Analytica®
ANALISI | STRATEGIA | SCENARI



Policy Brief

Occultamento e sopravvivenza delle forze terrestri

La signature managment

Autore
Denise Serangelo

analytica-intelligence.com

L’occultamento delle forze terrestri nell’era dello spettro elettromagnetico

Il conflitto russo-ucraino e quello mediorientale hanno evidenziato e accelerato una trasformazione strutturale del combattimento terrestre contemporaneo, investendo uno dei suoi presupposti meno discussi ma più rilevanti: la capacità di una forza di rimanere non rilevata fino al momento dell’impiego e di sottrarsi all’ingaggio avversario. La progressiva contrazione degli spazi di occultamento ha determinato un ambiente operativo caratterizzato da crescente trasparenza informativa, nel quale *survivability*, mobilità e massa risultano sempre più interdipendenti.

La diffusione di costellazioni satellitari commerciali, UAS a basso costo, capacità GEOINT, strumenti OSINT, sistemi di guerra elettronica e algoritmi di analisi automatizzata ha modificato il rapporto tradizionale tra terreno, occultamento e libertà di manovra. La *fog of war*, elemento permanente della riflessione strategica da Clausewitz in poi, non è stata eliminata, ma profondamente riconfigurata: il problema delle forze terrestri contemporanee non consiste più soltanto nel comprendere la situazione operativa, ma nel pianificare e condurre la manovra generando effetti in un ambiente nel quale l’avversario dispone di capacità persistenti di *detection, tracking, identification e targeting*.

In tale contesto, l’occultamento deve essere ricondotto alla più ampia funzione di *signature management*, quale componente della moderna *Force Protection* e requisito della sopravvivenza operativa.

È questa la principale discontinuità introdotta dall’attuale ambiente operativo. Nel paradigma tradizionale della guerra terrestre, la protezione della forza dall’osservazione e dagli effetti cinetici era perseguita mediante terreno, fortificazioni, profondità, corazzatura, camouflage e dispersione. Nel paradigma emergente, tali strumenti rimangono essenziali, ma devono essere integrati in una gestione sistemica della signature. Una brigata, un battaglione o una singola unità non producono infatti una firma univoca, ma un insieme di indicatori simultanei — visuali, termici, elettromagnetici, acustici, cinetici, logistici e comportamentali — la cui correlazione può consentire all’avversario di ricostruire progressivamente identità, posizione e attività della forza. Il problema dell’occultamento evolve pertanto dalla semplice riduzione dell’osservabilità alla gestione della probabilità di detection e della successiva correlazione degli indicatori, intervenendo sulla catena informativa che conduce dall’individuazione al targeting.

In questo nuovo contesto operativo, la trasformazione più significativa consiste nella contrazione degli intervalli temporali e spaziali di non osservabilità entro i quali una forza può muovere, disporsi e generare effetti senza essere efficacemente acquisita dall’avversario. La persistenza della sorveglianza, unita alla crescente disponibilità di sensori distribuiti e fonti ISR eterogenee, riduce infatti la possibilità di considerare l’occultamento come una condizione stabile. La non osservabilità diventa

una condizione dinamica, da conseguire e preservare attraverso mobilità, dispersione, disciplina delle emissioni, deception e controllo della signature lungo l'intero ciclo operativo.

Qualsiasi forza impegnata in attività cinetiche produce oggi una pluralità di indicatori che possono essere acquisiti da sensori differenti e successivamente correlati attraverso sistemi C4ISR, capacità di data fusion e processi di analisi automatizzata. Ne deriva un cambiamento fondamentale: l'occultamento non coincide più con la mera capacità di sottrarre una forza alla vista, ma con la capacità di impedire o ritardare la ricostruzione della sua presenza, disposizione, composizione, intenzione e comportamento operativo. La *signature management* assume quindi una funzione direttamente connessa alla *survivability*, agendo a monte dell'ingaggio e mirando a interrompere o rallentare la catena *detect-identify-track-target-engage*.

Questo passaggio modifica radicalmente anche il rapporto tra sensore ed effetto. La tradizionale sequenza "osservazione-decisione-ingaggio" tende progressivamente a comprimersi, mentre la disponibilità di sensori distribuiti consente di trasformare molteplici indicatori deboli in una situational awareness sufficientemente robusta per alimentare il *targeting*. Non è quindi necessario che un singolo sensore disponga di un quadro completo: la fusione di dati provenienti da domini e fonti differenti può generare una traccia operativa coerente e sufficientemente persistente da orientare l'azione cinetica. La superiorità informativa assume così una marcata dimensione temporale: la forza individuata non è necessariamente sconfitta, ma la forza che permane osservabile per un tempo sufficiente aumenta progressivamente la propria esposizione al *targeting*, riduce la libertà di manovra e trasferisce l'iniziativa all'avversario.

La crisi della massa militare, la dispersione e la gestione della firma

Questa dinamica produce una conseguenza strategica particolarmente rilevante: la progressiva crisi della concentrazione di grandi masse militari a favore di un modello di forza maggiormente distribuito, modulare e "molecolare". La massa, tuttavia, non perde la propria funzione: rimane indispensabile per generare effetti decisivi, sostenere il combattimento e conquistare o mantenere il terreno. Ciò che diventa problematico è la concentrazione della massa in configurazioni fisiche e digitali facilmente rilevabili, persistenti e correlabili dall'avversario. La sfida per le forze terrestri contemporanee consiste quindi nella capacità di generare massa di effetti senza necessariamente generare una firma proporzionale alla massa fisicamente impiegata, riducendo la possibilità che l'avversario ricostruisca, attraverso la correlazione di molteplici indicatori, consistenza, disposizione e intenzione della forza. La contraddizione operativa del nuovo ambiente consiste pertanto nel concentrare rapidamente il potere di combattimento, evitando di concentrare altrettanto rapidamente gli indicatori che ne consentono la scoperta e il targeting. In questa prospettiva, la dispersione non rappresenta semplicemente una misura difensiva, né può essere considerata una risposta automatica alla crescente osservabilità del campo di battaglia: costituisce una delle opzioni attraverso cui realizzare la signature management, con vantaggi e costi operativi che devono essere valutati in relazione alla missione, alla minaccia e alla capacità di comando e controllo. Una forza distribuita può infatti ridurre la vulnerabilità dei singoli nodi e aumentare la resilienza del dispositivo, ma introduce contestualmente maggiori esigenze di C2, comunicazioni, logistica, coordinamento e interoperabilità. In assenza di reti di comando distribuite, capacità di comunicazione alternative, autonomia decisionale e procedure operative adeguate, la dispersione può trasformarsi da fattore di *survivability* in frammentazione della capacità di combattimento. Il problema, pertanto, non consiste nella scelta binaria tra concentrazione e dispersione, ma nella capacità di concentrare rapidamente gli effetti, distribuire il dispositivo e modificare dinamicamente la propria signature in funzione dell'evoluzione della situazione operativa. In tale quadro, la disciplina elettromagnetica assume una rilevanza crescente quale componente della *Force Protection* e della gestione della firma. Il problema non è necessariamente l'eliminazione delle emissioni — spesso incompatibile con le esigenze di C2, ISR e coordinamento delle operazioni — quanto la loro gestione in termini di intensità, persistenza, prevedibilità e correlabilità, impedendo che esse possano essere associate con sufficiente affidabilità a una specifica unità, funzione o intenzione operativa. La crescente connettività delle forze produce infatti un paradosso: l'integrazione digitale aumenta la *situational awareness* e la capacità di coordinamento, ma può simultaneamente ampliare la superficie di osservabilità elettromagnetica e informativa del dispositivo.

La *signature management* diventa quindi una funzione di equilibrio tra connettività, efficacia operativa ed esposizione.

La stessa dinamica investe il dominio informativo e modifica profondamente il rapporto tradizionale tra Stato, forze armate e disponibilità dell'informazione. La diffusione dell'OSINT, delle capacità commerciali di osservazione e degli strumenti digitali di acquisizione e analisi ha progressivamente ridotto il monopolio statuale sulla produzione di informazioni militarmente rilevanti. Un dato utile al processo ISR non deve necessariamente provenire da un sensore militare dedicato: immagini satellitari commerciali, dati geospaziali, contenuti open source, social media, osservazioni locali, applicazioni geolocalizzate e sistemi automatizzati di elaborazione possono essere combinati per ricostruire pattern of life, movimenti, attività logistiche e variazioni nella postura di una forza. Si assiste così a una progressiva democratizzazione della capacità di osservazione, nella quale anche soggetti privi di una sofisticata architettura ISR nazionale possono acquisire, aggregare e correlare informazioni sufficienti a contribuire alla scoperta e alla caratterizzazione di un obiettivo. In questo ambiente, la firma non è quindi prodotta esclusivamente dalle piattaforme militari, ma anche dall'ecosistema informativo nel quale esse operano. Movimenti, emissioni, attività logistiche, comunicazioni, immagini pubblicate inconsapevolmente e pattern comportamentali possono concorrere alla costruzione di una digital signature della forza, rendendo la gestione dell'esposizione una responsabilità trasversale all'intero ciclo operativo. Tale trasformazione modifica anche la funzione della *deception*. In un ambiente caratterizzato dalla disponibilità di fonti molteplici e dalla crescente capacità di *data fusion*, l'inganno non può essere limitato alla generazione di falsi bersagli, ma deve concorrere a condizionare il processo attraverso il quale l'avversario attribuisce significato agli indicatori raccolti. L'obiettivo non è necessariamente conseguire l'invisibilità — condizione difficilmente sostenibile in un ambiente di sorveglianza persistente — ma aumentare l'incertezza dell'avversario e degradarne la capacità di correlazione, classificazione e previsione. Una forza può quindi essere osservata senza essere correttamente interpretata; può essere localizzata senza che l'avversario riesca a determinarne con sufficiente affidabilità consistenza, funzione, intenzione e successiva direttrice di movimento. La deception diventa in questo senso complementare alla *signature management*: la prima agisce sulla percezione e interpretazione dell'indicatore, la seconda sulla sua produzione, esposizione e controllabilità. Il paradigma emergente non è dunque quello dell'invisibilità assoluta, ma quello della ambiguità operativa, ottenuta attraverso la combinazione di dispersione, mobilità, disciplina delle emissioni, *deception*, *camouflage* e gestione multidimensionale della firma.

La conseguenza più rilevante riguarda infine il concetto stesso di Force Protection e survivability. Per decenni la protezione della forza è stata associata prevalentemente alla capacità di assorbire o neutralizzare gli effetti di un attacco attraverso corazzatura, protezione balistica, fortificazioni, sistemi attivi e passivi e profondità. Nell'ambiente operativo contemporaneo questa concezione risulta incompleta, perché una piattaforma può essere tecnicamente altamente protetta ma rimanere vulnerabile se viene acquisita, classificata e seguita con sufficiente anticipo. La *survivability* deve pertanto essere considerata lungo l'intero engagement sequence, anticipando la fase cinetica e intervenendo sulla probabilità che la catena *detect-identify-track-target-*

engage possa essere completata. La domanda non è quindi soltanto se una piattaforma possa sopravvivere all'effetto di un'arma, ma quanto sia probabile che venga individuata, classificata, tracciata e ingaggiata e per quanto tempo possa continuare a generare effetti prima che l'avversario riesca a trasformare la sua osservazione in un'azione cinetica efficace. In questa prospettiva, la signature management non sostituisce la Force Protection, ma ne costituisce una dimensione preventiva e trasversale: agisce prima dell'ingaggio per ridurre l'esposizione, preservare la libertà di manovra e aumentare la resilienza del dispositivo. La sopravvivenza della forza non dipende quindi esclusivamente dalla capacità di resistere all'attacco, ma anche dalla capacità di ritardare la scoperta, degradare la qualità della traccia, interrompere la correlazione degli indicatori, modificare rapidamente il dispositivo e mantenere la capacità di generare effetti sotto osservazione persistente. È in questo passaggio che la dispersione assume il proprio significato più ampio: non semplice separazione fisica delle unità, ma componente di una più complessa architettura di sopravvivenza nella quale massa, mobilità, C2, *deception*, disciplina elettromagnetica e gestione della signature devono essere sincronizzati per conseguire un obiettivo comune: concentrare il combattimento senza concentrare la vulnerabilità informativa della forza.

Conclusioni

La trasformazione dell'ambiente operativo impone di considerare la signature management non come una tecnica specialistica di occultamento, ma come una funzione trasversale della Force Protection, direttamente integrata nella pianificazione e nella condotta delle operazioni terrestri. Manovra, intelligence, ISR, guerra elettronica, C2, logistica, mobilità, deception e protezione delle forze concorrono infatti alla gestione dell'esposizione complessiva del dispositivo. Un posto comando, una batteria di artiglieria, un'unità corazzata o un nodo logistico non devono essere valutati esclusivamente in termini di capacità di combattimento e protezione fisica, ma anche in relazione alla quantità e alla qualità degli indicatori che rendono possibile la loro *detection, identification, tracking e targeting*. La firma diventa quindi una vera e propria variabile di pianificazione operativa, da considerare già in fase di progettazione della forza e della missione.

Per il decisore militare, ciò implica un primo cambiamento di paradigma: la *survivability* non può più essere valutata prevalentemente ex post, in funzione della capacità di assorbire l'effetto di un attacco, ma deve essere costruita ex ante attraverso la riduzione della probabilità di scoperta e la degradazione della qualità della traccia avversaria. La domanda non è soltanto se una piattaforma possa sopravvivere a un ingaggio, ma se il sistema di forze sia in grado di ritardare la scoperta, interrompere la correlazione degli indicatori, modificare il proprio dispositivo e continuare a generare effetti sotto condizioni di sorveglianza persistente. In questa prospettiva, la *signature management* diventa una componente della combat survivability e deve essere integrata nei processi di *force design*, addestramento, valutazione della readiness e pianificazione operativa.

Il secondo elemento riguarda il rapporto tra massa, dispersione e capacità di combattimento. L'esperienza dei conflitti recenti non dimostra la fine della massa, ma la crescente vulnerabilità della massa quando viene concentrata in configurazioni fisiche, elettromagnetiche o logistiche facilmente osservabili e persistenti. La risposta non consiste pertanto nella semplice dispersione delle unità, che può generare vulnerabilità proprie in termini di C2, sustainment e coordinamento, ma nella capacità di concentrare gli effetti e distribuire la firma. La forza futura dovrà essere progettata per passare rapidamente da configurazioni distribuite a configurazioni di concentrazione temporanea del potere di combattimento, per poi ristabilire rapidamente condizioni di dispersione e ridotta osservabilità. Ciò richiede mobilità, modularità, autonomia tattica, resilienza delle reti e capacità di operare in condizioni di connettività degradata. Il terzo elemento riguarda la crescente integrazione tra connettività e osservabilità. La digitalizzazione del campo di battaglia costituisce un moltiplicatore di efficacia, ma genera contemporaneamente nuove superfici di esposizione. Ogni incremento della connettività può produrre ulteriori emissioni, pattern di attività e dipendenze infrastrutturali suscettibili di essere acquisiti e correlati dall'avversario. La pianificazione della forza dovrà quindi perseguire un equilibrio tra *information superiority* e signature control, evitando che la ricerca della massima connettività trasformi il *network* stesso in un indicatore persistente della presenza e della disposizione della forza. La resilienza del C2, le comunicazioni alternative, la gestione

dello spettro elettromagnetico e la capacità di operare temporaneamente in modalità degradate devono diventare elementi strutturali della *readiness*.

Un quarto profilo riguarda la trasformazione del rapporto tra sensore, informazione ed effetto. La crescente disponibilità di sensori distribuiti, fonti commerciali e capacità OSINT rende sempre meno efficace una concezione della *Force Protection* basata esclusivamente sulla protezione delle piattaforme. La minaccia non proviene necessariamente da un singolo sensore militare avanzato, ma dalla possibilità che molteplici indicatori apparentemente marginali vengano aggregati attraverso data fusion, analisi automatizzata e correlazione multi-dominio fino a generare una traccia sufficientemente affidabile per alimentare il *targeting*. Per questo motivo, la gestione della firma deve estendersi all'intero ecosistema informativo della forza, includendo non soltanto le emissioni dei sistemi militari, ma anche pattern logistici, comportamentali, comunicativi e digitali.

In questo quadro, anche la deception assume una funzione diversa. Non deve essere concepita esclusivamente come produzione di falsi bersagli, ma come capacità di alterare la qualità dell'interpretazione avversaria, aumentando l'incertezza sulla reale consistenza, disposizione, funzione e intenzione del dispositivo. La combinazione tra signature management e deception consente quindi di perseguire non l'improbabile obiettivo dell'invisibilità assoluta, ma quello più realistico della ambiguità operativa: essere osservabili senza risultare immediatamente identificabili, classificabili e prevedibili. Per il decisore questo significa considerare la deception, la disciplina delle emissioni, la mobilità e la dispersione come componenti complementari di un'unica architettura di sopravvivenza.

La conseguenza per la readiness è altrettanto rilevante. Una forza rapidamente dispiegabile non può essere considerata realmente pronta se, una volta inserita nel teatro operativo, non è in grado di sopravvivere alla sorveglianza persistente, operare sotto guerra elettronica, modificare rapidamente il proprio dispositivo e mantenere la continuità del C2 in condizioni di degrado. La readiness deve quindi essere valutata anche attraverso la capacità di generare e mantenere effetti militari sotto osservazione e targeting avversari, includendo parametri relativi alla gestione della firma, alla dispersione, alla mobilità, alla resilienza delle comunicazioni e alla capacità di rigenerazione del combattimento. La protezione della forza non può più essere misurata soltanto dalla robustezza delle piattaforme, ma dalla capacità complessiva del sistema di forze di preservare la propria efficacia nel tempo.

Per le forze armate europee questo comporta infine una revisione delle priorità di force design e investimento. La superiorità tecnologica delle piattaforme rimane essenziale, ma deve essere accompagnata da disponibilità numerica, capacità di sostituzione, modularità, sistemi autonomi, sensori distribuiti, effettori a basso costo, resilienza delle reti e capacità industriale di rigenerazione. Una piattaforma estremamente sofisticata, costosa e difficilmente sostituibile, ma rapidamente individuabile e vulnerabile al targeting di precisione, può produrre un rapporto costo-effetto sfavorevole in un conflitto caratterizzato da sorveglianza persistente e attrizione prolungata. Il requisito emergente non è quindi semplicemente "*more capable*", ma "*more survivable, more distributed and more regenerable*".

La principale implicazione strategica è pertanto il superamento di una concezione lineare della Force Protection. La sopravvivenza non deve essere ricercata esclusivamente nella capacità di resistere all'attacco, ma nella capacità di impedire che l'avversario completi la catena sensor-to-shooter. Questo richiede di agire simultaneamente sulla produzione della firma, sulla sua acquisizione, sulla correlazione degli indicatori, sulla classificazione del bersaglio e sulla possibilità di trasformare l'informazione in effetto cinetico. La firma diventa così una dimensione della potenza militare al pari della mobilità, della massa e della potenza di fuoco.
Per la pianificazione militare occidentale, la lezione non è più quindi che "chi vede per primo vince", ma che il vantaggio operativo appartiene progressivamente a chi riesce a vedere, comprendere e ingaggiare l'avversario mantenendo contemporaneamente sotto controllo la propria osservabilità. Il campo di battaglia non è diventato trasparente né privo di incertezza; è diventato un ambiente nel quale la possibilità di sopravvivere dipende dalla capacità di gestire continuamente ciò che l'avversario può rilevare, correlare, interpretare e trasformare in targeting. La transizione più significativa è quindi dalla protezione della piattaforma alla protezione del sistema; dalla concentrazione della forza alla concentrazione degli effetti; dalla superiorità della singola piattaforma alla resilienza del force system; dall'occultamento statico alla signature management dinamica. È su questa capacità di controllare l'esposizione e preservare la libertà d'azione che dovrà essere misurata una parte crescente della superiorità terrestre nel prossimo ambiente operativo.

Note Bibliografiche

U.S. Army, FM 3-90, Tactics, May 2023.

NATO, AJP-3.14, *Allied Joint Doctrine for Force Protection.*

NATO *Army Armaments Group, Camouflage, Concealment and Deception, AC/225-N/194, 1984.*

Tollast, R., *"Drones and the War for the Transparent Battlefield", RUSI Defence Systems, 20 January 2026.*

"Emergent Approaches to Combined Arms Manoeuvre in Ukraine", RUSI, 2025.

Auchenbach, K., *"The Centrality of the Space Domain", in Insights for Future Conflicts from the Russia-Ukraine War, CSIS.*

Rantakokko, J., *Nygårds, J., Unmanned Systems for Ground Combat - Experience from Ukraine, FOI-R--5723--SE, 2025.*

Iorillo, P., *Simonetti, R.M., "Electromagnetic Operations in Ukraine", RUSI Journal, 6 October 2025.*

"The Russo-Ukraine War: Preliminary Observations for Land Warfare", The Journal of Slavic Military Studies, 2026, DOI 10.1080/13518046.2026.2666976.

Sługocki, W.Ł., *"War under exposure: battlefield filtering and the narrowing of military choice in Ukraine", Security and Defence Quarterly, 2026, DOI 10.35467/sdq/224572.*

U.S. Army, *"Like Moths to a False Flame: Lethality and Protection through Deception Operations", 2025.*

"Hard to Find, Hard to Kill: Foundational Protection in a Transparent Battlefield", Army Chemical Review, 2026.

The Future of Deception in War: Lessons from Ukraine, 2025.

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.