COMANDO PER LA FORMAZIONE, SPECIALIZZAZIONE E DOTTRINA DELL'ESERCITO

PSE 3.14
PROTEZIONE

2017

PAGINA INTENZIONALMENTE BIANCA

AVVERTENZE

La presente pubblicazione è stata approntata secondo quanto previsto dalla Circ. 1001 "Modalità per l'approntamento delle pubblicazioni dell'Esercito Italiano" Ed. 2016 e successive modificazioni e integrazioni.

La presente pubblicazione è diramata con la lettera in Annesso I.

PAGINA INTENZIONALMENTE BIANCA

PUNTI DI CONTATTO

Ente editore

COMFORDOT – SM Ufficio Dottrina
Caserma "Arpaia"
Viale dell'Esercito, 170 - 00143 ROMA

caufdot@comfordot.esercito.difesa.it
Telefono: 06 5023 6635
Sotrin: 1056635

casezdotcscss@comfordot.esercito.difesa.it
Telefono: 06 5023 6630
Sotrin: 1056630

Custode

Ten. Col. Antonio D'AGOSTINO
Email: antonio.dagostino3@esercito.difesa.it

Autori

Magg. Giovanni DE SANTIS
Email: giovanni.desantis1@esercito.difesa.it

Eventuali commenti, suggerimenti e proposte di modifica possono essere inviate direttamente agli indirizzi e-mail sopra riportati.

PAGINA INTENZIONALMENTE BIANCA

PREMESSA

Il rango della dottrina descritta in questa pubblicazione è il più elevato in ambito Forza Armata in materia di "Protezione". Conseguentemente, essa costituisce la *cornerstone* di riferimento per tutte le pubblicazioni di dottrina analitica[1] e d'impiego[2] di prossima elaborazione, oltreché la guida concettuale imprescindibile per i Comandanti, i *leader*[3], gli *staff*, i docenti e gli istruttori militari.

Nonostante la volontà comune, condivisa tra politici, militari e italiani, di condurre "Operazioni a perdite zero" (*Zero Casualty Operations*)[4], le minacce e i rischi ad esse connesse non possono essere azzerati. Il primo concetto essenziale, che deve fin da subito risultare chiaro al lettore, è che **qualsiasi Operazione comporta l'assunzione prudente[5] di rischi**. Non fanno eccezione neanche le

---

1 Pubblicazioni di Supporto dell'Esercito – PSE.

2 Pubblicazioni d'Impiego dell'Esercito – PIE.

3 Col termine *leader* si intendono coloro che guidano dei processi professionali o gruppi di persone, ma che non sono Comandanti (non ne posseggono l'Autorità e la Responsabilità). Esempi di *leader* sono i Capi Gruppi di Lavoro o anche i Capi Ufficio, Branca o Sezione.

4 Sono le operazioni militari che non prevedono la possibilità di perdita di vite umane. Va specificato che la non accettazione di perdite non si riferisce solo alle forze nazionali, amiche e ai civili, ma si estende anche alle eventuali forze ostili.

5 I rischi non possono essere azzerati, ma devono essere assunti senza mai prescindere dalla loro gestione, cercando di minimizzarli il più possibile. Il termine "prudente" indica proprio che, anche nella scelta ritenuta essenziale per l'assolvimento della missione, i Comandanti devono comunque considerare gestire i rischi e fare il possibile per ridurli.

Operazioni in tempo di pace e in territorio nazionale. I rischi vanno individuati, valutati e gestiti con fermezza e responsabilità. Questo è uno dei principi cardine del *Mission Command*. La Missione assegnata a un Comandante è la sua guida ed egli, supportato dallo *staff*, deve perseguirla con tutte le sue forze. L'assunzione prudente dei rischi è, forse, l'elemento che più di tutti evidenzia le virtù e l'arte militare che è patrimonio dei migliori Comandanti, soprattutto nel complesso ambiente operativo contemporaneo. Nessun Comandante, infatti, vorrebbe mettere a rischio la vita dei propri uomini. A volte però, assumere rischi, utilizzando un atteggiamento offensivo oppure ricercando lo sfruttamento di circostanze favorevoli, può produrre effetti di protezione più efficaci rispetto la difesa stessa. Per quanto detto, lo spirito d'iniziativa e la libertà decisionale dei Comandanti va supportata da tutti i livelli: soprattutto i sovra-ordinati e i non militari. Inoltre, in tale ottica, durante la condotta delle operazioni, la carenza o l'indisponibilità di equipaggiamenti o sistemi protettivi, non può rappresentare motivo ostativo o giustificativo per rinunciare alla manovra o peggio ancora, per assumere un atteggiamento passivo, remissivo o immobilista[6] che, spesso, rappresenta in operazione la più pericolosa delle minacce.

Per quanto finora detto, è evidente che **la dottrina non può fornire regole o ordini prefissati su come le forze devono o possono essere protette**. Disposizioni in tal senso provocherebbero l'effetto opposto a quello desiderato: la staticità e la rigidità dei Comandanti, delle forze e quindi delle operazioni, con conseguente aumento dei rischi e delle vulnerabilità.

Un ulteriore principio cardine da apprendere, è che **vi sono diversi modi per proteggersi**. La funzione Protezione, come detto, va considerata in qualsiasi Operazione e può essere pensata e realizzata in molteplici forme, non solo mediante la realizzazione di posizioni o difese passive.

Le principali innovazioni dottrinali introdotte dal documento sono:

- la descrizione del concetto di "Protezione" sia come elemento della Potenza di Combattimento[7] (*Combat Power*) sia come funzione operativa terrestre (*Combat Function*);
- il riconoscimento dell'*Intelligence* come la funzione indispensabile, abilitante, per poter pianificare qualsiasi sistema, azione o mitigazione per incrementare la protezione: senza la chiara definizione delle minacce, l'individuazione e la

---

[6] Cfr. SMD III REP - CID, PID/S1 *La Dottrina Militare Italiana*, Ed. 2011, pag. 46: "Una corretta applicazione del principio della sicurezza si ottiene mediante l'attuazione di una serie di misure finalizzate alla protezione delle unità e al contenimento degli effetti delle azioni dell'avversario, senza tuttavia rinunciare alla propria libertà d'azione. Il rispetto della sicurezza non deve tuttavia portare ad un'eccessiva cautela, poiché l'audacia rimane condizione necessaria per il successo di un'operazione militare".

[7] Definita anche come Capacità Operativa. Consiste nell'applicazione della Forza Militare (*Fighting Power*), esercitata attraverso l'uso della struttura delle funzioni operative (*functional framework*).

previsione di possibili azioni ostili, non si può preparare né metter in atto alcun tipo efficace protezione;

- il processo di "Gestione del Rischio Composito[8]" (*Composite Risk Management* - CRM), definito come il procedimento continuo necessario a integrare la funzione Protezione nel "Processo delle Operazioni"[9];
- i principi e il metodo per determinare le priorità in termini di Protezione.

L'innovazione dottrinale probabilmente più rilevante, soprattutto dal punto di vista pratico, è probabilmente l'introduzione di due strutture concettuali (*conceptual framework*) che, nel più breve tempo possibile, devono diventare patrimonio di tutto l'Esercito Italiano: gli "11 Compiti di Protezione" e le "5 Forme di Protezione".

Gli "11 Compiti della Protezione" sono:

- Difesa da Minaccia Aerea (*Air Defense*);
- Protezione CBRN (CBRN *Protection*);
- Protezione dai pericoli degli ordigni esplosivi (*Explosive Hazards Protection*);
- Sopravvivenza (*Survivability*);
- Sicurezza dell'Area delle Operazioni (*Operational Area Security*);
- Sicurezza delle Operazioni (*Operations Security*);
- Recupero del Personale (*Personnel Recovery*);
- Evitare il Fuoco Fratricida (*Fratricide Avoidance*);
- *Information Protection*[10];
- Protezione Sanitaria (*Health Protection*);
- *Safety*[11].

Le "5 Forme di Protezione" consistono in:

- Deterrenza;
- Prevenzione;
- Sicurezza attiva;
- Difesa passiva;
- Mitigazione.

Utilizzare gli strumenti appena proposti in maniera schematica, agevola grandemente l'attività dei Comandanti, dei *leader* e degli *staff* nel concepire e visualizzare le azioni e i comportamenti che, sulla base delle risorse disponibili,

---

8 Composito: eterogeneo, costituito da più elementi.

9 Con il termine "processo delle operazioni" si intende la struttura concettuale necessaria all'esercizio del *Mission Command*. Tale struttura è composta dalle seguenti attività continue: pianificare (*plan*), preparare (*prepare*), condurre (*execute*) e valutare (*assess*) le operazioni.

10 Si è deciso di mantenere il termine inglese, senza tradurlo, per evitare incomprensioni nel lettore.

11 *Ibidem*.

possono generare Protezione. Tali schemi evidenziano, inoltre, come la Protezione possa essere realizzata e applicata attraverso la combinazione e l'integrazione di capacità complementari o concorrenti, al fine di preservare la Potenza di Combattimento o per proteggere personale, assetti, infrastrutture o informazioni.

Dal punto di vista terminologico, vale la pena soffermarsi sulla scelta di utilizzare il termine "Protezione" per denominare la funzione operativa terrestre (*Combat Function*), rispetto quella del livello interforze nazionale[12] di "Protezione delle Forze" (*Joint Function*). Innanzitutto, va sottolineato che tale scelta è allineata alla più recente pubblicazione della NATO[13] e non mira a creare discrasie dottrinali ma, piuttosto, a contestualizzare tale funzione alle specificità delle forze terrestri rispetto quelle delle altre F.A.[14]. Inoltre, si è preferito il termine "Protezione" rispetto quello di "Protezione delle Forze", per dare un senso più ampio ai possibili effetti protettivi generati dalle attività terrestri. Nella sua accezione più ampia, infatti, il termine include non solo la difesa delle risorse e delle capacità militari (sia quelle tangibili sia quelle intangibili) cui la parola forza allude. Essa include, infatti, l'opzione che talune attività militari possano essere volte esclusivamente a proteggere altre tipologie di *target*, ad esempio personalità ad altro rischio (*High Risk Personnel* – HRP), grandi eventi, infrastrutture critiche[15], personale civile nazionale o anche straniero[16].

In conclusione, è essenziale che i Comandanti e i *leader* a tutti i livelli comprendano l'importanza di utilizzare i principi e gli strumenti concettuali contenuti nel documento. La dottrina è la guida intangibile e il riferimento cognitivo che, senza porre vincoli o restrizioni, deve ispirare tutto il "Processo delle Operazioni", al fine di

---

[12] Cfr. SMD III REP - CID, PID O/3.14 *La Protezione delle Forze*, Ed. 2012.

[13] Cfr. NATO, AJP 3.2 *Allied Joint Pubblication for Land Operations*, Ed. 2016.

[14] Tutte le F.A. considerano, ad esempio, la Protezione della manovra delle proprie forze (navali, aeree e terrestri). Tuttavia, le minacce connesse con tali manovre possono essere completamente diverse. Per una flotta, ad esempio, la priorità in termini di protezione potrebbe essere assegnata ai sommergibili nemici o le mine marine; per le formazioni aeree invece, la minaccia maggiore potrebbero essere i velivoli da caccia nemici o le difese controaerei nemici; per le forze terrestri gli ordigni esplosivi improvvisati o le imboscate. Considerando i rischi invece, si pensi agli effetti del fuoco a bordo di una nave, un aeroporto o un accampamento. È evidente che tali effetti sarebbero completamente diversi e gli addetti alla gestione del rischio gli assegnerebbero priorità molto differenti. Va da se che, essendo le minacce e i rischi che le F.A. fronteggiano diversi, anche in termini di effetti e percezione, diverse saranno le priorità assegnate, le attività e i compiti tipici connessi per minimizzare le vulnerabilità.

[15] Alla protezione delle infrastrutture critiche, quelle la cui neutralizzazione o distruzione potrebbe causare effetti particolarmente rilevanti sulla popolazione (ad esempio centrali nucleari o dighe di dimensioni rilevanti), è riservato un intero allegato del presente documento.

[16] La condotta di attività militari di tipo "specialistico" a favore di enti, infrastrutture o personale civile è trattata nelle seguenti PIE: *L'impiego del Genio*, *L'impiego dell'Artiglieria Controaerei* e *La Difesa CBRN Specialistica*.

identificare, prevenire o anche mitigare gli effetti delle minacce e dei rischi connessi con le Operazioni stesse. Lo scritto seguente costituisce, conseguentemente, l'ausilio cognitivo essenziale per identificare le attività, i compiti e le modalità più idonee per "proteggere" o "proteggersi", nell'assolvimento della missione ricevuta. La pubblicazione fornisce la filosofia e i principi, mantenendo un carattere generale, tale da consentire ai Comandanti ed agli operatori del settore di adattare i contenuti alla realtà contingente, con possibilità di integrarli o modificarli a seconda dei vincoli imposti dalla condizione operativa in atto.

Approvo la Pubblicazione di Supporto dell'Esercito PSE 3.14 *Protezione,* Edizione 2017.

Roma,

IL COMANDANTE PER LA FORMAZIONE,
SPECIALIZZAZIONE E DOTTRINA DELL'ESERCITO
Gen. C.A. Pietro SERINO

PAGINA INTENZIONALMENTE BIANCA

INDICE

INDICE DELLE FIGURE

INDICE DELLE TABELLE

PAGINA INTENZIONALMENTE BIANCA

1. LA PROTEZIONE

1.1 GENERALITÀ

In questo capitolo, il concetto di Protezione viene definito sia in termini di elemento della Potenza di Combattimento (*Combat Power*) che come Funzione Operativa Terrestre[17]. La Protezione va considerata in qualsiasi attività militare: nelle attività condotte in guarnigione e in quelle fuori area, nelle attività addestrative così come nella condotta di tutto lo spettro delle operazioni militari terrestri. Non c'è scelta! Sia in fase di generazione della forza che durante la definizione dei compiti essenziali per la missione (*Mission Essential Task List* – METL), i Comandanti devono essere consapevoli della presenza di rischi e minacce connessi con l'adempimento della missione ricevuta. Le valutazioni e le decisioni successive, inclusa la gestione e la connessa imprescindibile assunzione dei rischi, rientrano nella competenza precipua dei Comandanti e dei *leader* militari.

Per fornire un ausilio concettuale alla gestione di tale responsabilità, vengono introdotti in questo capitolo i concetti di:

- Forme di Protezione;
- Principi della Protezione;
- Gestione del Rischio Composito (*Composite Risk Management* - CRM).

Inoltre, il costrutto, le metodologie e i processi di seguito definiti, offrono un supporto determinante per la sincronizzazione delle attività militari rivolte a generare Protezione e alla loro integrazione nel Processo delle Operazioni.

1.2 DEFINIZIONE

La Protezione (Funzione Operativa Terrestre - *Combat Function*) consiste nell'insieme delle misure e dei mezzi per ridurre al minimo la vulnerabilità del personale, delle strutture, degli equipaggiamenti e delle operazioni rispetto a qualsiasi minaccia e in tutte le situazioni, al fine di preservare la libertà d'azione e l'efficienza operativa delle forze.[18]

---

[17] Già cit. NATO, AJP 3.2 *Allied Joint Pubblication for Land Operations*, Ed. 2016, rif. 0239: "We explain the functional framework (the combat functions) as: An analytical tool for commanders and staff that provides a complete description of everything that military organizations do prior to, during and after operations, as a list of functions".

Trad.: "Noi (N.d.T. l'Alleanza) definiamo la "struttura per funzioni" (le funzioni del combattimento – N. d. T. funzioni operative) come: Uno strumento analitico per i Comandanti e gli staff che fornisce una descrizione completa di tutto ciò che fanno le organizzazioni militari prima (N.d.T. pianificazione e preparazione), durante (N.d.T. condotta) e dopo (N.d.T. valutazione) le operazioni, consistenti in una lista di funzioni".

[18] Già cit. NATO, AJP 3.2 *Allied Joint Pubblication for Land Operations*, Ed. 2016, rif. 0258: "Protection is the function that traditionally considers Allied troops under threat – force protection. Force protection is defined as: all measures and means to minimize the vulnerability of personnel, facilities,

1.3 RUOLO DELLA PROTEZIONE

Le attività e le operazioni militari sono intrinsecamente pericolose. I Comandanti e i *leader* incaricati di guidare e condurre le operazioni devono affrontare rischi ogni giorno, gestendoli, sulla base della rilevanza della missione ricevuta, delle esigenze operative e delle opportunità che gli si presentano. Nel combattimento, questa realtà definisce il "sacro" rapporto di fiducia e rispetto che deve esistere tra *leader* e Soldati e che consiste nel bilanciamento delle esigenze di assolvere la missione e di proteggere la forza. È compito imprescindibile di qualsiasi Comandante proteggere in ogni modo lecito la propria unità ma questo dovere non deve mai generare l'avversione all'agire o la limitazione della libertà d'azione necessaria a mantenere l'iniziativa, il ritmo dell'azione o il raggiungimento dei risultati decisivi nel corso delle operazioni. I *leader* bilanciano queste responsabilità opposte e prendono decisioni rischiose, gestendo i rischi sulla base dell'esperienza, dell'etica e del ragionamento analitico, in considerazione della conoscenza dell'unità, della situazione, dell'intuizione e della propria arte militare. È attraverso la Protezione che i Comandanti e i *leader* preservano la Potenza di Combattimento, riducono il rischio di perdita, di danneggiamento e d'infortunio delle proprie unità o formazioni.

La Protezione è sia un elemento della Potenza di Combattimento sia una Funzione Operativa Terrestre.

È elemento del Potere di Combattimento perché, sulla base di quanta parte della Forza militare viene destinata a "Proteggere", il Potere di Combattimento viene plasmato di conseguenza. Ad esempio, assegnata una quantità definita di forza militare a un Comandante, tanta più parte ne viene destinata alla difesa dei fianchi, tanta meno potrà essere utilizzata per un attacco; e viceversa. La potenza di combattimento ha quindi un valore e potenziale (dipende ad esempio dalla forma di manovra, dalla organizzazione delle forze, dalle priorità e dalla

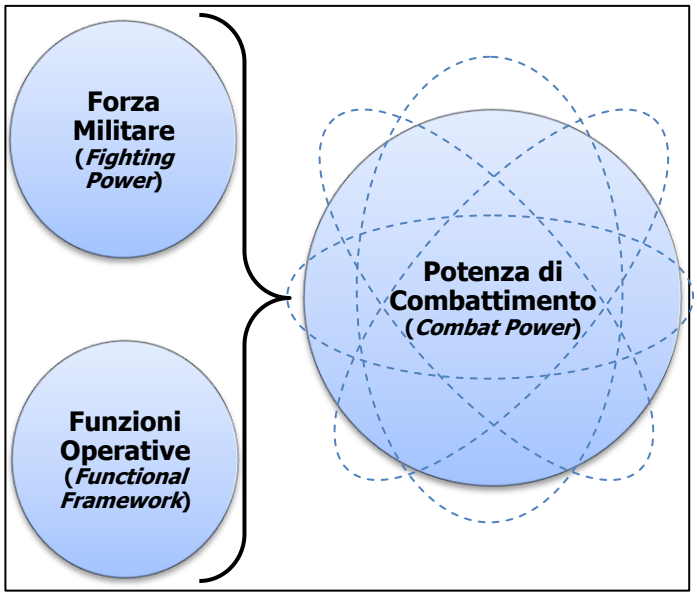


Figura 1: Potenza di Combattimento

equipment and operations to any threat and in all situations, to preserve freedom of action and the operational effectiveness of the force. It is essential for maintaining combat power and freedom of action. As well as protecting our own forces against attack and the environment, we have a moral and legal duty to protect non-combatants. Most obviously, we need to protect other agencies with whom we operate in the comprehensive approach".

gravitazione del fuoco) che viene definita attraverso l'utilizzo della struttura concettuale delle funzioni operative. Il concetto estremo di tale ragionamento è che, come funzione operativa, la protezione è una delle sette tipicamente necesssarie per condurre un'operazione militare, ma non rappresenta il motivo della missione. Come elemento della Potenza di Combattimento al contrario, può rappresentare il tutto, la ragion d'essere dell'operazione stessa, ad esempio la difesa di una infrastrattura critica o di un grande evento per la cui protezione viene dedicata l'intera Potenza di Combattimento del dispositivo militare terrestre.

Come funzione operativa terrestre, la Protezione si riferisce agli 11 Compiti di Protezione già elencati in premessa e che vengono illustrati in dettaglio nel successivo capitolo.

È facile confondere questi due costrutti. Tuttavia, a parte la terminologia e le nozioni prettamente dottrinali, ciò che deve restare chiaro nel lettore è il fatto che la Protezione richiede risorse e il loro uso ha effetto sulla capacità di combattimento dell'unità e, conseguentemente, sulle possibilità di assolvere o meno la missione.

I Comandanti e i *leader*, normalmente, pensano e danno disposizioni utilizzando le Funzioni Operative. Questo strumento consente di identificare e organizzare con maggiore semplicità gli specifici compiti dai quali le operazioni e le missioni saranno sviluppate. In tale contesto, la funzione Protezione consente di:

- focalizzare l'ampio spettro di attività militari e misure che generano protezione in specifici compiti che vanno integrati, semplificati e sincronizzati all'interno del Processo delle Operazioni;
- descrivere gli 11 Compiti che devono essere analizzati durante la fase di pianificazione, organizzati in preparazione, monitorati e valutati durante l'esecuzione, continuamente analizzati ed eventualmente corretti, allo scopo di proteggere dalle minacce e i rischi.

Tutte le attività militari includono, per loro stessa natura, capacità di protezione. Tali capacità possono essere combinate e utilizzate in maniera complementare o combinate tra loro. In particolare:

- **Capacità di protezione complementari**

  Le capacità e le attività complementari sono quelle che, nonostante appartengano ad altre funzioni operative, generano comunque effetti di protezione. Ad esempio, il fuoco erogato da un complesso tattico per fissare elementi di forze nemiche (funzione operativa terrestre Fuoco), genera contemporaneamente la protezione della manovra di altre forze amiche incaricate di colpire le stesse (funzione operativa terrestre Manovra).

- **Capacità di protezione combinate**

  Consistono nella combinazione e integrazione di sistemi o capacità simili appartenenti alla stessa funzione operativa ma che, conocorrendo, ne

determinano un aumento di efficacia complessiva. Si pensi ad esempio alla realizzazione di un campo minato a protezione di un caposaldo. La capacità difensiva della posizione subisce un incremento esponenziale della capacità di protezione.

La dottrina contenuta in questa pubblicazione mira ad ottenere effetti reali e fornire pratico ausilio alla F.A. A tal fine appare assolutamente necessario uscire dalla filosofia e fornire quanti più esempi pratici possibile.

L'applicazione del concetto di Protezione a un Convoglio, attività tattica abilitante, consiste principalmente nell'assegnare il compito a specifi Elementi/Forze di Sicurezza[19], all'utilizzo di assetti di Sorveglianza[20] e, eventualmente, anche ad assetti di *Route Clearance* del Genio[21].

La Protezione a una personalità ad alto rischio (HRP), militare o civile che sia, consiste normalmente nell'utilizzo di una "scorta" (*Close Protection Team* - CPT) costituita da un *team* addestrato e costituito *ad hoc* in funzione della specifica minaccia.

Le barriere fisiche, i fossati, i muri, le concertine e qualsiasi altra tipologia di ostacolo fisico, possono essere adoperati per rinforzare le capacità di protezione di una base o di un accantonamento, o anche per proteggere degli specifici corridoi o percorsi.

Le vaccinazioni, le profilassi e l'implementazione delle necessarie misure organizzative e procedurali atte a ridurre il rischio infortunistico, sono l'applicazione pratica del concetto di protezione ai Soldati. Esse mirano infatti a ridurre al minimo sostenibile le probabilità e i danni conseguenti a potenziali infortuni e malattie.

L'applicazione di segni identificativi o marchi su veicoli e sulle uniformi, l'uso di sistemi e procedure di riconoscimento, attive e passive, sono evidenti metodi per proteggere le forze dal rischio di Fuoco Fratricida.

La Protezione si realizza anche attraverso la ri-organizzazione/ri-articolazione delle forze sulla base delle Variabili della Missione (METT-TC[22]). Tali cambiamenti possono

---

[19] Sono incaricate dei seguenti compiti: Guardia (*Guard*), Schermo (*Screen*) e Copertura (*Cover*).

[20] Nelle operazioni contemporanee, a tale scopo vengono sempre più spesso utilizzati, per capacità ed efficacia, *Unmanned Air System* (UAS) e *Unmanned Groung System* (UGS) tattici.

[21] Tali assetti, benché potrebbero utilizzare gli stessi mezzi e procedure tipici delle Operazioni di Bonifica (*Clearing Operations*), non avrebbero il compito di bonificare itinerari ma, per specifici tratti, normalmente pianificati, supporterebbero la protezione del convoglio. In altri termini non sarebbero inseriti nell'Avanguardia del convoglio per tutto l'itinerario ma entrebbero in azione esclusivamente in corrispondenza di Aree Critiche pianificate (a elevato rischio di presenza IED) o su ordine del comandante del dispositivo.

[22] *Mission, Enemy, Terrain and weather, Troops and support available, Time available, Civil condiderations*. L'acronimo METT-TC serve a ricordare gli elementi/variabili della missione da considerare, iniziando ovviamente dalla missione. L'utilizzo del METT-TC, aiuta grandemente i *leader*, a tutti i livelli, a considerare l'ambiente in maniera schematica, inclusa l'individuazione delle minacce e dei rischi connessi.

avere lo scopo di rinforzare capacità già presenti ovvero quello di utilizzare alcune forze per produrre effetti diversi. Ad esempio possono essere utilizzati elementi *combat* prima operanti in funzione *Intelligence* o Manovra, in funzione Protezione: si riducono il numero delle pattuglie di ricognizione riassegnando dette forze a quelle di sicurezza.

Va peraltro notato che la tipologia stessa di movimento e manovra condotta dai complessi tattici, soprattutto in funzione del ritmo tenuto, dal controllo di punti, aree o itinerari chiavi e dall'imprevedibilità dei percorsi, consente di incrementare la protezione delle forze.

La funzione operativa che più di tutte è "complementare", spesso essenziale per una efficace Protezione, è l'*Intelligence*. L'utilizzo delle previsioni e dei prodotti d'*Intellingence* consente di trarre enorme profitto dall'uso del terreno, delle condimeteo e del buio per celare o proteggere la manovra, per anticipare le TTP ostili e per contrastarle, attivamente e passivamente. Alcune caratteristiche del terreno possono produrre maggiori effetti protettivi di altre e vanno considerate come elementi complementari per lo schieramento, anche temporaneo, delle forze.

Ancora, la dispersione delle forze, consente di incrementare gli effetti prodotti da strutture di protezione passive mentre, le azioni contro l'*Intelligence* ostile, possono essere fattore fondamentale per rinforzare le capacità difensive, in particolar modo per celare eventuali ammassamenti in presenza di posti comando.

Infine, va sottolineato il concetto che l'elemento fondamentale per generare Protezione è la conoscenza e la comprensione dell'Ambiente Operativo. Le valutazioni e le previsioni *Intelligence*, ad esempio quelle contenute nell'*Intelligence Summary* (INTSUM), rappresentano gli strumenti essenziali per fornire ai Soldati gli indicatori e gli avvisi (*Warning*) per proteggersi dalle specifiche minacce. Tale intelligenza permette di identificare e compiere specifiche azioni idonee a prevenire o ridurre la probabilità di successo e gli effetti delle tattiche offensive nemiche.

1.4 L'AMBIENTE OPERATIVO

L'ambiente operativo (AO)[23] è definibile come "l'insieme complesso delle condizioni, circostanze e influenze che hanno effetto sull'impiego delle capacità militari e sono rilevanti per le decisioni del Comandante"[24]. Il compito dei Comandanti e dei *leader* incaricati di fornire o garantire la Protezione delle proprie forze, deve iniziare dalla comprensione dell'AO, delle minacce, dei rischi e delle opportunità che in esso risiedono, delle vie e dei modi disponibili per preservare il potere di combattimento attraverso la funzione operativa in argomento.

---

[23] *Operational Environment* – OE.

[24] Cfr. NATO, AAP-6 *NATO Glossary of Terms and Definitions*, Ed. 2013: "A composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander".

La dottrina militare definisce otto sistemi costituenti il sistema AO (*Political, Military, Economic, Social, Information, Infrastructure, Physical Environment and Time* – PMESII-PT) che possono forniscono la base concettuale per analisi e valutazioni a livello strategico e operativo. Tali sistemi possono essere ulteriormente definiti a livello tattico. L' *Intelligence Preparation of the Operational Environment* (IPOE[25]), rappresenta lo strumento fondamentale, per le unità terrestri dotate di staff (da Corpo d'Armata a Gruppo Tattico), per supportare il Comandante e il Processo delle Operazioni nella comprensione dell'AoO.

I *leader* utilizzano i fattori del METT-TC per esaminare l'AO, in particolare gli effetti che questo produce sulla propria Missione, identificando Minacce e Rischi.

1.5 MINACCE E RISCHI

La funzione operativa Protezione preserva il potere di combattimento potenziale e la capacità di sopravvivenza delle forze attraverso la protezione dalle minacce e dai rischi. E necessario allora definire entrambi i termini.

1.5.1 Minacce

Con il termine minaccia s'intende una o più persone, gruppi, nazioni, condizioni o fenomeni naturali capaci di danneggiare o distruggere vite, risorse o istituzioni. I Comandanti focalizzano la propria attenzione sulle minacce alle operazioni militari che sono generalmente rappresentate da attività ostili o informazioni coercitive, deliberatamente condotte o messe in atto da forze nemiche. Dette minacce, in funzione della tipologia e degli scopi che questa pubblicazione si prefigge, possono essere categorizzati nelle seguenti quattro tipologie:

- irregolari;
- catastrofiche;
- tradizionali;
- perturbatrici.

Tale categorizzazione può essere utilizzata per identificare e analizzare le minacce, supportare lo sviluppo di piani, operazioni e ordini. Sia le minacce sia i rischi possono ridurre il potere di combattimento e l'efficienza operazionale della forza. Per tale ragione, la loro valutazione e mitigazione è condotta attraverso il processo di CRM e applicata a tutto il Processo delle Operazioni. I Comandanti individuano e sviluppano misure di riduzione dei rischi e strategie di controllo e mitigazione per tutte le fasi delle Operazioni e attività.

1.5.2 Rischi

Il rischio è una condizione che, potenzialmente, può causare:

- l'infortunio o la malattia del personale con la conseguente riduzione del potere di combattimento e dell'efficienza operazionale;

[25] Coincide con l' *Intelligence Preparation of the Battlespace* (IPB).

- la morte del personale;
- il danneggiamento o la perdita di equipaggiamento, veicoli, materiali o altre proprietà;
- il degradamento della missione.

I rischi sono normalmente prevedibili e preventivabili. Essi devono essere individuati quindi, stimati attraverso una corretta valutazione e, di conseguenza, gestiti.

I Comandanti, individuati i pericoli[26] e valutati i rischi[27], sviluppano strategie di protezione e priorità d'intervento, sincronizzando le attività e allocando le risorse disponibili nello spazio e nel tempo.

1.6 LA POTENZA DI COMBATTIMENTO

Come detto, la Potenza di Combattimento consiste nell'applicazione/utilizzo della Forza Militare attraverso le Funzioni Operative. Tradizionalmente, la Potenza di Combattimento veniva definita come il "Complesso delle capacità distruttive o di neutralizzazione che un'unità è in grado di utilizzare contro l'avversario in un determinato momento"[28]. Tuttavia oggi, la moderna concezione delle Operazioni Militari Terrestri, coinvolge un'ampissima gamma di situazioni e opzioni d'impiego. Le forze militari assolvono compiti che possono determinare effetti assolutamente diversi dalla distruzione o neutralizzazione. Peraltro, non è neppure detto che esista un nemico in senso stretto. Pertanto, il *Combat Power* va rivisto come una misurata capacità della forza che può essere applicata a diversi tipi di missione e che necessita una continua generazione, anche per un ampio lasso di tempo. Il *Combat Power* quindi, non è soltanto il complesso delle capacità distruttive o di neutralizzazioni, ma include anche capacità costruttive e informative che un'unità, o una formazione militare, può applicare in un determinato spazio e tempo[29].

La combinazione delle Armi (*Combined Arms*) consiste nell'applicazione sincronizzata e simultanea delle Armi per raggiungere un effetto maggiore rispetto a quello raggiungibile dalle stesse separatamente e in maniera sequenziale.

La Potenza di Combattimento non può essere esattamente quantificata e la ricerca della sua misurazione porta, inevitabilmente, a valutazioni e analisi generiche. Ciò che invece può essere misurata è l'efficacia (*Measure of Effectiveness* – MoE) e il rendimento (*Measure of Performance* – MoP) delle azioni e delle attività militari. I

---

[26] Proprietà o qualità intrinseche di un determinato fattore avente il potenziale di causare danni (ad esempio il pericolo di esplosione delle sostanze esplosive o pericolose).

[27] Probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione.

[28] Cfr. SME – RIF, Pub. n. 5895 *Nomenclatore Militare (ESERCITO)*, Ed. 1998.

[29] Cfr. già cit. NATO, AJP 3.2. *Allied Joint Pubblication for Land Operations*, Ed. 2015.

leader interpretano tali misurazioni e usano tali deduzioni per guidare le operazioni e portare a termine la missione ricevuta.

Come elemento del *Combat Power*, la Protezione rappresenta un potenziale. Essa ha una qualità latente che dipende dalla *leadership*, dalla qualità e quantità delle risorse assegnate, dalle priorità e dai vincoli imposti dalla missione. Come valore potenziale può essere massimizzato attraverso la coordinazione e l'integrazione degli altri elementi della Potenza di Combattimento (ad esempio il Fuoco e le Attività Informative). Elemento essenziale, che permea qualsiasi operazione del livello tattico, nell'ambito di tutto il Processo delle Operazioni, è il bilanciamento e l'integrazione tra Protezione e la libertà d'azione. Gli effetti più evidenti sono esprimibili esclusivamente attraverso l'individuazione e l'integrazione delle predette capacità di protezione complementari e di concorrenti.

1.7 LE 5 FORME DI PROTEZIONE

La Protezione può assumere diverse forme. Allo scopo di organizzare gli elementi e le capacità che forniscono Protezione, sono state definite 5 forme di protezione. Questo schema serve a supportare i Comandanti, i *leader* e gli *staff* a individuare le attività e le capacità connesse. Esse non sono consequenziali e, alcune attività militari, possono supportare, allo stesso tempo, più di una forma di protezione, proprio come assolvono più di una funzione operativa. Indistintamente dalla manovra, le forme di protezione si orientano in base al terreno, gli assetti protetti e il nemico.

Figura 2: Le 5 Forme di Protezione

1.7.1 Deterrenza

La Deterrenza è il potere di dissuadere qualcuno dal compiere un'azione dannosa per timore di una punizione, una reazione o una rappresaglia. Esempi di deterrenza possono essere la postura dei singoli soldati e delle formazioni di combattimento. La presenza stessa di truppe ben equipaggiate, addestrate e disciplinate, può essere a volte sufficiente per evitare conflitti, scontri o atti ostili determinando così il successo stesso delle operazioni. Veicoli ben armati e strutture fortificate e soprattutto reattive, possono anch'esse disincentivare azioni ostili. Inoltre, va considerato che la

condotta di prove di allarme o altre attività, attivate anche randomicamente, producono l'effetto di scoraggiare l'*insider 9lusi* e gli atti terroristici.

1.7.2 Prevenzione

Prevenire significa agire per evitare o ridurre i rischi di accadimento di fatti dannosi. Conseguentemente, la prevenzione include l'abilità di neutralizzare, precludere o ridurre un possibile rischio o un imminente attacco, di qualsiasi forma esso sia, prima che questo avvenga. Può essere condotta attraverso una serie di attività programmate o come effetto di specifiche azioni. Il *Situational Awareness* è uno degli elementi fondamentali per ridurre, prevenendolo, un attacco o un incidente. La Prevenzione non è tuttavia, come si potrebbe immaginare, riconducibile esclusivamente ad azioni offenzive, ma, una funzione dei pericoli, anche attraverso altri tipi di misure quali ad esempio la medicina preventiva, l'*engagement*, il CIMIC o il *Public Affairs*.

1.7.3 Sicurezza Attiva

Consiste in azioni dinamiche condotte allo scopo di individuare, interdire, disarticolare, neutralizzare e distruggere minacce o pericoli, mantenendo al contempo la capacità di agire e manovrare, generando protezione a favore dell'Operazione stessa o della forze in generale. Il fuoco, il pattugliamento attivo, la sicurezza degli itinerari e delle aree circostanti le basi o le infrastrutture critiche, rappresentano ulteriori esempi di difesa attiva. I sistemi d'arma controaerei, sono assetti tipici della sicurezza attiva.

1.7.4 Difesa Passiva

La protezione può essere raggiunta anche attraverso la realizzazione di posizioni difensive, fortificazioni e altre forme di barriere fisiche, pensate e posizionate al fine specifico di proteggere da definite minacce o pericoli. Alcuni gradi di protezione possono essere raggiungibili anche dalla selezione di appropriate aree d'insedimento o assembramento. La valutazione del terreno e lo sfruttamento degli ostacoli naturali sono elementi essenziali per rinforzare le capacità di Protezione. Le basi, i posti comando, i posti rifornimento e le aree logistiche avanzate in generale, sono tutte posizionate dopo l'attenta valutazione delle caratteristiche morfologiche del terreno. Inoltre, la presenza di pericoli e minacce, inclusa la presenza di sostanze o siti esplosivi, inquinabili o anche di acqua, può influenzare in maniera consistente la vulnerabilità delle forze. L'inganno, il mascheramento, l'occultamento e l'oscuramento in tutte le sue forme, contribuiscono grandemente all'incremento della protezione passiva.

1.7.5 Mitigazione

Mitigare significa rendere più mite, cioè meno aspro, meno gravoso o, meno intenso, l'effetto determinato dal verificarsi di un evento dannoso.

Ai fini della Protezione, la mitigazione consiste, principalmente, nelle seguenti attività e capacità:

- Disporre della capacità di minimizzare gli effetti;
- Gestire le conseguenze e le emergenze di attacchi o incidenti che coinvolgono personale, assetti e informazioni;
- Mantenere elevato il potenziale, la capacità e l'efficienza della forza o delle capacità;
- Generare una protezione qualitativamente efficace.

1.8 I PRINCIPI DELLA PROTEZIONE

I seguenti rappresentano i principi fondamentali della Protezione:

1.8.1 Multidimensionalità

Gli sforzi profusi per generare Protezione, tengono conto e valutano i rischi e le minacce provenienti, in qualsiasi momento, da tutte le direzioni e su tutti gli ambienti/domini. Ogni qualvolta un Soldato riceve una missione o gli interessi nazionali lo richiedono, dalla Caserma in Patria sino all'Area delle Operazioni più remota, la funzione Protezione viene attivata e tenuta sempre in massima considerazione. Il *Situational Awareness* è nuovamente essenziale per supportare tale principio ed è la base essenziale per "aggiustare" continuamente e prontamente la Protezione. La Protezione si estrinseca nell'utilizzo sinergico di strutture concettuali, processi, sistemi, capacità, compiti e attività complementari tra loro e disponili da parte dei Comandanti.

1.8.2 Integrazione

La Protezione va sempre pensata e organizzata in integrazione con le altre funzione operative, terrestri[30] e interforze[31], al fine di ricercare e generare la maggiore Potenza Militare possibile. La Protezione è quindi complementare alle altre funzioni operative terrestri. Conseguentemente, essa non inibisce le altre e, in particolare, non ostacola la capacità né la volontà di combattere e di manovrare e non mette quindi a rischio l'assolvimento della missione. Gli strumenti più utili a mettere in pratica il principio dell'Integrazione sono il *Combined Arms*, il *Mission Command* e il largo ricorso a gruppi di lavoro multifunzionali (ad esempio quelli di INFO OPS, C-IED o *Targeting*).

[30] Le Funzioni operative terrestri (*combat function*) sono: Comando, *Intelligence*, Manovra, Fuoco, Attività Informative e Sostegno Logistico (*Command, Intelligence, Manoeuvre, Fires, Information Activities and Sustainment*).

[31] Le Funzioni operative interforze (*joint function*) sono: Comando e Controllo, *Intelligence*, Manovra e Fuoco, Attività Informative, Sostegno Logistico e CIMIC (*Command and Control, Intelligence, Manoeuvre and Fires, Information Activities, Sustainment and* CIMIC).

1.8.3 Stratificazione

Le capacità di Protezione sono pensate e organizzate utilizzando un approccio a strati, idoneo a realizzare forza e profondità al sistema di protezione in generale. La stratificazione del concetto, consente anche di ridurre gli effetti distruttivi delle minacce e dei pericoli attraverso la dissipazione dell'energia o il raggiungimento del culmine operativo da parte delle forze ostili e può fornire quel tempo in più necessario a consentire l'identificazione, la valutazione, l'acquisizione degli *target* o comunque risposte o reazioni più efficaci. La costituzione di aree interdette, la posa di ostacoli, l'uso di parole d'ordine o di tesserini di riconoscimento (*security badge*), sono esempi di TTP e risorse per la Protezione.

1.8.4 Ridondanza

La ridondanza assicura che specifiche attività, sistemi, sforzi e capacità critiche per il successo della protezione nel suo complesso abbiano alternativa/opzione/possibilità secondaria o ausiliaria, di valore pari o superiore. La ridondanza delle capacità non consiste tuttavia nella mera duplicazione: essa consiste nella sovrapposizione delle capacità cosicché non ci siano punti di cucitura e vulnerabilità tra di esse. Chiaramente, la ridondanza va ricercata ma non può essere implementata in tutte le misure di protezione. È necessario individuare tali debolezze e possibili punti critici della funzione che possono determinare il fallimento del sistema e, al limite, della missione. Normalmente la ridondanza viene maggiormente ricercata in corrispondenza di capacità di protezione connesse con la minaccia e i pericoli più probabili o attesi. La generazione di energia elettrica e la produzione d'acqua potabile, sono normalmente capacità che necessitano di sistemi di produzione ridondanti.

1.8.5 Durevolezza

La durevolezza[32], è una proprietà tipica della Protezione che, tra le altre cose, la distingue dalla difesa e dalle operazioni di sicurezza in genere. Mentre un complesso tattico difende fino al momento in cui esso non riesce a riprendere l'offensiva e una formazione fornisce sicurezza per mantenere la libertà d'azione, la Protezione ha un carattere persistente che serve uno scopo comunque dominante: la preservazione dell'assetto, forza o capacità protetto. Il carattere di durevolezza può influenzare la libertà d'azione e la fornitura di risorse.

1.9 LE FUNZIONI OPERATIVE TERRESTRI

La Protezione è una delle sette Funzioni Operative Terrestri. La struttura delle Funzione Operative (*Functional Framework*), secondo la più recente definizione, è "uno strumento analitico per i Comandanti e gli *staff* che fornisce una descrizione

[32] La proprietà di durare nel tempo senza deteriorarsi.

completa di tutto ciò che fanno le organizzazioni militari prima, durante e dopo le operazioni. Consistono in una lista di funzioni"[33].

I Comandanti e i *leader* comprendono, visualizzano, descrivono e dirigono in termini di Funzioni Operative, poiché esse rappresentano compiti tangibili che vengono trasformati in piani, ordini e missioni.

1.10 LA FUNZIONE OPERATIVA TERRESTRE PROTEZIONE

La Funzione Operativa Terrestre Protezione consiste nei compiti e sistemi (personale, materiali, organizzazioni, informazioni e processi) che preservano le Forze. Preservare le Forze include la protezione di:

- personale (combattente e non combattente);
- assetti;
- informazioni.

Tali elementi non sono esclusivamente nazionali ma, in base al mandato, anche appartenenti a *Partner* internazionali.

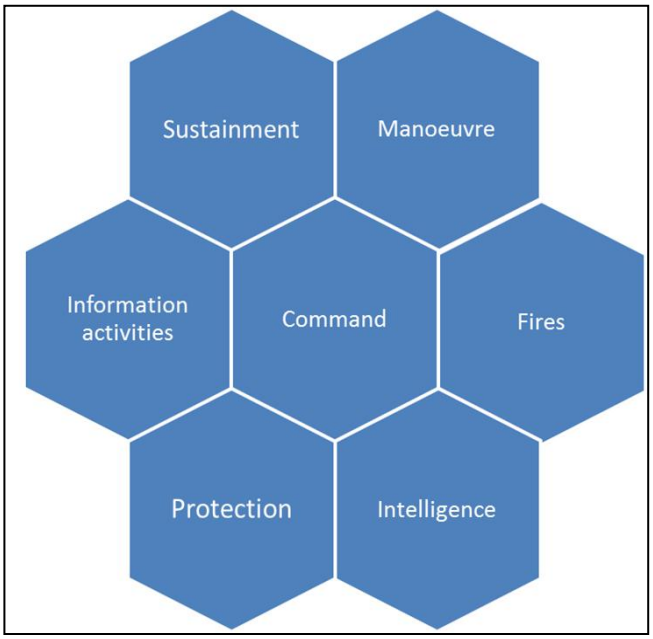


Figura 3: *Combat Function*

Mentre come elemento della Potenza di Combattimento, come visto, la Protezione ha un valore potenziale, come Funzione Operativa serve per indirizzare gli sforzi negli undici Compiti o Sistemi di Protezione:

- Difesa da Minaccia Aerea (*Air Defense*);
- Protezione CBRN (CBRN *Protection*);
- Protezione dai pericoli di esplosione (*Explosive Hazards Protection*);
- Sopravvivenza (*Survivability*);
- Sicurezza dell'Area delle Operazioni (*Operational Area Security*);
- Sicurezza delle Operazioni (*Operations Security*);
- Recupero del Personale (*Personnel Recovery*);
- Evitare il Fuoco Fratricida (*Fratricide Avoidance*);
- *Information Protection*;
- Protezione Sanitaria (*Health Protections*);

[33] Cfr. già cit. NATO, AJP 3.2 *Allied Joint Doctrine for Land Operations*, Ed. 2015: *"Functional Framework: An analytical tool for commanders and staff that provides a complete description of everything that military organizations do prior to, during and after operations, as a list of functions".*

- *Safety*.

Come minimo, i Comandanti e i *leader* di qualsiasi livello e grado, considerando a modo di lista di controllo le undici alinee precedenti, dispongono di uno strumento pratico per pensare in ordine e considerare i compiti o sistemi fondamentali per generare Protezione.

1.11 LA GESTIONE DEL RISCHIO COMPOSITO (*COMPOSITE RISK MANAGEMENT* – CRM)

I Comandanti e i *leader* dell'Esercito Italiano gestiscono i rischi sulla base della valutazione delle informazioni disponibili, delle valutazioni e predizioni ricevute, del proprio giudizio e intuito. Il rischio è funzione della probabilità che un evento possa accadere e della severità dell'evento stesso, espresso in termini di grado d'impatto dell'incidente sulla Potenza di Combattimento o sulla capacità residua di assolvere la missione. Il CRM è pertanto un processo fondamentale che permea tutto il Processo delle Operazioni e, in particolare, il Processo Decisionale e di Pianificazione Militare. Va da se che i Comandanti che non dispongono di Staff dovranno usarlo come strumento concettuale per ragionare sul come proteggere e poi decidere. I comandanti supportati da uno staff invece, sono agevolati nelle valutazioni e, qualora la situazione lo consenta, devono fare ampio uso dello strumento qui proposto, in particolare, per quanto concerne la protezione delle basi in operazioni[34]. Esso è essenziale per ragionare e identificare i pericoli e controllare costantemente il livello di rischio attraverso tutta la gamma delle missioni, funzioni, operazioni e attività. Consiste in un processo di "cinque passi" come di seguito schematizzato.

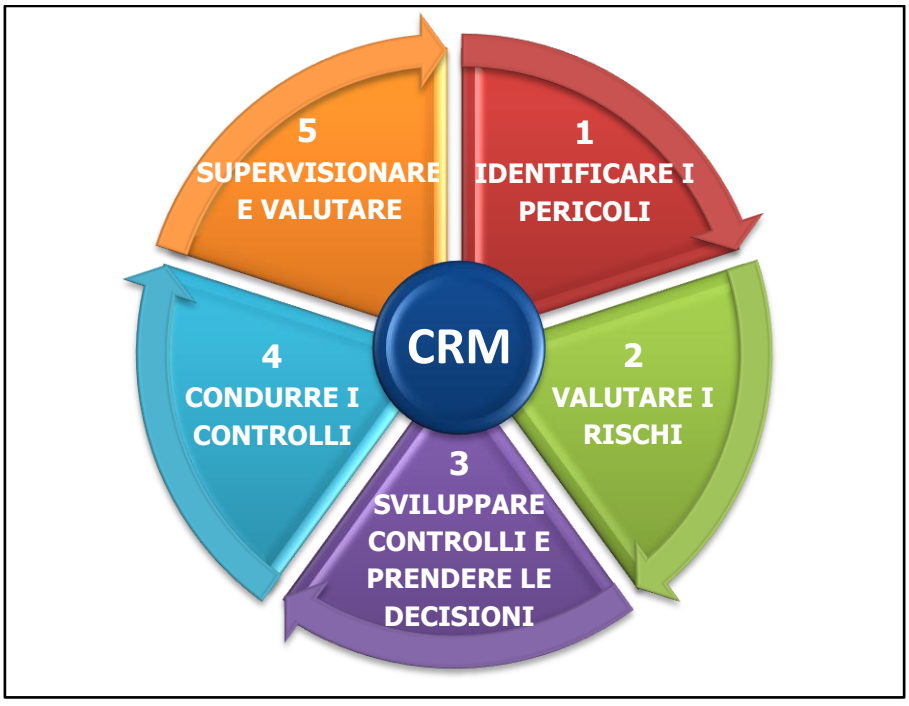


Figura 4: Il Processo di Gestione del Rischio Composito (CRM)

[34] Cfr. COMFORDOT, PSE-3.14.05.02 *La Protezione delle Basi Militari in Operazioni*, Ed. 2017.

Il processo agevola, tra l'altro, la quantificazione, soggettiva, della probabilità e della severità del Rischio attraverso l'uso della seguente matrice, utile a determinare il livello del rischio stesso. Detto livello è fondamentale per informare e allertare i *leader* in sede di scelta o cambiamento della *Course of Action* (COA) e per l'allocazione delle risorse. Il CRM è assolutamente rilevante anche per decidere quando e dove applicare le capacità di protezione.

		PROBABILITÀ DI ACCADIMENTO				
SEVERITÀ		Frequente	Probabile	Occasionale	Raro	Improbabile
	Catastrofico					
	Critico					
	Marginale					
	Trascurabile					

Tabella 1: Probabilità e severità del Rischio

È fondamentale infine comprendere che, come anticipato, il CRM non è un passo né uno strumento del Processo Decisionale. È un processo cognitivo continuo che permea tutto il Processo Decisionale, integrandosi con gli elementi di pianificazione e condotta delle operazioni. È trasversale, parimenti agli altri due processi fondamentali di *Intelligence Preparation of the Battlespace* (IPB) e *Targeting*. Questi devono imprimersi nella mente dei Comandanti e dei *leader*, divenire una *routine* mentale per coloro che decidono e gli *staff* che ne supportano la funzione, prescindendo dalla presenza di personale esperto o di cellule dedicate.

La tabella seguente illustra come il CRM si integra nel Processo Decisionale Militare Tattico (PDMT), in uso dalle unità terrestri dotate di staff (da C.A. a Gruppo Tattico).

In conclusione, il processo di CRM fornisce una struttura logico-deduttiva generale, idonea a individuare, valutare e gestire i rischi a tutti i livelli che, normalmente, viene supportata e si integra con altri strumenti e processi di valutazione ed esecuzione.

		Passi del Processo di Gestione del Rischio Composito (CRM)				
		Identificare i pericoli	Valutare i rischi	Sviluppare controlli e prendere decisioni	Condurre i controlli	Supervisionare e valutare
Processo Decisionale Militare Tattico **(PDMT)**	1. Ricezione della Missione	X				
	2. Analisi della Missione	X	X			
	3. Sviluppo COA	X	X	X		
	4. Analisi COA	X	X	X		
	5. Confronto COA			X		
	6. Approvazione della COA			X		
	7. Emanazione Ordine				X	
Prova		X	X	X	X	X
Condotta		X	X	X	X	X
Valutazione		X	X		X	X

Tabella 2: Integrazione CRM e PDMT

PAGINA INTENZIONALMENTE BIANCA

2. LA FUNZIONE OPERATIVA TERRESTRE PROTEZIONE

Le operazioni si basano sulla condotta di un numero variabile di compiti tattici. La funzione operativa "Protezione", in particolare, mira a focalizzare l'assegnazione di determinati compiti, anche all'apparenza molto differenti tra loro, a un effetto specifico: proteggere. Questo capitolo illustra, nel dettaglio, i Compiti o Sistemi tipici della funzione operativa terrestre Protezione.

2.1 COMPITI/SISTEMI DELLA PROTEZIONE

Le Operazioni militari sono complesse per loro stessa natura. I Comandanti devono costantemente pianificare e integrare l'applicazione della Forza Militare contro un nemico ma, allo stesso tempo, devono anche proteggere le proprie unità, preservando la Potenza di Combattimento. Per portare a termine la missione assegnata, è essenziale che Comandanti e leader utilizzino un approccio basato sulla ricerca della riuscita della missione, quindi sulle capacità disponibili. Attraverso l'uso dello strumento concettuale funzioni operative, vengono assegnati i compiti alle unità o elementi dipendenti. Così si determina il Potere di Combattimento. I Comandanti possono quindi sviluppare strategie di protezione per ciascuna fase delle operazioni che guidano. Essi integrano e sincronizzano i compiti al fine di ridurre i rischi, mitigare le vulnerabilità e sfruttare le opportunità che dovessero eventualmente presentarsi. È attraverso tale approccio che la funzione operativa "Protezione" può efficacemente proteggere la forza, preservare la Potenza di Combattimento e incrementare la probabilità di successo della missione.

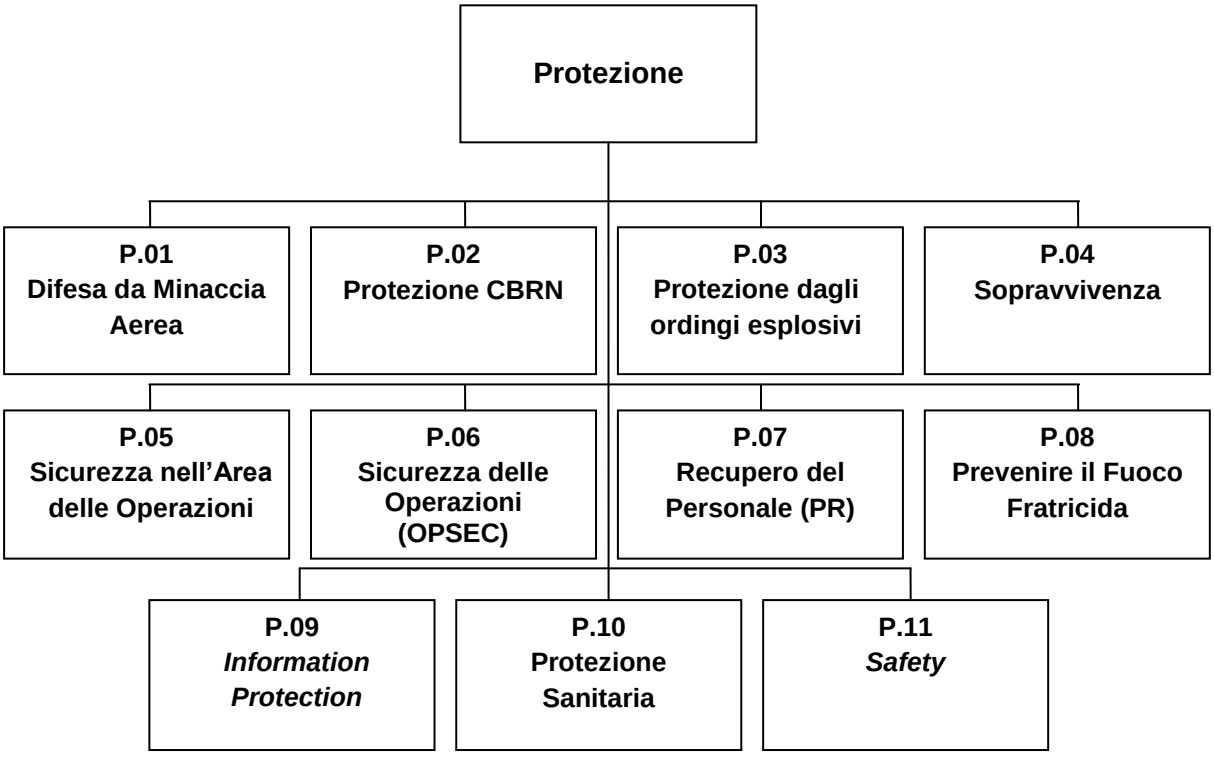


Figura 5: Gli 11 Compiti della Protezione

2.2 DIFESA DA MINACCIA AEREA (*AIR DEFENSE* - AD)

2.2.1 La Minaccia Aerea

Col termine Minaccia Aerea s'intende la possibilità che una forza ostile effettui azioni dannose contro il personale (incluso quello alleato, amico o civile), le vulnerabilità critiche della forza o della manovra, aree, basi o le infrastrutture critiche, utilizzando per tale fine le diverse tipologie di vettore operanti nella Terza Dimensione. In generale, i vettori attraverso i quali può essere perpetrata tale minaccia sono classificabili come segue:

- piattaforme pilotate, ad esempio, aerei ed Elicotteri da Esplorazione e Scorta (EES) e da trasporto;
- sistemi a pilotaggio programmato (*Drone*) e Sistemi Aeromobili a Pilotaggio Remoto (SAPR)[35];
- missili balistici a traiettoria prefissata (Tactical Ballistic Missile – TBM) a corta o media gittata[36], a portata intermedia[37] e intercontinentali[38], missili antiradiazione (*Anti Radiation Missile* – ARM), munizionamento stand-off[39] aria-superficie (*Air-to-Ground Missile* – AGM), guidato da vari tipi di sensori[40], e missili da crociera (*Cruise*);
- munizionamento autopropulso non guidato (razzi aria-superficie e superficie-superficie di grosso calibro a guida inerziale), non autopropulso guidato (bombe plananti e non, sganciate da aereo, proietti di artiglieria e bombe di mortaio) e non guidato (bombe a caduta libera sganciate da aereo, proietti di artiglieria e bombe di mortaio);
- sistemi tradizionali del tipo *Long Endurance Multi-intelligence Vehicles* (LEMV)[41] e *balloons*;

---

[35] I mezzi aerei pilotati da equipaggi operanti in stazioni remote di Comando e Controllo sono noti nei diversi contesti, civili o militari, come *Unmanned Aerial Vehicle* (UAV) o *Tactical Aerial System* (T-UAV) e *Unmanned Aerial System* (UAS), ma anche *Unpiloted Aerial Vehicle/Unpiloted Aerial Vehicle System* (UAVS), oppure, come in ambito europeo, *Remotely Piloted Aircraft System* (RPAS).

[36] *Theatre Ballistic Missiles* (TBM), missili balistici di teatro di gittata compresa fra 300-3500 km; comprendono missili balistici a corto raggio (*Short-range Ballistic Missiles* - SRBM) con gittata fino a 1000 km. e missili balistici a medio raggio (*Medium-range Ballistic Missiles* - MRBM) con gittata compresa tra 1000-3500 km.

[37] *Intermediate-Range Ballistic Missiles* (IRBM) con gittata compresa fra 3000-3500 km.

[38] *Intercontinental Ballistic Missiles* (ICBM) con gittata fino a 5500 km.

[39] Il velivolo lancia l'armamento offensivo rimanendo fuori dalla portata massima delle difese controaerei.

[40] Ad esempio, televisivo (*TV-guided Missile* - TVGM), a guida infrarossa (*Infra-Red Missile* - IRGM) o a puntamento *laser* (*Laser Guidance*).

[41] Termine col quale vengono denominati gli *Hybrid Air Vehicle* (HAV).

- non ultimo, sistemi improvvisati, ad esempio i deltaplani, gli ultra-leggeri o gli *Small Unmanned Aerial Vehicles (mini/micro*-UAV*)*.

2.2.2 Compiti essenziali

Un efficace sistema di Difesa da Minaccia Aerea include la protezione dai possibili attacchi condotti attraverso l'uso dei vettori precedentemente descritti e garantisce un'efficace sorveglianza dello spazio. Nel sistema rientrano tutti gli elementi della forza che devono essere preparati a contribuire a incrementare le capacità di difesa attraverso l'osservazione, la trasmissione degli allarmi e l'impiego del fuoco diretto.

P.01 Difesa da Minaccia Aerea (*Air Defense*)
P.01.01 Processare le piattaforme aeere tattiche
P.01.01.01 Cercare piattaforme aereo tattiche
P.01.01.02 Rilevare le piattaforme aereo tattiche
P.01.01.03 Localizzare le piattaforme aereo tattiche
P.01.01.04 Identificare le piattaforme aereo tattiche
P.01.01.05 Localizzare le piattaforme aereo tattiche
P.01.02 Distruggere piattaforme aereo tattiche
P.01.02.01 Cercare piattaforme aereo tattiche
P.01.02.02 Rilevare le piattaforme aereo tattiche
P.01.02.03 Localizzare le piattaforme aereo tattiche
P.01.02.04 Identificare le piattaforme aereo tattiche
P.01.03 Negare lo spazio aeree alle forze ostili
P.01.04 Reagire all'attacco aereo nemico
P.01.05 Pianificare difesa da attacco missilistico
P.01.06 Condurre difesa da attacco missilistico
P.01.07 Gestire la configurazione del sistema
P.01.08 Pianificare la difesa da razzi, obici e mortai
P.01.09 Condurre la difesa da razzi, obici e mortai

Tabella 3: Compiti Essenziali della Difesa da Minaccia Aerea

2.2.3 Forme di Protezione

2.2.3.1 Deterrenza

Le azioni di deterrenza contro la Minaccia Aerea consistono, principalmente, in tutta la gamma di *Information Activities* idonee a scoraggiare eventuali volontà ostili a usare qualsiasi piattaforma area come strumento di offesa contro la forza, le infrastrutture o il personale civile da proteggere. Tra le varie azioni di deterrenza, particolare menzione merita lo schieramento di sistemi d'arma controaerei (*show the force*) che hanno un elevatissimo potere dissuasivo per la minaccia in trattazione. Inoltre, tanto più i sistemi d'arma sono moderni, credibili e "visibili", tanto più l'effetto di deterrenza risulterà efficace.

2.2.3.2 Prevenzione

L'elemento essenziale per prevenire la minaccia in argomento è la capacità di sorvegliare lo spazio dell'AoO. Un efficace sistema di sorveglianza consente d'individuare le possibili minacce il più presto possibile. Questa possibilità rappresenta l'esigenza primaria per poter intervenire sulla minaccia aerea.

La sorveglianza dello spazio aereo consiste nelle tre seguenti funzioni di base:

- **avvistamento/scoperta**: consente di rivelare la presenza di piattaforme aeree attraverso il controllo dello spazio aereo d'interesse, alla maggiore distanza possibile, al fine di ottimizzare i tempi di reazione dei vari sistemi d'ingaggio. La disponibilità di sensori elettronici (*radar*) con ausili optoelettronici (telecamere a raggi infrarossi – IR) aumentano grandemente la capacità di scoprire;
- **acquisizione**: permette di determinare, in relazione al tipo di sensore utilizzato, i parametri della piattaforma avvistata (posizione, rotta, quota, velocità);
- **identificazione**: permette di determinare la natura (amica o ostile) di un aeromobile.

In assenza di capacità di Sorveglianza e Controllo specialistiche necessarie all'avvistamento/scoperta, è comunque possibile realizzare un sistema di sorveglianza e allarme di tipo visivo. Tale sistema consente, attraverso l'utilizzo dei più comuni sistemi di segnalazione e allarme, la possibilità di un imminente attacco, intrusione o inserzione aerea nella propria AoO. Gli **stati di allerta** del sistema in argomento sono:

- **Rosso**: *warning* relativo ad una minaccia imminente o in corso;
- **Giallo**: si è in presenza di una probabile minaccia;
- **Bianco**: riguarda una situazione in cui un attacco aereo è improbabile.

2.2.3.3 Sicurezza attiva

Le misure attive sono prese per distruggere, neutralizzare o ridurre l'efficacia della minaccia di attacchi aerei.

Le capacità specialistiche per la condotta di attività di sicurezza attiva sono quelle inquadrate nei Reggimenti di Artiglieria Controaerei. La capacità d'interdire il fuoco indiretto consiste nell'individuare e distruggere i razzi, i colpi di artiglieria e da mortaio.

In linea con la classificazione NATO, i *Ground Based Air Defence* (GBAD) sono suddivisi, in funzione della portata (quota/distanza), come riportato nella figura successiva.

I sistemi in dotazione all'E.I. sono:

- **<u>Sistemi a cortissima portata (V-SHORAD)</u>**

  I *Very Short Range Air Defence* sono impiegati, di norma, per fornire una protezione diretta ai complessi tattici di minore entità o vengono adottati per la difesa di obiettivi selezionati di limitate dimensioni (*Vital/Key Capability*) contro attacchi condotti prioritariamente alle bassissime quote.

  L'unico assetto in dotazione alla F.A. che rientra in tale tipologia, è il sistema del tipo missilistico, portatile e spalleggiabile STINGER, un *Man Portable Air Defence System* (MANPAD) dotato delle seguenti caratteristiche principali.

- **<u>Sistemi a corta gittata (SHORAD)</u>**

  Il sistema in dotazione è lo "*Skyguard-Aspide".* Viene schierato a difesa di obiettivi selezionati, areali o puntiformi, contro attacchi condotti prioritariamente alle basse quote.

- <u>Sistemi *Medium Range Surface to Air Missile* (MRSAM)</u>

  Vengono normalmente impiegati per la difesa di aree o di obiettivi di una certa consistenza e valore contro attacchi indirizzati prioritariamente alle medie quote. L'unico assetto in dotazione alla Forza Armata che rientra in tale tipologia di sistemi è il Superficie Aria a Media Portata Terrestre (SAMP/T). Nel contesto TBMD[42], i sistemi MRSAM come il SAMP/T o altri assetti equivalenti in dotazione ad altri Paesi dell'Alleanza, vengono normalmente inseriti nei sistemi difesivi denominati intercettori *Lower Layer*.

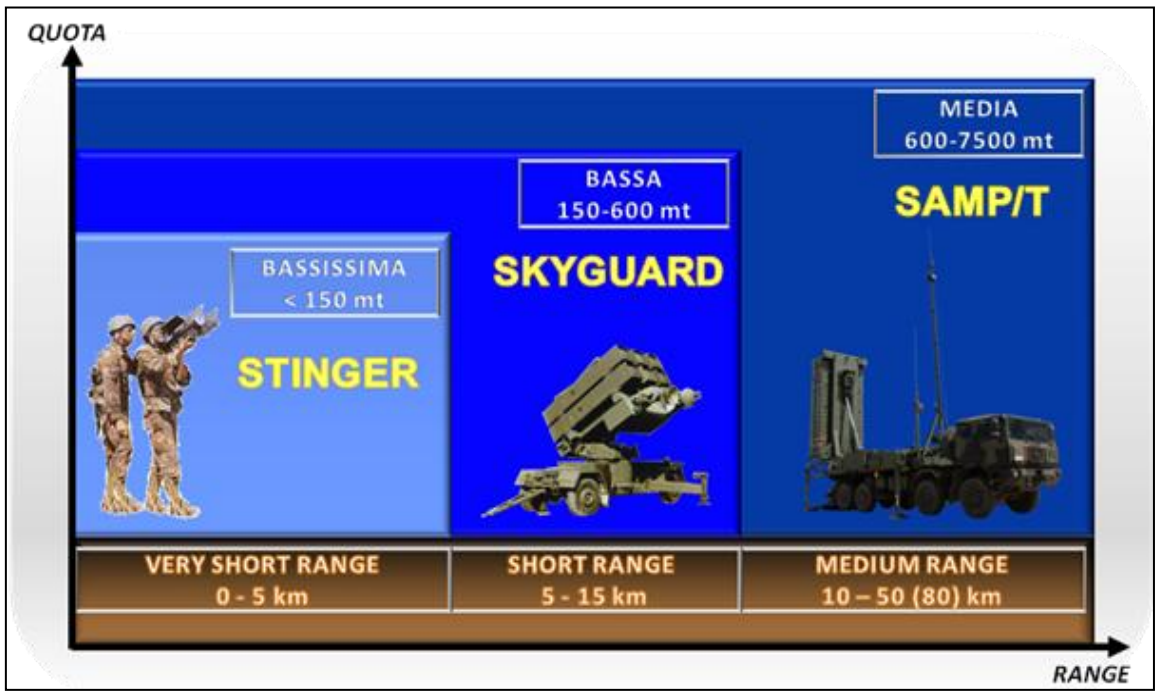


Figura 6: I Ground Based Air Defense (GBAD) dell'E.I.

[42] *Theatral/Ballistic Missile Defence.*

Menzione particolare va dedicata agli assetti denominati *Counter-Rocket Artillery and Mortars* (C-RAM). Tale capacità è l'unica, attualmente, in grado di intervenire attivamente ed efficacemente contro le minacce costituite dal munizionamento autopropulso non guidato, non autopropulso guidato e non guidato.

I principi fondamentali che regolano la difesa attiva da minaccia aerea sono:

- supporto reciproco;
- fuoco bilanciato;
- copertura ponderata;
- *engagement* tempestivo;
- difesa in profondità.

In particolare, va sottolineato che la capacità di colpire al più presto possibile le sorgenti di fuoco ostili con qualsiasi mezzo disponibile, prima che possano intervenire, rappresenta un'altra tipologia di sicurezza attiva (ad esempio tramite l'uso di elicotteri d'attacco o l'intervento delle Basi di Fuoco – *Fire Base*).

Infine, oltre all'impiego dei sistemi di difesa specialistici, tutte le unità e complessi tattici devono essere in grado di mettere in atto misure di sicurezza attiva utilizzando le armi in dotazione. Misura essenziale per la prontezza dell'erogazione del fuoco, quindi per l'efficacia della difesa stessa, è il Controllo dello Stato delle Armi (*Weapon Control Status*). Tale misura di controllo è decisa dai Comandanti ai vari livelli e si applica a tutti i sistemi d'arma e mezzi da combattimento (inclusi gli aeromobili). La definizione della misura più idonea è basata sulla situazione operativa che determina il grado e il livello di controllo necessari per un determinato sistema d'arma. Lo *staff* addetto alla *Force Protection*, ove presente, propone al Comandante lo stato più idoneo.

Figura 7: Team V-SHORAD specializzato Anfibio

Si distinguono tre **stati di controllo delle armi**:

- ***Weapons-free***: l'erogazione del fuoco è autorizzata contro tutto ciò vola e che non è stato riconosciuto come amico[43]. Nella pratica significa che, anche nel dubbio, si deve aprire il fuoco. È la misura di controllo meno restrittiva.

[43] Definizione in linea con quella della NATO. È lo stato di controllo più idoneo per le unità che conducono operazioni in profondità, tipicamente in aree controllate da forze ostili e dove non si

- ***Weapons-tight***: l'erogazione del fuoco è autorizzata verso obiettivi identificati come ostili, secondo i criteri definiti in fase di pianificazione;
- ***Weapons-hold***: l'erogazione del fuoco è autorizzata solo in caso di autodifesa o su ordine. È la misura di controllo più restrittiva.

2.2.3.4 Difesa passiva

La difesa passiva si concretizza, prioritariamente, nella realizzazione di opere e manufatti resistenti agli effetti provocati dalle differenti minacce aeree (ad esempio Bunker anti-aerei, coperture e infrastrutture anti mortaio). Il documento COMGENIO, SOP *Tecniche e procedure per la difesa passiva delle basi militari in operazioni (force protection engineering)*, costituisce il riferimento tecnico primario per la realizzazione delle opere e dei manufatti.

Le principali misure di difesa passiva dalla minaccia aerea, sono il mascheramento, la copertura, l'occultamento e l'OPSEC.

2.2.3.5 Mitigazione

Le misure tipiche di mitigazione sono:

- il diradamento delle forze, degli assetti e della manovra;
- la capacità di reagire all'attacco, implementabile attraverso l'individuazione e la prova di procedure d'allarme, reazione, raccolta del personale in aree protette e risposta agli effetti prodotti.

2.3 PROTEZIONE CBRN (CBRN *PROTECTION*)

2.3.1 Minaccia e rischi CBRN

Sebbene la probabilità d'impiego delle armi CBRN[44] convenzionali sia, dal tempo della guerra fredda, progressivamente diminuito, esso risulta ancora tutt'altro che trascurabile. Tra i pericoli più probabili è da annoverare la proliferazione delle armi di distruzione di massa e dei loro sistemi di lancio. In particolare essa consiste nel:

- rischio di utilizzo di armi chimiche e biologiche;
- probabile incremento del raggio d'azione dei missili balistici;
- possibile impiego di WMD[45] tramite metodi non-convenzionali (dispositivi dormienti, aerei e navi civili);
- potenziale difficoltà nel negoziare o affrontare attori non-statali dotati di WMD;
- possibile accesso per elementi ostili ad armi a letalità ritardata, con tecnologia basata, ad esempio, sull'utilizzo di impulsi elettromagnetici, agenti radiologici o cancerogeni.

---

possiede la superiorità aerea locale. È tipica ad esempio, degli assetti c/a inseriti nelle Forze di Sbarco o di Aviosbarco delle Operazioni Anfibie o Avioportate.

[44] *Chemical, Biological, Radiological and Nuclear*.

[45] *Weapons of Mass Destruction* – Armi di distruzione di massa.

I moderni ambienti operativi sono caratterizzati dalla presenza dei seguenti rischi CBRN:

- rischi diffusi, costituiti dalla suddetta proliferazione delle WMD e dei relativi sistemi di lancio;
- rischi tecnologici-industriali (*Toxic Industrial Materials* – TIM) derivanti dal rilascio di sostanze nocive da parte di impianti industriali o reattori nucleari danneggiati a seguito di azioni volontarie, accidentali o connesse a possibili catastrofi naturali;
- rischi terroristici, derivanti da azioni condotte da gruppi che nei loro atti di violenza intimidatoria potrebbero far ricorso ad armi non convenzionali;
- rischi connessi ai trasporti, conseguenti alla movimentazione di materiali sensibili sul suolo, negli spazi aerei, nelle acque nazionali e internazionali, conseguenti anche al traffico illecito di materiali "*Dual Use*"[46].

2.3.2 Compiti essenziali

I compiti tipici essenziali connessi con il contrasto alla minaccia e ai rischi CBRN sono:

- il contributo[47] alla prevenzione dalla proliferazione di WMD;
- la Difesa CBRN;
- le attività di gestione delle conseguenze di un evento CBRN.

In particolare, la Difesa CBRN è costituita dalle misure prese e dalle attività condotte allo scopo di neutralizzare o ridurre gli effetti negativi sulle operazioni, sul personale e sulle infrastrutture, derivanti da un incidente CBRN e, in particolare, da:

- minaccia o uso di armi CBRN;
- minaccia o uso di congegni CBRN (atti terroristici);
- rischio o rilascio nell'ambiente di TIM;
- rilascio di agenti CBRN o TIM causato da azioni militari contro sistemi d'arma CBRN, depositi/siti di stoccaggio di WMD avversari o siti di produzione industriale (*Counter-Force Targeting*).

Pertanto, l'incidente CBRN può manifestarsi sia per un'azione deliberata, sia per cause accidentali o come conseguenza secondaria di operazioni militari.

---

[46] Cfr. Unione Europea, Regolamento (CE) n.428/2009, 05/05/2009, art. 2 comma 1: *"dual use* (Trad. "duplice uso") sono prodotti che possono avere un uso sia civile sia militare. Possono essere materiali, sostanze, componenti, macchinari, prodotti finiti, semilavorati, software che vengono commercializzati a scopo civile ma che possono essere utilizzati anche per la costruzione di armi o in programmi per la proliferazione chimica, biologica, nucleare, ecc."

[47] Contributo perché il contrasto alla proliferazione di WMD può avere successo solo se condotto in modo interagenzia e multinazionale.

P.02 Protezione CBRN (*CBRN Protection*)
P.02.01 Supportare la prevenzione dalla proliferazione di WMD
P.02.01.01 Supportare le attività di Cooperazione sulla sicurezza delle WMD e Assistenza a favore di Partner civili o altre Forze di Sicurezza
P.02.01.02 Supportare la Cooperazione per la riduzione della Minaccia WMD
P.02.02 Condurre Difesa CBRN
P.02.02.01 Condurre Difesa CBRN Attiva
P.02.02.02 Condurre CBRN Passiva
P.02.03 Gestire le Conseguenze da incidente CBRN
P.02.03.01 Rispondere a Incidenti CBRN
P.02.03.02 Supportare le Operazioni di Recupero a seguito di incidente CBRN
P.02.04 Fornire Consulenza e Expretise tecnica CBRN
P.02.04.01 Fornire Consulenza Legale in materia di WMD
P.02.04.02 Fornire Consulenza Tecnica nell'ambito TECHINT

Tabella 4: Compiti Essenziali della Difesa CBRN

Tra le operazioni militari CBRN a supporto della prevenzione dalla proliferazione di WMD rientrano:

- supporto alle attività di cooperazione sulla sicurezza delle WMD: consta di un'ampia gamma di attività finalizzate a promuovere le relazioni e supportare lo sviluppo/miglioramento delle capacità dei Paesi alleati o *Partner* per supportare, in maniera progammata, le lotta alla proliferazione delle WMD;
- assistenza militare specialistica CBRN: consiste in qualsiasi forma di assistenza fornita a istituzioni civili o militari, nazionali o estere, in un ambiente permissivo, finalizzate a garantire la sicurezza fisica, a ridurre, smantellare, reindirizzare e/o migliorare la protezione dei programmi, delle scorte e delle capacità di contrasto alla proliferazione di WMD in uno Stato;
- operazioni d'interdizione di WMD: operazioni condotte al fine di tracciare, intercettare, individuare e fermare il traffico di WMD;
- operazioni offensive contro WMD: operazioni condotte al fine di disarticolare, neutralizzare o distruggere una minaccia WMD prima che essa si concretizzi;
- operazioni di eliminazione di WMD: attività condotte in un ambiente ostile o incerto per localizzare, qualificare, disabilitare o distruggere sistematicamente i programmi WMD e le relative capacità.

2.3.3 Forme di Protezione

2.3.3.1 Deterrenza

La deterrenza alla minaccia in argomento, è esercitabile esclusivamente attraverso *Information Activities*, in primis tramite un adeguato Profilo, Presenza e Postura (*Profile*, *Presence* e *Posture* – PPP) della forza. Inoltre, la disponibilità di unità specializzate, mezzi, equipaggiamenti e materiali moderni ed efficace sono sicuramente elemnti ulteriori per scoraggiare attacchi CBRN. Va da se che, per incidenti dovuti a cause accidentali o come conseguenza secondaria di operazioni militari non c'è alcuna attività di deterrenza possibile.

Figura 8: Squadra Paracadutisti in addestramento CBRN

2.3.3.2 Prevenzione

L'attività essenziale per prevenire la minaccia in argomento, richiede, prioritariamente, uno sforzo internazionale, interagezia e interforze che miri al Controllo degli Armamenti, il Disarmo, la Non Proliferazione delle WMD, oltreché allo sviluppo di un'efficace sistema e capacità integrata di protezione.

In ambito militarte terrestre, la prevenzione viene condotta, prevalentemente, attraverso le seguenti attività:

- contributo alle attività di contrasto al traffico illecito di agenti e materiale CBRN, tramite tracciamento dei sistemi (incluso ricerca e sviluppo di sostanze CBRN, loro produzione, stoccaggio, trasporto e impiego) e la disattivazione di WMD;
- contributo al processo di investigazione per l'attribuzione di responsabilità con la raccolta di campioni CBRN per scopi forensi (SIBCRA[48]);
- raccolta e analisi delle informazioni a supporto della funzione *Intelligence* mediante la sorveglianza, ricognizione ambientale e campionamento forense;
- Individuazione, Identificazione e Monitoraggio (*Detection, Identification and Monitoring* – DIM).

Tra le attività di prevenzione, rientrano quelle informative sulla minaccia/pericolo, sugli effetti da essi prodotti e sulle contromisure mediche e supporto sanitario.

[48] *Sampling, Identification, Biological, Chemical, Radiological Agents*.

Queste ultime sono le misure medico-sanitarie predisposte per ridurre la suscettibilità del personale agli effetti CBRN letali o dannosi all'organismo e alla cura delle lesioni provocate dall'esposizione a tali pericoli. Comprendono:

- pre-trattamento;
- post-trattamento;
- gestione di personale colpito in ambiente CBRN;
- evacuazione;
- adozione di misure igienico-profilattiche di sorveglianza e di limitazione alla circolazione per il personale potenzialmente esposto.

Figura 9: Attività preparatorie di un Team SIBCRA

2.3.3.3 Sicurezza Attiva

Consiste nel prendere tutte le misure necessarie ad annullare gli attacchi CBRN attraverso la condotta di attività, se necessario anche letali, che hanno lo scopo di neutralizzare o distruggere le armi o i mezzi intenti a colpire i *target* selezionati.

2.3.3.4 Difesa Passiva

La difesa passiva è realizzabile le predisposizioni e attività tese ad assicurare la sopravvivenza del personale e a ridurre il grado di vulnerabilità delle unità dagli effetti conseguenti a incidenti CBRN. Le misure di protezione fisica CBRN si distinguono in:

- protezione individuale: assicurata con l'equipaggiamento di protezione individuale (*Individual Protective Equipment* – IPE[49]);
- protezione collettiva (*Collective Protection* – COLPRO): essenziale per la condotta di operazioni che richiedono la lunga permanenza in aree contaminate e può essere di tipo fisso, mobile, trasportabile ed ibrida;
- protezione equipaggiamento e materiali: allo scopo di evitare il contatto diretto con gli agenti CBRN.

2.3.3.5 Mitigazione

Le attività tipiche, condotte per mitigare gli effetti di un incidente o attacco CBRN, sono:

- sostegno alle operazioni di ricerca e soccorso nelle zone d'incidente CBRN;

[49] Costituito da: maschera e filtro, indumento protettivo, cartine rivelatrici di aggressivi chimici e dosimetro individuale, corredo per l'autosoccorso, polveri decontaminanti.

- supporto alla gestione e trattamento del personale contaminato (*triage* e registrazione);
- decontaminazione del personale contaminato e delle vittime, tenendo in considerazione, laddove possibile, gli aspetti socio culturali e di genere dei coinvolti;
- svolgere le attività afferenti alla riduzione delle conseguenze degli incidenti CBRN tra le quali: raccolta, stoccaggio e smaltimento di sostanze tossiche o di materiali sospetti.

2.4 PROTEZIONE DAGLI ORDIGNI ESPLOSIVI (*EXPLOSIVE ORDNANCE HAZARDS PROTECTION*)

2.4.1 Minaccia e rischi

La Protezione dai pericoli degli ordigni esplosivi (*Explosive Ordnance* – EO), consiste in tutte quelle attività e misure prese per eliminare o ridurre gli effetti prodotti dall'esplosione degli ordigni esplosivi, allo scopo di proteggere il Potere di Combattimento, contribuire alla protezione del personale civile o delle infrastrutture critiche.

Figura 10: Intervento di un Team EOD su bomba d'Aereo

Gli EO più comuni[50] sono:

- mine;
- bombe d'aereo;

[50] Cfr. COMANDO GENIO, SOP *Tecniche e Procedure per la condotta di Explosive Ordnance Disposal (EOD)*, Ed. 2014.

- munizioni a caricamento chimico e biologico;
- bombe a grappolo e sub-munizioni;
- munizioni perforanti;
- razzi e missili;
- proietti d'artiglieria;
- ordigni esplosivi improvvisati (*Improvised Explosive Devices* – IED);
- razzi e mortai artigianali;
- IED a caricamento chimico o biologico (con o senza contenuto esplosivo);
- Dispersori chimici e biologici.

I pericoli connessi con la presenza di EO non sono molto mutati nel tempo. Tuttavia, gli IED rappresentano quelli tipicamente utilizzati nel combattimento non convenzionale[51], facili da realizzare ed economici. Conseguentemente rappresentano una delle minacce più probabili da affrontare nei teatri operativo attuali e, presumibilmente, anche nei prossimi.

Ma i pericoli di esplosione non sono connessi esclusivamente agli EO utilizzati dalle eventuali forze ostili. Occorre considerare e proteggersi anche dai pericoli connessi con lo stoccaggio, il trasporto e l'uso degli ordigni e propri. In tale ottica, i malfunzionamenti e gli inceppamenti dei sistemi d'arma, il maneggio degli ordigni, le mancate esplosioni, anche in poligono, rappresentano tutti pericoli da cui le proprie forze devono essere protette.[52]

2.4.2 Compiti essenziali

Gli assetti EOD (*Explosive Ordnance Disposal*) rappresentano gli attori imprescindibili per proteggere dalle minacce e pericoli appena esposti. Essi sono specializzati nella condotta delle operazioni di bonifica degli ordigni convenzionali e non convenzionali in tutto lo spettro delle operazioni. I *team* vengono generati[53], addestrati, equipaggiati e organizzati sulla base della missione da assolvere, della situazione operativa e delle minacce da fronteggiare.

---

[51] SME III RIF-COE, ND *L'Ambiente Operativo e le Forze Terrestri*, Ed. 2014.

[52] Su tale principio sono elaborate e aggiornate le linee guida sulla gestione/stoccaggio in sicurezza di munizionamento/esplosivi e sulla valutazione del rischio da adottare in contesti multinazionali e fuori dai confini nazionali - *Explosive Safety and Munition Risk Management* (ESMRM).

[53] I *team* EOD, oltre gli operatori EOD che costituiscono la componente imprescindibile, possono includere, a seconda delle variabili della Missione (METTT-TC) varie tipologie di elementi quali ad esempio infermieri professionali, nuclei sicurezza, mezzi speciali del Genio, nuclei Guastatori del Genio, addetti alle comunicazioni e interpreti. In genere comunque, a seconda dello specifico teatro d'operazione e della missione del contingente nella sua interezza, vengono stabilite specifiche tecniche, tattiche e procedure (TTP) che includono anche l'organizzazione e la composizione degli assetti. Le TTP da utilizzare vengono diramate e standardizzate tramite l'elaborazione di una specifica *Standing Operating Procedure* – SOP.

Gli operatori EOD, per standard NATO e qualifica nazionale, si distinguono come segue:

	Standard NATO	Qualifica Italiana	Tipologia di Missione
EOD	**CMD** *Conventional Munition Disposal*	**Artificiere**	**Attività Operativa di 1° Grado (territorio nazionale in tempo di pace)** Bonifica dei manufatti esplosivi in dotazione (esclusi i missili ASPIDE, ASTER-30 e il razzo GMLRS-U)
		Operatore CMD	**Attività Operativa di 2° Grado (territorio nazionale in tempo di pace)** Bonifica di EO regolamentari di ogni tipo, compresi i residuati bellici
			Attività Operativa in Te. Op. Bonifica di EO regolamentari di ogni tipo
	IEDD *Improvised Explosive Device Disposal*	**Operatore IEDD**	**Attività Operativa in Te. Op.** Bonifica di EO di circostanza o improvvisati
	BCMD *Biological & Chemical Munition Disposal*	**Operatore BCMD**	**Attività Operativa in Te. Op.** Bonifica di EO regolamentari con caricamento B e C
	Nil	**Operatore BC IEDD**	**Attività Operativa in Te. Op.** Bonifica di EO di circostanza o improvvisati con caricamento B e C
	Nil	**Nucleo di Bonifica del Centro Tecnico Logistico Interforze NBC**	**Attività Occasionale (territorio nazionale in tempo di pace)** Bonifica di EO e residuati bellici con caricamento B e C

Tabella 5: Qualifiche e competenze degli Operatori EOD

Il personale e gli assetti EOD:

- identificano EO/IED, ordigni convenzionali e di circostanza;
- conducono una valutazione iniziale del munizionamento rinvenuto;
- assistono i Comandanti, fornendo supporto all'*intelligence,* ai piani di difesa EW, sviluppando ed implementando le risposte d'emergenza EOD;
- si occupano di neutralizzare gli EO;
- forniscono assistenza tecnica alle unità preposte alle attività di bonifica degli itinerari, delle aree e dei campi minati;

- supportano le risposte ad eventi/incidenti chimici, fornendo consulenza tecnica e cercando di mitigarne gli effetti;
- inquadrati nei *Weapons Intelligence Team* (WIT)[54], forniscono conoscenza su esplosivi e ordigni;
- forniscono supporto ai *Team* WIT nel recupero di componenti degli EO/IED e li forniscono, unitamente alle proprie valutazioni, agli enti preposti alla valutazione tecnica;
- analizzano gli aspetti post-esplosione:
  - assistendo gli addetti all'*Intelligence* e/o alle investigazioni;
  - acquisiscono informazioni su EO/IED di nuova concezione o fattura, eventualmente rinvenuti per la prima volta;
  - assistono e forniscono consulenza alle autorità civili e militari durante le investigazioni post-esplosione che riguardano ordigni ed esplosivi militari.

I Guastatori del Genio, con particolare riferimento alle Operazioni Contro Ordigni Esplosivi, sono specializzati nella riduzione degli effetti provocati dagli EO. Il loro impiego preferenziale non è tuttavia da inquadrare *tout cour* nell'ambito della funzione operativa Protezione. L'effetto desiderato è normalmente quello di abilitare o garantire la libertà di movimento, quindi la Manovra nell'AoO. Occorre peraltro evidenziare due elementi particolarmente significativi. Innanzitutto, la Libertà di Movimento, quindi la possibilità di Manovrare, è un'Attività concorrente a qualsiasi attività o compito connesso con la Protezione poiché indirettamente, produce sempre effetti protettivi. Inoltre, le attività di *Route Clearance* condotte nell'ambito del contrasto alla minaccia EOD, rappresentano un'eccezione al concetto precedentemente espresso; esse rappresentano infatti attività tattiche abilitanti da catalogare nell'ambito della funzione Protezione. Tali attività, condotte da complessi tattici pluriarma denominati *Route Clearance Package* – RCP, includono come elementi essenziali (*framework*) gli assetti specialisti del Genio il cui personale è costituito da Guastatori.

Infine, capacità preziose da menzionare e inserire tra quelle particolarmente idonee a contrastare le minacce in argomento, sono fornite dagli assetti cinofili del Genio che utilizzano quadrupedi specializzati come segue:

- *Scout Dog*;
- *Mine Detecntion Dog* (MDD);

Improvides Explosive Detection Dog (IEDD).

[54] I *Weapons Intelligence Team* - WIT rappresentano le fonti TECHINT per eccellenza. Sono generati e organizzati sulla base della tecnologia d'interesse. Normalmente prevedono la presenza di operatori EOD. L'utilizzo che se n'è fatto nelle recenti esperienze, soprattutto in Afghanistan, nell'ambito del C-IED, è una possibilità d'impiego, non un principio dottrinale.

P.03 Protezione dai pericoli degli Ordigni Esplosivi (*Explosive Ordnance Hazards Protection*)
P.03.01 Condurre Operazioni di Bonifica di UXO[55] e ERW[56]
P.03.02 Intervenire sui sistemi d'arma in caso di malfunzionamento o inceppo
P.03.03 Condurre Operazioni di Contrasto agli Ordigni Improvvisati (C-IED *Operations*)
P.03.03.01 Pianificare attività C-IED
P.03.03.02 Condurre attività C-IED
P.03.04 Condurre Operazioni EOD BC
P.03.05 Fornire Supporto EOD alle operazioni contro la proliferazione di WMD
P.03.06 Condurre Operazione di protezione da IED e UXO
P.03.06.01 Fornire consulenza e supporto EOD per l'ispezione e la gestione dei depositi munizioni
P.03.06.02 Fornire supporto ai programmi di controllo armamenti e di disarmo[57]
P.03.04.03 Condurre TECHINT su UXO, IED e EO a caricamento speciale
P.03.04.04 Analizzare crateri, frammentazioni ed effetti post esplosione
P.03.04.05 Supporto EOD alle operazioni di recupero e gestione del personale deceduto (*Mortuary Affairs Operations*)
P.03.07 Condurre Operazioni EOD di sostegno logistico
P.03.08.01 Fornire supporto EOD alle Operazioni di Bonifica Sistematica dei Poligoni
P.03.08.02 Distruggere munizionamento inservibile
P.03.08.03 Condurre Operazioni EOD a supporto delle Operazioni di Sicurezza in Patria (*Homeland Security Operations*)[58]
P.03.08.04 Condurre Operazioni EOD a supporto di Autorità Civili[59]
P.03.08.05 Informare e addestrare il personale sulle minacce e pericoli derivanti dalla presenza di EO (*risk education*)
P.03.08.06 Condurre Operazioni EOD a favore dei Servizi

[55] *Unexploded Explosive Ordnance* – Ordigno Esplosivo Inesploso.

[56] *Explosive Remnant of War* – Residuato Bellico Esplosivo.

[57] Ad esempio, nell'ambito di programmi di *Disarmament, Demobilization and Reintegration* – DDR.

[58] Ad esempio, le operazioni EOD condotte nell'ambito dell'operazione "Vespri Siciliani", "Strade Sicure" e "EXPO 2015".

[59] Ad esempio, quelle a favore delle Prefetture o consulenze a favore di Tribunali.

Tabella 6: Compiti Essenziali della Protezione dai pericoli di esplosione

2.4.3 Forme di Protezione

2.4.3.1 Deterrenza

Azioni di deterrenza possono essere condotte solo contro la volontà delle forze ostili a utilizzare gli ordigni esplosivi. Tra queste, le *Information Activites* rappresentano certamente l'opzione principale da perseguire. In particolare, le misure di PPP hanno grande effetto sia nei confronti delle forze ostili, sia nella percezione della popolazione locale che deve essere estraniata dalle reti che conducono attacchi mediante l'uso di IED. Come per le altre attività di Protezione, la disponibilità di capacità specialistiche efficaci e moderne, ad esempio i *Team* EOD e RCP[60], contribuisce in modo rilevante alla deterrenza dall'uso di EO.

2.4.3.2 Prevenzione

I cardini della prevenzione dai rischi connessi con l'esplosione di EO sono la formazione e l'addestramento (individuale e collettivo) del personale. Al fine di coordinare le attività in tutti i processi della F.A., il Comando Genio elabora e aggiorna le Circolari e le Direttive in materia di protezione del personale e riduzione dei rischi dovuti alla presenza e all'utilizzo di EO. Inoltre, sulla base delle esperienze, dell'*Intelligence* e della pratica, la dottrina d'impiego e, se necessario, le prescrizioni, vengono ulteriormente affinate per le specifiche Operazioni tramite l'elaborazione di SOP e Ordini Permanenti. Va sottolineato peraltro che, la disponibilità di dottrina e disposizioni non sostituisce l'esigenza pratica di sapere fare le cose. È necessario pertanto che, soprattutto durante le fasi di Approntamento e di Preparazione alle specifiche operazioni, il personale analizzi e provi praticamente le TTP necessarie a ridurre gli effetti delle esplosioni di EO. È fondamentale che tali attività siano testate, anche tramite l'utilizzo di sistemi di simulazione, per valutare le performance delle forze e per verificarne la capacità e la reattività.

Per quanto concerne la prevenzione dai rischi connessi con il maneggio, l'uso e lo stoccaggio di ordigni, munizioni e esplosivi propri, questa si estrinseca principalmente nella valutazione dei rischi e, conseguentemente, nell'individuazione dei comportamenti da tenere e nelle procedure da utilizzare. Queste sono emanate attraverso appositi documenti non dottrinali (prevalentemente Circolari) che contengono le istruzioni e le prescrizioni necessarie a ridurre i rischi, oltreché gli esercizi e le prove da condurre per impararle.

2.4.3.3 Sicurezza Attiva

Consiste nel condurre tutte le azioni necessarie per ridurre e se possibile eliminare la minaccia e i rischi degli EO. Lo spettro delle azioni conducibili è quindi molto ampio, soprattutto se si considerano le operazioni C-IED (si pensi ad esempio all'importanza

[60] Complesso tattico inter-arma incaricato di condurre *Combined Arms Route Clearance Operations*. La struttura base degli RCP è normalemente, ma non esclusivamente, rappresentata da assetti del Genio (cfr. già cit. COMFORDOT, PSE 3.2.14 *Ostacolo e Operazioni di Mobilità*, Ed. 2015.

connessa con la neutralizzazione di una cellula terroristica o del finanziatore del Sistema IED).

Inoltre, per quanto concerne le azioni da condurre in presenza di EO nell'AoO, occorre considerare che non riguarda solo i genieri perchè chiunque, ad esempio, potrebbe trovarsi in un campo minato e conseguentemente dover essere in grado di reagire all'imprevisto gestendo al meglio il pericolo connesso. La soluzione di tale problema è stato individuato nel cosiddetto approccio "progressivo". Con tale approccio s'intence che, la risposta al pericolo, deve essere condotta prima dal più esperto/specializzato presente o comunque disponibile a intervenire. Quindi, il personale EOD è certamente il primo che in condizioni "normali" dovrà intervenire. Successivamente però, qualora gli assetti EOD non fossero disponibili ovvera in situazioni di combattimento o comunque in presenza di altre minacce o rischi maggiori, progressivamante, i guastatori prima e tutti gli altri soldati poi, devono reagire. Va da se che il concetto della progressività appena descritto è tanto più rilevante e conseguentemente va chiarito e condiviso con tutto il personale, quanto più l'operazione è ad alta intensità e le risorse EOD scarse.

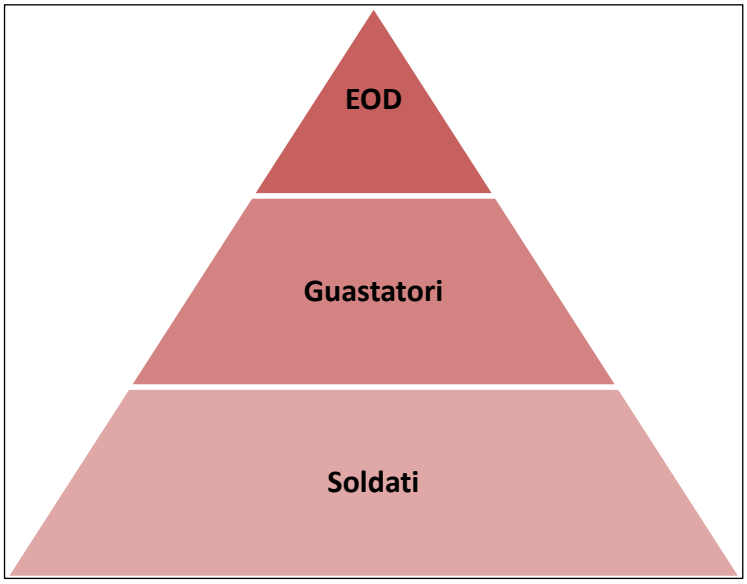


Figura 11: Livelli di risposta progressiva agli EO

Gli elementi "attivi" non sono quindi esclusivamente gli specialisti del Genio. Tutta la forza deve essere in grado di contrastare attivamente i pericoli derivanti dagli EO.

2.4.3.4 Difesa Passiva

La difesa passiva si esplica, principalmente, nell'utilizzo di sistemi di protezione individuale (ad esempio indumenti anti-esplosione e anti-frammentazione), nell'uso di mezzi protetti, di barriere protettive di vario genere e nella realizzazione di manufatti e lavori in terra idoei a limitare o annullare gli effetti delle esplosioni.

2.4.3.5 Mitigazione

Il diradamento delle forze, la capacità di segnalare e reagire agli incidenti, sono i cardini delle misure utili a mitigare gli effetti degli EO.

2.5 SOPRAVVIVENZA (*SURVIVABILITY*)

2.5.1 Minaccia e rischi

La Sopravvivenza (*Survivabiliy*) consiste in tutte quelle attività e misure prese per eliminare o ridurre l'efficacia dei sistemi d'arma nemici o di altri elementi ostili contro *target* puntiformi costituiti da personale, sistemi d'arma o equipaggiamenti propri, amici o civili. Inoltre, la Sopravvivenza mira anche a gestire i rischi connessi con la presenze materiali dei materiali inquinanti e pericolosi.

2.5.2 Compiti essenziali

La Sopravvivenza nell'AoO riguarda tutti gli aspetti relativi alla protezione del personale, delle armi, dei rifornimenti e, eventualmente, del personale civile e delle infrastrutture critiche. Le operazioni di sopravvivenza nell'AoO consistono principalmente nell'organizzare una buona difesa, muoversi spesso, sfruttare l'occultamento, il mascheramento e l'inganno, allestendo posizioni da combattimento o anche sfruttando le *Electronic Counter Measures* (ECM).

Le Operazioni di Sopravvivenza abilitano e sono spesso essenziali per la condotta di altri compiti della protezione (ad esempio la Difesa c/a, l'*Operational Area Security* e la Difesa CBRN). Inoltre, le Operazioni di Sopravvivenza possono essere parte di più ampie Operazioni di Sicurezza, Mobilità e Contromobilità.

Tuttavia è fondamentale comprendere la distinzione tra le attività di Sopravvivenza nell'AoO e quelle di Sicurezza dell'AoO che consiste nella già citata caratteristica di puntiformità delle prime rispetto le altre. In altre parole la Sopravvivenza si riferisce alla singola persona, sistema d'arma, ecc. La Sicurezza dell'AoO ha carattere areale e consiste nell'integrazione di tutte le altre attività e compiti di Protezione insistenti nell'Area.

Le capacità/attività inerenti la sopravvivenza possono essere suddivise nelle seguenti quattro aree:

- **mobilità**: la capacità sopravvivenza delle forze amiche è maggiore se esse sono in grado di muovere e riposizionarsi rapidamente nell'AoO;
- **comprensione della situazione**: è il frutto dell'analisi e del giudizio delle informazioni rilevanti, al fine di determinare la relazione tra le variabili della missione e, allo stesso tempo, facilitare il Processo Decisionale. Essa richiede la capacità di identificare, sviluppare e comprendere gli elementi critici delle informazioni inerenti quanto accade nell'AoO, permettendo un'efficace valutazione dei rischi e dei pericoli;
- **rafforzamento**: consiste nell'uso e integrazione dei materiali e ostacoli naturali e artificiali, al fine di proteggere personale, equipaggiamenti e infrastrutture. Le misure adottate mirano a proteggere le risorse amiche da esplosioni, fuoco diretto e indiretto, radiazioni e dagli effetti della guerra elettronica. Il rafforzamento si

realizza attraverso i Lavori sul Campo di Battaglia[61] (LCB), l'uso di barriere, muri, scudi, demolizioni, ordigni esplosivi e anche sistemi non letali. Il rafforzamento ha come scopo quello di eliminare o mitigare gli effetti di un attacco e include l'allestimento di posizioni da combattimento, l'impiego di veicoli corazzati e lo sfruttamento efficace del sistema informativo;

- **mascheramento, occultamento e inganno**: è l'uso di materiali e tecniche allo scopo di nascondere le vulnerabilità e le capacità, al fine di evitarne l'individuazione. Le attività di mascheramento, occultamento ed inganno contribuiscono attivamente nel prevenire che il nemico individui o identifichi le unità amiche, le loro attività, i loro equipaggiamenti, le loro installazioni e, allo stesso tempo, provvede ad oscurare, schermare o "ingannare" il campo di battaglia.

P.04 Sopravvivenza (*Survivability*)
P.04.01 Proteggersi dagli attacchi nemici
P.04.01.01 Proteggere individui e singoli sistemi
P.04.01.02 Preparare posizioni da combattimento
P.04.01.03 Preparare posizioni protette
P.04.01.04 Utilizzare equipaggiamento protettivo
P.04.01.05 Reagire al fuoco diretto
P.04.01.06 Reagire al fuoco indiretto
P.04.02 Disperdere le Forze
P.04.03 Gestire materiali inquinanti e pericolosi
P.04.04 Organizzare la Sicurezza Locale

Tabella 7: Compiti Essenziali della Sopravvivenza (*Survivability*)

Infine, anche la lotta agli incendi (*fire fighting*) rientra tra le attività connesse con la Sopravvivenza ed è condotta attraverso l'uso di capacità che possono essere categorizzate come segue:

- **antincendio generale**: riguarda tutte quelle capacità che si sviluppano sistematicamente nel corso dell'anno e che possono riguardare anche il trasporto di personale, carburante, munizioni ed esplosivi;
- **antincendio tattico**: richiese capacità specialistiche ed è solitamente fornita dal genio, dalla *host nation* o da altre unità specializzate nell'antincendio. In aggiunta alle normali attività, questa capacità può riguardare il primo soccorso, la gestione iniziale di incidenti che vedono il coinvolgimento di materiali/sostanze esplosive, il

[61] Pubblicazione in via di elaborazione a cura di COMGENIO.

recupero di personale intrappolato o ferito in aerei, edifici, mezzi, acqua o spazi ristretti.

2.5.3 Forme di Protezione

2.5.3.1 Deterrenza

Come per i compiti di protezione già analizzati, le attività di deterrenza sono varie *Information Activites*, miranti a scoraggiare le forze nemiche o ostili dal condurre attacchi contro la forza, i civili o le infrastrutture critiche.

2.5.3.2 Prevenzione

Le attività utili a prevenire le azioni ostili sono connesse principalmente correlate con la funzione *Intelligence*, con la capacità di capire e prevedere come e dove le forze ostili potrebbero condurre attacchi.

Per quanto concerne invece i pericoli connessi con la presenza di materiali inquinanti e pericolose, le attività di prevenzione devono sempre rappresentare lo sforzo principale. Le attività d'informazione e formazione del personale sono l'essenza stessa di una efficace prevenzione.

2.5.3.3 Sicurezza Attiva

La sicurezza attiva consiste nella condotta di azioni volte principalmente ad anticipare possibili azioni ostili ovvero a reagire ad esse. Consistono essenzialmente in azioni di fuoco o d'impiego di sistemi attivi capaci di inibire o neutralizzare la minaccia (ad esempio i sistemi *chaff*[62] e *flare*[63]).

Figura 12: Cecchino

2.5.3.4 Difesa Passiva

La Difesa Passiva è la forma classica, la più utilizzata, per Sopravvivere sul campo di battaglia. Nonostante tutte le forze conducono operazioni di sopravvivenza, le capacità del Genio di movimentare le terre e realizzare opere di protezione di vario genere rappresentano senz'altro gli elementi più efficace, essenziali per raggiungere i livelli di protezione più elevati. Si definiscono *Survivability*

[62] Contromisura per confondere i radar, oltreché una tecnica di *Electronic Attak* – EA.

[63] Contromisura di difesa utilizzata dagli aeromobili, ma anche da mezzi navali e terrestri, per ingannare i sensori ottici a guida IR dei missili.

Operations quelle caratterizzate da attività militari che alterano l'ambiente fisico allo scopo di creare o aumentare la protezione, l'occultamento e il mascheramento.

Le opere di difesa passiva consistono in:

- **Opere di protezione passiva - *Cover***: muri, coperture, terrapieni, barriere, ecc., idonei a proteggere dal tiro diretto, tiro indiretto, incendio e esplosioni;
- **Posizioni da Combattimento – *Fighting Positions***: forniscono protezione passiva, occultamento e mascheramento a personale e sistemi d'arma, consentendo agli stessi di combattere. Possono essere di tipo pianificato o di circostanza;
- **Posizioni protette – *Protective Positions***: sono realizzate per proteggere veicoli e sistemi d'arma che non sono direttamente coinvolti nei combattimenti;
- **Occultamento e Mascheramento**.

Rientra nella protezione passiva anche l'utilizzo di mezzi, sistemi ed equipaggiamento protetti o di protezione (si pensi ad esempio all'elmetto e al Giubbetto anto-proiettile).

2.5.3.5 Mitigazione

Consiste principalmente nella capacità di reagire in modo pronto ed efficace a situazioni impreviste o avverse. Ad esempio realizzando posizioni da combattimento o posti comandi alternati (da utilizzare in caso di compromissione o neutralizzazione delle principali) o anche instaurando delle procedure di reazione rapida che prevedano l'intervento di una forza in soccordo di una personalità scortata sotto attacco.

2.6 SICUREZZA DELL'AREA DELLE OPERAZIONI (*OPERATIONAL AREA SECURITY*)

2.6.1 Minaccia e rischi

La Sicurezza dell'AoO consiste in tutte le attività e misure prese per ridurre i rischi e contrastare la condotta di qualsiasi attacco contro la manovra, la forza, sistemi d'arma o equipaggiamenti propri, amici o civili, in una specifica AoO.

2.6.2 Compiti essenziali

La Sicurezza dell'AoO può rappresentare il metodo migliore per proteggere aree che sono necessarie per facilitare lo schieramento delle forze, per condurre la manovra o per il reperimento delle risorse essenziali per il Sostegno delle Operazioni. La Sicurezza dell'AoO è un concetto particolarmente efficace anche per la protezione di civili, di infrastrutture e per fornire sicurezza e controllare aree nell'ambito delle Operazione di Stabilizzazione.

La Sicurezza dell'AoO viene espressa attraverso la condotta delle Operazioni di Sicurezza (*Security Operations*)[64], il cui scopo è la protezione delle forze, delle installazioni, degli itinerari e di tutte le attività svolte all'interno dell'AoO stessa. Nonostante sia essenziale per il successo di qualsiasi operazione militare, la Sicurezza dell'AoO assume rilevanza fondamentale quando è necessario garantire la continuità delle Operazioni di *Sustainment* e supportare le Operazioni *Decisive* e *Shaping*[65].

Figura 13: Comandante di Pattuglia Paracadutisti schiera gli OP

Il concetto di Sicurezza dell'AoO viene messo in pratica nella protezione delle aeree di spiegamento delle forze o per pianificare attività tattiche di stabilizzazione quali, ad esempio, la Sicurezza e il Controllo. L'efficacia delle attività connesse viene enfatizzata nelle operazioni in cui l'AoO è costituita da aree non contigue. L'organizzazione e l'integrazione di molteplici attività e capacità, incluse le basi e il fuoco, diventano in tal caso l'unico modo per fronteggiare la limitatezza delle risorse rispetto l'ampiezza e la complessità dell'AoO e per il controllo di zone estese non presidiate.

Le Operazioni di Sicurezza, oltreché la Ricognizione, si focalizzano in corrispondenza delle NAI, allo scopo di rispondere alle CCIR, abilitando di fatto il *Mission Command* attraverso la conferma o negazione della presunta minaccia.

In tali Operazioni:

- le forze sono organizzate in modo da enfatizzare la mobilità, forza letale e capacità di comunicazione;
- sfruttano le misure di sicurezza locali adottate da tutte le unità indipendentemente dalla loro posizione nell'AoO.

In tali operazioni, i Comandanti, a tutti i livelli, generano/organizzano il *Combat Power,* dedicando assetti/capacità alla Protezione sulla scorta dell'analisi che viene condotta attraverso l'utilizzo del METT-TC. Le variabili di missione aiutano a

[64] Da non confondere con l'*Operation Security* – OPSEC) che consiste nella sicurezza delle operazioni che verrà trattata successivamente.

[65] L'*Operation Framework* è costituito da *Shaping*, *Decisive* e *Sustaining Operations* (cfr. già cit. NATO, AJP-3.2 *Land Operations*, Ed. 2015).

comprendere e valutare quali risorse siano essenziali e quali più vantaggiose/efficaci rispetto ad altre per l'assolvimento delle specifiche missioni. Il CRM è utile per prendere decisioni, gestiore il problema e allocare risorse. Criticità, vulnerabilità e recuperabilità sono gli aspetti principali che un Comandante deve considerare nel definire le proprie linee guida per la protezione

In tale contesto, le unità del Genio possono ammassare le loro capacità ed equipaggiamenti al fine di realizzare posizioni da combattimento nelle posizioni difensive o negli *strongpoint* e rinforzare quelli preesistenti. In un ambiente contraddistinto dalla minaccia di attacchi missilistici, il Genio può contribuire efficacemente a migliorare le fortificazioni campali focalizzando sugli assetti chiave che potrebbero costituire un obiettivo per i missili nemici.

Le attività di LCB, sebbene siano riconosciute come un compito classico delle unità del Genio, implicano la partecipazione di tutte le unità, a qualunque livello, per quanto riguarda il concorso di risorse non specializzate, la manutenzione e il miglioramento delle postazioni, così come dei *bunker* o delle *Forward Operating Base* – FOB.

L'*Area Security Operations* pongono particolare attenzione alle seguenti attività e assetti:

- **difesa di una o più basi**: la difesa di una base prevede l'attivazione di una serie di misure, sia di *routine* sia finalizzate ad annullare o ridurre gli effetti prodotti dagli attacchi da parte di forze ostili. Nel caso in cui l'esigenza riguardi più basi contemporaneamente, il livello ordinativo delle unità preposte a garantirne la difesa può raggiungere anche quello di G.U.;
- **sicurezza di assetti critici**: consiste nella protezione e nella sicurezza del personale, degli assetti e/o delle informazioni individuate e ritenute essenziali per l'assolvimento della missione, nonché delle risorse richieste per garantire la protezione;
- **protezione delle capacità di Comando e CIS:** la protezione dei posti comando e del CIS in generale, consiste nell'applicazione di una serie di tecniche che implicano lo spiegamento a strati ed integrato di un dispositivo di sicurezza. Tale organizzazione prevede la costituzione di un'area "polmone" per mitigare gli effetti di eventuali esplosioni e, allo stesso tempo, garantire una copertura dal fuoco diretto e dall'osservazione nemica;
- **sicurezza di HRP**: come detto, gli *High-Risk Personnel* sono soggetti che, per il grado, funzione o incarico che ricoprono, rappresentano dei potenziali *target* per il nemico. A tal riguardo devono essere adottate particolari precauzioni al fine di garantire un'adeguata sicurezza e protezione areale a questi individui e alle loro famiglie (ad esempio la protezione dell'abitazione o dei lughi dove operano);
- **sicurezza fisica**: consiste in una serie di misure fisiche volte a tutelare l'incolumità del personale, a prevenire l'accesso non autorizzato a installazioni,

materiali, equipaggiamenti e documenti, nonché a salvaguardarli dalla minaccia di spionaggio, sabotaggio, danneggiamento e furto. Può essere richiesto il supporto generale del genio per identificare le potenziali vulnerabilità fisiche del personale, delle basi e del materiale che possono essere oggetto di attacchi terroristici. Nel pianificare il dispositivo di sicurezza, le linee guida devono considerare la minaccia locale, le vulnerabilità specifiche del sito, le criticità degli assetti e le risorse disponibili;

- ***response force operations*:** assetti che rinforzano le unità organiche dedicate alla protezione e il cui impiego è finalizzato all'eliminazione della minaccia (esempio sono le *Quick Reaction Force* – QRF);
- **sicurezza delle LOC:** la sicurezza e la protezione delle Linee di Comunicazione (*Line of Communication* – LOC) rappresenta una delle maggiori criticità nell'ambito di un'operazione militare. Le attività militari finalizzate a garantire la sicurezza delle strade e degli itinerari sono di natura difensiva e *terrain oriented*. Le unità dedicate a quest'attività, tipicamente del Genio, hanno il compito di evitare che il nemico impedisca od ostacoli il movimento delle forze amiche lungo le LOC e di stabilire dei corridoi di movimento, all'interno dei quali, condurre in modo sincronizzato attività di ricognizione, di mobilità, di sicurezza e di raccolta informazioni. I corridoi di movimento possono essere stabiliti temporaneamente (ad esempio in un'area ad alto rischio) o per tutta la durata di un'operazione;
- ***checkpoint* e avamposti:** sono elemnti necessari ai fini del controllo dell'AoO. Vengono resi operativi per un determinato periodo di tempo o per tutta la durata dell'operazione. I *Check-Point* (CP), posti di controllo fissi o mobili (*Vehicle Check-Point* - VCP), e gli avamposti (*Combat Out-Post* – COP) vengono ormalmente attivati lungo le LOC o in prossimità di *Key Position* (identificate attraverso il METT-TC).

  Lo scopo dei CP è quello di controllare, regolare e monitorare il movimento, mentre quello dei COP si esplica nell'attività di *Information, Surveillance and Reconnaissance* – ISR, di supporto alle operazioni o per negare la manovra in una specifica area;
- **sicurezza dei convogli**: sono attività finalizzate alla protezione dei convogli. Possono essere condotte contestualmente o in integrazione alle attività di sicurezza delle LOC[66];
- **sicurezza delle aree portuali e dei moli:** il Comandante che ha nella propria AoO delle aree portuali, nel pianificare la sicurezza areale considera la protezione dei porti, dei moli, dei cargo e, allo stesso tempo, organizzare e sviluppare l'addestramento, le linee guida d'impiego e definire l'equipaggiamento delle forze responsabili della protezione di tali siti;

[66] Cfr. COMFORDOT, PSE 3.14.05.02 *La Scorta Convogli*, Ed. 2016.

- **sorveglianza:** è la sistematica osservazione dello spazio aereo, terrestre e del sottosuolo attraverso apparecchiature elettroniche, visive, sonore e fotografiche. La determinazione degli assetti o dei siti da sorvegliare è il risultato di un processo di analisi finalizzato ad individuare tutte quelle criticità che possono costituire obiettivi per il nemico. Può essere condotta con strumenti a elevato contenuto teconologico (ad esempio droni o sensori) o in maniera classica, ad esempio integrando pattuglie, posti di controllo e posti di osservazione e allarme;
- ***area damage control*:** si tratta dell'attività disposta dal Comandante quando il danno e la portata dell'attacco avversario sono limitati e, pertanto, il ripristino della situazione può essere condotto con assetti e risorse a propria disposizione. L'*Area damage control* consiste nel mantenimento o nel ripristino dell'ordine, nell'evacuazione dei feriti e nell'isolamento di zone considerate pericolose (ad esempio a seguito dell'esplosione di un'ordigno improvvisato è necessario sgomberare e controllore l'area al fine di investigare sulle TTP utilizzate e condurre l'*exploitation*).

P.05 Sicurezza dell'Area delle Operazioni (*Operational Area Security*)
P.05.01 Condurre Operazioni di Sicurezza
P.05.07.01 Copertura (*Cover*)
P.05.07.02 Guardia (*Guard*)
P.05.07.03 Schermo (*Screen*)
P.05.07.04 Scorta (*Escort*)
P.05.02 Proteggere le Basi in Operazione
P.05.03 Proteggere Installazioni e Infrastrutture Critiche
P.05.04 Stabilire la Sicurezza Locale
P.05.04.01 Attivare Posti di Guardia
P.05.04.02 Attivare Posti Controllo (*Check Points*)
P.05.04.03 Stabilire Sicurezza Perimetrale
P.05.04.04 Attivare Posti Osservazione e Allarme – POA (*Observation Points* – OP)
P.05.04.05 Controllare gli Ingressi[67]
P.05.04.06 Utilizzare i Sistemi Integrati di Protezione[68]
P.05.04.07 Proteggere i Posti Comando
P.05.05 Fornire Protezione a Personalità ad Alto Rischio
P.05.06 Condurre *Response Force Operations*

Tabella 8: Compiti Essenziali della Sicurezza dell'Area delle Operazioni

[67] Il compito Controllo degli Ingressi include il controllo degli accessi a equipaggiamenti, materiali, veicoli, installazioni e documenti.

[68] Cfr. COMGENIO, PTE-4.05.16 *Sistemi integrati per la protezione delle basi*, Ed. 2016.

La maggior parte degli elementi specializzati nelle Ricognizioni e Operazioni di Sicurezza sono inquadrati nei Reggimenti di Cavalleria di Linea e del Genio Guastatori. Sono dotati di capacità diverse in funzione della tipologia di forze cui appartengono (leggere, medie e pesanti) e dell'addestramento al combattimento in ambienti particolari (Paracadutisti, Anfibi e Truppe da Montagna).

I Guastatori[69] del Genio infine, rappresentano le forze base per la costituzione di complessi tattici per la condotta delle Operazioni di Bonifica Areale e d'Itinerari (*Combined Arms Route and Area Clearance Operations*)[70]. Sono normalmente impiegati a livello minimo di quartina[71] o squadra, specializzati nella ricerca e segnalazione degli ordigni inesplosi, della condotta di azioni contro mine e contro trappole. Quando dotati di mezzi speciali (ad esempio i VTTM Orso nelle varie configurazioni), equipaggiamenti e materiali adeguati, oltreché propriamente addestrati, costituiscono gli assetti *Route Clearance* (*team*/squadra/plotone che, in funzione del METT-TC, costituisce la base per costituire i *Route Clearance Package* – RCP, complessi tattici specializzati nella bonifica di itinerari). I Guastatori, sempre in considerazione del METT-TC, possono essere supportati da Team EOD e da altri assetti speciali ritenuti indispensabili per la specifica missione.

2.6.3 Forme di Protezione

2.6.3.1 Deterrenza

Come già evidenziato in altri Compiti della Protezione già trattati, la condotta di *Information Activities*, in particolare legate alla PPP, costituiscono l'elemento principale per generare Sicurezza nell'AoO.

2.6.3.2 Prevenzione

La disponibilità di prodotti e previsioni Intelligence è fondamentale. Inoltre, la disponibilità di forze e di assetti di sorveglianza, unitamente alla capacità d'intervenire prontamente contro forze ostili, fornisce un enorme contributo per prevenire azioni ostili.

2.6.3.3 Sicurezza Attiva

La sicurezza attiva si estrinseca, principalemente, nella condotta delle Operazioni di Sicurezza e nella capacità di colpire le forze ostili, garantendo alla forza militare, alle infrastrutture e ai civili da proteggere, di portare a termine la missione o le attività previste.

---

[69] Esclusivamente il personale qualificato Guastatore a termine del corso di specializzazione presso il Comando Genio dell'Esercito.

[70] Cfr. già cit. COMFORDOT, PSE 3.2.14 *Ostacolo e Operazioni di Mobilità*, Ed. 2015.

[71] Cfr. già cit. COMFORDOT, PSE 3.31 *L'Impiego del Genio*, Ed. 2015 (Annesso 1 Allegato "A": Guastatori Paracadutisti).

2.6.3.4 Difesa Passiva

Esempi di difesa passiva possono essere costituiti dalla realizzazione di tunnel o camminamenti protetti. Tutte le opere in terra di difesa perimetrale e la realizzazione di fossati c/c rappresentano i primi elementi di difesa fisica per proteggere una base.

2.6.3.5 Mitigazione

Gli effetti prodotti da un attacco o dal verificarsi dei rischi connessi con le Operazioni sono mitigabili attraverso il cambiamento di itinerari, l'uso di forme di manovra più appropriato e il diradamento delle forze. Inoltre, la disponibilità di procedure

2.7 SICUREZZA DELLE OPERAZIONI – OPSEC (*OPERATIONS SECURITY*)

2.7.1 Minaccia e rischi

Il rischio è che gli Elementi Essenziali delle Informazioni Proprie (*Essential Elements of Friendly Information* – EEFI) siano svelati dalle forze ostili o avverse. L'effetto provocato dalla compromissione di tali informazioni è talmente grave che, in alcune operazioni (si pensi ad esempio a una Dimostrazione Anfibia[72]), provoca immediatamente l'insuccesso dell'operazione.

Va da sé che, essendo tale rischio sempre presente, l'OPSEC si applica a tutte le fasi del Processo delle Operazioni, a tutte le Operazioni e interessa l'intero spettro dei conflitti.

Figura 14: *Team* acquisizione *Target*

[72] Cfr. COMFORDOT, PSE *Le Operazioni Anfibie*, Ed. 2005.

2.7.2 Compiti essenziali

L'OPSEC è il processo attraverso il quale si identificano gli EEFI e, successivamente, si analizzano le attività amiche al fine di:

- individuare le azioni che possono essere monitorate dall'*intelligence* nemica;
- determinare gli indicatori dell'*intelligence* nemica che possono essere interpretati o raggruppati al fine di ricavare tempestivamente delle informazioni critiche;

selezione ed attuare misure finalizzate a eliminare o ridurre la vulnerabilità delle azioni amiche.

P.06 Sicurezza delle Operazioni (*Operations Security* – OPSEC)
P.06.01 Condurre OPSEC
P.06.01.01 Identificare gli Elementi Essenziali delle Informazioni Proprie (*Essential Elements of Friendly Information* – EEFI)
P.06.01.02 Applicare appropriate misure di OPSEC
P.06.01.03 Eseguire piani d'emergenza per la distruzioni di documenti classificati e materiali
P.06.02 Mettere in atto procedure di sicurezza fisica
P.06.02.01 Mascherare, occultare e ingannare
P.06.02.02 Disciplinare rumore, luce, tracce termiche e fisiche
P.06.03 Contrastare la minaccia
P.06.03.01 Condurre Operazione di *Counter-Intelligence*
P.06.03.02 Condurre Operazioni Contro-Inganno

Tabella 9: Compiti Essenziali della Sicurezza delle Operazioni (OPSEC)

2.7.3 Forme di Protezione

2.7.3.1 Deterrenza

Le azioni di deterrenza, anche per il compito OPSEC, consistono in appropriate *Information Activities* rivolte a scoraggiare le azioni ostili.

2.7.3.2 Prevenzione

Il passo fondamentale per prevenire le azioni avversarie consiste nell'identificazione degli EEFI. Senza una corretta identificazione delle informazioni critiche, qualsiasi successiva azione o misura risulterebbe vana.

2.7.3.3 Sicurezza Attiva

La principale forma di Sicurezza Attiva consiste nel condurre azioni che non svelino alle forze ostili le nostre reali intenzioni. Tra tali azioni rientra anche l'inganno o la condotta di finte o attacchi dimostrativi. Altre azioni utili a mettere in sicurezza le operazioni costitono nel cercare e colpire gli elementi dell'*Intelligence* avversaria prima che possano riportare le informazioni acquisite ovvero attraverso l'inganno, influenzando o facendo credere alle forze ostili di aver carpito informazioni critiche.

Le Operazioni di *Counter-Intelligence* e di Contro-Inganno, costituiscono ulteriori forme di sicurezza attiva.

2.7.3.4 Difesa Passiva

Si attua, principalmente, attraverso il mascheramento e l'occultamento di mezzi, materiali ed equipaggiamenti, allo scopo di celare le reali intenzioni. Ulteriori tecniche di difesa passiva consistono nel disciplinare o celare alcune azioni quali ad esempio rumore, luce, tracce termiche e fisiche.

2.7.3.5 Mitigazione

Consiste nel redigere e poi eseguire piani d'emergenza, ad esempio quelli connessi con la distruzione dei documenti e dei materiali classificati.

2.8 RECUPERO DEL PERSONALE (*PERSONNEL RECOVERY*)

Consiste nell'insieme delle attività e misure necessarie, incluso le risorse civili e diplomatiche se necessario, per effetturare il recupero e il reinserimento del personale rimasto isolato o disperso prima che venga catturato/detenuto. Nel caso in cui quest'ultime due ipotesi si fossero già verificate, individuarlo e estrarlo attraverso specifiche operazioni.

2.8.1 Minaccia e rischi

L'analisi e la comprensione dell'AO è essenziale e include le complesse e dinamiche relazioni tra forze amiche, ostili e la popolazione. Comprendere l'ambiente permette ai Comandanti di visualizzare e descrivere il proprio intento che deve sempre includere il recupero del personale. In particolare, dall'analisi del terreno, devono e mergere le possibili azioni nemiche, le E-TTP, gli itinerari di movimento, inclusi gli alternativi e quelli di emergenza, le possibili Zone d'Atterraggio e le aree di maggiore vulnerabilità.

2.8.2 Compiti essenziali

Le attività di Recupero del Personale (PR) si integrano nell'ambito dell'intero spettro delle operazioni. A seconda del livello e del rischio di isolamento valutato, includono, in modo coordinato, il contributo non solo degli assetti militari ma anche di forze amiche e civili, asempio mediatori e personale diplomatico. Per tale ragione, nei piani di recupero, vanno sempre definite in maniera chiara le relazioni di comando, chi supporta e chi è supportato nelle varie fasi delle operazioni. sia nella fase di pianificazione che durante la condotta del recupero del personale.

Nella creazione dei piani di PR, ciascun Comandante considera e affina le linee guida espresse dal Comandandte sovraordinato. Nei complessi tattici di livello meno elevato, normalmente inferiore al gruppo tattico (compreso), le linee guida sul PR si traducono in istruzioni, anche tramite briefing, sul comportamento da tenere in caso di isolamento (*Isolated Soldier Guidance* – ISG). Le ISG definiscono, in modo chiaro e semplice, in quali situazioni si parla di personale "isolato" e quali sono le attività da

condurre per il recupero dello stesso. Le informazioni che devono sempre essere incorporate nelle ISG sono:

- definizione della situazione di "isolamento": spiega chiaramente in quali circostanze devono essere applicate le misure contenute nell'ISG;
- "dove andare": devono essere sempre individuati dei punti ti raccolta (*rally point*), tenendo conto di quelli definiti dal comando superiore. Possono essere specificamente connessi col PR o essere utilizzati anche per altri scopi. Il "dove andare" può anche essere costituita, più semplicemente, da una direzione, tramite un angolo di rotta o il riferimento di una strada o un fiume.

  In ogni caso, i fattori da tenere in debita considerazione e che possono influenzare l'attività di PR sono: schema di manovra, situazione amica e nemica, nonché le misure già prestabilite del comando superiore.
- "cosa fare": descrive le azioni che il personale da recuperare deve compiere dall'inizio alla fine del suo isolamento;
- comunicazioni: questo aspetto riguarda tutte le fasi dell'isolamento fino al *link-up* con la forza preposta al recupero. Include l'equipaggiamento individuale del soldato e, eventualmente, le procedure specifiche per il *link-up* con le forze addette al recupero e le istruzioni sull'impiego delle formule di riconoscimento e degli apparati radio.

Figura 15: Recupero di personale ferito

P.07 Recupero del Personale (*Personnel Recovery*)
P.07.01 Assicurare l'approntamento e la preparazione pratica del personale
P.07.01.01 Formare e Addestrare il personale
P.07.01.02 Delineare la struttura e le misure di coordinamento delle operazioni di recupero
P.07.02 Condurre i compiti di Protezione connessi col Recupero del Personale
P.07.02.01 Generare i complessi tattici indispensabili per le missioni
P.07.02.02 Schierare i complessi e generare il necessario potere di combattimento
P.07.02.03 Sostenere le capacità di Recupero del Personale
P.07.02.04 Rischierare i complessi tattici
P.07.03 Pianificare le Operazioni di Recupero del Personale
P.07.03.01 Redigere i piani di contingenza necessari
P.07.03.02 Condurre azioni isolate[73]
P.07.03.03 Condurre il Recupero Immediato del Personale
P.07.03.04 Condurre il Recupero Pianificato del Personale
P.07.03.05 Condurre il Recupero del Personale non militare
P.07.03.06 Condurre il Recupero del Personale delle Forze per Operazioni Speciali
P.07.03 Supportare le attività di Ricerca e Salvataggio nell'ambito delle operazioni di Sicurezza in Patria

Tabella 10: Compiti Essenziali del Recupero del Personale (Personnel Recovery)

Il successo delle Operazioni di Recupero del personale dipende dall'attenzione che i *leader*, ai vari livelli, pongono nella pianificazione, preparazione e condotta di tali attività. Anche il reinserimento deve essere ben pianificato. L'informazione e l'assistenza durante tutto il processo delle operazioni, deve riguardare non solo il personale recuperato ma anche le rispettive famiglie. Il PR infine, viene condotto con procedure differenti a seconda che il personale da estrarre sia costituito da militari o da civili, addestrati o meno all'estrazione.

2.8.3 Forme di Protezione

2.8.3.1 Deterrenza

Non è possibile condurre azioni di deterrenza contro la minaccia di isolamento.

2.8.3.2 Prevenzione

Le attività e misure di prevenzione consistono nel tentativo di limitare al minimo la probabilità che il personale si trovi in situazioni d'isolamento. La prima azione utile

[73] Ad esempio, le azioni di Evasione e Fuga di personale catturato.

consiste nel limitare i movimenti e le attività all'essenziale per l'assolvimento della missione.

2.8.3.3 Sicurezza Attiva

Consiste in tutte le attività e misure attive prese per intervenire a favore del personale isolato. Tali misure includono tutte le funzioni operative. Ad esempio, l'uso del fuoco terrestre e/o aereo è spesso fondamentale per proteggere il personale in attesa di essere recuperato.

2.8.3.4 Difesa Passiva

La difesa passiva si esplica nell'utilizzo di misure e soprattutto mezzi ed equipaggiamenti idonei alla protezione del personale che deve essere recuperato.

2.8.3.5 Mitigazione

Il metodo principale per mitigare gli effetti connessi con l'isolamento del personale in operazioni consiste nel serio e motivato approntamento e preparazione pratica del personale. Le fasi di pianificazione e preparazione dell'operazione devono sempre includere, qualora esiste il rischio, il PR.

Figura 16: *Silhouette* e colore

Ulteriore strumento di mitigazione del pericolo è l'uso di dispositivi per il tracciamento della posizione delle forze. Ciò abilita una *Overall Picture* immediata e, conseguentemente, la prontezza di reazione all'evento tramite le procedure di PR stabilite.

Infine, la ridondanza dei sistemi di comunicazione, allarme e localizzazione, contribuisce ulteriormente a mitigare il pericolo. Tale ridondanza consente, anche in caso di malfunzionamento o perdita di collegamento, di poter localizzare le forze e intervenire con maggiore probabilità di successo.

2.9 EVITARE IL FUOCO FRATRICIDA (*FRATRICIDE AVOIDANCE*)

Il fratricidio è l'uccisione o il ferimento involontario di forze amiche o neutrali attraverso il fuoco amico. Il potere distruttivo e la portata delle armi moderne,

insieme all'alta intensità ed il ritmo incalzante del combattimento, aumentano le possibilitàdi fratricidio, il cui verificarsi è legato anche alla manovra tattica, al terreno e alle condizioni meteorologiche.

Il fratricidio è accidentale ed è solitamente il prodotto finale di un errore di un *leader* o di un soldato. La conoscenza, attraverso lo scambio d'informazioni accurate, circa le posizioni e le attività in corso delle forze amiche, neutrali e nemiche, nonché un dettagliato piano di gestione dello spazio aereo, supportano i Comandanti a ridurre il rischio di fratricidio. A tal riguardo, i *Liaison Officer* (LNO) rivestono un ruolo molto importante poiché, grazie al loro contributo, soprattutto in termini di conoscenza dell'intento e della visione dei comandanti, favoriscono il *situational awareness* nelle condizioni più difficili e incremento l'interoperabilità tra i reparti. Inoltre, anche il contributo dei *leader* e dei singoli soldati è importante: ad esempio essi devono conoscere la gittata dei propri sistemi d'arma e gli effetti del munizionamento in dotazione al fine di evitare danni collaterale o eccessivi, inclusi quelli causati dai colpi di ricaduta.

I Comandanti e i *leader* sono i primi responsabili nel prevenire il fratricidio. Essi devono gestire lo specifico rischio riducendo la probabilità che l'evento si verifichi (senza intaccare il coraggio e la mentalità offensiva dei uomini) attraverso un'efficace *leadership*, un attento controllo delle proprie armi e del relativo stato, del movimento delle unità e, non ultimo, attraverso lo sviluppo di disciplinate procedure operative.

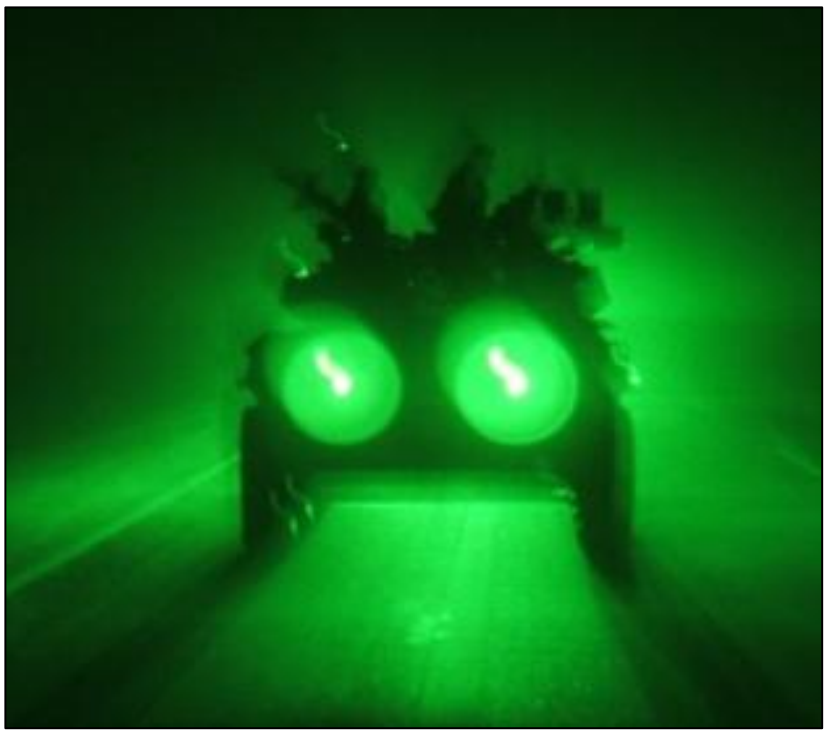


Figura 17: *Silhouette* e luce

La pratica insegna che il rischio di fratricidio diminuisce laddove i soldati possono agire con prontezza, decisione e organizzazione, senza il timore di essere colpiti dal fuoco delle forze amiche. La conoscenza dei reparti e degli uomini, l'addestremento e la preparazione alle operazioni solo essenziali. Le reazioni negative dei *leader* e dei soldati, vittime di incidenti di fuoco amico, si materializzano solitamente, nella perdita di fiducia nei superiori e colleghi, nell'esitazione, nell'eccessiva prudenza e nella perdita d'iniziativa.

Al fine di evitare il fratricidio, pertanto, si ricorre solitamente ad una strategia di protezione che enfatizza la prevenzione centrata su aree fondamentali che sono:

- ***situational awareness***: è l'immediata conoscenza dello stato dell'operazione e dei vincoli geografici e temporali. Essa include la consapevolezza della propria posizione, di quella delle forze amiche e nemiche nella propria AO, nonché le loro attività ed intenzioni;
- **identificazione del *target***: consiste nell'accurata e tempestiva descrizione di un oggetto individuato sul campo come amico, nemico, neutrale o sconosciuto. Quest'ultimo di norma non deve essere ingaggiato, fatta eccezione per la *Weapon Free Zone* (WFZ)[74] dove può essere fatto oggetto di fuoco tutto ciò che non è identificato come amico.

P.08 Evitare il Fuoco Fratricida (*Fratricide Avoidance*)
P.08.01 Individuare e stabilire procedure positive di riconoscimento di amici, nemici e non combattenti
P.08.01.01 Rilevamento dei *Target*
P.08.01.02 Decidere se combattere il *Target*
P.08.01.03 Combattere i *Target* ostili
P.08.01.04 Valutare gli effetti dei combattimenti
P.08.02 Mantenere aggiornata la situazione operativa

Tabella 11: Compiti Essenziali per Evitare il Fuoco Fratricida

2.9.3.1 Deterrenza

Non è possibile condurre azioni di deterrenza contro il pericolo di fratricidio.

2.9.3.2 Prevenzione

La prevenzione è la forma più importante di protezione per evitare il fuoco fratricida. Ciò è possibile principalmente attraverso il continuo aggiornamento della situazione, in particolare il posizionamento delle forze, l'individuazione e l'attuazione di procedure positive di riconoscimento di amici, nemici e non combattenti.

Non va tuttavia tralasciata l'importanza fondamentale della preparazione, dell'addestramento e della preparazione fisica delle forze. L'implementazione delle procedure appena citate è praticabile solo laddove esistano soldati preparati a fare il proprio mestiere, in particolare ad usare e maneggiare correttamente le armi. A tale fine, i seguenti elementi sono essenziali per gestire il rischio di fuoco fratricida: maneggio, stato di controllo delle armi (cfr. para 2.2.3.3), ROE, procedure a bordo di mezzi e di stazionamento, procedure di controllo, procedure di riconoscimento delle truppe amiche.

[74] Porzione di spazio aereo definita al fine di assicurare la massima protezione contraerea a dispositivi terrestri di vitale importanza.

Infine, come anticipato, anche l'aspetto psicologico e morale del combattente hanno un impatto determinante sulla gestione del pericolo in argomento.

In ogni caso, l'azione dei leader è fondamentale, a tutti i livelli. Essi devono essere preparati e capaci di prendere immediate decisioni per prevenire, ove possibile, il verificarsi del pericolo.

2.9.3.3 Sicurezza Attiva

Non è possibile condurre azioni di sicurezza attiva contro il pericolo di fratricidio.

2.9.3.4 Difesa Passiva

La difesa passiva consiste nel condurre le stesse azione e misure già illustrate nel compito *Survivability*, indirizzate in questo caso alla protezione dalla minaccia di fuoco amico. Quindi ad esempio la realizzazione di muri di protezione in prossimità dei posti scaricamento armi o l'utilizzo di equipaggiamento anti proiettile.

2.9.3.5 Mitigazione

Consiste principalmente nel definire le reazioni alle situazioni in cui si verifica un incidente. Include, ove possibile, il pronto intervento di assetti sanitari e l'eventuale sgombero del personale coinvolto.

2.10 *INFORMATION PROTECTION*

Consiste nell'insieme delle misure attive e passive adottate al fine di proteggere le informazioni e i sistemi connessi, garantirne l'usabilità e negarne l'acquisizione e il successivo sfruttamento da parte dell'avversario o di possibili avversari.

2.10.1 Minaccia e rischi

L'ampio ricorso all'*Information Technology* (IT), particolarmente utile per velocizzare e rendere più efficaci processi e sistemi, porta con sé un incremento della vulnerabilità connessa agli attacchi mediante i seguenti vettori:

- accesso non autorizzato;
- *malicious software*;
- inganno elettromagnetico;
- attacco elettronico;
- distruzione fisica;
- propaganda.

2.10.2 Compiti essenziali

La *Information Protection* si sviluppa sulla base dei seguenti tre elementi:

- *Electronic Protection*;
- *Computer Network Defence* (CND);
- *Information Assurance.*

2.10.2.1 *Information Assurance*

Consiste nella pianificazione, messa in atto e condotta di programmi e procedure idonee per proteggere le informazioni e i relativi sistemi, allo scopo di tutelarne:

- disponibilità: accesso sicuro a informazioni e servizi da parte di utenti autorizzati;
- integrità: protezione da cambiamenti non autorizzati, inclusa la distruzione;
- autenticazione: certezza degli utenti o l'identificazione dei destinatari e l'autorizzazione a ricevere specifiche categorie di informazione;
- tutela dell'informazione: protezione dalla rivelazione non autorizzata;
- non ripudio: la prova dell'avvenuta ricezione del messaggio e l'identificazione del mittente così che nessuno possa mainegare di aver elaborato l'informazione.

L'*information assurance* protegge tutte le reti, i sistemi d'informazione, i *computer*, gli apparati radio, la realizzazione di infrastrutture, le porte, i *router* e gli *switch*.

2.10.2.2 *Computer Network Defense* (CND)

La CND comprende tutte le misure e azioni condotte contro le attività non autorizzate contro nelle reti di *computer*. Include le attività di monitoraggio, individuazione, risposta e ripristino. Queste attività sono condotte attraverso varie discipline o branche tra le quali Operazioni, *Intelligence*, *Counter-intelligence*, Amministrazione di reti.

2.10.2.3 *Electronic Protection*

Consiste nella pianificazione e nella condotta delle azioni e misure[75] volte a proteggere il personale, le strutture e l'equipaggiamento dagli effetti prodotti dalla Guerra Elettronica (*Electronic Warfare* – EW). Si mira quindi a minimizzare la possibilità che le azioni elettromagnetiche condotte dalle forze ostili, e involontariamente anche le proprie, possano degradare, neutralizzare o distruggere le informazioni in possesso delle forze amiche.

P.09 *Information Protection*
P.09.01 *Information Assurance*
P.09.01.01 *Information Security* (INFOSEC)
P.09.01.01 *Communications Security* (COMSEC)
P.09.01.01 *Emission Security*
P.09.02 *Computer Netwoek Defense* (CND)
P.09.03 *Electronic Protection*

Tabella 12: Compiti Essenziali per *Information Protection*

[75] Ad esempio la Negazione delle Comunicazioni o le Misure di Comunicazioni Anti-Jamming.

2.10.3 Forme di Protezione

In generale, la protezione interna ed esterna evita che utenti o dati sconosciuti o non autorizzati entrino nelle reti. Le attività di protezione dall'esterno includono la sicurezza delle comunicazioni (COMSEC), *Router Filtering*, *Acces Control List* e *Security Guards*. Quando necessario le unità isolano o posizionano fisicamente delle barriere tra le reti protette e quelle non protette. La protezione della rete interna consiste nell'utilizzo di *Firewall* e *Router Filters* che costituiscono delle vere e proprie barriere all'interno delle comunità (*communities*).

2.10.3.1 Deterrenza

La pianificazione e la condotta di *Information Activities* consentono di influenzare possibili azioni ostili anche nell'ambito IT. In particolare, la disponibilità di tecnologia e *software* avanzati, scoraggia male intenzionati dal tentare azioni contro la forza.

2.10.3.2 Prevenzione

La prevenzione, basata sulla formazione, la condivisione e la consapevolezza di quanto i comportamenti e il rispetto delle procedure siano fondamentali per proteggere le Informazioni da ogni tipo di minaccia e rischio.

Inoltre, tra le misure di COMSEC rientrano quelle connesse con il rispetto delle distanze dalle

2.10.3.3 Sicurezza Attiva

Le misure attive di protezione delle informazioni consistono in quelle misure che abilitano la protezione e la reazione fino al contrattacco contro le minacce rivolte alle informazioni e ai sistemi delle informazioni. Ad esempio *Jammers* o software capace di individuare e colpire le minacce.

2.10.3.4 Difesa Passiva

Le misure passive di protezione riguardano le operazioni quotidiane e hanno un impatto diretto sugli utenti; sono concepite per nascondere o vietare la consultazione delle informazioni, proteggerle da modifiche o da distruzioni non autorizzate. Le misure includono l'implementazione dei controlli sull'accesso, sulle applicazioni di sicurezza, sulla sicurezza fisica, sulle istruzioni alla sicurezza delle comunicazioni e della rete, sullo schermo delle emissioni. Tutte queste misure passive devono essere standardizzate a livello delle unità. Tuttavia, sebbene attentamente concepite e implementate, le misure passive non garantiscono la totale protezione delle informazioni ma si limitano a ridurne i rischi.

2.10.3.5 Mitigazione

Le principali forme di mitigazioni consistono nel disporre e poter mettere in atto delle procedure idonee a mitigare gli effetti di un possibile attacco, limitandone gli effetti e salvaguardando quante più informazioni possibili.

2.11 PROTEZIONE SANITARIA (*HEALTH PROTECTION*)

Per Protezione Sanitaria s'intendono tutte le misure e le azioni prese dai Comandanti, dai *leader*, dai soldati e dal sistema Sanitario Militare per promuovere, migliorare e conservare il benessere fisico e comportamentale dei soldati. Tale concetto di Protezione Sanitaria non va confuso esclusivamente con le attività condotte dal Corpo di Sanità e Veterinaria dell'Esercito, benché questo rappresenti senza dubbio l'organizzazione con la maggior parte delle capacità specialistiche ed essenziali per garantire livelli di protezione adeguati alle moderne esigenze.

Lo sviluppo di un efficace sistema di protezione sanitaria necessita della definizione e messa in atto di veri e propri programmi che promuovano lo sviluppo della capacità da parte di tutto il personale, prescindendo dalla funzione, dal grado e dalla posizione ricoperta, di assolvere i propri compiti in condizioni difficili, mutevoli, con prontezza e per periodi di tempo anche considerevoli.

2.11.1 Minaccia e rischi

L'indebolimento della salute fisica e psichica del personale, con la conseguente perdita, temporanea o permanente, della capacità di combattere o comunque operare, rappresenta una minaccia sempre presente, non solo nelle operazioni di combattimento, da contrastare con vigore, utilizzando tutte le risorse necessarie. Essere in salute è un requisito imprescindibile per qualsiasi soldato. Non esiste ambito più appropriato per la locuzione latina del Giovenale: ***mens sana in corpore sano***. Nell'Esercito questo è un *must* che va messo in pratica senza esitazione e rappresenta, a livello individuale, a qualsiasi età e grado, la prima e la più importante misura di protezione sanitaria.

2.11.2 Compiti essenziali

Per contrastare la specifica minaccia, è necessario che i Comandanti e i *leader* a tutti i livelli siano pienamente consapevoli della sua natura. Stessa consapevolezza deve essere acquisita da tutto il personale che deve essere edotto e apprendere come perseguire e mantenere uno stato di benessere psico-fisico adeguato e, di conseguenza, una condizione di piena operatività.

Tra i compiti fondamentali connessi con la Protezione Santiaria, i seguenti sono i principali:

- **Servizi di Medicina Preventiva**

  È essenzialmente finalizzata a prevenire malattie e ferite non da combattimento, dalla vita in guarnigione al dispiegamento, al combattimento, sino al rientro in base. Il personale sanitario provvede, nell'AoO, a monitorare le malattie e a condurre attività preventive quali, *screening*, immunizzazioni e profilassi sanitari, nonché a fornire *Subject Matter Expert* – SME in caso di esposizione a forti rumori, *Toxic Industrial Material* – TIM e condizioni climatiche estreme.

- **Controllo/Monitoraggio/Sorveglianza Medica (*Medical Surveillance*)**

  Consiste nella raccolta sistematica e continua, nell'analisi e nell'interpretazione dei dati derivanti dalle richieste di cure mediche e dalle valutazioni mediche. La sorveglianza medica è fondamentale per la pianificazione, l'attuazione e la valutazione dei problemi sanitari pubblici. Questa attività rappresenta un valido strumento per supportare l'azione dei Comandante che, sulla base dell'analisi di tutti questi dati, può gestire con maggiore efficacia i rischi di natura sanitaria che contraddistinguono la propria AoO.
- **Controllo/Monitoraggio/Sorveglianza dell'igiene nell'AoO (*Environmental Health Surveillance*)**

  Si esplica nella sistematica raccolta, analisi, archiviazione, interpretazione e disseminazione delle informazioni relative all'igiene. Ciò al fine di monitorare ogni singolo individuo e poter intervenire tempestivamente per prevenire, trattare o controllare le malattie o le ferite. Tali attività vanno inserite in un processo continuo.
- **Servizio Veterinario**

  Il *focus* del Servizio è il cibo e gli animali. Nella fattispecie, esso è responsabile della verifica della qualità del cibo durante tutte le fasi di approvvigionamento, conservazione e distribuzione, dell'assistenza medica ai cani militari e, seppure in maniera limitata, agli animali locali presenti nell'AoO. Include, inoltre, le attività di medicina veterinaria preventiva, nonché il supporto alle attività investigative su eventuali morti inspiegabili di bestiame nell'AoO.
- **Controllo dello *stress* Operazionale[76] e da Combattimento**

  Le unità specializzate della "salute mentale", conducono le proprie attività a supporto dei reparti attraverso la condotta di programmi finalizzati alla prevenzione, consultazione, formazione, istruzione e recupero dei soldati soggetti a questo tipo di *stress*. Questi programmi sono rivolti ai *leader* e ai soldati che sono sottoposti ad un prolungato e pesante *stress* da combattimento. Lo scopo principale di queste attività è quello di reintegrare in maniera definitiva ed efficace, stilando un accurato rapporto su quelle che sono le condizioni e la diagnosi dei loro comportamenti.
- **Servizi Medici di Laboratorio (*Medical Laboratory Service*)**

  Le unità mediche preposte a questi servizi si occupano di identificare e valutare tutti i rischi sanitari connessi all'ambiente e all'impiego delle unità. Nella fattispecie, conducono test di laboratorio su agenti biologici e chimici e su malattie endemiche e zoonotiche.

[76] Si è qui utilizzato il termine "Operazionale" per distinguerlo da quello "Operativo" che potrebbe essere confuzo col secondo. Il primo si riferisce al fare le cose, il secondo a quello specifico degli effetti dovuti al combattimento vero e proprio.

- **Odontoiatria Preventiva**

  È finalizzata a ridurre o eliminare condizioni sanitarie che possano infierire sullo stato di salute dei soldati, limitandone o impedendone l'impiego, condizionandone l'assolvimento della missione. Quest'attività deve essere condotta, secondo un programma specifico, prima e durante dell'impiego del militare in operazioni, in particolare in quelle di lunga durata e laddove non vi sia la possibilità d'intervenire in caso di necessità. Tale attività è necessariamente condotta in fase di *predeployment*.

P.10 Protezione Sanitaria (*Health Security*)
P.10.01 Fornire medicina preventiva
P.10.01.01 Condurre Sorveglianza Medica (*Medical Surveillance*)
P.10.01.02 Condurre Sorveglianza Sanitaria (*Health Surveillance*) occupazionale e ambientale
P.10.02 Fornire servizi veterinari
P.10.03 Fornire servizi di prevenzione dello *Stress* da Combattimento e da partecipazione a Operazioni
P.10.04 Fornire servizi di Odontoiatria preventiva
P.10.05 Fornire servizi di Laboratorio Analisi a favore per valutare i pericoli incidenti l'AoO

Tabella 13: Compiti Essenziali della Protezione Sanitaria (*Health Protection*)

2.11.3 FORME DI PROTEZIONE

L'intero concetto di Protezione Sanitaria si basa sulla Prevenzione. Non esistono altre forme di Protezione ad essa connessa poiché si ricadrebbe nel trattamento o comunque nel supporto Sanitario e Veterinario di altro genere. Ma questi sono compiti e attività tipiche della Funzione Operativa Sostegno Logistico, non della Protezione.

Disporre di personale in salute e in efficienza psico-fisica, quindi di un'adeguata componente fisica del *fighting power*, è un obiettivo da perseguire di valore strategico per l'Esercito.

È importante diffondere il concetto che per conseguire tale obiettivo non è necessario investire ingenti risorse finanziarie quanto piuttosto impegnarsi sistematicamente per accrescere la cultura del benessere e della sicurezza fisica (*Health and Safety culture*) che deve invece al più presto divenire solido patrimonio culturale di tutti gli appartenenti alla Forza Armata.

Tuttavia, questo approccio non può avere un effetto immediato. Necessita tempo, condivisione d'intenti e perseveranza. Una volta in atto però è assolutamente efficace e rafforza l'abilità e le capacità di ciascuno di adottare comportamenti salutari ed esercitare, soprattutto se in un contesto di gruppo, un efficace controllo sui

determinanti della salute: il così detto *empowerment.* Tale termine, introdotto negli anni sessanta nell'ambito degli studi sulla psicologia delle comunità, definisce il processo attraverso il quale le persone acquisiscono controllo sulla propria vita e sul proprio contesto ambientale determinando un miglioramento delle proprie condizioni psico-fisiche e di *performance.*

A carattere generale, le attività fondamentali sono:

- esercizio fisico funzionale e programmato;
- corretta dieta alimentare;
- igiene dentale;
- sviluppo della capacità di gestione dello *stress*;
- riposo.

La chiave di tutte queste attività, siano esse 59lusivamente preventive o protettive, è l'informazione. L'informazione deve essere condivisa prima dell'impiego delle forze in un determinato ambiente operativo, comprendendo e analizzando come esso può influenzare direttamente o indirettamente l'operato dei militari. A tal riguardo, è determinante il ruolo della *Medical Intelligence* – MEDINT e della *Health Surveillance* che deve indirizzare la ricerca e raccolta di informazioni verso l'ambiente operativo. Il servizio sanitario fornisce un supporto capace di acquisire, immagazzinare, muovere e fornire informazioni che tempestivamente devono essere messe a disposizione degli utenti dopo averne verificato l'accuratezza, la rilevanza e l'utilità.

Figura 18: Addestramento Soccorritore Militare

Le attività e le misure preventive da attuare sono:

- programmi di promozione della salute rivolti a tutto il personale attraverso specifiche campagne che mirino a indirizzare verso corretti stili di vita (abolizione del fumo di tabacco, riduzione dell'uso di alcol, lotta alla sedentarietà, disciplina della condizione psicofisica e incentivazione ad una corretta alimentazione);
- diagnosi precoce di malattie prevenibili (dosaggio periodico della colesterolemia, misurazione periodica della pressione arteriosa, ricerca del sangue occulto nelle feci, dosaggio del PSA negli uomini, mammografia e *pap test* nelle donne);
- informazione e formazione del personale sulla tutela della propria salute e sicurezza nei luoghi di lavoro;
- campagne di vaccinazione del personale per prevenire malattie da agenti biologici specifici presenti sia in patria che nei vari T.O.;
- valutare tutti i rischi per la salute e la sicurezza del personale presenti nei luoghi di lavoro ed elaborare e aggiornare di continuo i Documenti di Valutazione dei Rischi;
- attenta selezione fisico-psico-attitudinale del personale nelle fasi concorsuali per individuare ed escludere eventuali individui ipersuscettibili;
- rigorosa applicazione delle direttive di Forza Armata sull'idoneità al servizio militare incondizionato nelle condizioni di eccesso ponderale;
- visite mediche periodiche del personale per verificare il mantenimento dell'idoneità psico-fisica al servizio militare incondizionato;
- sorveglianza sanitaria preventiva e periodica del personale esposto a rischi lavorativi specifici;
- corretto uso delle attrezzature e dei dispositivi destinati a essere utilizzati e/o indossati dal personale, in maniera collettiva o individuale, allo scopo di proteggerli da rischi specifici in grado di minacciarne la sicurezza o la salute;
- corretta gestione delle strutture adibite al confezionamento e alla somministrazione di alimenti finalizzata a ridurre il rischio di malattie oro-fecali trasmesse con gli alimenti che, se insorgono, potrebbero rendere non operativa un'intera comunità servita da tali strutture;
- somministrazione nelle mense di alimenti sani incrementando ad esempio le quantità di frutta e verdura e riducendo gli alimenti di origine animale;
- programmi di promozione della odontoiatria preventiva. Consistono in attività, semplici, economiche, facilmente attuabili e che non necessitano la presenza di specialisti presso ciascun reparto. Consistono principalmente nell'informare e monitorare l'uso di una corretta alimentazione e un'accurata igiene orale.

2.12 *SAFETY*

2.12.1 Minaccia e rischi

La sicurezza "fisica" è un dovere e riguarda lo svolgimento di tutte le operazioni militari, non solo le attività svolte in guarnigione. Deve essere chiaro al lettore,

tuttavia, che la sicurezza "fisica" del soldato e l'attenzione che va posta alla problematica da parte di tutti, non sono connesse esclusivamente a regolamentazioni nazionali in materia di lavoro, ma sono, prima di tutto, **un dovere morale e professionale che ogni Comandante e *leader* deve sentire** per due motivi fondamentali:

- è suo dovere prendersi cura dei propri soldati;
- è sua responsabilità garantire e mantenere elevato il Potere di Combattimento della propria unità al fine di portare a compimento la missione ricevuta.

Tuttavia, le operazioni militari sono rischiose per loro stessa natura. Il concetto espresso mira pertanto a diffondere la filosofia della **assunzione prudente dei rischi**. I rischi vengono assunti da parte dei Comandanti e dei *leader* perché ritenuti necessari per l'assolvimento della missione ricevuta, in linea con l'intento del Comandante, nel rispetto dei vincoli e dei regolamenti, a seguito del processo di CRM che include sempre la *safety*. Ciò significa che fa parte dell'essere soldati correre dei rischi. Quello che non è accettabile è ignorarli e non gestirli in maniera responsabile per minimizzarli.

Figura 19: Attività Addestrativa Funzionale

La normativa nazionale di settore si applica in tutti i luoghi e a tutte le attività svolte nell'ambito dell'Esercito e, di conseguenza, anche alle operazioni. Pertanto, il *modus operandi* dei Comandanti deve tendere all'osservanza della normativa prevenzionale generale e, come consentito dal legislatore, delle norme speciali di tutela tecnico-militare che regolano le esigenze connesse alla specificità della professione militare e, in particolare, alle operazioni.

Anche in considerazione del fatto che il processo di valutazione dei rischi infortunistici è per sua natura un procedimento iterativo, teso ad intervenire costantemente per il continuo miglioramento dei livelli di sicurezza e di tutela del personale dipendente, ciascun Comandante, a tutti i livelli gerarchici, ha il diritto/dovere di farsi promotore

dell'eventuale aggiornamento dei documenti posti a supporto di detta valutazione. Lo scopo di tale valutazione non deve essere la verifica dell'applicazione delle prescrizioni di legge, quanto piuttosto la ricerca di tutti quei rischi residui che rimangono in essere nonostante l'applicazione delle normative di settore. Ogni rischio andrà poi valutato tenendo conto del danno che da esso ne può conseguire e della relativa probabilità di accadimento.

Figura 20: Passaggio di Paracadutisti pronti per il lancio

La valutazione dei rischi viene posta in relazione alle caratteristiche dei luoghi di previsto impiego, alle esigenze da soddisfare, ai compiti specifici da assolvere e alla capacità operativa dell'unità in operazione.

L'Esercito deve oggi confrontarsi con i profondi mutamenti intervenuti nel quadro strategico mondiale che lo hanno proiettato in uno scenario di sicurezza che presenta nuove minacce e sfide che si sviluppano, oltre che sul territorio nazionale, anche in aree e regioni diverse, spesso molto diverse tra di loro. Tali sfide, oltre a nuove tecnologie, richiedono ai Comandanti di adottare misure in grado di fornire una protezione sempre più efficace per il patrimonio umano posto alle loro dipendenze.

In particolare, il concetto di Protezione, *Safety* incluso, deve costituire un elemento routinario della pianificazione, preparazione e condotta delle operazioni, così come per l'attività addestrativa e per quella svolta all'interno delle sedi stanziali. Lo scopo,

come detto, è il contenimento dei rischi derivanti da pericoli che potenzialmente possono ridurre la capacità operativa e, di conseguenza, avere un impatto negativo sulla missione. In fase di pianificazione, dunque, la valutazione del rischio connesso al possibile confronto con il nemico non deve essere disgiunta da quella del cosiddetto "rischio infortunistico", poiché, in ambito operativo, entrambi potrebbero inficiare l'efficienza dell'unità chiamata a svolgere un determinato compito.

L'approccio composito proposto ha come assunto che il processo di valutazione e di gestione del rischio antinfortunistico deve essere inteso quale parte integrante del Processo Decisionale Militare. La conoscenza del rischio infortunistico, in sintesi, è di fondamentale importanza per il processo decisionale dei Comandanti. Il CRM non deve essere visto come un processo autonomo o, peggio, come una formalità burocratica quanto, piuttosto, come un elemento di pianificazione integrata.

I rischi non sono un qualcosa di avulso dal contesto in cui le unità operano. Il CRM è un processo di *routine* che, includendo la sicurezza fisica del personale.

La responsabilità del *Safety* non ricade solo sui Comandanti, ma anche sullo *staff* e tutta la catena di comando, finendo con i singoli soldati. La sicurezza fisica è una responsabilità ma anche un compito che, per essere assolto nel migliore dei modi, deve prevedere una informazione, formazione e un addestramento specifico da parte di tutti i *leader* e i soldati nel riconoscere i rischi ed effettuare controlli, anche in autonomia, al fine di ridurre o mitigare i rischi connessi con le varie attività militari.

Lo *staff* specializzato, ove previsto:

- assiste i Comandanti, valutando tutti i problemi connessi alla sicurezza ed informandoli sulla situazione;
- mantiene uno stretto rapporto con la cellula preposta alla protezione;
- si muove all'interno dell'intera AO;
- fornisce consulenza e assistenza tecnica ai leaders e ai responsabili della pianificazione che sviluppano e attuano i programmi, piani, ordini e le SOP relative alla sicurezza.

2.12.2 Compiti essenziali

P.11 Sicurezza Fisica (*Safety*)
P.11.01 Condurre la Valutazione del Rischio Composito (CRM)
P.11.02 Sviluppare e mettere in atto i piani di Sicurezza Fisica
P.11.03 Minimizzare i Rischi connessi con la Sicurezza Fisica

Tabella 14: Compiti Essenziali della Sicurezza Fisica (Safety)

2.12.3 Forme di Protezione

2.12.3.1 Deterrenza

L'unica azione di deterrenza conducibile dai Comandanti è quella di dare alla questione *Safety* la necessaria importanza e prendere seri provvedimenti nei

confronti di coloro che mettono a rischio la sicurezza fisica e la salute propria e degli altri.

2.12.3.2 Prevenzione

La Prevenzione, come detto, è la forma di Protezione principale, quella fondamentale per ridurre al minimo la probabilità d'infortunio. L'efficacia della prevenzione, in particolare della formazione, si base sulla continuità nelle azioni tese ad informare i soldati. Tale attività deve essere condotta in modo coinvolgente, specifico e professionale. Nella pratica è fondamentale illustrare i rischi connessi con le specifiche attività militari, sportive e anche d'ufficio che ciascun soldato conduce. È pressoché inutile invece spiegare in modo burocratico le leggi che in alcun modo proteggono i militari e i civili in forza all'Esercito.

2.12.3.3 Sicurezza Attiva

Non ci sono attività del genere che contribuiscono ad aumentare il *Safety*.

2.12.3.4 Difesa Passiva

Tale forma di Protezione è molto importante e consiste nell'utilizzo dei Dispositivi necessari a ridurre i rischi. In guarnigione, si tratta degli stessi dispositivi previsti dalla vigente normativa. In Operazione, si pensi all'importanza degli occhiali balisti per tutti i tiratori, dei guanti, delle ginocchiere per andare a terra. Peraltro, tanto più l'attività è ardimentosa tanto più si sente la necessità di protezione. Il concetto è ben noto a Paracadutisti e Alpini che da sempre fanno della protezione individuale un criterio fondamentale per qualsiasi operazione.

2.12.3.5 Mitigazione

In ultimo, ma non in termini di importanza, anche la Mitigazione rappresenta una forma di Protezione fondamentale. Si pensi all'importanza delle procedure connesse con i comportamenti da tenere e le reazioni da condurre al verificarsi di incidenti.

3. LA PROTEZIONE DELLE OPERAZIONI TERRESTRI

3.1 LA PIANIFICAZIONE

Al livello operativo delle operazioni, Comandanti e *Leader* pianificano come utilizzare la Forza Militare disponibile e il *Combat Power* da generare e proiettare per assolvere la missione. Sulla scorta di come comprendono e visualizzano l'AO, essi sviluppano dei concetti operativi (CONOPS) che includono l'uso del Potere Terrestre. Attraverso l'utilizzo dell'Arte e della Scienza Militare, vengono definiti gli obiettivi e, conseguentemente, individuate le esigenze, in particolare quelle critiche, in termini di protezione. Porti, aree geografiche, aeroporti o zone lancio costituiscono spesso punti decisivi che sono pianificati e poi utilizzati per la loro specifica caratteristica di fornire un certo grado di protezione della Forza, della Missione o del Centro di Gravità. Conseguentemente, gli elementi del *Combat Power* vengono organizzati, le attività sincronizzate, le capacità combinate o usate in modo complemenre in funzione dello spazio e del tempo. Le capacità *Joint*, si pensi ad esempio alla disponibilità di fuoco di supporto aereo o navale, possono contribuire a ridurre ulteriormente i rischi e a incrementare la Protezione.

Al livello tattico delle operazioni, le AoO sono definite e assegnate sulla base del METT-TC e, in particolare, delle capacià delle unità. I confini, le restrizioni per il controllo del fuoco e le misure di controllo grafico aiutano a definire zone d'azione, combattimento (*Engagement Area* – EA) e annientamento (*Kill Zone*) che aiutano i Comandanti a ridurre i rischi di fratricidio e danni collaterali. Le ROE, i sistemi d'allarme e il controllo dello stato delle armi proteggono la Forza e la popolazione mediante l'applicazione controllata di azioni letali e non-letali. A tale fine, ai comandanti vengono spesso assegnati, anche in modo automatico[77], autorità e livelli di comando addizionali, ad esempio il Controllo Tattico (*Tactical Control* – TACON), al fine di garantire la sincronizzazione di tutti gli elementi operanti all'interno o in prossimità dell'AOO. Tale sincronizzazione è indispensabile per assicurare un'elevata capacità di reazione, di difesa e di protezione.

3.2 LE OPERAZIONI DI SICUREZZA (*SECURITY OPERATIONS*)

Il metodo più comune per proteggere le Operazioni Terrestri consiste nella condotta delle Operazioni di Sicurezza. Le Operazioni di Sicurezza sono rilevanti per tutte le operazioni militari e hanno lo scopo, elemento che le accomuna e le categorizza, di

[77] Esempio classico di procedura che prevede l'assegnazione automatica del TACON è il passaggio di linea e la sostituzione di truppe a contatto. Durante il periodo necessario al transito nell'AOO dell'unità che deve essere superata o sostituita, l'unità è automaticamente sotto TACON. All'atto del superamento della linea di riferimento, normalmente una *Phase Line* (PL), o finchè non avviene il cambio di autorità (*Transfer Of Authority* – TOA). Il TACON si rende necessario poiché l'unità avanzata o a contatto deve coordinare la circolazione e il fuoco nell'AOO.

proteggere la Forza dalle operazioni nemiche e di ridurre i rischi connessi con l'ignoto e con la sorpresa ostile. Dottrinalmente, le Operazioni di Sicurezza sono:

- Copertura (*Cover*);
- Guardia (*Guard*);
- Schermo (*Screen*);
- Sicurezza areale (*Area Security*);
- Sicurezza locale (*Local Security*).

La portata delle Operazioni di Copertura, Guardia e Schermo dipende molto dal livello di *Combat Power* che può essere applicato alla protezione ed è funzione del METT-TC. Inoltre. In tale ottica, la presenza di forze amiche, ad esempio operanti su un fianco, o la disponibilità di assetti tecnologici per la sorveglianza di ampi spazi sono elementi fondamentali da considerare per decidere dov'è più remunerativo gravitare con le attività di protezione.

In generale, le Operazioni di Guardia e Copertura hanno lo scopo di guadagnare tempo mediante la condotta di azioni di combattimento. Pertanto, esse vengono preparate per condurre attività tattiche difensive, tipicamente di difesa mobile, e dotate di adeguate capacità e autonomia. Le Operazioni di Schermo, invece, mirano prioritariamente ad allertare la Forza il più presto possibile, prevenendo possibili sorprese e azioni ostili (vedi Figura 22: Schermo). Va da se che, tutte le le Operazione di Sicurezza appena descritte, sono fortemente caratterizzate dalla condotta di ricognizioni.

3.2.1 Copertura

La Forza di Copertura è utilizzata per ridurre l'incertezza e l'ignoto tipici del combattimento, ottenere e mantenere il contatto con le forze nemiche e allertare il Grosso della Forza (*Main Body*). Le attività della Forza di Copertura focalizzano sulla protezione del Grosso piuttosto che sul terreno o sugli obiettivi nemici.

La Forza di Copertura può operare a varie distanze dal Grosso, in funzione del METT-TC. I comandanti la impiegano come e dove ritenuto più opportuno: sul fronte, sui fianchi o sul tergo. La comunicazione tra la Copertura e il Grosso deve essere continua. Le informazioni acquisite vengono passate al Grosso e alle unità amiche il più presto possibile. Il Comandante del Grosso, da parte sua, si assicura che le Forze di Copertura ricevano tutto il supporto e i prodotti d'*Intelligence* disponibili.

Le capacità delle Forze di Copertura sono amplificate dalla disponibilità di sensori comandanti a distanza e radar di sorveglianza. Tuttavia, occorre considerare che tali ausili tecnologici sono a loro volta oggetto di attività di contro sorveglianza da parte delle forze ostili.

Le attività delle Forze di Copertura vengono di norma concentrate in corrispondenza delle probabili vie tattiche nemiche, le *Named Area of Interest* (NAI), *Target Area of Interest* (TAI) e delle aree dove la conformazione del terreno degrada la capacità di

scoperta e sorveglianza dei sensori. L'assenza di sensori e ausili tecnologici genera il ricorso a quantità maggiori di *Combat Power* da destinare alla Copertura.

Il successo delle Operazioni di Copertura si fonda sui seguenti quattro elementi:

- Dare l'allarme e intervenire il più rapidamente possibile;
- Focalizzare sulla Forza o sulle infrastrutture da proteggere;
- Ricognire continuamente;
- Mantenere il contatto col nemico.

La forza di copertura si compone almeno di due elementi con compiti differenti: Schermo e Guardia. Ciascuno fornisce una differente e crescente capacità d'intervento e di reazione per la protezione della Forza. Lo Schermo consiste in un minimo livello di *Combat Power* e ha esclusivamente il compito di mettere in allarme il resto della Forza. Normalmente interviene solo quando entra in contatto con elementi da ricognizione nemici di consistenza inferiore, conducendo una *couter-intelligence operation*. La Guardia invece, dispone di sufficiente *Combat Power* per intervenire su forze nemiche più consistenti per distruggerle o conterne l'azione.

Vale sempre il principio che, tanto più parte di *Combat Power* viene destinato alle Forze di Sicurezza, tanto minore sarà la Potenza residua disponibile per lo sforzo principale.

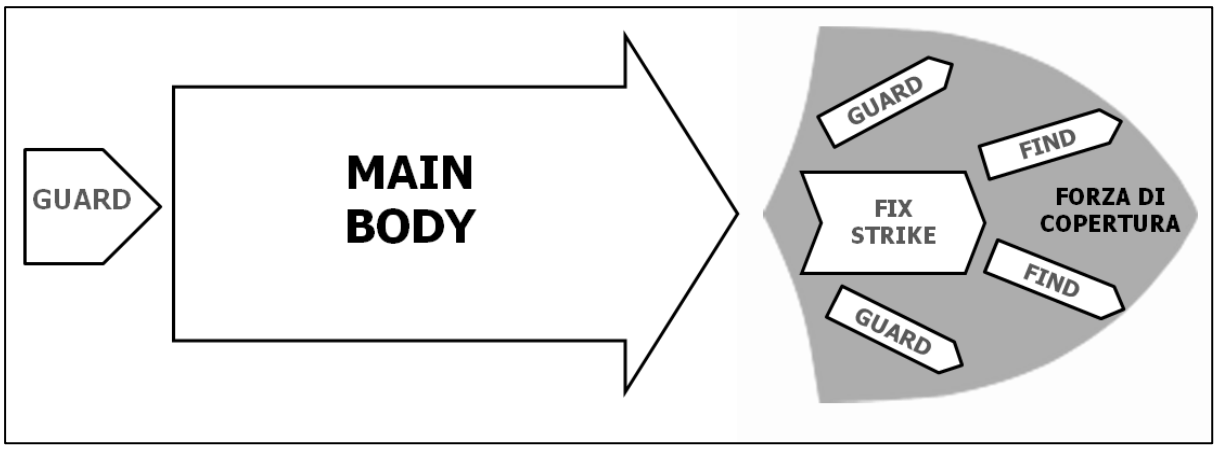


Figura 21: Effetti tipici degli elementi delle Forza di Copertura

Ulteriore principio fondamentale è che, ogni avanzata va guidata da una Forza di Copertura. Ciò prescinde dal livello ordinativo e dal *Combat Power* utilizzato. Gli elementi da ricognizione ne costituiscono, di norma, l'aliquota più avanzata. In tale contesto, la Forza di Copertura può ricevere i seguenti compiti:

- Localizzare e Definire le forze nemiche (Dislocazione, Entità, Natura, Atteggiamento e Movimento - DENAM);
- Trovare e sfruttare Gap;
- Ottenere informazioni sugli itinerari, ostacoli e terreno;

- Penetrare in profondità per disarticolare le linee di comunicazione e logistiche nemiche;
- Occupare punti o aree critiche (punti di attraversamento corsi d'acqua, ponti o gole);
- Sfruttare corridoio di mobilità alternativi;
- Condurre missioni contro unità nemiche sopravanzate;
- Fissare le forze nemiche;
- Proteggere i fianchi da attacchi.

3.2.2 Schermo

Lo Schermo è un elemento di sicurezza il cui compito fondamentale è osservare, identificare e riportare informazioni. Consiste principalmente nell'attività tattica di ricognizione vicina (*close reconnaissance*). Generalmente, lo Schermo combatte solo per auto-difesa ma può anche intervenire contro eventuali elementi da ricognizione ostili individuati, se ritenuto in grado di farlo. Di norma, i comandanti stabiliscono uno o più schermi in presenza di fianchi estesi, nelle retrovie, sulla fronte di una forza in movimento o in stazionamento. L'Operazione di Schermo consiste, essenzialmente, nello schieramento di Posti di Osservazione e Allarme (POA) o *Observation Point* (OP) che vengono posizionati lungo una linea di Schermo. Le Forze di Copertura, normalmente, conducono lo Schermo integrandolo con pattuglie che si muovono tra gli OP.

Lo Schermo condotto sul fianco di una Forza in movimento deve rimanere fisicamente legato al Grosso attraverso una serie di punti di contatto e di punti di coordinamento.

Il Comandante dello Schermo analizza il terreno circostante la linea di schermo assegnata utilizzando l'IPB. Egli poi stabilisce la linea di schermo dove vengono schierati gli OP e, cosa più importante, verifica che gli OP siano collocati in punti idonei all'osservazione, che i settori abbiano punti di saldatura con i contermini, onde evitare zone d'ombra e, possibilmente, ricerca la copertura e l'occultamento degli elementi schierati. La linea di schermo iniziale deve essere individuata in posizione che sia al contempo supportabile dal Grosso e sufficientemente lontana per dare

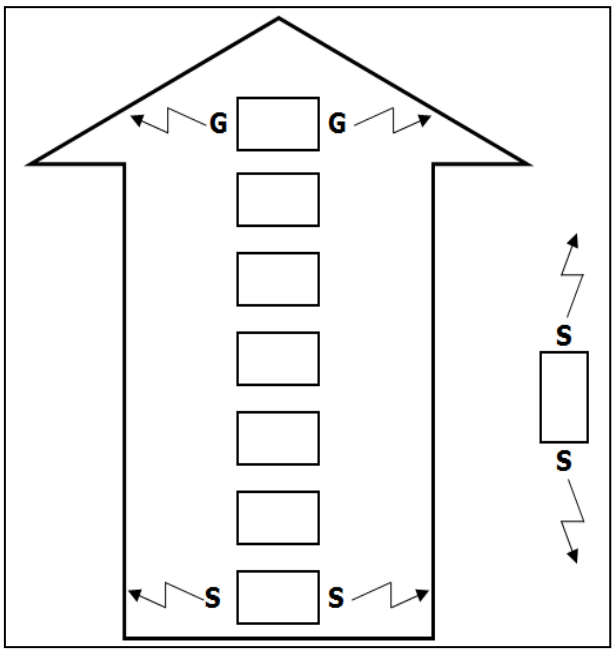


Figura 22: Schermo per una Forza in Movimento

l'allarme in tempo utile.

Il comandante di uno Schermo Mobile controlla il movimento nel settore assegnato designando successive linee di schermo come *Report Line* (RL). Il movimento a una successiva linea di schermoviene normalmente determinata dagli eventi, non da tempi prestabiliti. La temporizzazione, oltre a vincolare il *Mission Command* dei Comandanti, potrebbe mettere a rischio la missione dello Schermo che potrebbe essere costretto al contatto con forze nemiche.

3.2.2.1 Schermo Statico

Per Schermo Statico (*Stationery Screen*) s'intende quell'operazione il cui scopo è proteggere forze schierate o in stazionamento. Le azioni generalmente condotte in tale ambito sono:

- movimento e occupazione degli OP in corrispondenza della linea iniziale di schermo;
- attivazione dello schermo;
- rischieramento in corrispondenza delle successive linee di schermo;
- passaggio di consegna del combattimento (*Battle Handover* - BA) alle forze schierate;
- passaggio delle linee.

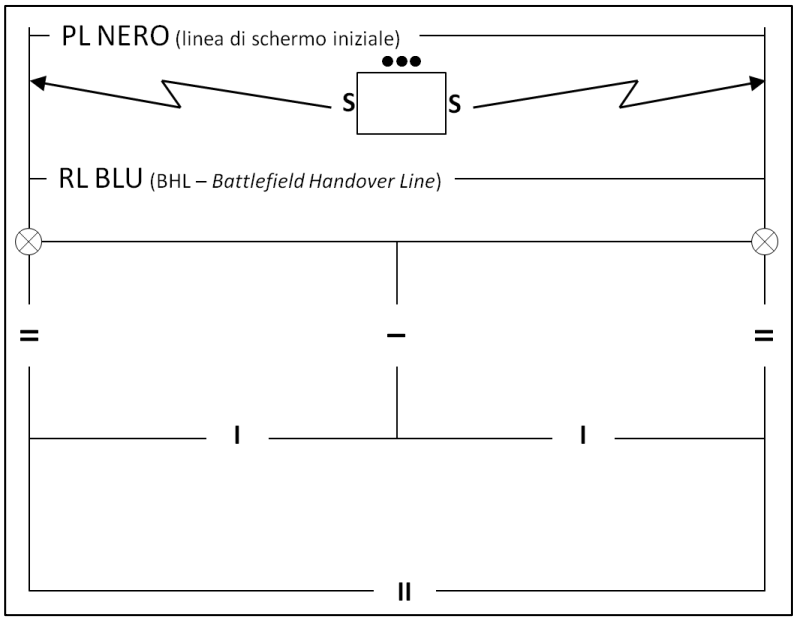


Figura 23: Schermo Statico

Nell'organizzare lo schermo, il Comandante stabilisce gli OP accertandosi che i settori di osservazione si sovrappongono e che i campi visivi coprano i principali corridoi di mobilità, dando maggiore profondita agli OP incaricati dell'osservazione delle vie che permettono una con maggiore velocità. Inoltre, il Comandante identifica gli itinerari che consentono il raggiungimento delle successive linee di schermo nella maniera più veloce e coperta possibile per la rapida occupazione degli OP successivi.

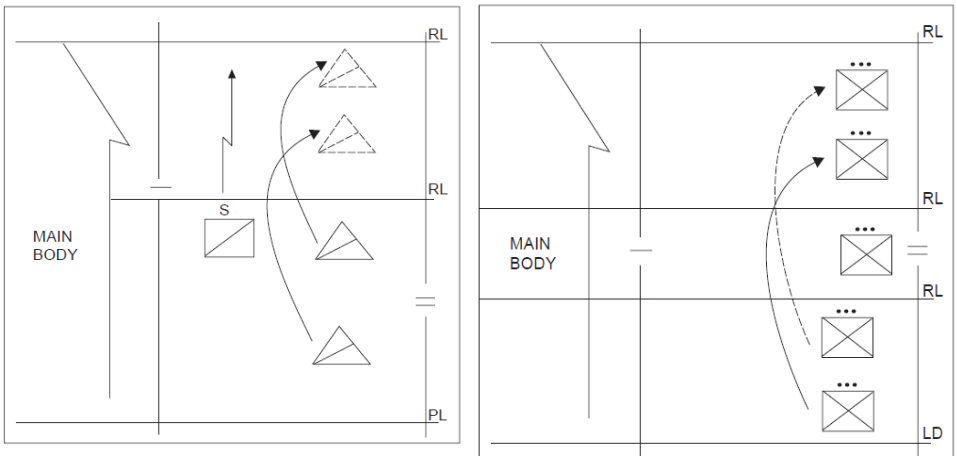
Come detto, il rischieramento verso OP successivi viene deciso sulla scorta degli eventi, non della pianificazione. Il fronte anteriore dell'area della battaglia (*Forward Edge of the Battle Area* - FEBA) coincide con il margine posteriore dello Schermo avanzato. Il Comandante definisce anche una PL per il passaggio di consegna della del combattimento (*Battle Handover Line* - BHL).

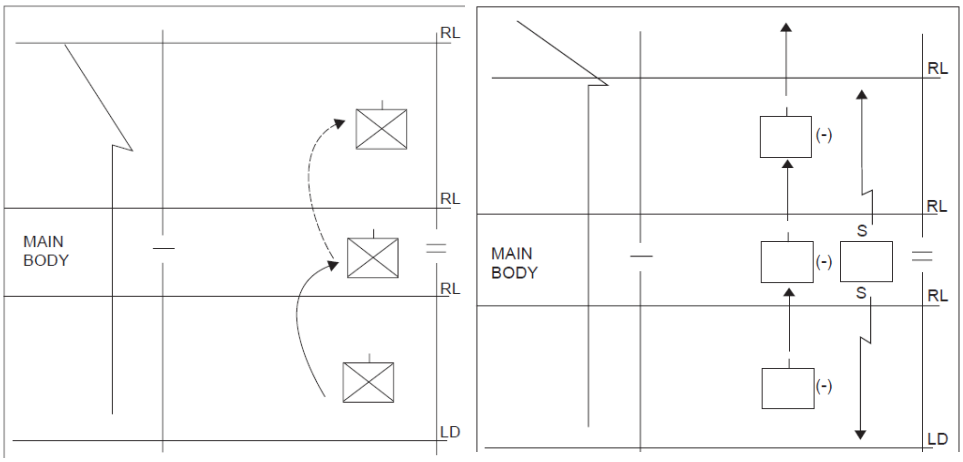
3.2.2.2 Schermo Mobile

Lo Schermo mobile serve a garantire la protezione di forze in movimento. Viene condotto sui fianchi o nelle retrovie del Grosso. Le responsabilità dello schermo mobile sui fianchi vanno dal fronte del Grosso alle retrovie dello stesso. Il movimento dello Schermo si regola sulla base di quello del Grosso e a questo deve continuamente adattarsi. Le seguenti sono le tecniche associate:

- la forza di Schermo supera la linea di partenza separatamente dal Grosso e posiziona gli elementi lungo la linea di schermo. Tale tecnica è la più veloce, utile quandi il Grosso deve muovere in maniera rapida, la linea di partenza non è contesa e l'*Intelligence* indica la scarsa probabilità d'incontrare forze nemiche nell'area di schermo. È la tecnica meno sicura tra le tre qui proposte;
- la forza di schermo può superare la linea di partenza separatamente dal Grosso ma viene guidata da elementi da ricognizione. Gli elementi designati per l'occupazione degli OP seguono. La linea di partenza non è contesa ma l'*Intelligence* indica la possibile presenza di forze nemiche nell'area di schermo. È una tecnica meno rapida della precedente ma garantisce una maggiore sicurezza;
- la forza di schermo può attraversare la linea di partenza con il Grosso e ricognisce la propria AoO. Questa tecnica è la più appropriata quando il Grosso può muovere lentamente, la linea di partenza coincide con la linea di contatto e la situazione nemica è vaga. Tale modalità è la più lenta ma garantisce la maggiore sicurezza possibile all'operazione.

Il movimento lungo la linea di schermo è determinata dalla velocità del grosso, la distanza dell'obiettivo e dalla situazione nemica. I quattro metodi per controllare il movimento lungo la linea di schermo sono mostrati tramite gli schemi seguenti.





3.2.2.3 Schermo Rinforzato

Lo Schermo Rinforzato è una organizzazione che permette di raggiungere una maggiore sicurezza. In pratica, consiste nel costituire degli OP capaci di condurre limitate operazioni da combattimento. Lo Schermo Rinforzato costituisce lo strumento che permette ai Comandanti di estendere le zone di sicurezza in profondità, quando ritengono necessario che gli OP restino in posizione fino al contatto col grosso avversario o quando ritengono che le forze possano essere circondate. Inoltre, lo schermo rinforzato può risultare particolarmente utile in terreni a limitata mobilità che preclude il pronto intervento da parte di unità mobili su mezzi.

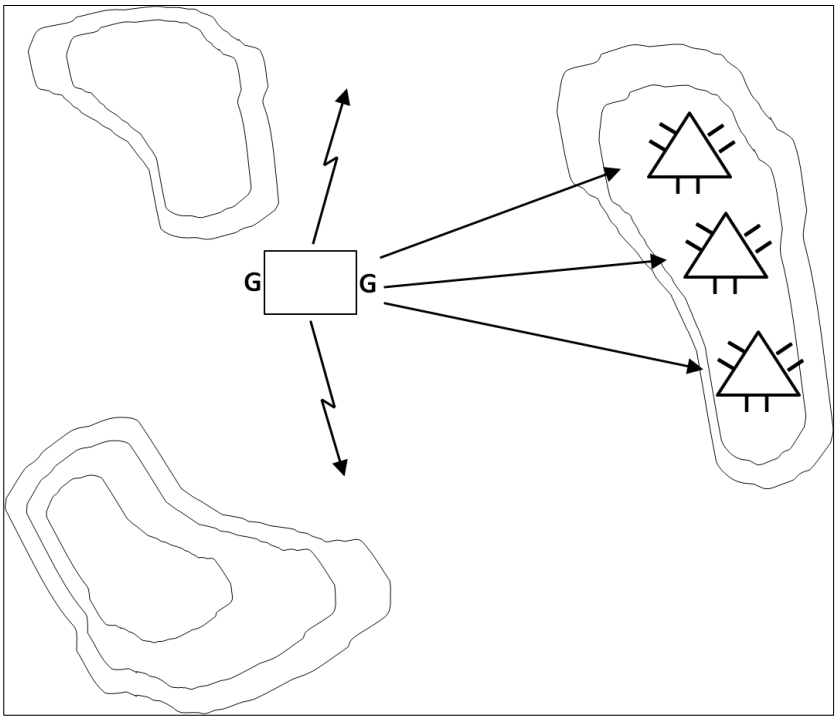


Figura 24: Schermo Rinforzato

Il numero e il *Combat Power* degli OP dipende dal METT-TC. Lo Schermo Rinforzato deve possedere una capacità di combattimento adeguata alle circostanze, senza però decrementare in modo critico il *Combat Power* del Grosso.

Gli OP sono organizzati e fortificati per combattere in ogni direzione, non solo da quella presumibile di provenienze delle forze ostili. Il nemico manovra.

Il Comandante pianifica il Ripiegamento (attività tattica abilitante) degli OP prima che la situazione degeneri e sia messa a rischio la loro capacità di combattimento.

Le forze costituenti lo Schermo Rinforzato possono condurre pattuglie da combattimento, ricercare e distruggere gli elementi da ricognizione nemici.

3.2.3 Guardia

La Guardia è l'elemento di sicurezza la cui missione primaria è la protezione del Grosso attraverso l'osservazione, e il combattimento per ottenere tempo. La differenza tra Schermo e Guardia consiste nella maggiore capacità di combattimento di quest'ultima. In ogni caso, in caso di necessità, il compito di schermo può essere variato in guardia.

Il complesso tattico incaricato di condurre la Guardia, sviluppa tale compito principalmente tramite le attività tattiche di ricognizione, attacco, difesa di posizione e frenaggio.

Il Comandante utilizza una forza di Guardia sulla fronte del Grosso (Avanguardia) o nelle retrovie (Retroguardia), elemento fondamentale per condurre l'attività tattica abilitante Ritirata. Inoltre, una Guardia può essere utilizzata anche per proteggere i fianchi dal presubile e rilevante intervento di forze nemiche.

3.2.3.1 Avanguardia (*Advanced Guard*). L'Avanguardia è il complesso tattico che guida una Forza. La sua missione primaria è quella di assicurare la continuità dell'avanzata del Grosso, senza interruzioni, allo scopo di:

- trovare e sfruttare *gap* nel dispositivo nemico;
- prevenire che il Grosso avanzi in territori ignoti;
- bonificare la fronte dalla presenza di forze nemiche e, qualora non disponga di sufficiente *combat power*, fissare le forze ostili in attesa dell'intervento del Grosso.

3.2.3.2 Guardia del Fianco (*Flank Guard*). La missione di Guardia viene assegnata quando esiste una significativa minaccia di contatto con forze nemiche, di osservazione ostile, di fuoco diretto e di attacchi di sorpresa che potrebbero colpire sul fianco il dispositivo di una Forza. Come per lo Schermo Mobile, il Comandante della Guardia muove la sua Forza in relazione al Grosso che protegge, principalmente

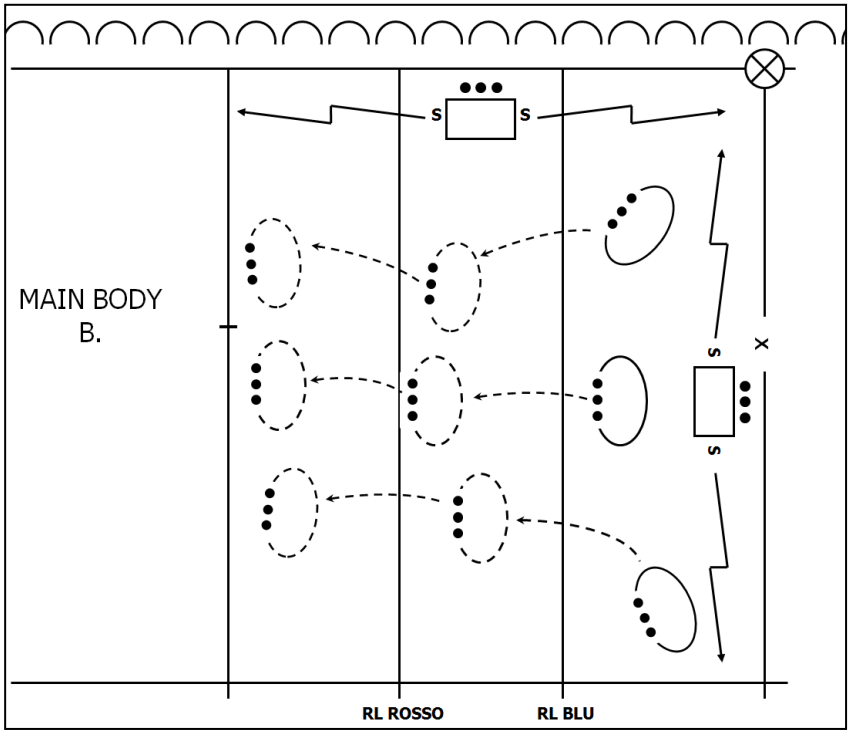


Figura 25: Guardia sul Fianco di una Forza in stazionamento

considerando gli assi di movimento, le capacità delle forze nemiche e tutte le possibili vie tattiche che adducono al Grosso in movimento. I settori assegnati alla Guardia devono essere sufficientemente ampi per permettere di rispondere tempestivamente alla minaccia e allarmare il più presto possibile il Grosso. Inoltre, la Guardia deve sempre mantenere una distanza dal Grosso che permetta a questo d'intervenire e supportare il primo, evitando l'isolamento dell'elemento di protezione.

La Guardia del Fianco è responsabile per la bonifica dell'area tra il Grosso e le posizioni della Guardia stessa. In generale, la Guardia del Fianco opera su un fronte minore di quello assegnato a uno Schermo.

Se un attacco nemico viene ritenuto imminente dai fianchi, la Guardia al Fianco occupa posizoni difensive speditive. Tale attività è un *Drill* che deve essere definito e provato dalle unità incaricate. Qualora la forza nemica sia troppo forte per la Guardia, l'attività tattica che viene condotta è il Frenaggio. Le Operazioni di Guardia del Fianco possono essere condotto sia a favore di un grosso in stazionamento che di uno in movimento.

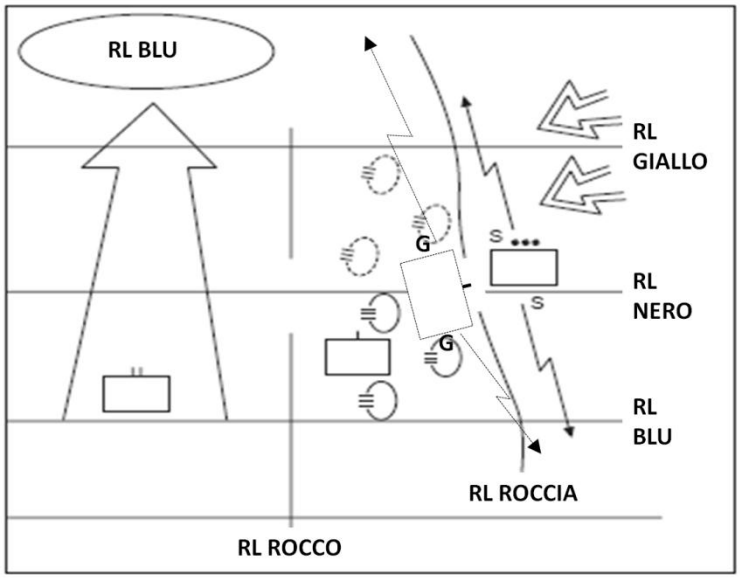


Figura 26: Guardia sul Fianco della Forza in movimento

Alcuni compiti sono quindi critici per la condotta di questa Operazione. La Forza incaricata deve sorvegliare con continuità l'area assegnata, focalizzando gli sforzi in corrispondenza delle vie tattiche. Le tecniche fondamentali per il movimento sono:

- continuo: preferibilmente utilizzabile quando le attività nemiche sono poco probabili e il Grosso muove con la massima velocità. La formazione in colonna è la più veloce ma ovviamente la tecnica meno sicura;
- posizioni successive: da preferirsi quando si presume solo attività ostili di bassa entità contro il fianco del dispositivo e non si prevedono lunghi stop da parte del Grosso in movimento;
- sbalzi alternati: è la tecnica migliore da utilizzare qualora ci si attenda una pesante azione ostile diretta sul fianco della Forza. Tale tecnica comporta una velocità d'avanzamento particolarmente bassa ma, al contempo, garantisce il più elevato livello di protezione del dispositivo.

È evidente che, maggiore è la sicurezza prodotta, minore è la velocità di movimento della Guardia. Il Comandante sceglie la tecnica di movimento sulla base della velocità

di movimento del Grosso, la probabilità che si concretizzi un attacco nemico e la distanza dall'obiettivo. Va infine sottolineato che le tecniche sopra illustrate possono essere utilizzate anche in modo sequenziale: il Comandante della Guardia può, ad esempio, sulla scorta della situazione, della distanza dall'obiettivo e dall'andatura del Grosso, disporre il passaggio tra una forma di movimento a un'altra.

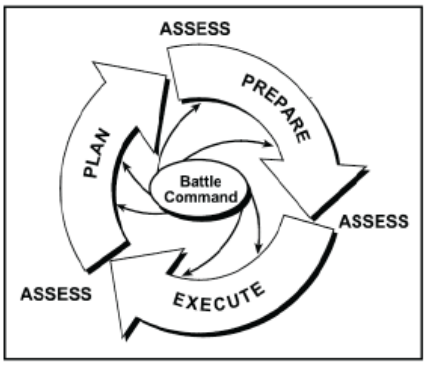
3.2.3.3 Retroguardia (*Rear Guard*). La Retroguardia serve a proteggere le retrovie. La Ritirata prevede sempre la presenza di tale Forza. La Retroguardia di una Forza in movimento viene generalmente attuata attraverso la realizzazione di successive posizioni da combattimento (*battle position*).

4. L'INTEGRAZIONE DEL CONCETTO DI PROTEZIONE NELLE OPERAZIONI TERRESTRI

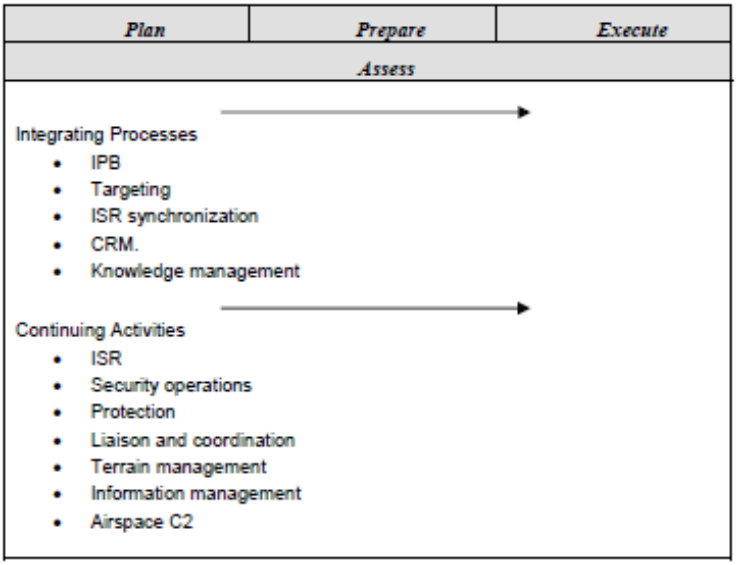
Questo capitolo descrive come la protezione si integra nel processo delle operazioni e come i Comandanti possono integrare tale funzione nella pianificazione, preparazione, esecuzione ed in sede di valutazione. In particolare viene, anche, illustrato come la cellula preposta alla protezione riduce le vulnerabilità delle forze amiche sviluppando apposite strategie di protezione (attraverso l'impiego delle proprie capacità e nel rispetto delle priorità che il Comandante ha stabilito).

IL PROCESSO DELLE OPERAZIONI *(PROCESS OPERATIONS)*

Tutte le operazioni seguono un ciclo generale noto come il "processo delle operazioni" che vede come protagonista il C2 e tutte le attività che esso svolge in termini di pianificazione, preparazione, esecuzione e valutazione continua delle operazioni e che possono avvenire sequenzialmente o simultaneamente (VEDI FIG……).



Attraverso il "processo delle operazioni", i Comandanti assolvono la missione impiegando dei "meccanismi" (quali ad esempio il *battle rhythm* che è una misura di controllo chiave) che facilitano l'integrazione e la sincronizzazione dei compiti e delle funzioni. Nel "processo delle operazioni" si susseguono una serie di attività e di processi che devono essere sincronizzati ed integrati fra loro nell'ambito delle operazioni (VEDI FIG……).



BATTLE COMMAND E LE STRATEGIE DI PROTEZIONE (*PROTECTION STRATEGIES*)

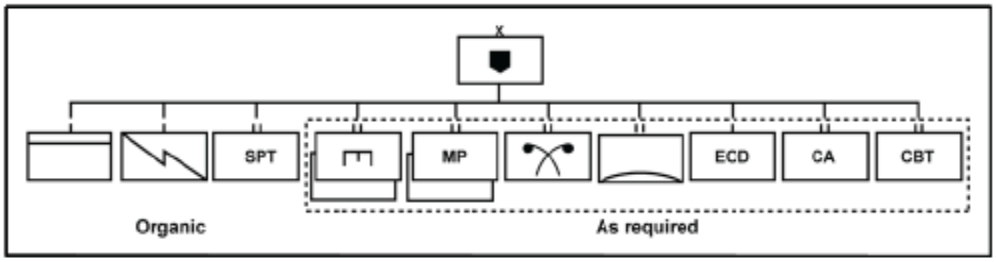
I Comandanti guidano il "processo delle operazioni" attraverso l'applicazione del *battle command*, che è l'arte e la scienza della comprensione, della visualizzazione, della descrizione, dell'orientamento, della direzione e della valutazione delle forze, al fine di imporre la volontà del Comandante sul nemico. Il *battle command,* attraverso la *leadership,* trasforma le decisioni in azioni, sincronizzando le forze e le funzioni operative nello spazio, nel tempo e nello scopo, al fine di assolvere la propria missione.

I Comandanti combinano l'arte e la scienza militare per tradurre le informazioni acquisite e la loro esperienza maturata nella capacità di prendere decisioni in tempi più brevi rispetto all'avversario. In particolare, i Comandanti concentrano i propri sforzi sulla responsabilità di proteggere e preservare le proprie forze mentre cercano di sfruttare ogni opportunità al fine di agire risolutamente. È imperativo, pertanto, che la protezione venga considerata nel "processo delle operazioni".

I Comandanti comprendono e visualizzano le considerazioni e le opportunità relative alla protezione, in relazione alla missione ed all'ambiente operativo. È necessario riconoscere i rischi prevedibili e le minacce che possono richiedere l'applicazione di determinate misure difensive o di sicurezza, al fine di garantire la protezione delle proprie forze.

L'assunzione dei rischi accettata da un Comandante varia in funzione della natura della minaccia, del tema della campagna, delle condizioni ambientali o dei fattori esterni. Lo *staff* assiste il Comandante nell'integrazione della protezione con le altre funzioni operative attraverso il "processo delle operazioni"; per far ciò, si avvale del processo del CRM. Quest'ultimo è utilizzato dalle cellule di *force protection* per identificare, valutare e monitorare le minacce ed i rischi.

Il processo di CRM costituisce un metodo univoco per assegnare un valore (in termini di rischio[78]) ad un'attività. Tale processo, inoltre, permette al Comandante di aggiornarsi sulle condizioni e sulle attività che possono influenzare negativamente la missione e che, di conseguenza, richiedono una sua decisone.
L'integrazione della funzione "protezione" nelle operazioni inizia con la definizione delle responsabilità per l'assolvimento dei compiti e per il monitoraggio dei sistemi della protezione. A tal riguardo, le cellule di *force protection* raccomandano (suggeriscono) l'attuazione di una *task organisation* che abbia come missione primaria la protezione e, qualora le necessità di protezione siano superiori alle capacità a disposizione, le cellule di *force protection* possono suggerire di identificare un C2 di livello superiore che permetta di rinforzare la *task force* e favorire una maggiore modularità della forza in funzione dei compiti della protezione (VEDI FIG……).



Le cellule di *force protection* combinano le linee guida, le capacità ed i risultati delle analisi allo scopo di definire le strategie di protezione, sempre nel rispetto dei suoi principi. Questi ultimi permettono di sviluppare una strategia di protezione coerente ed in stretto coordinamento con le attività e le forme di protezione già esistenti o in atto nell'ambiente operativo.

LA PROTEZIONE ED IL PROCESSO DELLE OPERAZIONI

Il "processo delle operazioni" è costituito da una serie di elementi che illustrano le attività ed i compiti necessari a condurre le operazioni.
Ogni compito e sistema della protezione ha una propria considerazione operativa e ognuna deve essere sincronizzata con una strategia di protezione coerente o con un concetto capace di garantire degli sforzi sinergici. Ad esempio, la difesa da minaccia aerea senza la sopravvivenza è meno efficace, così come lo è la sicurezza areale senza l'OPSEC e la sicurezza fisica. Al fine di garantire questa sinergia, le cellule di *force protection* devono sviluppare una strategia di protezione che permetta di stabilire le MOP e le MOE [g1]e, di conseguenza, monitorare e valutare il successo o il fallimento di ogni singolo sforzo profuso ai fini della protezione.
La valutazione della protezione è un'attività continua ed essenziale che si sviluppa attraverso il "processo delle operazioni" e, per quanto strano, mentre un fallimento nella protezione è facilmente individuabile, di contro il successo dell'applicazione di misure protettive può risultare difficile da valutare e quantificare. Ad esempio,

[78] determinando la probabilità del verificarsi di un evento pericoloso e la relativa gravità o l'esito in relazione alla missione o al personale.

sebbene la prevenzione e la deterrenza possano richiedere notevoli risorse facilmente quantificabili, l'assenza di incidenti o di minacce non necessariamente comporta che il piano di protezione sia efficiente o che i *leader* riescano a gestire efficacemente i rischi. Questo significa che un'attenta valutazione delle attività di protezione permette di determinare l'efficacia di un piano, di una *task organisation* o di un concetto operativo. I criteri presi in considerazione per monitorare e valutare la situazione o l'operazione, possono essere rappresentati dal MOP o dal MOE.

LA LISTA DEGLI ASSETI CRITICI (*CRITICAL ASSET LIST* - CAL)

È una lista, organizzata per priorità, degli assetti critici che dovrebbero essere protetti ed è di solito identificata con la fase di un'operazione[g2]. Una volta che le valutazioni delle minacce, delle criticità e delle vulnerabilità sono complete, vengono presentate al Comandante per l'approvazione; tale lista viene redatta in funzione dei limiti imposti dall'ambiente e dal *combat power* a disposizione. Pertanto le cellule di *force protection* determinano quali assetti sono da considerare critici per il successo della missione e raccomandano le priorità della protezione, sulla base delle risorse disponibili.

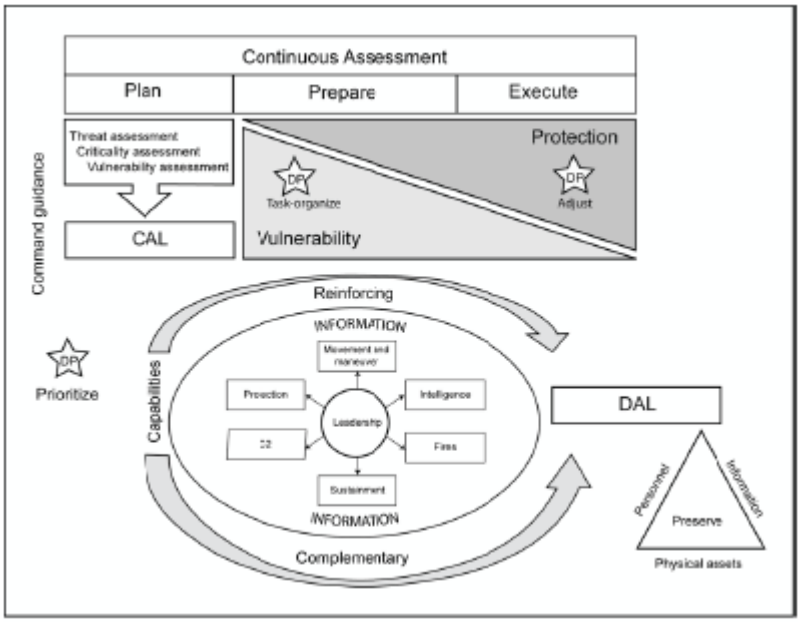
La CAL rappresenta cosa "potrebbe" essere protetto e comporta delle valutazioni sulle criticità e sulle vulnerabilità, che generalmente avvengono in modo sequenziale. Sebbene la valutazione delle criticità sia condotta prima, dopo o contemporaneamente a quella della minaccia, la stima delle vulnerabilità dovrebbe essere condotta dopo la minaccia e le valutazioni delle criticità per indirizzare gli sforzi della protezione verso le aree più importanti[g3].

Non tutti gli assetti indicati nella CAL riceveranno continuamente protezione mentre quelli che, invece, la riceveranno entreranno a far parte della lista degli asseti difesi (*Defended Asset List* –DAL).

LA LISTA DEGLI ASSETI DIFESI (*DEFENDED ASSET LIST* - DAL)

È la lista degli assetti della CAL che sono stati messi in ordine di priorità dal Comandante al fine di essere difesi impiegando le risorse a disposizione.

La DAL rappresenta cosa "può" essere protetto al fine di permettere ai Comandanti di allocare gli assetti disponibili per soddisfare le priorità della protezione. DAL e CAL sono entrambe liste dinamiche, ovvero in continua evoluzione poichè qualsiasi cambiamento relativo alla situazione ed all'ambiente può infierire sulle vulnerabilità delle forze, richiedendo di conseguenza un aggiustamento della CAL e della DAL (VEDI FIG……).



LA PIANIFICAZIONE

La pianificazione è il primo passo verso una protezione efficace. I Comandanti considerano le minacce più probabili e decidono quale personale, assetti fisici ed informazioni devono essere protetti, stabilendo poi le priorità della protezione per ogni fase o evento critico dell'operazione. Le strategie di protezione sono sviluppate sulla base delle informazioni che derivano dall'analisi della missione (durante la pianificazione), durante la quale ricopre un ruolo importante il processo di CRM; tale processo fornisce un contesto per identificare ed analizzare minacce e rischi prima della loro integrazione nella preparazione e nell'esecuzione (VEDI FIG……).

MDMP Steps	Risk Management Steps				
	Step 1. Identify Hazards	Step 2. Assess Hazards	Step 3. Develop Controls and Make Risk Decisions	Step 4. Implement Controls	Step 5. Supervise and Evaluate
Mission receipt	X				
Mission analysis	X	X			
COA development	X	X	X		
COA analysis	X	X	X		
COA comparison			X		
COA approval			X		
Orders production			X	X	
Rehearsal	X	X	X	X	X
Execution/assessment	X	X	X	X	X

Durante l'analisi della missione, la cellula di *force protection* sviluppa delle stime di esecuzione del loro specifico compito e del sistema della protezione, che servono a monitorare e valutare gli sforzi della protezione.

I pianificatori ricevono le linee guida del Comandante, ovvero come egli visualizza il concetto operativo ed il suo intento. Tra di esse, quelle iniziali relative alla protezione possono includere:

- priorità della protezione;
- priorità d'impiego degli assetti dedicati alla sopravvivenza (*survivability*);
- linee guida per il posizionamento degli assetti responsabili della difesa da minaccia aerea;
- fattori specifici meteorologici e del terreno;
- *focus* dell'*intelligence* e limitazioni degli sforzi per la sicurezza;
- eventi o aree dove i rischi sono accettabili;
- aree ed obiettivi protetti;
- vincoli per la sicurezza e la protezione dei veicoli e degli equipaggiamenti;
- C2 delle attività di *personal recovery*;
- misure di protezione sanitaria;
- INFOCON;
- comportamenti da assumere in presenza di UXO;
- tolleranza dei rischi in termini di OPSEC;
- ROE;
- l'*escalation* della forza e le linee guida sull'impiego delle armi non letali.

Le strategie della protezione sono sviluppate solo dopo la ricezione delle linee guida e prendono in considerazione le forme ed i principi della protezione in relazione alle variabili della missione ed ai compiti ed ai sistemi che prevede la funzione operativa della protezione, nel rispetto delle priorità individuate per area, unità, attività o risorse. [g4]

I pianificatori integrano la protezione delle azioni e delle informazioni attraverso specifici piani ed ordini. Alcuni dei più importanti prodotti del processo di pianificazione, relativi alla protezione, possono includere:

- strategia e concetto di protezione che supporta il concetto operativo;
- stime/valutazioni che riflettono i compiti ed i sistemi della protezione;
- livelli di rischio di eventi ed attività specifiche;
- MOP e MOE della protezione;
- raccomandazioni per le CCIR, che riflettono i criteri decisionali per i compiti ed i sistemi della protezione;
- CAL e DAL;
- *decision points* (DP), sulla base del livello di tolleranza del rischio.

In fase di pianificazione, le cellule di *force protection* possono valutare la COA sulla base di criteri derivanti dalla funzione operativa protezione al fine di determinare se una COA è fattibile, accettabile o adatta a proteggere le forze.

I pianificatori devono anche condurre una specifica analisi finalizzata a valutare la minaccia o la vulnerabilità e la criticità di un assetto che supporta un Comandante nel determinare le priorità della protezione o le decisioni relative alla *task organization*. Questo tipo di analisi è spesso richiesto quando l'operazione è duratura o richiede un

continuo sforzo in termini di protezione o quando le potenziali perdite di assetti dedicati alla protezione possono comportare delle conseguenze significative.

PRIORITA' DELLA PROTEZIONE

Determinare e stabilire le priorità della protezione può essere la più importante decisione che un Comandante, supportato dal suo *staff,* deve prendere . Raramente le risorse a disposizione sono sufficienti a garantire simultaneamente protezione allo stesso livello a tutti gli assetti e, per questa ragione, i Comandanti si avvalgono del CRM per identificare i rischi relativi alla condotta delle attività.
La maggior parte dei metodi impiegati per stabilire le priorità della protezione sono finalizzati a distinguere cosa è importante da cosa è urgente; pertanto in fase di pianificazione la sfida maggiore è rappresentata dal distinguere gli assetti critici da quelli importanti e, successivamente, determinare quale livello di protezione è possibile garantire con le risorse a propria disposizione.

PREPARAZIONE

La preparazione comprende l'applicazione delle misure attive e passive di protezione. Durante questa fase, la cellula di *force protection* può condurre o coordinare le seguenti attività:

- revisione e perfezionamento del piano;
- posizionamento di sistemi in grado di individuare le minacce contro le CAL;
- indirizzare le misure OPSEC;
- designare la QRF ed il movimento delle truppe;
- preparare e migliorare le *survivability positions*;
- collegamenti e coordinamenti con le unità adiacenti e protette;
- determinare gli indicatori ed i preavvisi per le operazioni ISR;
- *rehearsal*;
- addestramento con gli assetti difesi;
- confermare i *back brief*;
- sviluppare misure per ridurre le vulnerabilità.

Durante la preparazione, la cellula di *force protection* si assicura che i controlli o le misure individuate per mitigare i rischi, sviluppate durante la pianificazione, siano state implementate e riportate nei piani e nelle SOP (malgrado le minacce siano in continuo aggiornamento). Le cellule di *force protection* ed i gruppi di lavoro mantengono aggiornata una lista di minacce (riportandole in ordine di priorità), di condizioni avverse e di rischi, con l'obiettivo di individuarne le cause, al fine di definire la soluzione più efficace (in termini di protezione) da attuare e diffondere.
I Comandanti esercitano la propria azione di comando attraverso l'intero processo delle operazioni e di concerto con il CRM. Nella fase di preparazione, le azioni dei Comandanti possono anche:

- riconciliare la valutazione della minaccia con l'esperienza ed il giudizio personale;
- fornire linee guida sulla tolleranza dei rischi e sulle relative decisioni da prendere;

- dare enfasi ai compiti ed ai sistemi della protezione durante il *rehearsal*;
- minimizzare le interferenze non necessarie con le unità subordinate al fine di garantire il massimo tempo per la preparazione;
- favorire l'approvvigionamento e la disponibilità di risorse necessarie per lo sviluppo della protezione;
- richiedere ai comandi superiori il sostegno logistico alle attività di preparazione.

In base alla situazione ed alla minaccia, alcuni compiti della protezione possono essere condotti per brevi o lunghi periodi, al fine di coprire diverse missioni o intere operazioni.

ESECUZIONE

In questa fase i Comandanti applicano misure di controllo ed allocano risorse al fine di garantire una continua attività di protezione e, qualora necessario, integrare tale funzione. In questo contesto, la cellula di *force protection* può condurre le seguenti attività:

- assicurasi che il *focus* della protezione sia rivolto al supporto dell'operazione decisiva;
- rivedere ed affinare le CCIR derivanti dai compiti e dai sistemi della protezione;
- considerare le variazioni dei rischi relativi ad eventuali variazioni dei settori sul terreno, al fine di limitare il pericolo di fratricidio;
- monitorare l'impiego delle forze di sicurezza impiegate per colmare i *gap* della protezione;
- valutare l'efficacia del *liaisoning* per le attività della protezione;
- valutare il coordinamento ed il controllo del movimento per proteggere gli itinerari critici;
- monitorare le procedure di coordinamento delle unità adiacenti per la gestione delle vulnerabilità del terreno;
- monitorare la prontezza di risposta delle forze impegnate nella protezione dei siti fissi;
- monitorare la protezione sanitaria (FHP).

I Comandanti devono prestare particolare attenzione al calcolo dei rischi, in maniera tale da adeguare i tempi di prontezza in base alla disponibilità di risorse, in termini di *combat power*. Lo *staff,* dal suo canto, confronta la nuova situazione amica con quella nemica nota, sviluppa dei controlli, raccomanda le priorità ed i DP[g5]. Nella fattispecie, le cellule di force protection determinano:

- dove gli assetti della protezione possono assolvere al meglio i compiti con un fattore di rischio accettabile;
- se gli assetti dedicati alla protezione devono essere impiegati immediatamente o tenuti in riserva;
- se gli assetti devono essere mossi a causa di una variazione della DAL;

- se il Comandante necessita di richiedere assistenza e a quale scopo.

Le cellule di *force protection* monitorano e valutano lo sviluppo delle operazioni correnti al fine di confermare le *assumption* formulate in sede di pianificazione ed aggiornarle in funzione dell'evoluzione della situazione. Le cellule di *force protection* devono monitorare continuamente le minacce alla CAL e alla DAL e, di conseguenza, raccomandare le variazioni al piano di protezione, nonché monitorare la condotta delle operazioni ed individuare eventuali scostamenti che interessano la protezione dall'OPORD. Le cellule di *force protection*, inoltre, verificano lo *status* degli assetti dedicati alla protezione e valutano l'efficacia dei sistemi nell'ambito dei quali essi sono impiegati.

LESSON LEARNED

I Comandanti sviluppano dei sistemi per garantire la rapida disseminazione delle *lesson learned* approvate e delle TTP attuate per proteggere personale, equipaggiamenti ed informazioni. Le cellule di *force protection*, ad ogni livello di comando, valutano l'integrazione delle lezioni apprese e coordinano costantemente le lezioni relative alla protezione con lo staff dei vari livelli di comando.
Al termine dell'operazione solitamente;

- si identificano le minacce che non sono state identificate nell'*assessment* iniziale o quelle manifestatesi durante la condotta delle attività;
- si stimano lo sviluppo, l'esecuzione e la comunicazione dei controlli;
- si valutano l'attendibilità dei rischi residui e l'efficacia dei controlli nell'eliminazione dei pericoli;
- si verifica la conformità con i principi guida del CRM ovvero che:
  - il processo sia stato parte integrante in tutte le fasi delle operazioni in maniera ciclica e continua;
  - le decisioni prese in funzione dei rischi siano state ponderate accuratamente, ognuna al proprio livello.

ALLEGATO "A"
LA PROTEZIONE NELLE OPERAZIONI DI PROIEZIONE DELLA POTENZA DI COMBATTIMENTO

COMPITI E SISTEMI DI PROTEZIONE	**ATTIVITA' DI *PRE-DEPLOYMENT***	**MOVIMENTO VERSO IL POE**	**MOVIMENTO VERSO IL POD**	**RSOM**
DIFESA DA MINACCIA AEREA	- Valutazione della minaccia aerea - Definizione delle capacità essenziali per l'assolvimento della missione - Organizzazione per il *deployment*	Coordinazione delle misure di protezione relative al trasporto di armi, munizioni ed esplosivi	Mantenimento delle misure di protezione relative al trasporto di armi, munizioni ed esplosivi	Coordinazione del *deployment* dell'*Advanced Party*

PERSONNEL RECOVERY (PR)	- Valutazione della minaccia - Definizione delle attività e del personale a rischio d'isolamento - Organizzazione del PR - Coordinazione del personale dello *staff* - Integrazione delle procedure di PR con il personale non militare eventualmente incluso nell'operazione - Elaborazione di SOP specifico - Condotta di esercitazioni e prove pratiche (*rehearsal*)	- Organizzazione del PR - Coordinazione del personale dello *staff* - Integrazione delle procedure di PR con il personale non militare eventualmente incluso nell'operazione - Elaborazione di SOP specifico - Condotta di esercitazioni e prove pratiche (*rehearsal*) - Coordinazione del supporto al PR durante il movimento	- Organizzazione del PR - Coordinazione del personale dello *staff* - Integrazione delle procedure di PR con il personale non militare eventualmente incluso nell'operazione - Elaborazione di SOP specifico - Condotta di esercitazioni e prove pratiche (*rehearsal*) - Coordinazione del supporto al PR durante il movimento	- Aggiornare e monitorare la situazione del personale a rischio di isolamento - Mettere in atto l'organizzazione del PR - Coordinazione del personale dello *staff* - Analizzare eventuali gap del PR - Integrazione delle procedure di PR con il personale non militare eventualmente incluso nell'operazione - Eseguire le SOP sul PR - Condotta di esercitazioni e prove pratiche (*rehearsal*) - Coordinazione del supporto al PR durante la creazione del *Combat Power*

INFORMATION PROTECTION	• Deconflittualizzare le frequenze della HN, quelle non utilizzabili, quelle *radar* o *jammer* amici; • ensure uninterrupted access to joint distributed planning [g6](virtual collaboration) and training amongst geographically dispersed units; • acquisire informazioni sulla configurazione della rete del Teatro e sull'allocazione delle risorse.	• supportare la pianificazione delle missioni in corso ed aggiornare le informazioni critiche (ordini, *overlay*, *intelligence*).	• Garantire l'accesso immediato al sistema satellitare in caso di *blackout* delle comunicazioni.	• Coordinare in modo continuo le attività relative al recupero di personale coinvolto in disastri; • partecipare all'analisi dei rischi; • contribuire al coordinamento della sicurezza fisica (ambientale);
Evitare fuoco fratricida	Addestrarsi nell'identificazione dei processi e delle procedure di combattimento.	Mantenere la *situational awareness*.	Mantenere la *situational awareness*.	Rivedere le procedure di prevenzione del fuoco fratricida con le forze e controllare gli equipaggiamenti.

Operational area security	• Pianificare un'adeguata protezione durante il RSO&I; • pianificare accuratamente le fasi di schieramento per garantire un adeguato *combat power*; • stabilire le CAL.	• Coordinare e valutare la sicurezza dei porti e dei movimenti per raggiungerli; • coordinare i movimenti con le forze di polizia locali.	• Assegnare i *supercargo*; • Store cargo and measures in place.[g7]	Garantire la protezione delle forze durante il RSOM ed il movimento verso le AA tattiche.
Sopravvivenza	Valutare i requisiti della protezione del personale, degli equipaggiamenti e dei veicoli.	Condurre operazioni di sopravvivenza (*CONDUCT SURVIVABILITY*).	Condurre operazioni di sopravvivenza (*CONDUCT SURVIVABILITY*).	Garantire il supporto necessario a condurre operazioni di sopravvivenza (*CONDUCT NECESSARY SURVIVABILITY SUPPORT*).

Protezione sanitaria	• Coordinare lo sviluppo di programmi per la prontezza sanitaria individuale; • condurre indagini nell'ambito dell'AO al fine di determinare possibili minacce sanitarie; • pianificare e coordinare le richieste di supporto alla medicina preventiva; • valutare le possibili vulnerabilità del"acqua e del cibo; • pianificare e coordinare il servizio veterinario; • sviluppare procedure per controllare e monitorare campioni di cibo e di acqua; • pianificare programmi di prevenzione e controllo delle malattie degli animali; • sviluppare un piano per migliorare il controllo dello stress a livello individuale e di reparto; • informare i	Condurre continui *assessment.*	Condurre continui *assessment.*	Continuare ad eseguire il piano della missione, modificandolo al fine di proteggere il personale da potenziali minacce sanitarie.

<u>Protezione CBRN</u>	• Completare l'*assessment* della minaccia CBRN e la valutazione della capacità nemiche; • completare la valutazione dello stato delle forze amiche; • sviluppare un piano di difesa CBRN.	Mantenere la *situational awareness*.	Mantenere la *situational awareness*.	Rivedere il piano di difesa CBRN.

Sicurezza fisica	• Addestrare e qualificare il personale nella gestione dei materiali pericolosi; • verificare l'efficacia della sicurezza fisica; • sensibilizzare il personale sulla sicurezza attraverso la presentazione di briefing.	• provide quality assurance specialist ammunition surveillance support[g8]; • train load team to standards; [g9] • rivedere i dati relative agli incidenti /mancanze per sviluppare piani di riduzione delle perdite.	• Garantire ai soldati la possibilità di riposarsi e di idratarsi; • rivedere I dati relative agli incidenti /mancanze per sviluppare piani di riduzione delle perdite.	• Permettere al personale di acclimatarsi; • effettuare addestramento notturno; • incrementare le protezioni dei veicoli; • addestrare il personale sulla condotta di attività di recupero e ribaltamento; • supervisionare le attività relative alla sicurezza fisica; • supervisionare i briefing finalizzati a sensibilizzare il personale sulla sicurezza fisica; • rivedere I dati relative agli incidenti /mancanze per sviluppare piani di riduzione delle perdite.

OPSEC	• Indicare le CCIR; • condurre *assessment* sulla vulnerabilità dell'OPSEC; • condurre addestramento OPSEC; • considerare l'OPSEC nelle attività di pianificazione.	Condurre OPSEC.	Condurre OPSEC.	Condurre OPSEC.
EOD	• fornire *assessment* sulla minaccia EOD ed una valutazione del nemico; • far effettuare addestramento sull'IED *awareness*; • garantire l'efficienza dell'equipaggiamento.	Mantenere la *situational awareness*.	Mantenere la *situational awareness*.	• Rivedere le TTP nemiche e supporta il movimento alle AA tattiche; • fornire addestramento specifico in teatro.

ALLEGATO "B"
IDENTIFICAZIONE DELLE FORZE AMICHE

1.2 DEFINIZIONI

a. combat identification. L'uso delle misure d'identificazione per ridurre il fuoco amico e per aumentare l'efficacia operativa delle forze e dei sistemi d'arma.
b. Identification. Il processo per raggiungere/conseguire un' accurata descrizione di un' entità rilevata da qualsiasi atto o risorsa/mezzo così che l'elevata sicurezza/fiducia nelle decisioni in tempo reale, includa come può essere fatto l'ingaggio con le armi.
c. Target identification. Questo termine non è definito all'interno dell'AAP-06;tuttavia, ciò nonostante, è un termine normalmente usato che può essere ritenuto un sinonimo di identificazione. Lo scopo/obiettivo dell'identificazione del bersaglio, è identificare un'entità nel battlespace come amico, nemico, neutrale o non combattente.
d. Battlespace. L'ambiente, i fattori e le condizioni che devono essere comprese per applicare il Combat Power, proteggere la forza o completare con successo la missione.
e. Situational awareness. La conoscenza degli elementi nel battlespace necessarie per prendere delle decisioni essendo informati bene.

1.3 ESIGENZA E METODI PER L'IDENTIFICAZIONE DELLE FORZE SUL TERRENO

1.3.1 Generalità

Il problema delle forze di ricognizione sul battlefield o in area d'operazioni, saranno superati da una combinazione di procedure di controllo, conoscenza del battlespace, mezzi tecnici e un addestramento efficace. Perché le difficoltà nel riconoscere le forze aumentano con le grandi distanze, il terreno complesso e la ridotta visibilità, il principio principale (la prerogativa principale) per prevenire la in mancato riconoscimento e il fuoco fratricida, soprattutto al di sopra del livello dell'unità (a livello superiore) , sarà attraverso misure efficaci di comando e controllo. Lo scopo del combat identification è quello di costruire sopra la dottrina, l'addestramento e le regole d'ingaggio, tramite lo sfruttamento (l'ottimizzazione) del battlespace awareness, tecniche d'identificazione, e le capacità e dispositivi per aumentare l'efficacia del combattimento, che dia come risultato la limitazione gli incidenti da fuoco fratricida.

1.3.2 Identificazione di forze amiche

1. Le forze amiche si identificano (riconoscono) sul battlefield stabilendo un collegamento, e utilizzando i seguenti metodi e procedure di controllo:

a. Responsabilità del battlespace. Le misure di comando e controllo, spesso saranno esercitate attraverso l'uso di lineamenti di organizzazione. Questi includono:
   (1) Forward Line of Own Troops (FLOT);
   (2) fire support coordination measures;
   (3) airspace coordination measures;
   (4) phase lines; and,
   (5) confini, settori e aree.

b. Sistemi manuali e automatici di altolà e sistemi di risposta. Questi tipi di sistemi richiedono un interrogazione, cioè le persone o l'entità che intimano l'altolà e la replica (risposta), cioè le persone o l'entità che rispondono, la cui risposta indicherebbe l'affiliazione come amichevole o sconosciuto.
   I sistemi di intimazione l'altolà e di risposta includono i seguenti metodi:
   (1) Non verbale i metodi non verbali per intimazione l'altolà e di risposta includono:
      (a) L'uso di segnali di fumo colorato, luci,pirotecnici e panels
      (b) Metodi elettronici, inclusi chiamate radio su frequenze stipulate.
      (c) Metodi elettrro optici, inclusi i lasers.
   (2) Verbale I metodi per l'altolà che usa la guardia e le sentinelle sono descritti al capitolo 2.

c. Addestramento. L'utilizzo efficace delle capacità del combat identification è descritto in questo standard e afferisce su un rilevante (attinente) addestramento da parte degli utenti e degli operatori. L'addestramento al riconoscimento è stato deciso come essere la chiave (KEY) per quanto riguarda il combat identification. Sistemi di addestramento, metodi e standards cambiano/variano all'interno delle nazioni NATO, ma c'è il consenso che questo addestramento sia importante per un efficace operazione militare. L'identificazione essenziale/fondamentale è la condivisione delle caratteristiche dei veicoli, equipaggiamenti e dei soldati tra le forze NATO. Le Nazioni impiegano vari metodi di identificazione e riconoscimento del veicolo nell'addestramento pre-deplyment. La condivisione di informazioni per specifiche operazioni dovrebbe verificarsi durante la generazione della forza e attraverso (completamente) la condotta dell'operazione. Il fondamento, la base per l'addestarmento in teatro, è derivato dal minimo standard di combat identification impiegato inn operazioni, come designato dal Comandante appropriato.

d. Sistema di gestione del Battlespace. La consapevolezza del Battlespace, o la situational awareness, è riconosciuto/accettato come un key element, nell'impiego efficace delle forze sul campo di battaglia. La criticità per evitare il fuoco fratricida è la conoscenza dei luoghi e delle attività delle forze amiche. Svariati metodi sono utilizzati per tracciare/designare le informazioni necessarie/indispensabili del battlespace, che variano da quelli disegnati a mano a sistemi automatici collegati in rete. Si deve considerare la differenza di tempo tra la ricezione delle informazioni e la tracciatura e la visualizzazione di essi. Progredendo esattamente verso un sistema in rete (collegato in rete) di battlespace awareness, i rischi associati con informazioni scadute diminuiranno. Qualsiasi cambiamento/modifica delle misure esistenti per il controllo del fuoco e della manovra per supportare i sistemi automatizzati, dovrebbe mantenere l'intento che questa dottrina prende in considerazione.

2. caratteristiche e segnali di identificazione. L'identificazione delle forze amiche può essere stabilita e riconosciuta/compresa/stimata attraverso un serie di risorse/mezzi. L'efficacia di questi mezzi/risorse è direttamente connessa all'addestramento che i comandanti e i soldati ricevono prima dell'operazioni. Questi mezzi/risorse comprendono:

a. Aspetto/apparenza personale e equipaggiamento. L'aspetto incrementa/accresce il profilo, colore segni distintivi, layout e l'effetto visivo generale di elementi conformi alle disposizioni prescritte.
b. Comportamento direzione e modalità di movimento, velocità, uso dell'armamento, orientamento dell'armamento, e il tipo di formazione che assisteranno/contribuiranno al riconoscimento delle forze amiche. L'identificazione o il riconoscimento dovuti al comportamento richiede una buona conoscenza tattica della situazione corrente. Ciò includerà la conoscenza dei piani di movimento delle forze amiche.
c. Time L'aggiornamento della informazione, può aiutare nella valutazione del rischio associato, nel prendere decisioni che possono avere un impatto sulle forze amiche.; più giovane è l'informazione, più è probabile che le informazioni siano più accurate/precise, finchè la conversazione è vera con posizioni precise, deve essere considerata in congiunzione con altri fattori. Determinante/decisivo se le forze hanno incrociato una posizione designata, in uno specificato orario. Tutto questo contruibirà all'identificazione.
d. Sound Le distinte caratteristiche audio di alcune armi e equipaggiamenti aiuteranno nel riconoscimento e identificazione.
e. Emissioni elettroniche i sistemi elettronici possono in alcuni casi riconoscere o identificare emissioni elettroniche come amichevoli (specialmente equipaggianto radar).

f. Spettro infrarossi. (IR) Il riconoscimento e l'identificazione possono essere aiutati dallo sfruttamento dalle radiazioni IR di breve media e lunga distanza. Gli strumenti di intensificazione d'immagine (ad esempio occhiali da vista notturni), sfruttano le radiazioni NEAR-IR, ma sono solo in grado di funzionare operare durante l'oscurità. Gli strumenti di immagine termica, sfruttano, le medie e le lunghe radiazioni IR e sono in grado di operare sia di giorno che di notte. Esempi di capacità combat identification e i dispostivi che sfruttano lo spettro IR, saranno trattati nel capitolo 3.

g. Signals i segnali di riconoscimento stabiliti aiuteranno all'identificazione delle forze amiche. Ciò include/comprende l'uso di:
   (1) qualsiasi tipo di segnale usato in conformità con quanto prescritto dal piano o dalla KEY;
   (2) l'uso corretto dell'altolà e di risposta. (capitolo 2)

h. posizioni. La conoscenza delle posizioni delle forze o elementi amiche in riferimento alle caratteristiche del terreno chiaramente riconoscibili (es. campanili..) e ai limiti stabiliti per aree delle operazioni per ciascuna delle specifiche forze (elementi amichevoli) contribuiranno ad evitare il fuoco fratricida. Le misure di coordinamento del supporto di fuoco (per es. FSCL) e i punti di riferimento artificiali possono essere usati per il riconoscimento e l'identificazione degli elementi ground. Gli elementi ground sono responsabili della visualizzazione dei punti di riferimento artificiali ground per il riconoscimento e l'identificazione da parte degli elementi air, dopo aver coordinato il tempo/momento (orario?) e i luoghi con i comandanti air. Il riconoscimento dell'unità designata dalla posizione e traccia può essere determinato dalla
   (1) la posizione ricevuto/avuta dal SITREP;
   (2) La posizione presunta/riportata di un' unità designata come amica o ostile da un'autorità competente;
   (3) La conoscenza delle posizioni e dei confini tattici (aree di operazioni) di amici e nemici;

i. Pannelli di segnalazione Ground/Air possono essere utilizzati Pannelli Segnalatori fluorescenti, soggetti a limitazioni imposte dalla topografia/orografia o dalla possibile identificazione del nemico. Laddove i pannelli sono utilizzati, dovrebbero esser orientati per fornire la massima visibilità per le forze aeree amiche che attaccano o per le forze terrestri (ground) che transitano. Vedere capitolo 3

3. Limitazioni i segnali di riconoscimento e identificazione hanno certamente delle limitazioni che sono legate/collegate ai fattori umani e alla carenza di tecnologia. Queste limitazioni includono:

a. Il personale amico non può, in tutti i casi, conoscere l'attuale/corrente/vigente risposta all'altolà. (Reply/challenge);

b. L'apparecchiatura/equipaggiamento di riconoscimento del segnale potrebbe fallire/non riuscire;
c. Gli strumenti di identificazione richiedono un grado di manutenzione e pulizia per garantire il riconoscimento e il raggio visivo;
d. La mancanza di fornire una risposta corretta all'altolà (challenge) (sia visiva, verbale o elettronica), non deve essere presa come una prova dell' atteggiamento/postura del nemico (enemy character) . Gli elementi sia neutrali che non combattenti sul battlefield,(terreno/campo di battaglia) ad esempio civili o rappresentanti di NGO, non saranno attrezzati con/forniti di dispositivi di riconoscimento e non conosceranno parole d'ordine o altri signals; inoltre, la risposta (reply) potrebbe non essere conosciuta da alcune truppe amiche.
e. I segnali (Signals) possono diventare conosciuti (possono esser noti) al nemico e i dispositivi di identificazione possono esser copiati/imitati dai nemici. Tali dispositivi e segnali sono quindi considerati come indizio, ma mai come una prova della postura/atteggiamento delle truppe amiche (friendly character).
f. Alcuni metodi non sono efficaci di giorno o di notte, o in condizioni di scarsa visibilità. E' importante comprendere le limitazioni/restrizioni of combat identification capabnilities and devices, e fornire mezzi alternativi per mitigare queste limitazioni.

4. <u>Considerazioni aggiuntive</u> Altre procedure e considerazioni per aiutare nell'identificazione delle forze amiche sono:
   a. Ridurre il rischio di compromissione, altolà e risposta (challenges and replies), devono essere cambiati periodicamente e distribuiti solo in caso di necessità. Altolà e risposta (challenges and replies), e i loro sostituti sono solitamente emessi giornalmente dalla catena di Comando.
   b. Altolà e risposta (challenges and replies), non dovrebbero essere utilizzati davanti la FEBA, tranne in particolari circostanze (ad es. Collegamento con un brigata Airborne);
   c. Alternare Altolà e risposta (challenges and replies) e le configurazioni di identificazione saranno implementate/attuate/, in caso del loro effettivo, reale o sospetta compromissione.
   d. I comandanti ordinano l'impiego e la configurazione di specifiche capacità o dispositivi d'identificazione, attraverso le SOP o con direttive all'interno dell'ordine. Regolare la revisione e la configurazione di un diretto impiego è necessario per garantire l'attinenza e per mitigare il rischio di compromettere le non friendly forze.
   e. L'uso di dispositivi/strumenti d' identificazione passivi o attivi operativi/che operano nello spettro infrarosso, devono essere considerati alla luce delle capacità delle forze nemiche. L'uso di tali

soggetti/oggetti/articoli/dispositivi (items), può benissimo consentire alle forze nemiche di individuare più facilmente (more easily) le nostre truppe amiche utilizzando sistemi similari all'IR.

f. I dispositivi di identificazione devono essere protetti dalla divulgazione al nemico, possibilmente fino all'ultimo momento, per mantenere la sicurezza sul loro utilizzo.
g. L'aggiunta di blindature addizionali, reti di protezione da razzi, o personal kit all'esterno di un veicolo altererà le sue caratteristiche di riconoscimento e forse coprire qualunque/alcuni/qualche dispositivo di riconoscimento. I Comandanti devono essere consapevoli di questo e indicare le direttive/l'orientamento appropriato.
h. Il fumo rosso o bianco non devono essere utilizzati, in quanto non adatti per l'identificazione delle forze amiche.
i. Le luci rosse o pirotecniche non devono essere utilizzati, in quanto non adatti allo scopo voluto-
j. I potenziale uso nemico dei dipositivi CID, che devono essere un requisito per l'intelligence. LA consapevolezza dell'uso nemico dei dispositivi CID, aiuterà nel guidare/controllare/dirigere le azioni per mitigare questo rischio.

5. Scambio di informazioni sull'identificazione e il riconoscimento Il riconoscimento positivo delle forze amiche che operano sul battlefield deve basarsi sull'esatta conoscenza delle uniformi, equipaggiamento e veicoli utilizzati da tali forze. Ovviamente deve essere un focus costante/continuo di addestramento al riconoscimento a tutti i livelli delle nazioni appartenenti alla NATO. L'addestramento dovrà essere raffinato prima dell'inizio delle operazioni della coalizione, così che quegli equipaggiamenti tipici/caratteristici delle forze amiche e nemiche, in cui ci si imbatte sul battlefield, possono essere studiati in modo più dettagliato.
6. Responsabilità del Comando Tutti i Comandanti hanno la responsabilità di garantire che il personale posto sotto Comando operativo sia addestrati nel riconoscimento di entrambe le forze (amiche e nemiche) che si potrebbero incontarre nel battlefield.
7. Ordini Per garantire che gli argomenti (issue) del combat identification siano inseriti/indirizzati (addressed) nell'ordine, il sottoparagrafo dovrebbe essere collocato/posto sotto la voce "Coordinating Instructions" paragrafo Execution ed essere titolato "Combat Identification MEasures".
8. Direzione di Comando I comandanti sono responsabili della prescrizione degli altolà e delle risposte (challenges and replies) e della configurazione delle competenze/capacità e degli strumenti d'identificazione utilizzati sia in operazioni che in addestramento. I comandanti sono responsabili dell'assicurarsi in conformità con le direttive/istruzioni emanate dai comandi

superiori nelle operazioni coalizzate/ della coalizione. (identification configurations) La configurazione delle identificazioni e l'intimazione dell'altolà (challenges) verbale e non verbale sono decise in merito/in base al più alto livello di comando applicabile, e notificato in anticipo alle formazioni e unità subordinate. Le formazioni del livello superiore e quelle confinanti/adiacenti/attigue/vicine sono anche loro informate dei protocolli di altolà e risposta (challenge and reply)

1.4 IMPLEMENTARE QUESTA PUBBLICAZIONE

Questa pubblicazione è implementata/attuata messa in pratica quando gli ordini/istruzioni necessarie sono state emanate alle forze interessate comprendenti le procedure dettagliate, rendendo effettive le procedure dettagliate in questa dottrina inseriti. Inoltre questa pubblicazione è attuata/implementata/messa in pratica quando le forze interessate hanno ricevuto gli equipaggiamenti previsti da questa pubblicazione e sono pronti ad utilizzarlo.

CAPITOLO 2 (CHALLENGE) FORMULA (opp. PROCEDURA) DI RICONOSCIMENTO DI GUARDIE E SENTINELLE

2.1 DEFINIZIONI

Nel presente Capitolo saranno impiegati i seguenti termini e definizioni:

a. Formula (procedura) di riconoscimento. Qualsiasi processo effettuato da una unità o persona con l'obiettivo di accertare il carattere pacifico o ostile ovvero l'identità di qualcuno.
b. Replica. Una risposta ad una domanda.
c. Parola d'ordine. È spesso la combinazione di due o più parole, lettere o numeri che sono impiegati nella formula (procedura) di riconoscimento. Una parte della parola d'ordine è utilizzata nella formula (procedura) di riconoscimento e un'altra porzione di parola d'ordine è utilizzata nella replica. La definizione nella AAP-06 è diversa, però questa è l'applicazione comunemente intesa della parola d'ordine nel contesto di questa pubblicazione.

2.2 METODO

1. La formula (procedura) di riconoscimento tramite voce (?) è generalmente utilizzata per identificare persone sconosciute in avvicinamento a una posizione. È basata su una parola d'ordine, che normalmente cambia almeno una volta al giorno e che è comune nell'ambito delle formazioni nazionali ovvero all'interno di specifici gruppi o aree di comando.
2. Le parole impiegate per formare la parola d'ordine devono essere facilmente pronunciabili. La combinazione impostata in caso di procedura di riconoscimento, non dovrebbe avere una correlazione ovvia con quella che potrebbe essere la replica.

3. La parola d'ordine è decisa al più alto livello di comando e notificata in anticipo alle formazioni e unità subordinate.
4. Quando le forze di due o più nazioni sono inserite nella stessa formazione o Area di Operazioni, è necessaria particolare attenzione affinché la parola d'ordine individuata sia pronunciabile dalle lingue delle nazioni interessate. In tali circostanze dovranno essere usate due o più lettere dell'Alfabeto Fonetico NATO. Per maggior chiarezza sia la formula di riconoscimento sia la parola d'ordine dovrebbero essere ripetute due volte.

2.3 PROCEDURA

1. Nessuna formula di riconoscimento dovrebbe essere eseguita quando la controparte (?) è pronta ad avviare un'azione offensiva.

2. Deve essere impiegata la seguente procedura.

	Azione della sentinella	Azione di chi deve essere riconosciuto
Step 1	Informare prontamente il Comandante (della Guardia?) dell'avvicinamento di una persona/un gruppo. Controllare la persona/il gruppo con le armi.	
Step 2	Ordinare alla persona/al gruppo di fermarsi (ad esempio, ALT, MANI IN ALTO)	Si ferma e indica che non costituisce minaccia (ad esempio, alza le mani)
Step 3	Ordina a voce o gesti di avvicinarsi una persona (ad esempio, AVANZA UNO)	Una persona (ovvero il Capo del gruppo) avanza verso la posizione della sentinella
Step 4	Consentire alla persona da riconoscere di avvicinarsi abbastanza per l'identificazione visiva ovvero di pronunciare a bassa voce la formula (per il riconoscimento) e quindi di fermarla.	Si ferma
Step 5	Ove la persona sia sconosciuta, avvia la procedura (di riconoscimento) a bassa voce	Fornisce il riscontro convenuto
Step 6	Richiama gli eventuali altri componenti del gruppo, sia singolarmente dicendo Avanti Uno!, ovvero tutti insieme, dicendo Avanti! , coerentemente con la situazione contingente.	La seconda persona, o il resto del gruppo, avanza per essere identificato dalla sentinella, coadiuvato dalla persona riconosciuta inizialmente che si posiziona vicino alla sentinella stessa fino a che tutti non sono stati riconosciuti

2.4 FUOCO DELLE SENTINELLE

Le circostanze per cui una sentinella possa far fuoco contro una persona o un gruppo che abbia fallito la procedura di riconoscimento sono demandate all'Autorità nazionale e devono variamente dipendere dalla situazione particolare e dalle Regole di Ingaggio (RoE) che devono essere applicate.

CAPITOLO 3 STANDARDS, TECNICHE E PROCEDURE PER L'USO DI POSSIBILITÀ (CAPABILITIES) E STRUMENTI PER IL RICONOSCIMENTO OPERATIVO (IN OPERAZIONE, testualmente COMBAT).

3.1 PREMESSA

Gli strumenti per l'identificazione operativa (Combat Identification Devices – CID) sono impiegati congiuntamente ad appropriate procedure di acquisizione e di identificazione delle forze amiche. Esse costituiscono supplemento (supplement to aid) nell'identificazione di forze amiche, sul campo di battaglia ovvero in Area di Operazioni, in modo da ridurre il rischio di fuoco fratricida. A causa della loro possibile compromissione, detti strumenti (CID) dovrebbero essere impiegati o attivati per specificati e prestabiliti periodi di tempo. Un appropriato livello di comando fornirà linee guida temporali/limitazioni per l'impiego di tali strumenti.

3.2 DEFINIZIONI

Nel presente Capitolo saranno impiegati i seguenti termini e definizioni:

a. Attivo. /…/ attivo è un aggettivo applicato ad azioni o equipaggiamenti che emettono energia in grado di essere individuata.
b. Passivo. /…/ passivo è un aggettivo applicato ad azioni o equipaggiamenti che non emettono energia in grado di essere individuata.

3.3 CAPACITÀ DEGLI STRUMENTI PER L'IDENTIFICAZIONE OPERATIVA (CID)

1. Gli strumenti di identificazione operativa disponibili forniscono una varietà di opportunità (variety of means) che sono impiegati congiuntamente con i sensori di puntamento per fornire un'elevata sicurezza nell'identificazione delle forze amiche. È la combinazione tra strumento e sensore che caratterizza la capacità dello strumento di identificazione operativa (CID); però, un particolare strumento può essere osservabile impiegando diversi tipologie di sensori.

2. Visivi (Ottici). Gli strumenti ottici (visual devices) consentono l'osservazione impiegando la visione di uno (ARGH) così il sensore è l'occhio umano. Tali dispositivi includono pannelli passivi arancioni posti sulla parte superiore del veicolo per l'identificazione aerea in condizioni di luce diurna, luci colorate chimiche attive (CYALUME ?) insegne nazionali e marcatura dei veicoli. Talune nazioni hanno adottato insegne nazionali colorate che sono sia visibili in condizioni di normale illuminazione sia nell'illuminazione all'infrarosso-vicino di notte (lo spettrometro emette una radiazione che attraversa l'oggetto e restituisce la composizione fisica e chimica delle particelle di cui è composto l'oggetto osservato, NDR). LA Marcatura dei veicoli che prevedono numeri e simboli sono impiegati per identificare le unità; tali marcature possono essere effettuate anche da materiali che riflettano l'infrarosso-vicino.

3. Infrarosso. Le capacità degli strumenti di identificazione operativa che sfruttano lo spettro dell'Infrarosso sono normalmente categorizzati coerentemente con la banda e

con la lunghezza d'onda dell'infrarosso, e specificamente InfraRosso-vicino (0,7 – 1.0 micron), Infrarosso-medio

(approssimativamente 3 – 5 micron) e Infrarosso-lontano (approssimativamente 8 – 12 micron). L'infrarosso può essere utilizzato per descrivere (caratterizzare) lo strumento di identificazione e il sensore.

a. Infrarosso-vicino. È possibile osservare l'infrarosso-vicino (Near InfraRed – NIR) esclusivamente in condizioni di buio impiegando un sensore ad intensificazione di immagine (Image-Intensifyng, II, come ad esempio gli apparati per la visione notturna (Night Vision Goggles (NVG)). Un dispositivo all'Infrarosso-vicino può essere attivo o passivo. Esempi di dispositivi IR attivi sono i fari IR o le luci chimiche IR (?). i dispositivi passivi sono normalmente i nastri riflettenti, i patches (letteralmente sarebbe cerotti, ma????) e bandiere che possono essere illuminate con strumenti di puntamento laser ovvero con illuminatori laser per incrementrarne la visibilità con un sensore ad intensificazione di immagine.
b. Infrarosso-medio e Infrarosso-lontano. Le bande dell'infrarosso-medio e dell'infrarosso-lontano si riferiscono normalmente alla banda termica osservabile con strumenti a immagine termica (Camere Termiche), sia durante l'arco diurno che quello notturno. Gli strumenti di identificazione operativa ad immagine termica includono strumenti attivi come le camere termiche e strumenti passivi come i pannelli termici montati sui veicoli o trasportati da personale appiedato.

4. Domande e risposte (ritengo intendano dire "attivazione e reazione"). Le capacità di attivazione e reazione degli strumenti di identificazione operativa richiedono un (?) "interrogatore" (il tiratore) per l'emissione della segnale in radio-frequenza (RF) per determinare (letteralmente sarebbe "suscitare") una reazione (lett. Risposta) del transponder (il bersaglio) così che sia possibile identificare l'entità come amica o sconosciuta. Questa capacità può essere vantaggiosa nel caso in cui unità affiliate assegnate …… . Le tecnologie associate a questa capacità continuano a essere sviluppate e non sono descritte all'interno di questo documento. Ad ogni modo, per maggior comprensione, di seguito gli seguenti esempi di "domande e risposte" in via di sviluppo:

a. Dispositivi per l'identificazione dei bersagli sul campo di battaglia (BTID). Il BTID è un sistema radar intercetta-transponder, conforme con lo STANAG 4579. È principalmente impiegato su veicoli terrestri e sistemi d'arma di bordo. La forma d'onda del BTID garantisce al Digital Data Link (DDL) e al Data Exchange Model la capacità di creare una rete conoscitiva della situazione locale contro le piattaforme equipaggiate con BTID.
b. Radio Based Combat Identificazion (RBCI). Le basi della capacità RBCI sono le radio dotate di ricevitore GPS SINCGARS ASIP. L'RBCI scambia le informazioni di localizzazione GPS per garantire sicurezza nel tiro, tanto indiretto quanto aria-superficie. La Radio Based Situational Awareness (RBSA) impiega la funzione di segnalazione delle radio SINCGARS ASIP, sia veicolari che portatili, che consente alla

radio di trasmettere la sua posizione basando sull'incremento di tempo all'aumentare della distanza oppure quando la radio è bloccata.

c. Reverse Identification Friend or Foe (IFF) (Mode S/5). La modalità S/5 è una forma d'onda dell'IFF che fornisce una sicura e reciproca (?) identificazione degli assetti terrestri amici dai velivoli. L'IFF inverso sfrutta il protocollo IFF corrente, Mark 12, come definito nello STANAG 4193 (?).

3.4 STANDARD OPERATIVO MINIMO CID.

1. Lo Standard Operativo Minimo del CID include l'uso delle capacità nel visibile e nell'infrarosso. Lo standard operativo minimo riconosce che i soldati della coalizione e gli equipaggiamenti dovrebbero mostrare una segnatura riconoscibile agli altri sistemi della coalizione nel visibile, nello spettro dell'IR-vicino, medio e lontano.
2. Questo standard minimo non implica che debba essere impiegato un particolare strumento CID, ma consente a una nazione di selezionare la soluzione più appropriata e costo-efficace e che questo strumento conforme selezionato sarà accettato dagli altri partner della coalizione.

3.5 STRUMENTI CID.

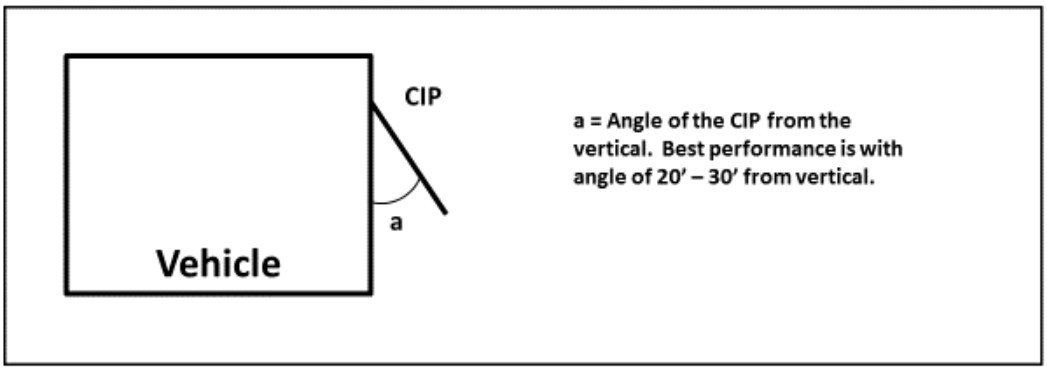
La seguente sezione descrive gli strumenti CID disponibili incluse possibilità d'impiego, limitazioni e considerazioni sull'uso di ciascun particolare strumento.

3.5.1. COMBAT IDENTIFICATION PANEL (CIP)

1. Concetto. Il CIP è un dispositivo all'Infrarosso-medio e lontano montato su veicoli, equipaggiamenti e installazioni, che produce un'immagine fredda di contrastoall'interno della segnatura del bersaglio, identificabile con sensori termici (Termal Imagery – TI). L'operatore (ad esempio, il mitragliere) può usare questo contrasto (ambiente più freddo e bersaglio più caldo) per determinare se il bersaglio è amico o sconosciuto; la mancanza di contrasto non identifica necessariamente il bersaglio come nemico, ma altresì non consente all'operatore di identificare positivamente il bersaglio come amico.
2. Descrizione. Il CIP è una tavola o una superficie rigida, delle dimensioni approssimative di 60 cm x 80 cm, che opera come uno specchio termico che riflette la temperatura contrastante più fredda dal cielo. Un CIP può essere un pannello piatto o una serie di pannelli vicini sovrapposti (a mo' di tende veneziane). Può essere fatto di qualsiasi materiale durevole, possiede una bassa emissione termica su una facciata ed è disegnata per essere invertita o mascherata. Un CIP è normalmente fissato a bordo di veicoli come anche su altri equipaggiamenti e piattaforme.
3. Montaggio e fissaggio di un CIP.
   a. Colore. Sarebbe l'ideale verniciare o ricoprire con nastro un CIP per far assumere la stessa colorazione della piattaforma su cui è installato e consentirne il mascheramento; anche l'altra parte del CIP dovrebbe essere analogamente mascherata.

b. Visibilità. I veicoli dovrebbero avere posizionati dai 4 ai 10 pannelli per far in modo di essere visibili nelle tre dimensioni.

c. Angolo di riflessione. Ogni CIP deve essere posizionato per garantire che sia riflessa ogni radiazione più fredda dal cielo mentre si fornisce sufficiente superficie per essere riconosciuta alla massima distanza di ingaggio per i sensori TI. Un CIP presenterà normalmente solo un distinto punto freddo se è impiegato



e

nte angolo per permettere un efficace riflesso ed è esposta una superficie sufficiente per il riconoscimento a Immagine Termica. Per essere efficace, il pannello deve essere posto con un'angolazione di 20/30 gradi dalla verticale.

a = angolo del CIP dalla verticale. Le migliori performance con un angolo di 20/30 gradi dalla verticale.

Veicolo

Figura 1: angolo di montaggio di un Pannello per l'Identificazione Operativa

d. Caratteristiche: le caratteristiche costruttive di un CIP richiedono durevolezza, uniformità e semplicità, poiché la perdita di un CIP montato potrebbe causare incertezza nel determinare la non ostilità dell'obiettivo osservato. La durevolezza è molto importante. L'uniformità di posizionamento assicura sicurezza nell'identificazione e l'uniformità della forma facilita la manutenzione e il riposizionamento. Semplicità di montaggio inoltre riduce la manutenzione e i costi di sistema.

e. Modalità di montaggio. Il miglior sistema di montaggio è una cornice metallica che consente al CIP di essere ribaltato, all'interno della cornice, o mascherato. In

tale configurazione il CIP è in modalità non operativa. La cornice di montaggio può essere fissata con supporti o ganci o molle.

4. Riconoscimento di un CIP.
   a. Limiti di distanza. Le capacità di un CIP dipendono dalla qualità del sensore termico e dalla dimensione della superficie esposta del pannello. Un CIP sarà meno efficace oltre i 2500 metri, specialmente per veicoli in movimento. L'impiego di un CIP in distanze superiori a 1500 metri è complicato in quanto i reticoli della camera termica possono oscurare l'immagine più fredda. Anche a distanze inferiori ai 1500 metri può essere difficile identificare quando si sta effettuando un'osservazione diretta sul bersaglio.
   Modulando la polarità dell'immagine termica da " bianco caldo" a "nero caldo" miglioreranno le probabilità di una identificazione positiva di un CIP nell'acquisizione e ingaggio di un bersaglio. Il contrasto freddo dell'immagine del CIP sulla superficie calda del veicolo risulterà più chiara nell'uso della polarità "nero caldo".
   b. Addestramento all'identificazione. Se identificato rapidamente e positivamente, un CIP supporterà i serventi alle armi nella decisione di non ingaggiare un veicolo amico. L'aggiunta di un CIP, comunque, dovrebbe essere prevista nel previsto addestramento al riconoscimento di Immagini Termiche. All'arrivo in Teatro, dovrebbero essere condotte prove per confermare le capacità del CIP prima di iniziare le operazioni. L'addestramento dovrebbe inoltre prevedere anche il riconoscimento o il posizionamento del CIP sulle piattaforme così da assistere il tiratore nella procedura di "interrogazione" del bersaglio. Ciò dovrebbe includere il riconoscimento con "bianco caldo" e con "nero caldo" prima dell'ingaggio. Dovrebbero essere inoltre sviluppate e impiegate in addestramento anche librerie di profili di minacce termiche.
5. Considerazioni sul CIP.
   a. Generalità. L'uso di CIP no dovrebbe riguardare solo i criteri di riconoscimento dei bersagli, ma anche come questi possono essere danneggiati o resi inutilizzabili a causa della polvere/sporco o persi dai veicoli. In aggiunta, le forze non combattenti che si trovano sul capo di battaglia non dovrebbero poter utilizzare detti strumenti. Un CIP dovrebbe essere inteso come l'unico strumento per il riconoscimento positivo di una entità.
   b. Degrado. A causa di talune circostanze le prestazioni posso essere ridotte. Il contrasto tra un CIP e un veicolo o una piattaforma può essere ridotto dagli effetti di nuvole basse, cortine fumogene, strati di foglie o accumulo di sporco/polvere sulla superficie di un CIP. L'andamento del terreno, degli alberi e/o altra vegetazione, la propria posizione di tiro defilata e altri ostacoli frammenteranno la forma del veicolo e ne renderà più difficoltosa l'identificazione.
   c. Sicurezza. L'impiego di particolari configurazioni di CIP non garantirà sicurezza per lunghi periodi di tempo. Il nemico sarà in grado di reagire agevolmente e rapidamente. Enfasi dovrebbe comunque essere posta nell'uso dei CIP tanto nel …….(non conosco quella frase idiomatica).

d. Inganno. Un CIP è altamente esposto all'inganno da parte del nemico così come possono essere simulati sia volontariamente che involontariamente. In ogni caso, il riconoscimento dell'entità, basata su caratteristiche e azioni, fatta con apparti termici o visivi, dovrebbe essere il fattore decisivo in ogni decisione di ingaggio.
   (1) Simulazione volontaria. In questo caso, il nemico intenzionalmente riproduce i pannelli così da sfruttare o indebolire la loro efficacia.
   La contromisura è quella di predisporre i pannelli delle forze amiche in modalità "non operativa" (in pratica di spegnerli - *NDR*).
   (2) Simulazione involontaria. In questo caso, elementi dell'entità (?) rileva un'immagine (termica) fredda simile a quella di un CIP. Questo effetto è stato osservato in alcuni veicoli con elementi quali parabrezza, cofani portaattrezzi, scomparti di stivaggio (portabagagli) o copri cingolo. Per ovviare ciò, è necessario un addestramento al riconoscimento della segnatura termica, con particolare riguardo allo sfruttamento dei segnali (cues ?) dell'immagine dell'intero bersaglio e non solo dei CIP.
e. Manutenzione. La semplicità del progetto lo rende particolarmente semplice da mantenere. Un CIP deve essere tenuto pulito per garantirne il riflesso (il riverberare, il riflettere). Un CIP dovrebbe essere rimpiazzato (sostituito) quando la vegetazione, il vento forte o altri effetti della battaglia (schegge *NDR*) causano danni o perdite del pannello.

6. Ispezione prima del combattimento. L'ispezione ai CIP montati dovrebbe essere una priorità nella condotta delle ispezioni prima della battaglia e nelle manutenzioni e nei controlli preventivi. Un'ispezione ad un CIP dovrebbe comprendere i seguenti passaggi:
   a. Montaggio dei CIP nella corretta posizione;
   b. Controllo di danni e perdite agli affusti;
   c. Ripianamento o riparazione di CIP danneggiati o persi;
   d. Rimozione dal CIP della polvere, fango, sabbia, neve e di altri elementi coprenti utilizzando (per pulirlo) un panno morbido, privo di sostanze oleose, grasse e benzina;
   e. Se impiegato nastro termico, assicurazione che sia ancora aderente al materiale;
   f. Verifica che ciascun CIP sia visibile attraverso la camera termica.

…… NON FINISCA VAI ATP 91

RIFERIMENTI

NAZIONALI

- SMD III REP – CID, PID/S-1 *La Dottrina Militare Italiana*, Ed. 2011
- SMD III Rep. – CID, PID/interim 3.14 *Dottrina Interforze Nazionale per la Protezione delle Forze*, Vol. I, Ed. 2012
- SME III RIF, *Vademecum sulle misure di protezione del personale contro rischi di natura ambientale e CBRN*, Ed. 2009
- SME III RIF-COE, ND *Effect Based Approach to Operations (EBAO)*, 1^ Def., Ed. 2009
- SME III RIF-COE, *Manuale per la pianificazione delle operazioni terrestri*, Ed. 2011
- SME III RIF-COE, ND *Principi generali e approccio alle operazioni militari terrestri*, Ed. 2013
- SME III RIF-COE, ND *La manovra delle forze terrestri*, Ed. 2014
- SME III RIF-COE, ND *L'ambiente operativo e le forze terrestri*, Ed. 2014
- COMFORDOT, PSE-3.2.14 *Ostacolo e Operazioni di Mobilità*, Ed. 2015
- COMFORDOT, PSE-3.4.5 *Le Operazioni di Stabilizzazione*, Ed. 2015
- COMFORDOT, PSE-3.10 *Le Operazioni Informative Terrestri*, Ed. 2014
- COMFORDOT, PSE-3.13.05 *Le Operazioni Anfibie*, Ed. 2015
- COMFORDOT, PSE-3.14.05.02 *La Protezione delle Basi in Operazioni*, Ed. 2017
- COMFORDOT, PIE-3.24.33.1 *La Difesa CBRN di reparto*, Ed. 2014
- COMFORDOT, PIE-3.29 *L'impiego dell'Artiglieria Terrestre*, Ed. 2015
- COMFORDOT, PIE-3.30 *L'impiego dell'Artiglieria Controaerei*, Ed. 2015
- COMFORDOT, PIE-3.31 *L'impiego del Genio*, Ed. 2015
- COMFORDOT, PIE-3.32 *L'impiego delle Trasmissioni*, Ed. 2015
- COMFORDOT, PIE-3.33 *La Difesa CBRN Specialistica*, Ed. 2015
- COMFORDOT, PIE-3.34 *L'impiego dell'Aviazione dell'Esercito*, Ed. 2015
- ISPETTORATO PER LA FORMAZIONE E LA SPECIALIZZAZIONE DELL'ESERCITO – POLO GENIO, Pub. 6708 *Procedimenti di impiego delle squadre guastatori nella bonifica e ricognizione di un'area minata o di un itinerario*, Ed. 2005
- COMSCUOLE – POLO Interforze per la Difesa NBC, Pub. 5921 *Nomenclatore NBC*, Ed. 2008
- COMSCUOLE – POLO Interforze per la Difesa NBC, Pub. 6620 *Manuale di Difesa NBC*, Ed. 2011
- COMSCUOLE – POLO GENIO, Pub. 6762 *Norme per la bonifica dei poligoni*, Ed. 2008
- COMFOTER – COMANDO GENIO, SOP *Tecniche e Procedure per la condotta di Explosive Ordnance Disposal (EOD)*, Ed. 2014
- COMSUP FOTER – POLO GENIO, Pub. 6760 *Procedimenti Tecnico-Tattici contro Ordigni Esplosivi Improvvisati (PTT C-IED)*, Ed. 2011
- COMGENIO, PTE-4.05.16 *Sistemi integrati per la protezione delle basi*, Ed. 2016.

RIFERIMENTI NATO

- NATO, AAP-6 *NATO Glossary of Terms and Definitions*, Ed. 2013
- NATO, AJP-1 *Allied Joint Doctrine*, Ed. D, December 2010
- NATO, AJP-2 *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, Ed. 2016
- NATO, AJP-3 *Allied Joint Doctrine for the Conduct of Operations*, Ed. 2011
- NATO, AJP-3.2 *Allied Joint Doctrine for Land Operations*, Ed. 2016
- NATO, AJP-3.5 *Allied Joint Doctrine for Special Operations*, Ed. 2009
- NATO, AJP-3.8 *Allied Joint Doctrine for CBRN Defence*, Ed. 2012
- NATO, AJP-3.14 *Allied Joint Doctrine for Force Protection*, Ed. 2015
- NATO, AJP-5 *Allied Joint Doctrine for Operational-Level – Planning*, Ed. 2013
- NATO, ATP-3.2.1 *Land Tactics*, Ed. 2009
- NATO, ATP-3.8.1 Vol. I *CBRN Defence on Operations*, Ed. 2010
- NATO, ATP-3.8.1 Vol. II *Specialist CBRN Defence Capabilities*, Ed. 2014
- NATO, ATP-3.16.1 *Countering Insider Threats (CIT)*, Ed. 2016
- NATO, ATP-91 *Identification of Land Forces on the battlefield and in an area of operation*, Ed. 2015
- NATO, STANAG 2143 *Explosive Ordnance Reconnaissance / Explosive Ordnance Disposal* (EOR/EOD), Ed. 2005
- NATO, STANAG 2287 *Task verbs for use in planning and the dissemination of orders*, Ed. 2006
- NATO, STANAG 2485 *Countermine Operations in Land Warfare*, Ed. 2002
- NATO, ACIEDP-01 *Counter-Improvised Explosive Device (C-IED) Training Requirements*, Ed. 2013
- NATO, AEODP-3(B) Vol. I & II *Interservice Improvised Explosive Device Disposal Operations on Multinational Deployment – A guide for Staff Officers/Operators*, Ed. 2014
- NATO, AJMedP-4 *Allied Joint Medical Force Health Protection Doctrine*, Ed. 2011

ALTRI RIFERIMENTI

- Unione Europea, Regolamento (CE) n.428/2009, 05/05/2009
- Dipartimento per la Protezione Civile, *Piano nazionale delle misure protettive contro le emergenze radiologiche*, Ed. 2010
- UK, JDP 3-64 *Joint Force Protection*, Ed. 2010
- UK, ADP *Operations*, Ed. 2010
- US, ADP 3-37 *Protection*, Ed. 2012
- US, ADRP 3-37 *Protection*, Ed. 2014
- US, ATP 5-19 *Risk Management*, Ed. 2014
- US, FM 7.15 *The Army Universal Task List*, Ed. 2009

ABBREVIAZIONI E SIGLE

AD	*Air Defence* – Difesa da Minaccia Aerea
AGM	*Air-to-Ground Missile*
AO	Ambiente Operativo
AoO	*Area of Operations*
ARM	*Anti Radiation Missile* – Missile Anti Radiazione
BCMD	*Biological & Chemical Munition Disposal*
BC IEDD	*Biological & Chemical Improvised Explosive Device Disposal*
BH	*Battle Handover* – Passaggio di consegna del combattimento
BHL	*Battle Handover Line* – Linea di passaggio di consegna del combattimento
BN	*Battalion*
BPC	*Building Partner Capacity*
CASEVAC	*CASualty EVACuation*
CBRN	*Chemical, Biological, Radiological and Nuclear*
CCIR	*Commander's Critical Information Requirements*
CDR	*Commander*
C-IED	*Counter Improvised Explosive Device*
CIMIC	*Civil-Military Cooperation*
CMD	*Conventional Munition Disposal*
CND	*Computer Network Defense*
COIN	*Counter-Insurgency*
COLPRO	*Collective Protection* – Protezione collettiva
COM	*Commander*
COMSEC	*Communications Security*
COP	*Combat Out-Post* - Avamposto
COS	*Chief of Staff*
CP	*Check-Point*
CPT	*Close Protection Team*
C-RAM	*Counter-Rocket Artillery and Mortars*
CRM	*Composite Risk Management* – Gestione del Rischio Composito
CS	*Combat Support*
DENAM	Dislocazione, Entità, Natura, Atteggiamento e Movimento
DIM	*Detection, Identification and Monitoring* - Individuazione, Identificazione e Monitoraggio
DIME	Diplomatico, *Information*, Militare, Economico
DDR	*Disarmament, Demobilization and Reintegration*
DOTLMPFI	*Doctrine and concept development, Organization, Training, Material, Leadership and education, Personnel and Facilities*
EA	*Electronic Attack*
EA	*Engagement Area*
ECM	*Electronic Counter Measures* – Contromisure Elettroniche

EES	Elicotteri da Esplorazione e Scorta
EO	*Explosive Ordnance – Ordigno esplosivo*
EOD	*Explosive Ordinance Disposal* – Bonifica di ordigno esplosivo
ESC	*Effective Security Campaigns*
ESMRM	*Explosive Safety and Munition Risk Management*
EW	*Electronic Warfare*
F.A.	Forza Armata
FEBA	*Forward Edge of the Battle Area* - Fronte anteriore dell'area della battaglia
FOB	*Forward Operating Base*
GBAD	*Ground Based Air Defence*
HRP	*High Risk Personnel* – personalità ad altro rischio
HQ	*Headquarters*
IED	*Improvised Explosive Device* – Ordigno esplosivo improvvisato
IEDD	*Improvides Explosive Detection Dog*
INFOSEC	*Information Security*
INTSUM	*Intelligence Summary*
IPB	*Intelligence Preparation of the Battlespace*
IPE	*Individual Protective Equipment* - Equipaggiamento di protezione individuale
IPOE	*Intelligence Preparation of the Operational Environment*
IR	*Infra-Red* - Infrarossi
ISG	*Isolated Soldier Guidance*
ISR	*Intelligence, Surveillance, Reconnaissance*
IT	*Information Technology*
JTAC	*Joint Tactical Air Controller*
EEFI	*Essential Elements of Friendly Information* - Elementi Essenziali delle Informazioni Proprie
E-TTP	*Enemy Tactics, Techniques, and Procedures* - Tecniche, tattiche e procedure Nemiche
LCB	Lavori sul Campo di Battaglia
LEMV	*Long Endurance Multi-intelligence Vehicles*
LEGAD	*Legal Advisor*
LNO	*Liaison Officer*
LOC	*Line of Communication* – Linea di Comunicazione
LOG	*Logistic*
LNO	*Liaison Officer*
LSF	*Local Security Force*
LT	*Liaison Team*
MAAR	*Monthly ANDSF Assessment Report*
MANPAD	*Man Portable Air Defence System*
MDD	*Mine Detecntion Dog*
MEDINT	*Medical Intelligence*
METL	*Mission Essential Task List* - Compiti essenziali per la missione
METT-TC	*Mission, Enemy, Terrain and weather, Troops and support available, Time*

	available, Civil condiderations – Variabili della missione
MC	*Military Cooperation*
MDD	*Mine Detecntion Dog*
MED	*Medic*
MEDEVAC	*MEDical EVACuation*
MoD	*Ministry of Defence*
MOE	*Measurement of Effectiveness*
MoI	*Ministry of Interior*
MOP	*Measurement of Performance*
MP	*Military Police*
MRBM	*Medium-range Ballistic Missiles*
MRSAM	*Medium Range Surface to Air Missile*
NAI	*Named Area of Interst*
NSE	*National Support Element*
OCC-R	*Operations Coordination Center – Regional*
OE	*Operational Environment*
OODA	*Observe, Orient, Decide, Act*
OP	*Observation Point*
OPSEC	*Operation Security* – Sicurezza dell'Operazione
PIE	Pubblicazione d'Impiego dell'Esercito
PL	*Phase Line*
PMESII-PT	*Political, Military, Economic, Social, Information, Infrastructure, Physical Environment and Time*
POA	*Posto Osservazione e Allarme*
PR	*Personnel Recovery*
PPP	Profile, *Presence* e *Posture* - Profilo, Presenza e Postura
PSE	Pubblicazione di Supporto dell'Esercito
QRF	*Quick Reaction Force*
RCP	*Route Clearance Package* – Complesso tattico specializzato nella condotta delle Operazioni di Mobilità *Clearing Operations*.
RL	*Report Line*
ROE	*Rules of Engagement*
RPAS	*Remotely Piloted Aircraft System*
SAMP/T	Superficie Aria a Media Portata Terrestre
S&R	*Stabilization and Reconstruction*
SAPR	Sistemi Aeromobili a Pilotaggio Remoto
SF	*Special Forces*
SFA	*Security Force Assistance*
SIBCRA	*Sampling, Identification, Biological, Chemical, Radiological Agents*
SHORAD	Sistemi a corta gittata
SME	*Subject Matter Expert*
SRBM	*Short-range Ballistic Missiles*
TACON	*Tactical Control* - Controllo Tattico
TACP	*Tactical Air Control Party*

TBM	*Theatre Ballistic Missiles*
TBMD	*Theatre Ballistic Missile Defence*
TF	*Task Force*
T.O.	Teatro Operativo
TOA	*Transfer Of Authority – Trasferimento di Autorità*
TIM	*Toxic Industrial Materials*
TTP	*Tactics, Techniques, and Procedures* - Tecniche, tattiche e procedure
T-UAV	*Tactical - Unmanned Aerial Vehicle*
UAS	*Unmanned Aerial System*
UAV	*Unmanned Aerial Vehicle – Unpilote Aerial Vehicle System*
UAVS	*Unpiloted Aerial Vehicle System*
UGS	*Unmanned Ground Vehicle*
VCP	*Vehicle Check-Point*
V-SHORAD	Sistemi a cortissima portata
WIT	*Weapons Intelligence Team*
WFZ	*Weapon Free Zone*
WMD	*Weapons of Mass Destruction* – Armi di distruzione di massa