausiliarie militari adibite a scopi speciali — quali le unità di ricerca idrografica e spionaggio della classe Yantar gestite dal Direttorato Principale per la Ricerca Sottomarina del Ministero della Difesa Russo (GUGI) — offrendo il vantaggio decisivo di una presenza capillare, persistente e non immediatamente attribuibile sul piano del diritto internazionale.

La prima direttrice tattica riguarda la mappatura dello spettro elettromagnetico attraverso l'impiego di sensoristica clandestina. L'architettura navale delle grandi petroliere e delle portarinfuse offre ampi volumi strutturali e una costante disponibilità di alimentazione elettrica per l'alloggiamento di apparati di guerra elettronica. L'installazione di sensori SIGINT ed ELINT camuffati da apparecchiature di navigazione ordinarie — come radar modificati, sensori passivi o antenne omnidirezionali celate da radome commerciali — trasforma la nave in un nodo di ascolto avanzato. Durante il transito lungo le SLOC e in prossimità delle basi navali o delle aree di esercitazione NATO, questi vettori intercettano e catalogano le emissioni radar, i ponti radio tattici e le comunicazioni criptate delle forze alleate, consentendo la mappatura dell'*Order of Battle* elettronico avversario per future operazioni di disturbo o saturazione.

In secondo luogo, la flotta ombra opera come nave madre informale secondo i principi della *Unconventional Maritime Warfare*, consentendo la proiezione di sistemi non pilotati in un quadro di completa non-attribuibilità. Le ampie superfici di coperta e le stive di carico offrono l'ambiente ideale per il trasporto, il montaggio e il lancio di UAV destinati alla ricognizione ottica o radar su porti commerciali, installazioni militari e navi da guerra in transito. Parallelamente, la messa a mare di UUV o droni sottomarini filo-guidati permette la scansione dei fondali e il monitoraggio delle infrastrutture marittime critiche come cavi dati intercontinentali e condotte energetiche. L'eventuale tracciamento o recupero di un drone non consente di risalire allo Stato sponsor, poiché la piattaforma di lancio rimane un vettore mercantile gestito da società di comodo dislocate in giurisdizioni *offshore*.

Prospettive e raccomandazioni strategiche

La neutralizzazione della minaccia multidimensionale posta dalla flotta ombra nel Mediterraneo Centrale impone un superamento concettuale dei tradizionali schemi di contrasto, promuovendo la transizione da un approccio meramente amministrativo e sanzionatorio a una strategia integrata di Difesa Marittima Multi-Dominio. La natura ibrida di questi vettori, in grado di oscillare fluidamente tra l'illecito commerciale e la condotta di operazioni coperte d'*intelligence* o di sabotaggio asimmetrico, richiede una riposta sistemica capaci di coniugare il diritto marittimo internazionale, l'innovazione tecnologica e la proiezione di potenza navale.
Il primo tassello di tale strategia risiede nel riesame e nell'adattamento dottrinale delle Regole di Ingaggio e dei quadri normativi d'intervento delle forze navali e di polizia marittima europee e alleate. In conformità con il regime giuridico stabilito dalla UNCLOS, con particolare riferimento all'articolo 110 relativo al Diritto di Visita, occorre codificare procedure operative standardizzate che consentano l'abbordaggio e l'ispezione coercitiva delle unità navali sospettate di falsa immatricolazione o di assenza di nazionalità L'assenza di un valido registro di bandiera o la prolungata disattivazione non giustificata del transponder AIS devono essere formalmente configurate come indicatori di rischio sistemico e presupposti legittimanti per l'esercizio della giurisdizione coercitiva dello Stato costiero o dell'autorità navale in alto mare, superando la passività derivante dalla rigida interpretazione del principio di esclusiva giurisdizione dello Stato di bandiera.

Un secondo pilastro fondamentale riguarda la protezione attiva e strutturata delle Infrastrutture Marittime Critiche con primario riferimento alle dorsali in fibra ottica, alle *Cable Landing Stations* e alle condotte energetiche intercontinentali che attraversano i fondali del Canale di Sicilia e del bacino centrale. In quest'ottica, la dottrina della *Maritime Domain Awareness* promuove l'istituzione normativamente codificata di Zone di Protezione Speciale Marittima attorno ai nodi infrastrutturali ad alto valore strategico. All'interno di tali perimetri deve essere precluso il transito, il stazionamento dinamico o l'ancoraggio non autorizzato per tutti i vettori commerciali che non mantengano una tracciabilità AIS continua, accurata e verificata. La sorveglianza di queste aree richiede l'integrazione di reti di monitoraggio acustico passivo sottomarino, pattugliamento navale persistente e sistemi d'intelligence satellitare a rilevamento termico e ad apertura sintetica (SAR), in grado di smascherare immediatamente le manovre di AIS Spoofing o il trascinamento deliberato delle ancore prima che si traducano in danni irreversibili.

Infine, l'efficacia operativa di un simile dispositivo difensivo dipende dall'interoperabilità e dallo scambio informativo inter-agenzia e multilaterale. La convergenza informativa deve integrare in tempo reale i flussi di intelligence militare forniti dalle Marina Militare e dagli organismi d'intelligence strategica (AISI e AISE) con i dati operativi e di monitoraggio commerciale gestiti dall'EMSA, da Frontex e

dalle autorità di navigazione civile. Questa architettura di condivisione deve estendersi attivamente ai Paesi partner del Mediterraneo Meridionale e Orientale attraverso quadri di cooperazione bilaterali e multilaterali (quali l'Iniziativa 5+5 Difesa). L'obiettivo strategico è la creazione di una rete d'allarme rapido (*Early Warning Network*) capace di tracciare, identificare e categorizzare i vettori opachi prima del loro ingresso nei colli di bottiglia (*choke points*) del Mediterraneo Centrale, privando le forze ostili del margine di sorpresa e del requisito di plausibile denegabilità su cui si fonda la loro condotta nella *Grey Zone*.

Note Bibliografiche

1- Patalano, A. (2023). *Sailing in the Grey Zone: Maritime Hybrid Threats and the Protection of Subsea Infrastructure. Royal United Services Institute (RUSI) Occasional Papers.*

2- Guilfoyle, D. (2009). *Shipping Interdiction and the Law of the Sea. Cambridge University Press.*

3- Kraska, J. (2022). *Maritime Power and the Law of the Sea. Oxford University Press.*

4- Treves, T. (2010). *Piracy, Law of the Sea, and Use of Force: Developments in the Law of the Sea. European*

5- *Journal of International Law*, 20(2), 399-414.

6- *Center for Research on Energy and Clean Air (CREA). (2023-2024). Tracking the Russian Shadow Fleet and Price Cap Evasion in European Waters. Policy Briefing Series.*

7- *International Maritime Organization (IMO). (2023). Resolution A.1192(33): Measures to Prevent Unlawful Operations of the 'Dark Fleet' or 'Shadow Fleet' in the Maritime Sector. IMO Assembly Publications.*

8- *Lloyd's List Intelligence & Windward. (2023-2024). Maritime Deception Techniques: AIS Spoofing, Flag Hopping, and Dark STS Transfers in the Mediterranean. Joint Industry Whitepaper.*

9- *Royal United Services Institute (RUSI). (2023). The Dark Side of the Sea: Shadow Fleets, Sanctions Busting and Maritime Security in Europe. RUSI Special Report.*

10- Bueger, C., & Liebetrau, T. (2023). *Protecting Subsea Infrastructure: Critical Seabed Infrastructure and Hybrid Threats. European Parliament - Subcommittee on Security and Defence (SEDE).*

11- NATO *Maritime Command (MARCOM). (2024). Critical Undersea Infrastructure Protection Strategy and the Role of Maritime Domain Awareness (MDA).* NATO *Policy Papers.*

Glossario

AIS (Automatic Identification System): Sistema di tracciamento radioelettrico a corto raggio obbligatorio per le navi di stazza lorda pari o superiore a 300 tonnellate (secondo la Convenzione SOLAS). Trasmette dati identificativi, posizione, rotta e velocità alle stazioni a terra e ai satelliti.

AIS Spoofing: Pratica di manipolazione informatico-radioelettrica mediante la quale un transponder AIS trasmette coordinate geografiche false, simulando la posizione della nave in un'area lontana da quella reale.

Anchor Dragging (Trascinamento dell'ancora): Manovra (volontaria o colposa) in cui l'ancora di una nave viene calata sul fondale durante il moto, potenzialmente in grado di tranciare o danneggiare cavi dati e condotte energetiche sottomarine.

Beneficial Ownership (Proprietà Beneficiaria): La persona fisica o l'entità statale reale che possiede o controlla in ultima istanza un'imbarcazione o ne trae profitto, celata da catene di società di comodo (shell companies).

Choke Point: Stretto o canale marittimo di rilevanza strategica caratterizzato da dimensioni geografiche ridotte ed elevata densità di traffico, la cui ostruzione vulnera le linee di comunicazione marittima (SLOC).

CMI (Critical Maritime Infrastructures): Infrastrutture marittime critiche situate sul litorale, in superficie o sul fondo del mare (cavi dati in fibra ottica, gasdotti, oleodotti, stazioni di approdo e parchi eolici offshore).

Dark Fleet / Shadow Fleet: Insieme di navi mercantili (prevalentemente petroliere) con assetti proprietari opachi, assicurazioni irregolari e bandiere di convenienza, utilizzate per eludere embarghi commerciali ed esercitare attività coperte.

ELINT (Electronic Intelligence): Attività di raccolta e analisi delle emissioni elettromagnetiche non comunicative avversarie, quali i segnali emessi da radar di navigazione, scoperta aerea o sistemi di difesa.

Flag-Hopping: Pratica consistente nel cambiare frequentemente e in brevi archi temporali il registro navale di immatricolazione della nave, spostandolo verso Paesi con controlli meno rigorosi.

Ghost Flagging: Uso di documenti e certificati di immatricolazione fittizi o rilasciati da enti non riconosciuti, con la conseguenza che la nave risulta priva di una valida nazionalità (stateless vessel).

Going Dark: Disattivazione volontaria e non autorizzata del transponder AIS da bordo della nave per nascondere il proprio tracciamento radar-satellitare.

Grey Zone Warfare: Spazio operativo di competizione strategica situato tra la regolare attività diplomatica/economica e il conflitto armato aperto, caratterizzato da ambiguità, aggressività non letale e difficoltà di attribuzione.

GUGI (Glavnoye Upravleniye Glubokovodnykh Issledovaniy): Direttorato Principale per la Ricerca Sottomarina del Ministero della Difesa Russo, organizzazione militare responsabile delle navi per operazioni speciali e missioni sui fondali marini.

HUMINT (Human Intelligence): Attività d'intelligence basata sulla raccolta di informazioni tramite fonti umane, agenti in copertura o infiltrazioni di personale.

ISR (Intelligence, Surveillance, and Reconnaissance): Insieme integrato di capacità per la raccolta, elaborazione e distribuzione di informazioni operative a supporto delle decisioni strategiche e tattiche.

Maritime Domain Awareness (MDA): Comprensione efficace di qualsiasi evento, fattore o elemento associato al dominio marittimo che possa impattare sulla sicurezza, la difesa, la salute o l'ambiente.

Glossario

Plausible Deniability (Plausibile Denegabilità): Capacità di uno Stato o attore di negare la propria responsabilità o paternità in un'azione ostile, sfruttando strutture intermedie, attori privati o la mancanza di prove dirette.

Port State Control (PSC): Regime d'ispezione ufficiale condotto dagli Stati costieri sulle navi straniere che approdano nei propri porti per verificare la rispondenza alle norme internazionali (sicurezza, inquinamento, condizioni del lavoro).

P&I Clubs (Protection and Indemnity Clubs): Associazioni mutualistiche d'assicurazione marittima che coprono la responsabilità civile degli armatori contro terzi, inclusi i disastri ambientali da versamento di idrocarburi.

Right of Visit (Diritto di Visita - Art. 110 UNCLOS): Facoltà concessa alle navi da guerra di abbordare e ispezionare in alto mare una nave mercantile straniera qualora vi sia il fondato sospetto che sia priva di nazionalità, eserciti la pirateria o la tratta degli schiavi.

SIGINT (Signals Intelligence): Attività d'intelligence fondata sull'intercettazione e analisi di segnali elettromagnetici, suddivisa in comunicazioni (COMINT) ed emissioni elettroniche (ELINT).

SLOC (Sea Line of Communication): Le principali rotte marittime commerciali e militari che collegano porti e bacini strategici a livello globale.

SOLAS (Safety of Life at Sea): Convenzione internazionale approvata dall'IMO per la tutela della sicurezza della vita umana in mare.

STS (Ship-to-Ship Transfer): Operazione di trasbordo di carico liquido (es. greggio) condotta in mare aperto direttamente tra due navi accostate, usata per miscelare o camuffare l'origine delle merci.

UNCLOS (United Nations Convention on the Law of the Sea): Convenzione delle Nazioni Unite sul Diritto del Mare (Montego Bay, 1982), il quadro giuridico di riferimento per l'uso degli oceani e dei mari.

UAV / UUV: Unmanned Aerial Vehicle (drone aereo non pilotato) e Unmanned Underwater Vehicle (drone sottomarino autonomo o filo-guidato).

VTS (Vessel Traffic Services): Sistemi e centri di controllo a terra predisposti dalle autorità marittime per monitorare e gestire il traffico navale nelle acque costiere e nei canali ad alta densità.

L’autore

Denise Serangelo

Denise Serangelo è analista specializzata in sicurezza internazionale, competizione strategica e minacce multidominio. Si è formata presso la Scuola di Applicazione dell’Esercito, in collaborazione con l’Università degli Studi di Torino.

Il suo principale ambito di ricerca è il Mediterraneo centrale, con particolare attenzione alla Libia, al fianco meridionale europeo e alle implicazioni delle dinamiche politico-militari regionali per la sicurezza nazionale ed europea.

Si occupa di analisi delle minacce emergenti, valutazione del rischio e scenari strategici, approfondendo l’interazione tra dimensione militare, geopolitica, tecnologia e infrastrutture critiche.

Ha maturato esperienza sul campo e svolge attività di consulenza e analisi strategica a supporto dei processi decisionali, elaborando report, studi e valutazioni per interlocutori istituzionali e operatori dei settori della sicurezza e della difesa.