COMANDO PER LA FORMAZIONE, SPECIALIZZAZIONE E DOTTRINA DELL'ESERCITO

PSE-3.14.05.02

LA PROTEZIONE DELLE BASI MILITARI IN OPERAZIONI

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

Fatte salve le esigenze di servizio, ufficio o istituto, nessuna parte di questa pubblicazione può essere riprodotta in qualsiasi forma a stampa, fotocopia, microfilm, scansione digitalizzata o altri sistemi, senza l'autorizzazione scritta dell'originatore.

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

PAGINA INTENZIONALMENTE BIANCA

PUNTI CONTATTI

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. Antonino MIDOLO

Email: casezdot@comgenio.esercito.difesa.it

Autori

Col. Valerio LUCIANO

Email: caufstdesp@comaca.esercito.difesa.it

Ten.Col. Antonio ASSORATI

Email: caufoai@rgtaca17.esercito.difesa.it

Magg. Giuliano LA ROCCA

Email: casezinfosec@scfant.esercito.difesa.it

Cap Marco CAROSI

Email: marco.carosi@esercito.difesa.it

Cap. Marco PALMISANO

Email: marco.palmisano1@esercito.difesa.it

Ten. Col. Massimiliano DE CICCO

Email: massimiliano.decicco@esercito.difesa.it

Magg. Daniele PIATTI

Email: daniele.piatti@esercito.difesa.it

Cap. Gianluca MEROLA

Email: mailto:gianluca.merola@esercito.difesa.it

Eventuali commenti, suggerimenti e proposte di modifica possono essere inviate direttamente all'indirizzo *e-mail* sopra riportato.

PREMESSA

Approvo la presente Pubblicazione di Supporto dell'Esercito PSE 3.14.05.02 *La protezione delle basi militari in operazioni*, Edizione 2017.

La Protezione delle basi militari, nell'ambito dello sviluppo delle attività riguardanti la Protezione, è fondamentale per garantire la sopravvivenza e la capacità operativa delle unità ivi accantonate e, di conseguenza, il successo delle operazioni.

Tale attività ricade sotto la responsabilità diretta dei Comandanti ai vari livelli che, per svilupparla, hanno la necessità di approntare un'organizzazione di *Force Protection* (FP), in termini di personale, strumenti, assetti, sistemi e materiali, attagliata alle esigenze operative della missione assegnata.

La presente PSE-3.14.05.02

- recepisce le linee guida della recente pubblicazione NATO, AJP 3.14 (A) vers. 1 *Allied Joint Doctrine for Force Protection*, Ed. 2015;
- integra le linee guida contenute nella SMD III REP/CID, PID/O-3.14 *La protezione delle Forze*, Ed. 2012;
- si pone quale documento di riferimento per l'organizzazione di FP da approntare ai fini della protezione delle basi militari in operazioni per tutte le unità ed i Comandi della F.A..

È stata articolata in modo da:

- richiamare in maniera semplificata, i concetti di base della citata PID inerenti alla FP, fornendo le linee guida per organizzare la sicurezza delle basi militari in operazioni, in relazione al rischio ed attraverso l'applicazione di un processo di *risk management* (gestione del rischio);
- illustrare le misure di FP da adottare per definire le predisposizioni da attuare a tutte le aree capacitive della FP di preminente interesse, ai fini della protezione delle basi militari in operazioni;
- essere applicabile, in maniera flessibile, a tutte le possibili esigenze ed ambienti operativi.

Al fine di trattare in modo esauriente la protezione ad ampio spettro, la presente pubblicazione è stata orientata principalmente al contrasto di una minaccia di tipo "ibrida", supportando lo sviluppo di operazioni di stabilizzazione. La sua applicazione, ai fini delle operazioni tradizionali, dovrà tenere conto anche delle diverse esigenze operative e dei ritmi dettati dalla manovra terrestre o nell'ambito della 3^ Dimensione. Pertanto, sarà cura dei Comandanti, ai vari livelli, adattare allo specifico contesto operativo le misure di protezione contemplate.

La Pubblicazione si rivolge:

- ai Comandanti;
- ai *leaders* e agli *staff*, in particolare delle Cellule S/G/J2 e 3;
- agli specialisti coinvolti nel processo di pianificazione delle misure di FP, quali ad esempio gli addetti CBRN, ISTAR, *Camp Site Manager*, ecc.

Inoltre, essa assume "valenza interforze" in quanto "costituisce il nuovo documento di riferimento, a livello tattico-operativo, per la realizzazione delle opere di protezione delle basi militari semipermanenti/permanenti, delle basi operative avanzate e degli accampamenti nelle operazioni di risposta alle crisi fuori dal territorio nazionale", in aderenza a quanto riportato nella già cit. PID-O 3.14 - Capitolo II, paragrafo 3., nota 3, pag. 11.

La presente Pubblicazione abroga e sostituisce:

- pub. n. 6864 PSE 3.14.1 *La Protezione delle basi militari in operazioni*, Ed. 2015;
- pub. n. 6712 *Manuale sulla protezione delle infrastrutture e delle basi militari nell'ambito delle Crisis Response Operations*, Ed. 2012.

Roma, 06 MAR. 2017

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

INDICE

1. LA PROTEZIONE DELLE BASI MILITARI 1

1.1. RICHIAMI SULLA FUNZIONE OPERATIVA *FORCE PROTECTION* (FP) 1

1.1.1 Definizione 1
1.1.2 Scopo 1
1.1.3 Caratteristiche 1
1.1.4 Aree di coordinamento 2
1.1.5 Elementi fondamentali 2
1.1.6 Ambiente operativo 3

1.2. CARATTERISTICHE DELLE BASI MILITARI 4

1.3. CONSIDERAZIONI DI CARATTERE OPERATIVO PER LA PROTEZIONE DELLE BASI MILITARI 6

1.3.1 Approccio sistematico FP 6
1.3.2 Orientamenti d'impiego per l'organizzazione della difesa 7
1.3.3 Scelta dei siti e delle infrastrutture 11
1.3.4 Sistemi di realizzazione delle basi 12

2. PIANIFICAZIONE E ORGANIZZAZIONE DELLA PROTEZIONE DELLE BASI MILITARI 15

2.1 PIANIFICAZIONE DELLA PROTEZIONE DI UNA BASE MILITARE 15

2.1.1 Avvio del processo di FP 15
2.1.2 Sviluppo del modello di FP 16

2.2 ORGANIZZAZIONE DI FP PER LA PROTEZIONE DI UNA BASE MILITARE 22

2.2.1 Principali attività di FP 22
2.2.2 Organizzazione di FP da approntare: 23
2.2.3 Compiti delle principali figure dell'organizzazione di FP 24
2.2.4 Emanazione delle direttive 29

2.3 *SITUATIONAL AWARENESS* 30

2.4 REDAZIONE DEI PIANI PER LA SORVEGLIANZA E LA PROTEZIONE DI UNA BASE MILITARE 31

2.4.1 Piano di difesa terrestre 31
2.4.2 Piano di difesa aerea 32
2.4.3 Piano di sorveglianza della TAOR 33
2.4.4 Piano per le emergenze 34
2.4.5 Piano per il recupero della capacità operativa 36

2.5 DIREZIONE, COORDINAMENTO E CONTROLLO DELLE MISURE DI PROTEZIONE PREDISPOSTE 37

2.5.1 Direzione 37

2.5.2 Coordinamento 37
2.5.3 Controllo 37

2.6 RICOGNIZIONE DI AREE E INFRASTRUTTURE AI FINI DELLA PROTEZIONE DELLA BASE 38

3. IL SISTEMA INTEGRATO PER LA PROTEZIONE DELLE BASI MILITARI 41

3.1 STANDARDIZZAZIONE DEL SISTEMA DI PROTEZIONE 41
3.1.1 Concetto Operativo 41
3.1.2 Definizione 41
3.1.3 Sviluppo e caratteristiche del sistema 41
3.1.4 Schema funzionale 45

3.2 ESIGENZE OPERATIVE PER IL CONTROLLO E LA PROTEZIONE DI UNA BASE MILITARE 47
3.2.1 Esigenze di carattere generale 47
3.2.2 Esigenze di carattere specifico 49

3.3 PROCEDURE PER LA VERIFICA DEL SISTEMA DI PROTEZIONE DELLA BASE ADOTTATO 52
3.3.1 A seguito di evento/incidente 52
3.3.2 Controlli preventivi 52

3.4 ATTIVITÀ/COMPITI CONNESSI CON LA PROTEZIONE 53
3.4.1 Difesa aerea e antimissile 53
3.4.2 Recupero del personale 59
3.4.3 Fuoco fratricida 59
3.4.4 Sicurezza dell'area delle operazioni della base (TAOR *Control*) 60
3.4.5 Sicurezza ed antiterrorismo 62
3.4.6 Protezione e sopravvivenza 63
3.4.7 Protezione sanitaria 67
3.4.8 Protezione CBRN 69
3.4.9 *Operations Security* (OPSEC) 72
3.4.10 EOD 73

ALLEGATI

A - APPROCCIO SISTEMATICO FP PER LA PROTEZIONE DI UNA BASE MILITARE IN OPERAZIONI

B - APPLICAZIONE DEL CICLO DELLE MISURE DI FP AI FINI DELLA PROTEZIONE DELLE BASI MILITARI

C - MATRICI PER L'ANALISI DEI RISCHI

D - CHECKLIST PER L'AUTOVALUTAZIONE DELLE MISURE DI FP E DEL SISTEMA DI PROTEZIONE ADOTTATO

ABBREVIAZIONI E SIGLE

GLOSSARIO

RIFERIMENTI

ANNESSO I: Lettera di diramazione

INDICE DELLE FIGURE

Figura 1: Gli elementi della Force Protection (JOINT) 2
Figura 2: La capacità nazionale per la protezione delle forze (Rif. PID/O-3.14) 3
Figura 3: Elementi della difesa attiva 8
Figura 4: Elementi della difesa passiva 9
Figura 5: Elementi per il controllo della TAOR 10
Figura 6: Modello di FP 17
Figura 7: Schema grafico della ricognizione di un sito della FP 39
Figura 8: Aree funzionali per la difesa (AFD) 43
Figura 9: Schema componenti e funzioni operative degli MFD 45
Figura 10: Organizzazione SIPROB 46
Figura 11: Schema di struttura di Difesa Integrata 48
Figura 12: Schema di difesa aerea delle basi 57

PAGINA INTENZIONALMENTE BIANCA

1. LA PROTEZIONE DELLE BASI MILITARI

1.1. RICHIAMI SULLA FUNZIONE OPERATIVA *FORCE PROTECTION* (FP)

1.1.1 Definizione

La funzione operativa FP è "l'insieme di misure e mezzi per ridurre al minimo la vulnerabilità del personale, delle installazioni, dei mezzi e delle attività rispetto a qualsiasi minaccia ed in ogni circostanza al fine di preservare la libertà d'azione e l'efficienza operativa delle forze"[1].

1.1.2 Scopo

La FP ha lo scopo di:

- contrastare la minaccia in tutte le sue forme;
- preservare l'integrità del personale, delle infrastrutture, dei mezzi, dei materiali, degli equipaggiamenti, delle attività e delle informazioni;
- prevenire i rischi eventualmente rappresentati da particolari caratteristiche dell'ambiente naturale, antropico ed operativo;
- mitigare il senso di incertezza e di indeterminatezza generato dalla presenza e dalle azioni condotte dall'avversario, infondendo nel proprio personale fiducia e sicurezza;
- evitare il fuoco fratricida.

1.1.3 Caratteristiche

La Protezione delle Forze assolve il ruolo di funzione operativa fondamentale per la riuscita delle operazioni militari. Essa è, pertanto, una responsabilità diretta dei Comandanti, ai vari livelli ordinativi, i quali devono curarne, avvalendosi del proprio staff, la valutazione delle problematiche in tutte le fasi della pianificazione e condotta delle operazioni.

La FP è caratterizzata dai seguenti fattori di primaria importanza:

- **l'ambiente operativo** in cui verrà svolta la missione;
- **la valutazione della minaccia**, da definire in sede di pianificazione delle misure di FP attraverso un processo di valutazione dei pertinenti elementi informativi;
- **la gestione del rischio**, direttamente connotata con la scelta delle priorità di realizzazione delle misure di FP e basata sullo sviluppo di un'attività ciclica di valutazioni continue che assicuri, di volta in volta, le necessarie verifiche ed i rapidi adeguamenti dell'organizzazione FP all'evoluzione della minaccia e della missione.

[1] Cfr. già cit. PID/O-3.14.

1.1.4 Aree di coordinamento

La FP è una funzione operativa "interforze", complessa e fondamentale per il successo delle operazioni. I Comandanti ai vari livelli, per svolgere la loro funzione, hanno la necessità di approntare un'organizzazione di FP, in termini di personale qualificato, strumenti, assetti, sistemi e materiali, attagliata alla missione assegnata.

La NATO, nell'ambito dell'aggiornamento della direttiva strategico-operativa sulla FP, ha definito tre "aree di coordinamento per la FP" [2]:

- **attiva** (*active defense*): misure, compiti ed attività per individuare, prevenire, annullare o ridurre l'efficacia di un'azione di forze ostili o rischi ambientali;
- **passiva** (*passive defense*): misure, compiti ed attività per minimizzare gli effetti di un'azione di forze ostili o rischi ambientali;
- **ripristino capacità operativa** (*recuperation*): misure, compiti ed attività per ripristinare la capacità operativa ridotta o annullata a seguito di un'azione di forze ostili o rischi ambientali.

1.1.5 Elementi fondamentali

In ambito NATO, con la già cit. AJP 3.14, vengono identificati anche i seguenti otto "elementi fondamentali" della FP (fig. 1):

- *Security;*
- *Military Engineer Support to FP;*
- *Air Defense;*
- *Tactical Area of Responsibility Control;*
- *Medical FP and Force Health Protection;*
- *CBRN Defense;*
- *Resilience;*
- *Consequence Management.*

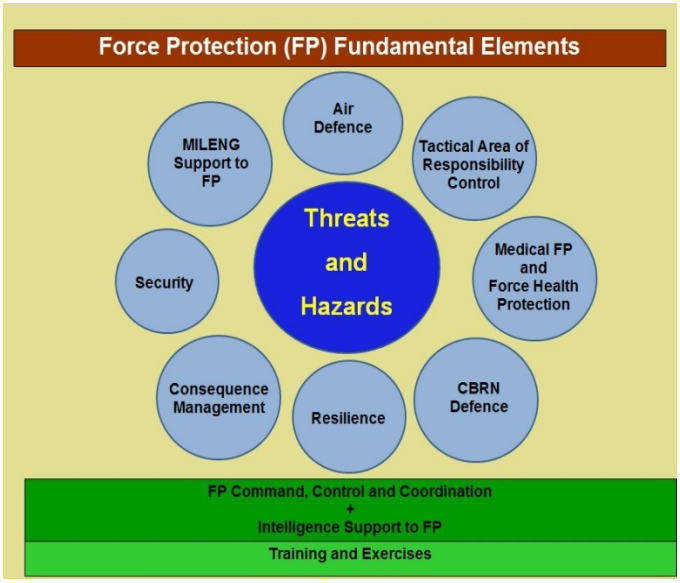


Figura 1: Gli elementi della Force Protection (JOINT)

In ambito nazionale, lo Stato Maggiore della Difesa ha invece definito, nel 2012[3], sei aree capacitive che identificano corrispondenti funzioni di supporto (fig. 2):

- Tutela Amministrativa del Segreto di Stato e delle informazioni classificate;
- Supporto del Genio alla Protezione delle Forze (*Force Protection Engineering* - FPE);

[2] Cfr. già cit. AJP 3.14.

[3] Cfr. già cit. PID/O-3.14.

- Protezione delle Infrastrutture (*Infrastructure Protection*) e Controaviazione Difensiva;
- Protezione Sanitaria e Ambientale (*Health & Environmental Protection*);
- Gestione delle Emergenze (*Consequence Management*);
- Difesa CBRN (CBRN *Defence*);

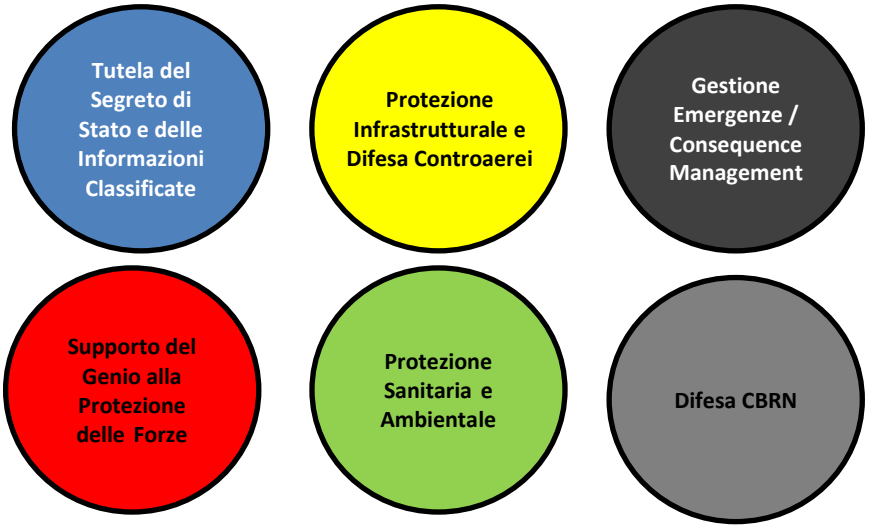


Figura 2: La capacità nazionale per la protezione delle forze (Rif. PID/O-3.14)

Alle citate aree di capacità, anche se non ancora inclusa nella predetta PID-O 3.14, deve essere considerata ai fini della FP anche quella che tratta della *Cyber Defence*.

1.1.6 Ambiente operativo

Ai fini dell'avvio del processo di FP l'ambiente in cui si sviluppa un'operazione può essere definito:

- **permissivo o semi-permissivo:** l'attività di contrasto delle forze/fazioni avverse o nemiche consente uno sviluppo quasi normale (senza cioè azione di contrasto condotta in maniera sistematica) dell'attività delle Forze, anche se il quadro di situazione generale può degenerare, richiedendo l'adozione, rapida, di misure di FP più restrittive. In tale tipologia di Ambiente Operativo, legato normalmente ai temi *Security* o *Peace Support Operations,* si possono sviluppare, a carattere episodico, attività di combattimento a bassa intensità, mentre sono da considerare eccezionali gli episodi che richiedono lo sviluppo di attività di combattimento a media e/o alta intensità;
- **non permissivo:** l'attività delle Forze è sottoposta ad azione di contrasto attraverso lo sviluppo di azioni di combattimento a media e alta intensità in maniera sistematica. Tale ambiente operativo richiede l'adozione di misure di FP adeguate all'elevato livello di minaccia che assicurino, comunque, una mobilità elevata dello strumento al fine di assicurare sia il controllo del territorio sia lo **svolgimento della missione.**

1.2. CARATTERISTICHE DELLE BASI MILITARI

Con il termine **base militare**, sia in ambito nazionale sia NATO[4], si intende "una zona dalla quale hanno inizio o sono appoggiate le operazioni"[5]. A tale concetto si associa comunemente anche quello di installazione. Nel senso che una base ha normalmente caratteristiche di solidità, durabilità e disponibilità di servizi. Col termine **accampamento** invece, si intende un'area di stazionamento delle unità in campagna che prevede, per l'alloggiamento del personale e la realizzazione dei servizi, l'utilizzo di materiali di attendamento o di contingenza. Gli accampamenti sono quindi strutture "temporanee" che, mediante l'integrazione di opere di tipo permanente, possono avere caratteristiche simili alle basi militari, venendo in tal caso denominati **accampamenti semi-permanenti**.

Ai fini della presente pubblicazione tuttavia, con la denominazione **base militare** si contemplano entrambe le tipologie di installazioni realizzate in Operazione, rinviando alla specifica SOP[6] la descrizione delle caratteristiche tecniche-operative ed i relativi standard abitativi per la loro realizzazione. Particolarmente significativa è la categorizzazione di tali strutture sulla base della funzione assolta nell'ambito della manovra. Al riguardo, è possibile individuare due tipologie di basi di tipo "avanzato" cioè di basi ubicate in un Teatro di Operazioni o nelle sue adiacenze, il cui scopo principale è quello di supportare la manovre delle operazioni militari: *Forward Operating Base* (FOB) e *Forward Support Base* (FSB). Sono entrambe strutture preminentemente "tattiche", in quanto la tipologia costruttiva ed il tempo di utilizzo sono normalmente di breve[7] o media durata, legate all'evoluzione della situazione operativa e della minaccia, in particolare quella connessa alle forze ostili o nemiche operanti nelle zone circostanti. Sono particolarmente idonee per la condotta della manovra terrestre nella 3^ dimensione e concepite prioritariamente per supportare le attività di C2 e di sostegno logistico dei complessi di forze che conducono le attività tattiche. Sono particolarmente idonee per manovrare in Aree di Operazione (AOO) non contigue. Tali infrastrutture includono Zone di Atterraggio (LZ) che possono essere piste permanenti o anche di circostanza, una o più banchine di ancoraggio (anch'esse permanenti o di circostanza) e servizi generali limitati o assenti. Sono realizzati in modo "temporaneo" o "semipermanente", in funzione della durata di utilizzo pianificata.

---

[4] Cfr. NATO, AAP-06 *Glossary of Terms and definitions of military significance for use in NATO*, Ed. 2015:
- Base 1: "*An area or locality containing installations which provide logistic or other support*";
- Base 2: "*A locality from which operations are projected or supported*".

[5] Cfr. SME III RIF/COE, Pub. 5895 *Nomenclatore Militare (Esercito)*, Ed. 1998.

[6] Cfr. COMANDO GENIO, SOP *Tecniche e procedure per la progettazione di contingenza di opere del genio*, Ed. 2014.

[7] Le FOB, tipicamente ma non esclusivamente legate alla manovra nella terza dimensione, possono essere realizzate anche per il supporto di una singola missione.

In particolare, in linea con la vigente normativa NATO[8] e quella nazionale[9], le basi militari da realizzare in operazioni hanno le seguenti caratteristiche:

- **Basi militari di tipo "tattico"**

  Sono caratterizzate da frequenti cambiamenti di localizzazione e temporaneità delle strutture componenti (alloggiamenti, logistica, ecc.), elevato diradamento e composte da attendamenti, equipaggiamenti ed attrezzature di sola dotazione regolamentare alle unità. Gli impianti campali vengono realizzati senza opere infrastrutturali di supporto, per via delle limitate condizioni di vivibilità, salvo che le condizioni operative ne impongano il mantenimento. Nelle loro vicinanze possono avvenire azioni di combattimento ad alta intensità La loro utilizzazione è legata allo sviluppo dell'operazione e, comunque, risulta conveniente fino ad un massimo di 2 mesi.

- **Basi militari di tipo "temporaneo"**

  Sono composte da veri e propri attendamenti, con servizi igienici su *shelters*, integrati o meno da infrastrutture esistenti rese idonee con piccoli interventi di manutenzione[10] e potenziati da misure attive e passive di difesa. Si distinguono in:

  - **"provvisorie"**: risultano la naturale trasformazione delle basi di tipo tattico, qualora queste debbano essere ancora utilizzate per periodi di media durata. Per gli *standard* previsti possono essere convenientemente utilizzate per un periodo di 2 - 4 mesi e sono sempre caratterizzate da alloggiamenti sotto tenda, diradati e con servizi ridotti all'essenziale. Nelle loro vicinanze possono avvenire azioni di combattimento anche di media-alta intensità. Nel loro contesto operativo permangono le possibilità di cambiamento di localizzazione e la decentralizzazione delle zone di vita, seppur possano essere realizzate limitate infrastrutture per il miglioramento delle condizioni di vivibilità (adottando i fabbricati esistenti in sito);
  - **"temporanee"**: sono l'evoluzione di una base provvisoria con un'utilizzazione ottimale di ulteriori 4 mesi. Il periodo di utilizzazione è estensibile sino a 12 mesi con la realizzazione di ulteriori opere integrative che ne migliorino le condizioni di vita. In tale situazione però è preferibile valutare l'opportunità di realizzare direttamente una base di tipo "permanente. La caratteristica di questa infrastruttura e del relativo periodo di utilizzazione discende dal fatto che non si svolgono operazioni di forze

---

[8] Cfr. NATO, ATP 3.12.1.4 (SD) *Deploy Force Infrastructures*, in corso di redazione e che sostituirà l'attuale PFP (NAAG-LCG/7)D(2008)0001 *Field Accommodation Guide*, Ed. 2008.

[9] Cfr. già cit. PID-O 3.14 (Allegato "F", para. 3) e Cfr. Comando Genio, SOP *Tecniche e procedure per la progettazione di contingenza di opere del genio*, Ed. 2014 (Allegato "B").

[10] Rifacimento di tratti di copertura, sostituzione di componenti sanitari, realizzazione di impianti con materiale campale o sostituzione e ripristino di parte di quelli esistenti, esecuzione di tinteggiature a tempera o con calce, realizzazione di infissi di circostanza, ecc.).

ostili di media o alta intensità in prossimità del suo sedime. Prevede alloggiamenti e servizi in container (tipo prefabbricati leggeri) o misti con tende.

- **Basi militari di tipo "permanente"**

  Da realizzare ove si presuppone una lunga permanenza delle unità (generalmente oltre gli 8 mesi) ma non risulta ancora opportuno né conveniente utilizzare/realizzare installazioni "fisse" (ovvero "accasermamenti"). Comportano la realizzazione di una tipologia di manufatti, opere impiantistiche ed oneri di urbanizzazione adeguati agli standard prefissati in termini di "qualità della vita" e "funzionalità" che consentano l'andamento delle operazioni e lo svolgimento delle attività secondo standard di vivibilità, di *comfort* e di *privacy* individuale migliori, più razionali e funzionali, specie durante le stagioni più avverse.

1.3. CONSIDERAZIONI DI CARATTERE OPERATIVO PER LA PROTEZIONE DELLE BASI MILITARI

Ai fini della definizione delle misure di protezione per una base militare va tenuto presente che la protezione delle basi è legata all'analisi dei seguenti fattori operativi:

- approccio sistematico FP;
- orientamenti d'impiego per l'organizzazione della difesa;
- scelta di siti e infrastrutture;
- sistemi di realizzazione delle basi.

1.3.1 Approccio sistematico FP

La definizione delle misure di protezione è basata su una dettagliata analisi della minaccia, attraverso un processo di *risk management* (risalente all'applicazione del modello del modello di FP sviluppato come descritto nel successivo Capitolo II) e combina tra di loro misure di sicurezza attiva e difesa passiva (si estrinsecano nella redazione di piani di difesa e di sorveglianza), misure per la gestione delle emergenze (piani di contingenza per le emergenze) e l'adozione di procedure standardizzate per il controllo degli accessi, il rilascio dei pass[11], il rilascio delle tessere di riconoscimento e per la gestione dei lavoratori/imprese locali che a vario titolo possono essere presenti (in via temporanea o permanente) nella base.

Ai fini della FP, le minacce ed i rischi cui può essere soggetta una base militare sono riconducibili non soltanto alle azioni delle forze ostili (attentati, IEDs, tiro diretto, tiro indiretto, ecc.) ma anche a quelle della malavita locale (contrabbando, delinquenza minorile ed organizzata, ecc.), delle emergenze naturali (incendi, alluvioni, terremoti, frane, ecc.) ed antropiche (fughe di materiale chimico volatile, incendi boschivi, inquinamenti ambientali a seguito di rilascio di sostanze tossiche industriali - TIMs)

[11] Lasciapassare: trattasi di un documento che sancisce l'autorizzazione temporanea o permanente per l'accesso ad una base militare.

con conseguenti possibili emergenze umanitarie. Pertanto, lo sviluppo dell'organizzazione di sicurezza di una base militare va effettuato sulla base di uno specifico "approccio sistematico FP" (Allegato "A") che funge da "linea guida" sia nell'analisi sistematica delle esigenze operative di FP durante il "modello di FP" sia nella definizione delle misure per eliminare le criticità e vulnerabilità durante il *risk management*.

1.3.2 Orientamenti d'impiego per l'organizzazione della difesa

È opportuno che la scoperta della minaccia avvenga il più lontano possibile dal perimetro ed in modo da:

- dare prontamente l'allarme al personale della base;
- allertare, per tempo, le unità di vigilanza e indirizzarle verso la direzione/località di provenienza della minaccia localizzata;
- assicurare l'intervento delle armi di difesa in dotazione dislocate lungo il perimetro (torri remotizzate o armi delle sentinelle ivi dislocate) o all'interno della base (mortai) alla massima distanza per un tiro efficace.

Al riguardo, la definizione del perimetro di una base e dei relativi accessi viene effettuata sulla base della scelta di un idonea area di sedime che assicuri non solo il favore della posizione sul terreno circostante (campi di vista e tiro ampi e dominanti di quota), ma garantisca anche un vantaggio nei confronti della minaccia sin dalla fase del suo avvicinamento al perimetro attraverso la possibilità di utilizzare le caratteristiche del terreno per la realizzazione di una serie di barriere fisiche e tecnologiche. Tale problematica tende a divenire un elemento critico dell'organizzazione di FP quando le unità abbandonano le posizioni sul terreno per trasferirsi negli agglomerati urbani (ovvero la dislocazione della base viene già definita in tali località sin dall'avvio della missione).

In tale diverso contesto:

- le distanze di sicurezza e la visibilità sono notevolmente ridotte;
- il traffico impone vincoli al controllo dei veicoli.

Pertanto, l'organizzazione della difesa di una base militare, viene realizzata attraverso diverse forme quali la sicurezza attiva, la difesa passiva e il controllo dell'intera Area di Responsabilità Tattica (*Tactical Area of Responsibility* - TAOR) assegnata alla base.

Le varie attività e compiti svolti nell'ambito di ciascuna modalità, consentono di assolvere le funzioni come di seguito indicato:

1.3.2.1 Sicurezza attiva (Figura 3)

Viene realizzata con una serie di misure/predisposizioni che, in relazione al tempo ed alle risorse disponibili, possono comprendere (esempio non esaustivo) i seguenti elementi:

- Controllo, Scoperta, Identificazione e Reazione:
  - Pattuglie motorizzate e/o appiedate in movimento nell'area interna, a cavallo della fascia perimetrale di sicurezza o all'esterno della base;
  - Veicoli Terrestri Senza Pilota (*Unmanned Ground Vehicle* - UGV) e Veicoli Aerei Senza Pilota (*Unmanned Aerial Vehicle* - UAV);
  - Personale di vigilanza su torri/altane di guardia o postazioni dotate di sistemi d'arma remotizzati;
  - Elicotteri Multiruolo e d'Attacco.
- Controllo, Scoperta e Identificazione:
  - sistemi integrati di FP controllati da una *Ground Control Station* (GCS) o da una *Remote Control Station* (RCS) presso il PC FP (sorveglianza a medio e lungo raggio);
- Reazione:
  - Sistemi attivi non letali;
  - Mortai;
  - Artiglierie;
  - unità di riserva o di pronto intervento (ad es. *Quick Reaction Force* – QRF o *Immediate Reaction Force* IRF).

Figura 3: Elementi della difesa attiva

1.3.2.2 Difesa passiva (Figura 4)

Viene realizzata mediante una serie di misure/predisposizioni che, in relazione al tempo ed alle risorse disponibili, possono comprendere i seguenti elementi (esempio non esaustivo):

- Scoperta, Rilevamento e Allarme:
  - sensori e barriere *Passive InfraRed* (PIR);
  - cavi microfonici, sensori acustici, sismici, geofonici e magnetici;
  - sistemi TVCC nelle aree interne o lungo il perimetro della base controllati da una GCS o RCS presso il PC FP o il Posto di Guardia (sorveglianza a corto raggio).
- Scoperta e reazione:
  - mine anticarro[12];
  - artifizi illuminanti d'allarme.
- Protezione:
  - barriere antiveicolo fisse, amovibili e elastiche;
  - barriere perimetrali balistiche e *antiblast*;
  - barriere per la compartimentazione di aree/luoghi affollati;
  - postazioni difensive;
  - protezioni contro il tiro indiretto per la protezione collettiva (*Collective Protection* - COLPRO).

Figura 4: Elementi della difesa passiva

[12] In aderenza agli accordi di OTTAWA non possono essere utilizzate mine antiuomo; l'area eventualmente minata, dovrà essere recintata e segnalata come previsto dal NATO, STANAG 2036 (Ed. 6) *Land Mine Lying, Marking, Recording and reporting Procedures* e dovrà essere utilizzata un'adeguata cartellonistica multilingue e con adeguati simboli per la popolazione locale. Qualora possibile, è bene considerare la condotta di attività informative a favore della popolazione locale. Uno specifico supporto in tal senso, può esser fornito dal Personale del Genio, PAO, CIMIC e LEGAD.

1.3.2.3 Controllo della TAOR (Figura 5)

Può comprendere i seguenti elementi (esempio non esaustivo):

- controllo, scoperta e identificazione;
- sistemi di video sorveglianza (TVCC) perimetrale;
- sistemi integrati di sorveglianza (radar + elettroottiche);
- UAV e UGV.

L'impiego di tali tipologie di sistemi comporta l'esigenza di integrare i piani di difesa terrestre con quelli di difesa aerea (tra le quali va considerato anche il sistema *Counter - Rocket Artillery and Mortar* (C-RAM).

Figura 5: Elementi per il controllo della TAOR

L'integrazione bilanciata di tali modalità consente di poter realizzare "barriere concentriche meccanico-elettroniche", secondo uno "schema concentrico ed in profondità" che ingloba tutte le aree della TAOR (area interna, area perimetrale, area visibile e non visibile dal perimetro all'occhio umano, alle ottiche o ai radar, illustrate in maniera approfondita nel successivo Capitolo 3).

In particolare, per quanto riguarda le aree perimetrali (essenzialmente le più critiche) è opportuno attuare:

- difese passive e/o meccaniche: recinzioni, strutture murarie, robusti cancelli mobili, serrature di elevata sicurezza, ecc.;
- difese attive e/o elettroniche: attività di sorveglianza[13] e vigilanza[14] con la specifica capacità di poter effettuare una reazione, un'azione di contrasto

[13] Osservazione sistematica di zone aeree, terrestri, marittime, sottomarine, di località, di persone o di cose, effettuata, a scopo informativo, con mezzi ottici, elettronici, fotografici o altri (cfr. SMD, SMD-G-024 *Glossario dei termini e delle definizioni*, Ed 2007 – Aggiornamento 1 – 2009). La sorveglianza si realizza con determinate modalità (palese, occulta, sistematica, saltuaria, permanente, mirata), al fine di poter anche individuare/prevenire qualsiasi forma di attività/evento ostile, o potenzialmente ostile, al fine di poter eventualmente attivare la catena di allertamento e/o di allarme e predisporre, o far attivare, le previste azioni di reazione e contrasto della minaccia.

[14] La vigilanza può essere fissa (il personale staziona nella posizione assegnata), mobile (il personale si può muovere per effettuare attività di pattugliamento, controllo e verifica) o dedicata (l'attività di pattugliamento, controllo e verifica è indirizzata unicamente a determinati punti o aree considerate sensibili/critiche/vitali). In tal

immediato nei confronti di un atto ostile o di una minaccia manifesta con l'impiego delle armi a disposizione; impianti di allarme antintrusione; impianti di videosorveglianza digitale; impianti di controllo degli accessi che possono utilizzare anche sofisticate tecnologie biometriche.

1.3.3 Scelta dei siti e delle infrastrutture

Le Lezioni Identificate negli ultimi anni[15] hanno evidenziato come la scelta del sedime e l'organizzazione funzionale[16] di una base militare ("zonizzazione" *o zoning*) siano i fattori fondamentali per assicurare sin dall'inizio un'adeguata organizzazione della sicurezza ed, in particolar modo, il raggiungimento di ottimali rapporti costi/efficacia delle opere di protezione fisica. Lo svolgimento di una ricognizione preventiva consente di verificare l'efficacia di quanto pianificato in Patria e di adottare, prima dello schieramento in AOO, i provvedimenti correttivi volti all'ottimizzazione delle esigenze/criticità emerse e riferite alla protezione delle forze. In alternativa, può essere effettuato uno studio dettagliato del sedime, possibilmente con ausili informatici che consentano l'attività di simulazione tridimensionale.

Riguardo al sedime vengono analizzati:

- morfologia, caratteristiche del terreno, idrografia e condizioni meteo avverse;
- risorse ed opere idriche utilizzabili/riparabili;
- risorse ed opere elettriche utilizzabili/riparabili;
- opere fognarie utilizzabili/riparabili;
- viabilità esistente utilizzabile/riparabile;
- manufatti in sito (infrastrutture esistenti che si intendono utilizzare, anche a fronte di modeste opere di ristrutturazione).

I risultati comparati con gli esiti del modello di FP, ove possibile, consentono la definizione:

- della "zonizzazione";
- delle attività e delle funzioni da dislocare all'interno di ciascuna zona e delle opere di protezione passiva da realizzare.

Inoltre, nella scelta del sedime si deve tener conto della presenza di linee di comunicazione sostenibili e difendibili.

senso, il servizio di vigilanza, inteso generalmente come attività dissuasiva o di deterrenza, è attuato da personale armato.

[15] Attività svolte dal Team Interforze FP del COI J3 (2006-2009), *Joint Analysis Team* (JAT) del COI AVAC (2008-2009) e Cellula FP di ISAF RC *West* (2012-2014).

[16] Suddivisione di una base militare in aree destinate a sostenere una o più attività umane/servizi, funzionalmente e dimensionalmente connesse tra di loro.

1.3.4 Sistemi di realizzazione delle basi

La realizzazione delle basi militari e delle singole attrezzature, ove possibile, contempla:

- la protezione dagli effetti delle armi impiegate dalla minaccia identificata (esplosioni, onda d'urto, frammentazione primaria e secondaria, effetti termici);
- la prevenzione di incendi e le misure da adottare in risposta all'emergenza;
- entrate, uscite e difese perimetrali per un controllo capillare degli accessi, per facilitare la difesa ed idonee strutturalmente a minimizzare i danni in caso di attacco;
- misure di diradamento e compartimentazione di aree con muri o terrapieni anti esplosione o frammentazione (dipende dalla valutazione della minaccia e dall'assunzione del rischio del Comandante dell'unità);
- blindature di vario spessore sulla parte superiore delle infrastrutture/impianti, rinforzando le strutture portanti esistenti e costruendo protezioni per il personale contro le varie minacce;
- adeguati sistemi di sorveglianza, rivelazione e allarme della minaccia.

Inoltre, allo scopo di ostacolare il più possibile l'accesso alle basi ad elementi ostili è utile adottare, specialmente in ambiente SEMI/NON PERMISSIVO, le seguenti misure integrative:

- decentrare e/o allontanare dal perimetro esterno gli stoccaggi di sostanze pericolose; in tal modo si ottiene un'intrinseca difficoltà al loro raggiungimento;
- installare robuste recinzioni lungo il perimetro del complesso, meglio se poste in maniera da formare un corridoio di sicurezza;
- mantenere chiusi i cancelli pedonali e carrai; devono essere aperti esclusivamente a seguito di identificazione sia della persona sia dell'eventuale autoveicolo e, comunque, soltanto se preventivamente autorizzato;
- consentire l'ingresso al personale esclusivamente per mezzo di PASSI e, ove necessario, con controllo biometrico attuato ai varchi d'ingresso pedonali;
- realizzare un percorso "a gincana" per l'accesso agli ingressi dedicati ai veicoli;
- posizionare elementi distanziatori allo scopo di creare una zona di rispetto anti-autobomba, in prossimità di pareti di edifici, di depositi o di impianti esposti al rischio di attentato;
- installare robuste barriere, a sollevamento verticale, con azionamento remoto (a scomparsa) che, fuoriuscendo dalla carreggiata, impediscano l'entrata a forte velocità di autoveicoli sospetti attraverso i varchi carrai dell'insediamento;
- prevedere il doppio bacino di contenimento degli stoccaggi di sostanze pericolose;
- interrare i serbatoio utilizzare vesciche protette da barriere perimetrali (*Bulk Fuel Installation* - BFI);
- proteggere i Posti Comando contro l'esplosione esterna; tali *Tactical Operations Center* possono essere, in pratica, realizzati come dei "ricoveri" in modo che il

personale possa continuare ad operare in sicurezza pur mantenendo le rispettive postazioni di lavoro.

PAGINA INTENZIONALMENTE BIANCA

2. PIANIFICAZIONE E ORGANIZZAZIONE DELLA PROTEZIONE DELLE BASI MILITARI

2.1 PIANIFICAZIONE DELLA PROTEZIONE DI UNA BASE MILITARE

La definizione delle misure e delle attività di protezione di una base militare viene effettuata attraverso due distinte fasi:

- avvio del processo di FP;
- sviluppo del modello di FP.

2.1.1 Avvio del processo di FP

Il processo di FP per la protezione di una base militare è inizialmente avviato sulla base di una realistica valutazione della minaccia e dei rischi da parte del S/G2 del complesso tattico che ha il Comando della base. Successivamente, la Cellula FP (S/G3) provvede alla valutazione delle vulnerabilità e all'esame dei citati rischi, definendo il valore e gli effetti dei rischi residui (cioè il livello di un dato rischio che permane nonostante l'applicazione di misure intese a minimizzarne gli effetti).

Tali informazioni sono diramate:

- al personale dello staff dello stesso Comando, deputato a trattare gli aspetti di FP;
- ai Comandanti subordinati, le cui unità possono essere dislocate nella stessa base o distaccate in altre basi dipendenti;
- ai Comandi di altre unità, siano esse nazionali o multinazionali, sotto TACOM o meno, che insistono nella stessa base, in modo che ciascuno possa definire i propri rischi residui e le misure/predisposizioni di FP da applicare per mitigarli in aderenza alle linee guida emanate dal Comandante della base.

Infatti, i Comandanti di una base, nell'ambito della TAOR loro assegnata:

- sono responsabili dello sviluppo di linee guida per il personale e le installazioni dipendenti, al fine di assicurare lo sviluppo unitario della pianificazione di FP e la relativa applicazione degli standard di FP;
- considerano i seguenti fattori per lo sviluppo del proprio processo decisionale:
  - minaccia corrente nella JOA (*Joint Operations Area*) e valutazioni del G/J2 del Comando superiore;
  - minaccia corrente nella TAOR della base, ivi compreso settori contermini e sovrapposti con le altre TAOR, e valutazioni locali del proprio S/G2;
  - rischi dovuti a tali minacce;
  - misure e predisposizioni per ridurre tali rischi;
  - regole d'ingaggio e relative restrizioni/limitazioni nazionali alla loro applicabilità;
- fanno in modo che le valutazioni e le predisposizioni definite dalla Cellula FP siano sempre supportate dal processo di intelligence, inclusi gli stati di

allertamento e le relative misure (codici per l'uniforme e l'armamento da indossare all'interno o all'esterno della base e per il movimento da effettuare all'esterno della base) che dovranno essere applicate nell'ambito della propria TAOR per ridurre la vulnerabilità del personale e dell'installazione;

- definiscono le priorità nell'implementazione delle misure di FP in relazione a minaccia, risorse disponibili (materiali e finanziarie) e tempo.

Ciò richiede, da parte dello *Staff*, una continua attività di valutazione della minaccia ed analisi dei rischi per poter determinare quali tra quelle esaminate può indurre un elevato livello di vulnerabilità ed il possibile impatto sulla missione, sulla sicurezza della base ovvero sulle attività delle IOs, GOs, NGOs o della popolazione.

2.1.2 Sviluppo del modello di FP

La definizione delle misure e predisposizioni di FP per la protezione di una base militare viene effettuata sin dalla fase di pianificazione di una missione, attraverso un'attività ciclica definita come "modello di FP"[17] (fig. 6). Esso consiste in una sequenza ciclica di attività interattive tra di loro, legate ad un ambiente operativo ed incentrate intorno alla valutazione della minaccia, alla valutazione della vulnerabilità ed al processo di *Risk Management* per la definizione delle misure di protezione della base.

Il Comandante della base, responsabile dell'implementazione della funzione operativa FP, si avvale dell'apporto del proprio *Staff*, nell'ambito del quale, normalmente, la Cellula S/G3 FP è deputata allo sviluppo del modello di FP con il supporto delle altre Cellule del Comando. Al riguardo, ciascun elemento dello *Staff*, designato dal proprio Capo Cellula alla gestione dei processi di FP riguardanti la propria Branca di applicazione, contribuisce all'analisi delle esigenze ed alla definizione delle misure di FP in seno ad uno specifico organo collegiale permanente denominato FP *Working Group* (FPWG). Sulla base dei vari livelli di valutazione della minaccia nell'ambiente operativo[18], è cura del Comandante della base definire i relativi stati di allertamento, le misure ed i controlli di FP da far attuare[19] in aderenza a quelli "di base" definiti dal Comandante sovraordinato. Infatti, gli stati di allertamento della base non possono essere mai inferiori a quelli stabiliti per la TAOR/AOO in cui insiste. Il "modello" prevede lo sviluppo dei passi di seguito elencati da parte del personale della Cellula S/G3 FP.

In **Allegato "B"** è riportato un esempio di applicazione del modello di FP applicato alle specifiche esigenze operative per la protezione di una base militare.

---

[17] Rappresentazione schematica delle funzioni, assetti, controlli, misure e meccanismi procedurali che supportano i Comandanti ed i propri staff nella pianificazione FP e nella risposta ad incidenti/eventi/attacchi in fase condotta.

[18] Cfr. già cit. PID/O 3.14, Cap. I, para 4.

[19] Cfr. già cit. PID/O 3.14, Cap. II.

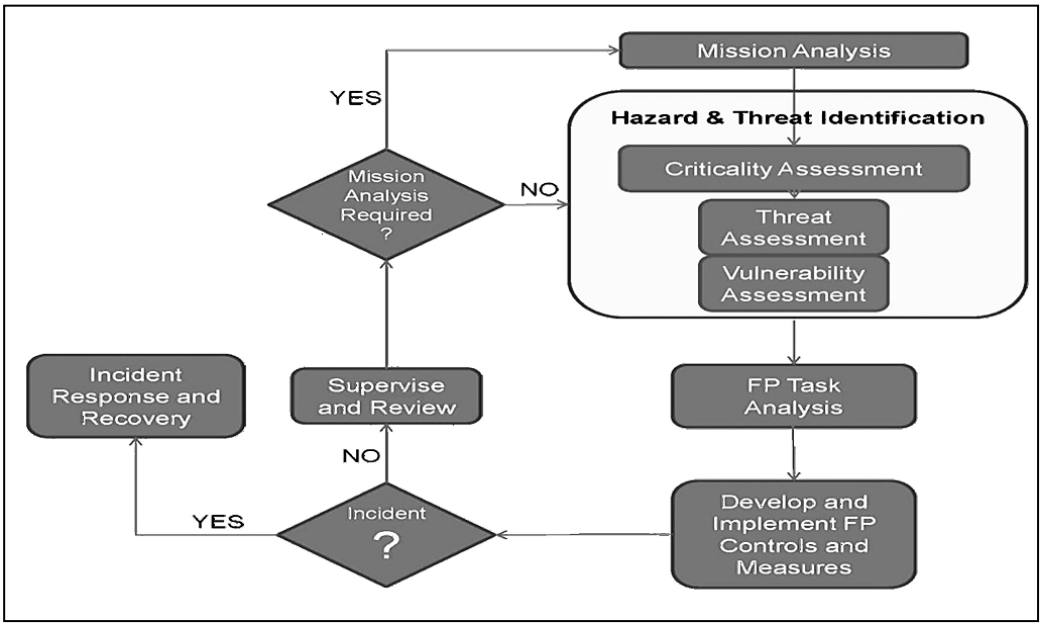


Figura 6: Modello di FP[20]

2.1.2.2 Analisi della missione (*Mission Analysis*)

Avvia lo sviluppo del modello, contemporaneamente alla fase di pianificazione della missione, esaminando l'intento del Comandante sovraordinato, il concetto d'azione del proprio Comandante, i compiti espliciti e quelli impliciti dell'unità e della base (che potrebbe accantonare anche diverse unità), nonché i vincoli in relazione alle esigenze operative di FP per il supporto dell'intera missione.

2.1.2.2 Identificazione dei rischi e della minaccia (*Hazard and Threat Identification*)

Riunisce tre attività tra di loro connesse e sequenziali:

- **Valutazione delle criticità (*Criticality Assessment*)**

  Identifica, partendo dagli elementi emersi nel corso dell'analisi della missione, gli elementi critici (tangibili e non) propri, dai quali dipende il successo dell'operazione: personale, materiali, sistemi, infrastrutture, informazioni ed attività che possono compromettere la sicurezza della base.

- **Valutazione della minaccia (*Threat Assessment*)**

  Identifica gli assetti e le capacità del nemico, nonché i fattori ambientali che possono ostacolare o influire negativamente sull'azione delle unità amiche, indicando anche le probabilità che rischi e minacce individuate possano verificarsi.

- **Valutazione delle vulnerabilità (*Vulnerability Assessment*)**

[20] Cfr. già cit. AJP 3.14.

Definisce, comparando gli esiti della valutazione della minaccia con gli elementi del proprio dispositivo (tangibili e non), quali di questi possono essere realmente influenzati negativamente dalle minacce e dai rischi identificati. Le vulnerabilità prendono in esame la pianificazione, l'addestramento, la protezione fisica, la ridondanza dei sistemi di collegamento e sorveglianza, la capacità di risposta e di ripristino della stessa in caso di evento o incidente.

In particolare, viene:

- verificato se tra i propri elementi di vulnerabilità vi siano quelli già individuati come "critici" e/o quelli che possono condizionare questi ultimi;
- stimato quali incidenze tali elementi possono avere sulla sicurezza e la sopravvivenza della base ;
- valutato se è possibile neutralizzare, anche parzialmente, gli elementi di vulnerabilità.

2.1.2.3 Valutazione del rischio (*Risk Assessment*) ed analisi dei compiti della FP (FP *Tasks Analysis*)

L'analisi dei compiti della Cellula S/G3 FP viene effettuata sulla base dei risultati dell'analisi della missione e dell'identificazione delle minacce e dei relativi rischi (valutazione del rischio).

In particolare, è necessario:

- determinare i potenziali effetti negativi dei rischi e delle minacce individuate nel precedente passo, la probabilità che possano verificarsi ed il grado di esposizione degli elementi del dispositivo approntato per la costituzione della base;
- identificare i compiti specifici della FP, associandoli ai vari rischi precedentemente individuati.

Al termine della valutazione sono assegnate delle priorità ai vari rischi e minacce ed individuati i relativi compiti specifici, misure ed attività di FP.

Ai fini dell'effettuazione di tale analisi, possono essere utilizzati, a seconda dell'esigenza operativa, due diverse matrici dei rischi (Allegato "C") tendenti rispettivamente a fornire le informazioni sul "rischio residuo" e sugli "effetti dei rischi nei confronti dell'organizzazione di sicurezza".

2.1.2.4 Definizione dei compiti, misure ed attività di FP (*Develop and Implement FP Measures, Tasks and Activities*)

Queste attività rientrano in quella che si definisce "la gestione del rischio" (*Risk Management*), nell'ambito della quale la decisione di accettazione dei rischi è una responsabilità "specifica" e "non delegabile" del Comandante della base.

Questa fase:

- viene sviluppata allo scopo di:
  - verificare che l'eventuale *gap*, determinatosi dal confronto esigenze/possibilità, non superi i limiti fissati dal Comandante nella sua

direttiva per la pianificazione, tenendo, altresì, conto degli esiti del ciclo *Operations Security* (OPSEC);

- valutare i rischi residui, evidenziati dall'applicazione delle misure e dei compiti specifici precedentemente individuati;
- individuare le misure di FP da adottare o le capacità da integrare per minimizzare i citati rischi residui;
- definire i compiti da assegnare allo staff ed alle unità dipendenti per l'approntamento dell'organizzazione della FP;
- identificare le attività da sviluppare ai fini della protezione delle forze;

– si conclude con:

- l'emanazione degli ordini: Annesso "J" all'OPORDER o FRAGO specifici;
- la redazione delle necessarie SOP.

2.1.2.5 Risposta all'incidente e ripristino della capacità operativa (*Incident Response and Recovery*).

Consiste nell'attuare tutte le misure necessarie al fine di annullare qualsiasi azione contro la base nonché limitare gli effetti causati da un incidente/evento, nonché di ripristinare con immediatezza la capacità operativa degli elementi dell'organizzazione delle forze soggetti agli stessi.

In particolare, si suddivide in due incidenti fasi distinte:

– **Risposta all'incidente (*Incident Response*)**

In questa fase, sono applicate dalle unità le misure di FP pianificate e quelle per la gestione delle emergenze relative al *Consequence Management*, attraverso il coordinato intervento di sistemi ed assetti dedicati alla FP:

- l'immediata reazione da parte della difesa e degli assetti specialistici in prontezza (antincendio, EOD, CBRN, sanità, MEDEVAC, ecc.) allo scopo di contenere, isolare, minimizzare i danni causati dall'evento/incidente;
- il coordinamento delle attività attraverso un centro per la difesa e per la gestione dell'emergenza che provveda anche ad un continuo scambio informativo (TOC[21]/BDOC[22]);
- l'implementazione e l'integrazione delle misure pianificate (piani di difesa, di contingenza, ecc.) e relative procedure (SOP);
- la raccolta delle evidenze e delle informazioni sull'evento per il rapporto sulla situazione al termine dell'evento/incidente (necessarie per lo sviluppo della fase di *Supervise & Review*);

---

[21] *Tactical Operations Center*.

[22] *Base Defense Operations Center*, che a livello cpls min può coincidere con il TOC.

- l'applicazione delle misure di INFO OPS per ridurre o annullare gli effetti dell'informazione delle forze ostili in merito all'azione attuata e minimizzare il senso di incertezza nella popolazione e nelle forze;
- l'implementazione delle misure per il trattamento e l'evacuazione dei feriti.

– **Ripristino capacità operativa (*Recovery*)**

In questa fase sono implementate ed applicate tutte le misure per minimizzare i danni causati e ripristinare:

- inizialmente: la capacità operativa essenziale ad assicurare la sopravvivenza della base;
- successivamente: la capacità operativa prevista per il pieno supporto all'assolvimento del compito delle unità accantonate.

In particolare, vengono:

– ripristinati in tempi brevi:
  - l'efficienza delle infrastrutture danneggiate (ingresso, recinzione, elementi critici, ecc.);
  - le comunicazioni interrotte (ponti radio, satellitari, ecc.);
  - la viabilità, sia interna che esterna (*route and area clearance*);
  - l'utilizzazione di aree soggette ad eventi speciali (bonifica da ordigni esplosivi, contaminazione CBRN, ecc.);
  - i sistemi di sorveglianza e reazione danneggiati (PSS, elettro-ottiche, radar, TVCC, UGV, ecc.);
  - la capacità operativa delle unità di manovra, logistiche, per la difesa della base e gli assetti in prontezza (IRT, QRF, IEDD. EDD/MDD, MEDEVAC, SAR, ecc.) in termini di personale, mezzi, dotazioni;
– sostituiti i materiali e le attrezzature danneggiate;
– completate le attività di trattamento e sgombero dei feriti.

2.1.2.6 Controllo e revisione delle misure attuate (*Supervise and Review*)

Consiste nell'esame comparato dell'incidente/evento occorso e delle relative capacità di reazione messe in atto allo scopo di identificare i gaps dell'organizzazione, ovvero aggiornare gli elementi di conoscenza sulla minaccia e predisporre le misure integrative (emanazione di specifici FRAGO, aggiornamento pianificazione di contingenza o piani difesa, ecc.). Ciò potrebbe comportare anche il riavvio del ciclo.

2.1.2.7 Attività specifiche per la pianificazione delle misure di protezione di una base militare

Ai fini della protezione della base, la pianificazione delle attività di *Force Protection* è condizionata da una serie di azioni preliminari e si sviluppa in maniera diversificata a partire dall'interazione tra S/G2 e S/G3 dell'unità cui è stato assegnato il compito di provvedere alla difesa della base, coinvolgendo svariati attori, tra cui il FP *Officer* (FPO) che svolge anche attività di *Advisor* del Comandante della base. Essa si riflette in ogni piano di operazione e di contingenza discendente e, più in particolare, per la FP, nella redazione ed aggiornamento dell'Annesso "J" all'Ordine di Operazioni, nella pianificazione delle operazioni correnti e nella redazione dei rispettivi FRAGO per la loro condotta.

L'attività di Staff per la FP ha inizio con la definizione delle linee guida del Comandante della base che indica l'organizzazione di FP da approntare. In particolare, attraverso il proprio concetto operativo[23], fornisce allo *staff* tutte le indicazioni e le priorità inerenti a:

- lineamenti dell'organizzazione di FP da costituire;
- responsabilità dei Comandanti dipendenti e dello Staff nell'ambito del processo di FP;
- sviluppo del processo di analisi della minaccia, tenendo conto dei rischi legati all'ambiente operativo, a quello naturale ed antropico;
- indirizzi per lo sviluppo del modello di FP per l'attività di *risk management*;
- organizzazione e capacità minime delle Forze designate per la sicurezza della base e relativo stato di prontezza;
- misure di coordinamento nel caso nella base fossero presenti diverse unità (specialmente in ambiente multinazionale);
- sistemi di C2 e *Communication Information Systems*;
- linee guida per lo sviluppo di SOP e piani per la difesa della base;
- linee guida per lo sviluppo di SOP e piani per l'emergenza (*Major Incident* e *Mass Casualties/Disaster Relief*, antincendio, CBRN, ecc.);
- linee guida per lo sviluppo di piani e SOP per la prevenzione degli incidenti sui luoghi di lavoro per le attività assoggettabili alla normativa nazionale;
- lineamenti per l'impiego dei sistemi di sorveglianza, per la scoperta e per la reazione assegnati;
- lineamenti per l'impiego delle armi disponibili in dotazione;

[23] Può avvalersi dell'*Advisor* FP.

- lineamenti per l'impiego di sistemi e procedure per l'identificazione amico-nemico IFF (*Identification Friend or* Foe) e CID (*Combat Identification Devices Systems*), al fine di minimizzare i rischi legati al fuoco fratricida;
- linee guida per il controllo degli accessi, il rilascio dei pass e la pianificazione dei movimenti dei veicoli all'interno della base;
- linee guida per il controllo e l'autorizzazione all'accesso dei lavoratori locali, compreso il processo di verifica dei requisiti per l'assunzione;
- attività di *Training* FP (per l'approntamento e per il mantenimento missione durante);
- esercitazioni di FP per lo Staff, per le unità e gli assetti specialistici alle dipendenze e/o ricevuti in rinforzo.

2.2 ORGANIZZAZIONE DI FP PER LA PROTEZIONE DI UNA BASE MILITARE

2.2.1 Principali attività di FP

Ai fini della definizione delle misure di protezione per la sicurezza della base, la Cellula FP dovrà provvedere allo sviluppo delle seguenti attività:

2.2.1.1 Fase di pianificazione:

- definire i lineamenti per l'organizzazione di un sistema di difesa in profondità, che assicuri l'identificazione della minaccia ed il controllo della TAOR della base, le necessarie strisce perimetrali di sicurezza, adeguati settori e distanze di tiro, itinerari per il controllo del territorio esterno, responsabilità e modalità d'intervento delle unità in ciascuno dei settori assegnati e modalità per la saldatura di quelli contermini;
- emanare le direttive per l'impiego delle unità (assicurando un adeguato stato di "reazione"), degli equipaggiamenti disponibili per la sorveglianza e la rilevazione della minaccia (ISTAR, WLR[24], Sistemi Integrati di FP, ecc.) ed i necessari collegamenti (radio, filo, ecc.);
- identificare le adeguate distanze di sicurezza (*stand off*) in merito alla possibile minaccia (IED, tiro diretto, indiretto, attacchi non convenzionali);
- determinare gli effetti della minaccia ed individuare le adeguate infrastrutture ed opere di protezione necessarie;
- stabilire le procedure per il controllo degli accessi, il rilascio dei pass e la pianificazione dei movimenti dei veicoli all'interno della base;
- stabilire le procedure per il controllo e l'autorizzazione all'accesso dei lavoratori locali, compreso il processo di verifica dei requisiti per l'assunzione;

[24] *Weapon Location Radar*.

- stabilire le attività di controllo lungo le LOC (considerando ogni possibile linea / itinerario di comunicazione incluse le vie d'acqua esterne quali i canali navigabili, fiumi, laghi o zone costiere che possono essere utilizzati per i collegamenti o per il controllo della TAOR) e i punti di accesso alla base.

2.2.1.2 Fase condotta:

- verificare che sia stato redatto il piano di sorveglianza e difesa della base e delle basi dipendenti e che entrambi tengano conto delle unità e dei sistemi/materiali disponibili e contengano consegne chiare ed inequivocabili;
- definire le direttive per l'approntamento di una QRF per le esigenze di protezione specifiche della base ed a favore delle basi dipendenti;
- verificare che siano stati assegnati alle diverse unità della base un proprio settore di responsabilità per l'intervento in caso di evento ostile;
- verificare l'esistenza e l'idoneità delle procedure e l'impiego dei sistemi per il controllo dei pedoni e dei veicoli;
- verificare l'esistenza e l'idoneità delle misure di protezione nei luoghi di lavoro, di ritrovo collettivo, negli alloggiamenti e nei ricoveri (*Bunkers*);
- definire le procedure per assicurare in sicurezza la captazione, il trattamento, il controllo, l'immagazzinamento e la distribuzione dell'acqua;
- definire le misure di protezione delle stazioni tecnologiche per la produzione di energia elettrica;
- verificare la disponibilità di un'adeguata capacità sanitaria, l'esistenza e l'idoneità delle misure di prevenzione da rischi ambientali, vettori ed epidemie;
- integrare la pianificazione di contingenza per gli aspetti legati alla sopravvivenza della base;
- definire gli obiettivi informativi specifici di FP da richiedere alla cellula S/G2.

2.2.2 Organizzazione di FP da approntare:

La gestione delle attività del modello di FP ai fini della protezione della base militare risale alla Cellula FP dello Staff dell'unità che ha il Comando della base, inquadrata nell'ambito della Cellula S/G3. La Cellula FP si avvale del contributo di un gruppo di lavoro permanente che incentra la sua attività nel processo di *Risk Management* e che è:

- costituito ad hoc nell'ambito dello Staff (FP *Working Group*-FPWG, che dipende, di norma, dal S/G/J3[25]);
- coordinato dal Capo Cellula FP.

La Cellula FP è organizzata tenendo presente:

- la missione assegnata;

[25] Potrebbe dipendere anche direttamente dal COS o dal DCOS OPS.

- le caratteristiche dell'ambiente operativo in cui si sviluppa (PERMISSIVO, SEMI-PERMISSIVO e NON-PERMISSIVO);
- le tipologie della minaccia relative all'ambiente operativo;
- le capacità che assicurano lo sviluppo delle attività di FP. Tali capacità si esprimono attraverso l'impiego di specifico personale delle Varie Armi o dei Corpi qualificato nella FP, in numero adeguato alle esigenze operative, per ricoprire le seguenti figure della cellula FP:
  - Capo Cellula FP;
  - Ufficiale/Sottufficiale addetto alla FP;
  - Ufficiale addetto alla difesa CBRN.

Indicativamente, al fine di assicurare le attività di *Monitoring & Advising*, la Cellula FP dovrebbe essere composta da:

- 1 Capo Cellula FP ed 1 Ufficiale/Sottufficiale Addetto FP in ambiente PERMISSIVO;
- 1 Capo Cellula FP, 1 Ufficiale Addetto FP, 1 Sottufficiale Addetto FP, 1 Ufficiale addetto alla difesa CBRN in ambiente SEMI/NON-PERMISSIVO.

Ovviamente, al fine di assicurare una piena flessibilità ed aderenza al singolo contesto operativo, si rimanda alle specifiche Direttive Operative Nazionali di ciascuna Operazione ed alle scelte dei vari Comandanti, significando che l'organico adottato dovrà tenere conto della tipologia di ambiente operativo e dei compiti che la cellula deve svolgere per assicurare la piena capacità di gestione.

2.2.3 Compiti delle principali figure dell'organizzazione di FP

2.2.3.1 Ufficiale Addetto alla FP:

- avvia il ciclo di pianificazione della FP e predispone le relative direttive/linee guida da far approvare al Comandante;
- supporta la pianificazione in caso di emergenza in seno allo *Staff*;
- supporta le unità della base (ovvero delle basi dipendenti) nella definizione delle misure di sicurezza, procedure e organizzazione/capacità delle forze di sicurezza e nell'autovalutazione delle misure di FP adottate o che si intendono adottare, in aderenza alle direttive del Comandante della base;
- fornisce le linee guida sull'impiego dei sistemi integrati FP (sia di sorveglianza che di reazione) e dei materiali necessari per la protezione delle infrastrutture critiche della base;
- valuta l'efficacia dei piani e relativi SOP sulle misure di protezione della base;
- sviluppa attività di collegamento con la *Host Nation*;
- valuta la pianificazione delle misure di protezione antincendio;
- fa aggiornare, di volta in volta, le misure di FP in funzione dell'evoluzione della minaccia;
- analizza le *Check List* sull'autovalutazione delle unità dipendenti per valutare eventuali aggiornamenti/diposizioni integrative da far attuare;

- integra il piano di sorveglianza della TAOR e difesa area con quello terrestre della base;
- coordina le attività del FPWG;
- svolge funzione di *FP Advisor* per il Comandante della base.

2.2.3.2 Ufficiale/Sottufficiale Addetto alla FP:

- monitora l'andamento dell'applicazione delle misure di FP e loro aderenza alle direttive/ordini emanati dal Comandante della base;
- effettua sopralluoghi tecnici di FP presso le unità dipendenti e le aree della base per esaminare le varie esigenze operative o richieste di concorsi rappresentate;
- monitora l'impiego e lo stato di conservazione dei sistemi e dei materiali di FP dislocati nella TAOR della base (barriere, gabbioni metallici, attrezzature per il rilevamento di esplosivi, ecc.), richiedendo l'intervento di tecnici per la loro manutenzione/riparazione o la loro sostituzione;
- gestisce il processo di LId/LL in relazione alla FP.

2.2.3.3 Ufficiale Addetto alla Difesa CBRN:

- valuta e monitora la minaccia CBRN nella TAOR assegnata alla base ed i relativi rischi;
- definisce le linee guida e le direttive per lo sviluppo dei piani inerenti la CBRN;
- assicura la funzione di *CBRN Warning and Reporting* sia a livello di procedure manuali che per il tramite dei software di *modelling and simulation* (detta funzione deve essere integrata all'interno dell'apposita rete di *Warning and Reporting* esistente nella TAOR);
- supporta lo sviluppo dei piani di emergenza;
- valuta il grado di capacità di sopravvivenza CBRN delle Unità/Comandi della base;
- coordina con cadenza predeterminata (settimanale, quindicinale etc..) l'attività di campionamento presso la base da effettuarsi da parte dell'Unità specialistica CBRN presente nella TAOR al fine di garantire un monitoraggio continuo relativo alla possibile presenza di agenti contaminanti;
- verifica e valuta i possibili rischi derivanti da sedimi industriali presenti nelle vicinanze della base definendo a priori le possibile *Hazard areas.*

2.2.3.4 Ufficiale del genio addetto alla FP:

- valuta e monitora la minaccia FPE nella TAOR assegnata alla base ed i relativi rischi;
- definisce le misure di protezione passiva delle basi e degli elementi critici delle stesse (per la protezione collettiva, per l'integrazione/potenziamento delle strutture della difesa attiva, a supporto della protezione CBRN, sanitaria e ambientale e per assicurare la sopravvivenza delle unità);
- definisce le misure di protezione antincendio, valutando anche i relativi piani redatti dalle unità dipendenti;

- gestisce l'iter del processo di FPE per la realizzazione delle strutture/opere di protezione passiva;
- supporta l'FPO nella gestione dei sistemi di sorveglianza e reazione;
- definisce le misure per lo sviluppo dei piani di inganno e quelle per il mascheramento;
- analizza le *Check List* sull'autovalutazione delle unità dipendenti per valutare eventuali aggiornamenti/diposizioni integrativa da far attuare;

2.2.3.5 Ufficiale Medico (Medical FP):

- valuta e monitora la minaccia sanitaria e ambientale nella TAOR assegnata alla base ed i relativi rischi;
- verifica la realizzazione di tutte le fasi del processo *Force Health Protection* (FHP);
- fornisce valutazioni sanitarie sull'ambiente;
- fornisce consulenza in merito ai rischi sanitari aventi un impatto sull'operazione;
- fornisce raccomandazioni sulle misure preventive di FHP e durante tutte le fasi dell'operazione, incluse il pre e post-schieramento;
- fornisce consigli sulla prontezza sanitaria della forza;
- istituisce e gestire un sistema campale di sorveglianza delle malattie e della salute;
- monitora le misure di FHP attuate in teatro;
- fornisce indicazioni FHP per il contributo sanitario da sviluppare durante la fase di pianificazione.

2.2.3.6 Ufficiale Veterinario

- fornisce supporto sanitario relativo alla prevenzione, controllo e attività di sensibilizzazione al personale per il contrasto al randagismo, epidemie, insetti, cura dell'igiene negli ambienti di lavoro;
- effettua i controlli sulle acque, sul confezionamento del cibo, sulla validità dei viveri e delle bevande.

2.2.3.6 Ufficiale Addetto alla Difesa da minaccia Aerea

- valuta e monitorare la minaccia aerea nella TAOR assegnata alla base ed i relativi rischi;
- sviluppa il piano di difesa area della base;
- supporta lo sviluppo dei piani per la difesa terrestre e di sorveglianza della TAOR della base;
- monitora l'impiego e lo stato di conservazione dei sistemi e dei materiali per la difesa aerea dislocati nella TAOR della base.

2.2.3.7 Ufficiale OPSEC

- valuta e monitora la minaccia alle informazioni nella TAOR assegnata alla base ed i relativi rischi;

- revisiona i documenti dello Staff, i sistemi per la gestione e lo scambio delle informazioni aggiornando le EEFI;
- identifica e consiglia il FPO sulle misure per la protezione delle informazioni;
- predispone i piani e le SOP ai fini dell'OPSEC.

2.2.3.8 Ufficiale Addetto alla Sicurezza

- valuta e monitora la minaccia nella TAOR assegnata alla base ed i relativi rischi;
- raccoglie e dissemina le informazioni su tale minaccia;
- valuta lo stato dell'allertamento in vigore sulla base dell'evoluzione della minaccia;
- definisce le procedure per il controllo degli accessi,
- predispone il piano di difesa terrestre della base;
- stabilisce le procedure per il controllo degli accessi, il rilascio dei PASS e la pianificazione dei movimenti dei veicoli all'interno della base;
- stabilisce le procedure per il controllo e l'autorizzazione all'accesso dei lavoratori locali, compreso il processo di verifica dei requisiti per l'assunzione;
- stabilisce le attività di controllo lungo le LOC, le vie d'acqua esterne e dei punti di accesso alla base;
- stabilisce le procedure per il rilascio delle tessere di riconoscimento individuale;
- stabilisce le procedure per le attività di controllo biometrico agli ingressi;
- definisce le attività addestrative ed esercitative del personale della difesa.

2.2.3.9 FP *Working Group* (FPWG)

Viene costituito in seno allo *Staff* dell'unità che gestisce la sicurezza della base ed è composto dai rappresentanti di tutte le Cellule del predetto Comando[26], dal personale specializzato delle unità dipendenti o di altre unità ivi accantonate (CBRN, EOD/IEDD, MP, ecc.), dai Comandanti delle unità addette alla sicurezza delle basi distaccate nella TAOR, dai responsabili della sicurezza delle unità che sono accantonate nella base e, qualora ritenuto necessario, può esse chiamata a partecipare ai lavori anche una rappresentanza della *Host Nation* (HN).

Il FPWG è presieduto dal Capo Cellula S/G/J3 o dal COS/DCOS OPS, coordinato dal FPO/Capo Cellula FP (che svolge le funzioni di segretario e coordinatore) e si riunisce nei tempi e nei modi stabiliti dal Comandante nello specifico SOP per le attività di FP[27], secondo una tempistica differente in relazione all'ambiente operativo.

---

[26] Partecipano in qualità di membri permanenti: *Chief* S3 (Capo Gruppo di Lavoro), S1, S2, S3 FPO, S4, S5, INFOSEC, CAII, S3-Eng/EOD, INFO OPS, Difesa CBRN, *Medical Advisor*, MP, Difesa da minaccia Aerea, Guerra Elettronica, Legad, Polad).

[27] La struttura del SOP è reperibile sul NATO FP *Handbook* (ed. 2007).

In tale WG sono esaminate tutte le problematiche connesse con la FP e definite le misure ritenute necessarie da proporre al Comandante, in funzione del livello e della tipologia della minaccia, al variare di uno di essi o di entrambi.

I vari rappresentanti partecipano, di volta in volta e sulla base delle esigenze operative del Capo Cellula FP, allo svolgimento di ricognizioni tecniche di FP (*Vulnerability Assessment Teams*) mirate alla identificazione di vulnerabilità e criticità dell'organizzazione di FP attuata: verifica delle misure di protezione (protezione attiva, passiva e sorveglianza), validità delle procedure di controllo adottate, ecc.

Al riguardo, la partecipazione di ciascun elemento viene:

- definita, di volta in volta, dal Capo Cellula FP sulla base della situazione operativa o delle esigenze operative/problematiche di FP da esaminare;
- legata all'esame delle problematiche di FP connesse con la propria Cellula:
  - **S/G1**: analisi delle problematiche relative all'organico delle unità addetta alla difesa della base;
  - **S/G2**: analisi della minaccia e dei rischi (attraverso il collegamento con gli organi informativi nazionali e della HN e l'esame di CI *reports*, informazioni e documenti classificati);
  - **S3/G-Eng:** misure per mitigare gli effetti della minaccia ed aumentare la protezione fisica e strutturale e le capacità di sopravvivenza della base, attività EOD/IEDD, *route & area clearance* e *military search*;
  - **S/G4**: organizzazione dei convogli, scorte e controllo delle LOC, sicurezza durante il caricamento e scaricamento dei materiali, stoccaggio e sicurezza dei relativi depositi ed infrastrutture di supporto (in coordinamento con il S/G2 ed il S/G3 FP); interventi per la protezione ambientale (con il supporto della S3/G-Eng e del *Camp Site Manager* della base);
  - **S/G4 Med**: misure per la salute fisica, dentale e mentale del personale, le misure di medicina preventiva (pronto soccorso, igiene, preservazione dell'ambiente, controllo dei vettori epidemici, ecc.), *medical intelligence information*;
  - **S/G6 INFOSEC**: misure preventive e di controllo COMPUSEC e COMSEC per la protezione, la trattazione e la trasmissione di informazioni classificate e non;
  - **S/G8:** richiesta e gestione dei fondi per le attività di FP;
  - **CIMIC:** supporto della popolazione civile (condizioni, attitudini ed intenzioni nei confronti delle Forze);
  - **POLAD:** implicazioni politiche, collegamento con GOs e NGOs;
  - **LEGAD:** ROE, legislazione nazionale e internazionale, accordi e trattati politici, persecuzione criminalità, forze di polizia;

- **PI:** deputato al controllo, analisi, valutazione e gestione degli organi di informazione;
- **MP:** attività di polizia militare ai fini del controllo degli accessi e delle aree critiche/riservate della base, nonché sincronizzazione delle attività di Polizia Militare con quelle per il controllo e la difesa delle LOC e della base;
- **EPO:** valutazione dei rischi derivanti dall'ambiente (impatto ambientale) e definizione delle relative misure di protezione;
- **ESO**: valutazione dei rischi connessi con la gestione dei depositi munizioni e definizione delle relative misure di ESMRM (attività svolta in coordinamento con l'*Explosive Safety Board* – ESB).

2.2.4 Emanazione delle direttive

Come evidenziato al sottopara b., la fase di *Risk Management* si conclude con:

- l'emanazione degli ordini: Annesso "J" all'OPORDERer o FRAGO specifici;
- la redazione delle SOP necessarie.

Le misure, i compiti e le attività riguardano le seguenti tematiche:

- procedure;
- personale;
- materiali;
- infrastrutture;
- informazioni;
- responsabilità.

Ferma restante la responsabilità del Comandante di un Complesso Tattico in merito all'applicazione delle misure di FP nell'ambito delle sue unità dipendenti, ovvero delle basi delle unità alle dirette dipendenze (anche dislocate in località diverse), le responsabilità del Comandante di una base nell'ambito della quale sono accantonate anche diverse unità (specialmente se multinazionali) è strettamente correlata con la delega d'Autorità ricevuta dal Comandante delle Forze, con le restrizioni nazionali (*caveats*) e con il grado di controllo sulle risorse comunque disponibili. Alcune di esse sono alle dirette dipendenze mentre altre lo possono essere all'atto di una emergenza o sulla base di piani di contingenza.

In tale contesto, il Comandante di una unità cui viene assegnato il Comando di una base militare in Te. Op. dove insistono anche unità non dipendenti dalla sua, valuta, in qualità di "Responsabile alla sicurezza della base"[28] ,ovvero attraverso la nomina di un proprio Ufficiale addetto alla sicurezza della base (*Security Officer*), che per ciascuna delle unità sotto la sua responsabilità e tutela vengano applicate in maniera omogenea, in accordo con gli stati di allertamento in vigore nell'AOO stessa, le

[28] Tale funzione deve essere espressamente indicata sull'Annesso J "FP" all'Ordine di Operazioni e sulla SOP FP.

misure e le procedure di FP definite dall'Ordine di Operazioni (Annesso "J" FP) e dalle relative SOP discendenti (FP, CBRN, ecc.).

Al riguardo, il predetto Ufficiale coordina e verifica:

- la corretta applicazione di direttive e procedure sulla sicurezza (OPSEC, controllo degli accessi alla base veicolari e pedonali, controllo e autorizzazioni per l'accesso alle aree e documenti classificati, ecc.);
- lo sviluppo di programmi di "*Security & Education Awareness*";
- l'attuazione del processo di ricerca e scambio delle informazioni;
- la redazione/integrazione dei piani di FP, che devono tenere conto della mutua attività di sorveglianza e di supporto operativo tra le varie unità della base e tra questa e le altre basi dipendenti nell'AOO assegnata;
- l'emanazione delle disposizioni di sicurezza, inclusi i requisiti tecnici, procedurali e operativi al fine di incrementare la sicurezza definendo le linee guida le procedure per l'accesso alle infrastrutture di mano d'opera locale e *civil contractors*;
- l'applicazione delle misure di protezione per il personale, siano esse individuali, collettive o per i VIP;
- l'effettuazione delle attività di *improcessing, key leader training* e *security clearances.*

Le direttive afferenti la FP NATO e/o Multinazionali (nel caso di missione a guida NATO) non devono essere adottate rigidamente ma possono essere integrabili o modificabili in base alle Regole di Ingaggio ed esigenze nazionali in materia di FP (Annesso FP alla Direttiva Operativa Nazionale) che comunque, qualora risultino più restrittive, devono essere considerate prioritarie.

2.3 *SITUATIONAL AWARENESS*

Le misure di FP (stati di allertamento e relative misure, codici per il movimento, l'armamento e l'uniforme da indossare in ciascun settore della base militare o per l'effettuazione di specifiche attività, particolari misure relative agli accessi, ecc.) vengono incluse nel SITREP per il Comando superiore.

Particolare attenzione va posta nell'evidenziare le varie località dove uno stato di allertamento può essere diverso dal livello generale dell'AOO. Ogni cambio di stato di allertamento deve essere comunicato immediatamente al JOC/TOC del Comando superiore.

Il S/G3 è responsabile per la diffusione degli stati di allertamento alle basi dipendenti.

Tutti i Comandanti si assicurano che tali informazioni:

- vengano diramate in maniera idonea;
- siano visibili nelle varie sale operative, aree critiche, ingressi e nelle aree ritenute appropriate per divulgare tali informazioni.

Anche le informazioni riguardanti la minaccia (*terrorist threat warnings*) vengano disseminate tra il personale dipendente.

Lo scambio delle informazioni inerenti la FP avviene, a cura della Cellula FP, attraverso:

- le normali procedure di *Report & Returns* standardizzate (SITREP, INTSUM, ecc.);
- reti LAN classificate (ad es. costituzione di un blog per la discussione delle problematiche di FP e l'esame di soluzioni adottate.

2.4 REDAZIONE DEI PIANI PER LA SORVEGLIANZA E LA PROTEZIONE DI UNA BASE MILITARE

La pianificazione per la FP prevede la redazione di piani tendenti ad assicurare la protezione e la sopravvivenza di una base militare in operazioni. Essa deve prendere in esame le aree tematiche della FP sulla base delle risultanze del modello di FP, attraverso lo sviluppo del *Risk Management*. La pianificazione, sulla base delle linee guida del Comandante della base, prevede la redazione dei seguenti piani e delle SOP discendenti per lo sviluppo armonizzato e dettagliato delle procedure da applicare:

- "piano di difesa terrestre";
- "piano di difesa aerea" (può essere anche compreso nel precedente piano laddove la difesa aerea della base sia già stata compresa in un piano del livello superiore o gli assetti siano ridotti e facilmente gestibili da una sola sala operativa);
- "piano per la sorveglianza della TAOR";
- "piano per le emergenze" (incendi, CBRN, ecc.);
- "piano per il recupero della capacità operativa" (a seguito di un evento/incidente causato dalla minaccia identificata e il relativo *Consequence Management*).

La succitata pianificazione dovrà essere:

- integrata con i documenti di pianificazione della "protezione ambientale" (*Environmental Baseline Study* – EBS) redatto dall'*Environmental Protection Officer* (EPO), della "protezione igienico-sanitaria" (*Force Health Protection* - FHP) radatta dal Medical FP e della valutazione dei rischi connessi alla gestione dei depositi munizioni nell'ambito delle attività di *Explosive Safety Munition Risk Management* (*Explosive Safety Site Plan* – ESSP) eseguita dall'*Explosive Safety Officer* (ESO).
- esaminata nell'ambito del FP *Working Group* prima di essere sottoposta all'approvazione del Comandante della Base.

2.4.1 Piano di difesa terrestre

2.4.1.1 Scopo

Delineare l'organizzazione della difesa terrestre di una base militare.

2.4.1.2 Analisi dell'esigenza operativa

Il piano generalmente contiene:

- minacce individuate e possibili aree della base interessate;
- TTP delle forze ostili;
- caratteristiche degli elementi critici della base;
- sistema di protezione della base adottato;
- organizzazione di Comando e Controllo della FP (compiti, composizione e collegamenti del BDOC - *Base Defense Operations Center*);
- sistemi per le comunicazioni radio-filo;
- definizione degli assetti, compiti, procedure per il loro allertamento e intervento e relative misure di coordinamento;
- predisposizioni per la pianificazione delle misure antincendio, CBRN e per il ripristino (*Consequence Management*);
- procedure per il controllo degli ingressi e loro integrazione con le strutture di protezione per potenziare le attività difesa attiva (vigilanza della base);
- procedure per il rilascio dei pass a pedoni e veicoli;
- procedure per l'accesso dei VIP e delle relative scorte;
- procedure per la custodia di personale o veicoli sospetti;
- attività di coordinamento con la Polizia Militare;
- stati di allertamento;
- procedure per il controllo dei lavoratori locali per evitare la minaccia *insider threat;*
- modalità per la pianificazione e l'esecuzione di esercitazioni per gli assetti della vigilanza e per l'emergenza.

2.4.1.3 Predisposizioni per la redazione del piano

Il predetto piano:

- viene redatto dal *Security Officer* (S/G2) dell'unità che gestisce la difesa della base tenendo conto delle capacità d'intervento delle armi e dei sistemi di controllo in dotazione e delle regole d'ingaggio vigenti, prendendo in considerazione gli eventuali *caveats* nazionali delle unità multinazionali che possono essere accantonate nella base;
- è integrato con il piano della difesa aerea e di sorveglianza;
- viene approvato dal Comandante della base.

2.4.2 Piano di difesa aerea

2.4.2.1 Scopo

Delineare l'organizzazione della difesa aerea di una base militare.

2.4.2.2 Analisi dell'esigenza operativa

Il piano contiene:

- minacce individuate e possibili aree della base interessate;

- TTP delle forze ostili;
- caratteristiche degli elementi critici della base;
- le misure di difesa aerea attive e passive;
- organizzazione di Comando e Controllo della FP (compiti, composizione e collegamenti dell'ATOC - *Air Tactical Operations Center* o degli elementi che devono essere integrati nel BDOC, qualora l'ATOC non venisse attivato);
- sistemi per le comunicazioni radio-filo;
- definizione degli assetti, compiti, procedure per il loro allertamento e intervento (modi di operazione per l'esercizio del Controllo Tattico; ordini di Controllo Tattico; misure di controllo dello spazio aereo; modalità d'identificazione dei velivoli; modi d'intervento; messaggistica da impiegare) e misure di coordinamento con le Agenzie di controllo dello spazio aereo;
- caratteristiche dei sistemi e lineamenti d'impiego;
- modalità per la diffusione dell'allarme;
- modalità per la pianificazione e l'esecuzione di esercitazioni per gli assetti specialistici e dell'emergenza.

In particolare:

- difesa aerea (*Theatre Missile Defence & Surface Based Air Defence*):
- a media ed alta quota: misure di difesa attiva (operate da sistemi *Medium Range Surface to Air Missile* -MRSAM) e passiva, per localizzare e annullare la minaccia dovuta a velivoli (compresi anche i mini/micro UAV), missili o ridurne gli effetti;
- a bassa/bassissima quota: modalità per l'impiego ed il controllo del fuoco di tutte le armi portatili e di reparto della base e relative misure di sicurezza; impiego integrato di sistemi *Short Range Air Defense* (SHORAD) e *Very Short Range Air Defense* (V/SHORAD) eventualmente disponibili;
- *Counter Rocket Artillery & Mortar* (C-RAM): misure per la scoperta, l'allarme e l'intercettazione di razzi, artiglierie e mortai.

2.4.2.3 Predisposizioni per la redazione del piano

Il predetto piano:

- viene redatto dal G/S3 Air dell'unità che gestisce la difesa della base tenendo conto delle capacità d'intervento dei velivoli, delle armi contraeree e dei sistemi di controllo in dotazione e delle regole d'ingaggio vigenti, tenendo anche presente gli eventuali *caveats* nazionali delle unità multinazionali che possono essere accantonate nella base;
- è integrato con il piano della difesa terrestre e di sorveglianza;
- viene approvato dal Comandante della base.

2.4.3 Piano di sorveglianza della TAOR

2.4.3.1 Scopo

Delineare l'impiego dei sistemi di sorveglianza in dotazione ed installati nella base ai fini del controllo della TAOR.

2.4.3.2 Analisi dell'esigenza operativa

Il piano generalmente contiene:

- caratteristiche e capacità dei sistemi in dotazione;
- aree/settori di controllo e relative priorità d'intervento;
- localizzazione nella base e collegamenti con il BDOC, deputato alla gestione della difesa della base;
- lineamenti per l'impiego, manutenzione e riparazione dei sistemi;
- personale per il loro impiego e relative turnazioni e modalità per l'allertamento di quello a riposo;
- modalità per l'aggiornamento della *Situational Awareness* al TOC (*Tactical Operations Center*), che gestisce tutte le attività operative nell'ambito dell'AOR assegnata e da cui dipende il BDOC;
- misure di coordinamento con l'ATOC o il personale c/a del BDOC per il supporto alla difesa aerea;
- modalità per la pianificazione e l'esecuzione di esercitazioni per gli assetti specialistici e per l'emergenza.

2.4.3.3 Predisposizioni per la redazione del piano

Il predetto piano:

- viene redatto dal Security Officer (S/G2) dell'unità che gestisce la difesa della base, con il concorso, per quanto di specifico interesse, del S/G3 e del S/G3 FP, tenendo conto delle capacità e dei limiti d'impiego dei sistemi di controllo in dotazione e delle regole d'ingaggio vigenti, tenendo anche presente gli eventuali *caveats* legati alle limitazioni/vincoli legali al loro impiego della *Host Nation*;
- è integrato con il piano di difesa terrestre ed aerea;
- viene approvato dal Comandante della base.

2.4.4 Piano per le emergenze

2.4.4.1 Scopo

Pianificazione che deve contenere tutte le procedure da mettere in atto nel caso in cui si verifichi un evento dannoso. Nel particolare, il piano per le emergenze prende in esame le possibili tipologie di eventi di pericolo (naturali, meteorologiche o connesse con le attività svolte dall'avversario), che per loro natura ed estensione territoriale, richiedono normalmente un intervento coordinato. esso deve delineare le predisposizioni da attuare in caso di incendi, eventi CBRN (compreso materiale tossico), sanitari, calamità naturali o emergenze complesse (sia a causa di eventi naturali che antropici che rientrano nell'ambito del *consequence management*), allo scopo di ridurre i danni alle infrastrutture e materiali e le perdite del personale. Tale piano deve tenere conto anche del possibile intervento a favore delle popolazioni locali.

2.4.4.2 Analisi dell'esigenza operativa

Il piano generalmente contiene:

- **Misure antincendio**
  - valutazione della vulnerabilità delle aree e degli edifici della base;
  - dislocazione del materiale infiammabile sulla base delle valutazione dei carichi di incendio, della tipologia del materiale critico dislocato all'interno della base e delle possibili aree di propagazione degli incendi;
  - organizzazione antincendio: personale, compiti, materiali, misure di coordinamento per l'allertamento e l'impiego dei nuclei antincendio;
  - addestramento e qualifica del personale;
  - modalità per la pianificazione e l'esecuzione di esercitazioni per gli assetti antincendio.
- **Misure difesa CBRN**
  - procedure per i controlli da attuare ai fini dell'individuazione e identificazione di materiale CBRN;
  - procedure per la messa in sicurezza del materiale contaminante;
  - procedure per la gestione delle informazioni CBRN;
  - misure individuali e collettive per la protezione e l'esposizione ad agenti CBRN, in relazione agli stati di allertamento;
  - organizzazione CBRN: personale, compiti, materiali, misure di coordinamento per l'allertamento e l'impiego dei nuclei SIBCRA, decontaminazione ed EODBC;
  - modalità per l'aggiornamento della *Situational Awareness* al BDOC (CBRN W&R);
  - predisposizioni sanitarie per l'intervento in caso di evento CBRN;
  - addestramento e qualifica del personale;
  - modalità per la pianificazione e l'esecuzione di esercitazioni per gli assetti CBRN.
- **Misure per l'emergenza sanitaria**
  - misure per la medicina preventiva e la sorveglianza sanitaria delle aree della base ed i luoghi di lavoro;
  - procedure per i controlli dell'igiene ambientale, dell'acqua e delle vettovaglie;
  - organizzazione sanitaria: personale, compiti, materiali, misure di coordinamento per l'allertamento e l'impiego dei nuclei sanità;
  - predisposizioni per l'intervento in caso di *Mass Casualties*;
  - attività di supporto al *Consequence Management*;
  - attività di supporto in caso di eventi CBRN;
  - materiali sanitari per il primo soccorso e loro dislocazione.
  - elenco e compiti personale addetto al primo soccorso.
  - modalità trattamento ed evacuazione feriti presso ROLE 1, 2 e 3.
  - definizione aree sicure e postazioni per effettuare il primo trattamento dei feriti.

- modalità per la pianificazione e l'esecuzione di esercitazioni per tutto il personale specialistico e per l'emergenza.

2.4.4.3 Predisposizioni per la redazione del piano

Il predetto piano:

- viene redatto dal S/G3 dell'unità che gestisce la difesa della base (con il concorso del S3/G-Eng FPE, S/G3 CBRN, S/G4 Med) tenendo conto delle capacità e dei limiti d'impiego dei materiali in dotazione, delle possibilità d'intervento del livello superiore e tenendo anche presente la capacità della *Host Nation*;
- deve essere integrato con il piano di difesa terrestre, aerea e sorveglianza;
- viene approvato dal Comandante della base.

2.4.5 Piano per il recupero della capacità operativa

2.4.5.1 Scopo

Delineare le predisposizioni per ripristinare il più rapidamente possibile la capacità operativa a seguito di un evento ostile (*Post Event Measures*).

2.4.5.2 Analisi dell'esigenza operativa

Il piano contiene le misure, i compiti e le attività necessarie per il ripristino in tempi rapidi delle capacità operative essenziali per assicurare la sopravvivenza della base e l'esecuzione dei compiti per il proseguimento della missione assegnata:

- ripristino dei collegamenti per le attività di Comando e Controllo;
- ripristino dei sistemi di sorveglianza resisi inefficienti;
- rimessa in efficienza delle infrastrutture colpite dall'evento (impiego di unità del genio o ditte civili locali);
- ristabilimento della capacità operativa della vigilanza (rinforzo di personale, sostituzione di mezzi e materiali);
- reintegrazione delle scorte (viveri, acqua, carburanti, munizioni, ecc.).

2.4.5.3 Predisposizioni per la redazione del piano

Il predetto piano:

- viene redatto dal S/G3 dell'unità che gestisce la difesa della base tenendo conto delle capacità e dei limiti d'impiego di personale, equipaggiamenti e materiali in dotazione;
- è attuato con immediatezza durante la fase di "risposta ad un incidente" ed al *Consequence Management* sulla base degli esiti un'attività di verifica immediata dei danni subiti a causa dell'evento;
- è integrato con il piano per le emergenze;
- viene approvato dal Comandante della base.

2.5 DIREZIONE, COORDINAMENTO E CONTROLLO DELLE MISURE DI PROTEZIONE PREDISPOSTE

2.5.1 Direzione

È cura della Cellula FP assicurare la diffusione delle linee guida e delle informazioni afferenti alla FP, diramando, in particolare, tutti i risultati del modello di FP e delle Lezioni Identificate (LiD)/Lezioni Apprese (LL) che possono sostenere e migliorare la pianificazione e l'attuazione delle citate misure. La diramazione avviene facendo ampio uso di *format* standardizzati al fine di renderne più rapida la loro trasmissione e comprensione, specie nei contesti multinazionali[29].
Inoltre, la creazione di un Forum "classificato" dove scambiare informazioni e suggerimenti consente di ottimizzare il processo di gestione della FP.

2.5.2 Coordinamento

Le consuete forme di coordinamento[30], verticale e orizzontale, devono essere attuate per ogni tipo di operazione. Per quanto concerne le basi militari, il S/G3 è responsabile del coordinamento e del controllo delle attività relative alla FP, armonizzando gli *input* provenienti dal S/G2 e dalla dipendente Cellula FP.

2.5.3 Controllo

La verifica della validità delle misure di FP predisposte dall'unità che gestisce la base (ovvero dalle unità che insistono nella base, nonché delle basi delle unità dipendenti) è un'attività fondamentale ai fini della sicurezza complessiva e per la sopravvivenza della base stessa (ovvero del sistema di basi). La Cellula FP è competente per il controllo delle predette misure, con il supporto dello *Staff* e degli specialisti delle unità alle dipendenze, attraverso le seguenti attività:

- effettuazione di simulazioni ed esercitazioni, i cui risultati sono valutati in sistema con l'aggiornamento della situazione;
- sviluppo di AAR (*After Action Review*), subito dopo un incidente/evento dannoso occorso per l'individuazione tempestiva dei gap e dei correttivi da apportare (vanno valutati anche i risultati delle esercitazioni FP, di cui al punto precedente); elaborazione di Lid e attivazione del ciclo delle LL, da rendere disponibili per la divulgazione in tempi contenuti;
- individuazione delle vulnerabilità dell'organizzazione di FP approntata per la base in regime di "autovalutazione" effettuata dalla Cellula S/G3 FP dell'unità che gestisce la base (Allegato "D");
- verifica specialistica, denominata Vulnerability Assessment effettuata da un team di specialisti FP (*Vulnerability Assessment Team*) del Comando superiore per:

---

[29] Cfr. NATO, STANAG 2430 - AEngrP-2(B) *Land Forces Combat Engineer Messages, Reports and Returns*.

[30] Cfr. già cit. PID/O 3.14, Cap. III, para. 3.c.(3).

l'approfondimento delle vulnerabilità individuate dalla base militare attraverso la citata FP *self-evaluation*;
- l'analisi degli elementi critici della base in funzione dell'evoluzione della minaccia o delle valutazioni/esigenze operative di FP del Comando superiore.

2.6 RICOGNIZIONE DI AREE E INFRASTRUTTURE AI FINI DELLA PROTEZIONE DELLA BASE

L'attività di ricognizione di aree, siti, infrastrutture, ecc., ai fini della FP è svolta da personale FP del team di pianificazione inserito nell'*Advanced Party* e affiancato, ove possibile, da un nu. Progettazione Operativa di Contingenza (POC) delle unità del genio (CAMPALGENIO).

Ai fini della FP la ricognizione è finalizzata all'individuazione dell'area di sedime più idonea per l'accantonamento delle unità in un favorevole rapporto tra le condizioni di vivibilità e quelle di sicurezza dettate dalla situazione operativa. Inoltre, consente di quantificare compiutamente il materiale necessario alla realizzazione delle varie strutture e opere di protezione che si renderanno necessarie ai fini della FP, usufruendo, ove possibile, anche delle risorse locali disponibili (secondo il principio della sostenibilità ambientale).

Lo schema in fig. 7 sintetizza le attività che vengono attuate dal personale del genio durante la ricognizione:

- nell'area di responsabilità della Forza, per individuare e/o scegliere tra quelli possibili, e per quanto consentito dalla situazione politico-militare in loco, il sedime/infrastruttura più idoneo per l'alloggiamento e la protezione dell'unità;
- ad un sito, base, infrastruttura preesistente, dove i Reparti del Contingente nazionale e/o multinazionale sono da tempo dislocati, al fine di migliorare la protezione delle forze schierate e le condizioni di vita all'interno della base.

La ricognizione consente di esprimere valutazioni di ampio respiro che tengano conto non solo dei possibili siti ma anche della morfologia del terreno esterno alle aree identificate dallo studio preliminare. Risulta, infatti, molto utile conoscere se l'area si trova su un altopiano, in una depressione del terreno, alle falde di una formazione rocciosa, protetta su uno o più lati da un corso d'acqua, o un'area soggetta ad eventi sismici, ecc.. Tali considerazioni avranno una notevole influenza sulla tipologia di strutture di protezione da realizzare e sulla redazione del Piano di Difesa.

Inoltre, durante la ricognizione, nell'ambito della valutazione dei possibili rischi ambientali, devono essere presi in esame non solo le caratteristiche ambientali del sito (naturali e antropiche) ma anche:

- il quadro complessivo del rischio ambientale cui si va incontro (sia i rischi indotti dall'ambiente sulla base sia quelli che possono essere causati dalla base sull'ambiente ad essa circostante);

- l'adeguatezza delle misure preventive dell'inquinamento e quelle relative alla conservazione delle risorse disponibili (produzioni agricole e industriali, tutela del paesaggio e dell'eventuale patrimonio artistico presente);
- le misure di intervento per la protezione attuabili in caso di incidente.

In merito alle procedure ed alle schede da predisporre, vale quanto indicato dalle SOP "Tecniche e procedure per le ricognizioni del genio" e "Tecniche e procedure per la progettazione di contingenza di opere del genio", entrambe edizione 2014.

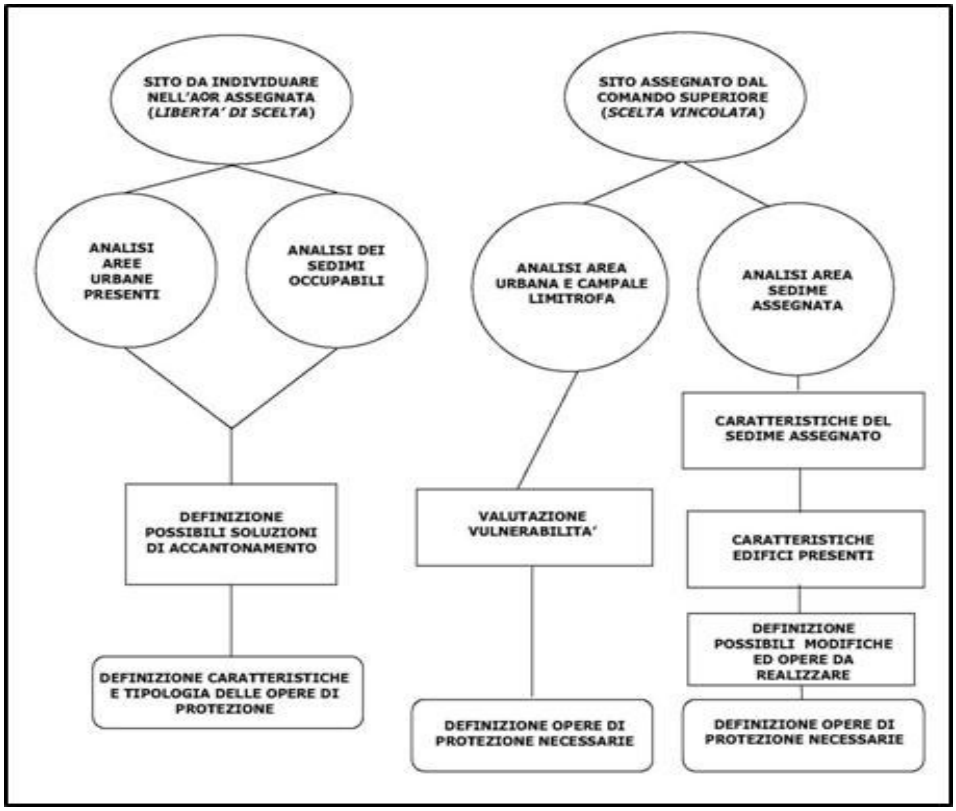


Figura 7: Schema grafico della ricognizione di un sito della FP

PAGINA INTENZIONALMENTE BIANCA

3. IL SISTEMA INTEGRATO PER LA PROTEZIONE DELLE BASI MILITARI

3.1 STANDARDIZZAZIONE DEL SISTEMA DI PROTEZIONE

3.1.1 Concetto Operativo

La TAOR di una base, elemento spaziale nell'ambito del quale localizzare gli assetti/sistemi/materiali di FP, è in genere caratterizzata da elevate estensioni, compartimentazioni e differenze di quota repentine.

In tale situazione operativa:

- le unità devono ricorre, per quanto possibile, alla "dispersione" sul terreno per poter assicurare il controllo di un vasto territorio al fine di contrastare efficacemente l'azione condotta dalle forze ostili;
- le basi militari, sulla base dell'approccio sistematico di FP, illustrato nel Capitolo II, devono adottare un sistema di protezione "standard" che:
  - risulti di tipo "concentrico" e tenga conto delle minacce individuate, possibilmente anch'esse standardizzate, ai fini dello sviluppo del modello di FP;
  - si articoli "in profondità" e comprenda nella propria TAOR:
    - le aree controllabili visivamente con il personale di vigilanza (sentinelle o pattuglie interne/esterne) ed i sistemi di video sorveglianza;
    - le aree non controllabili visivamente, compreso le LOC a supporto delle attività operative e logistiche della base, che possono essere tenute sotto controllo con pattuglie, *check point* (fissi o mobili), sorveglianza con elicotteri o UAV, ecc.;
  - assicuri:
    - l'integrazione di sistemi, assetti e materiali di FP assegnati per la protezione di una base;
    - l'unitarietà di Comando.

3.1.2 Definizione

Il **Sistema Integrato per la Protezione delle Basi Militari** (SIPROB) è definito come l'insieme di assetti, materiali, misure, strutture e procedure di FP che interagiscono tra di loro per la difesa delle basi militari in operazioni.

3.1.3 Sviluppo e caratteristiche del sistema

Tale sistema di protezione standard è stato sviluppato sulla base della già cit. PID-O 3.14 e del Concetto Operativo dello Stato Maggiore dell'Esercito posto alla base

dell'avvio del progetto "*Mission Need Urgent Requirement* per l'incremento della protezione delle FOB/FSB nel Te. Op. Afgano"[31].

Esso, per essere applicato flessibilmente alle diverse operazioni, è stato organizzato sulla base delle seguenti caratteristiche operative:

3.1.3.1 Categorizzazione della minaccia

La minaccia, fatte salve particolari situazioni operative contingenti che ne impongono, di volta in volta, un adeguamento, si può categorizzare[32] nei seguenti elementi:

- **Osservazione**:
  - **interna** (da parte di personale locale assunto come maestranze, ditte e fornitori civili, visitatori, ecc.): dipende dalla forma, dimensioni, organizzazione funzionale, compartimentazione e localizzazione di ciascuna base;
  - **esterna** (osservatori di elementi ostili): 50-500 m.
- **Azioni di fuoco diretto (tiro teso):**
  - armi individuali: 250-400 m;
  - lanciagranate e lanciarazzi c/c: 400-600 m;
  - armi di reparto: 800-1000 m.
- **Azioni di fuoco indiretto (tiro curvo):**
  - mortai leggeri: 2,5-5 km;
  - razzi/mortai pesanti: 9-12 km.
- **Attacchi non convenzionali:**
  - SVBIED - SIED - RCIED: 0-500 m;
  - CBRN: non definibile a priori, in quanto in funzione della tipologia delle sostanze, della struttura interna della base, delle condizioni atmosferiche e della velocità e direzione dei venti dominanti;
  - Minaccia interna (*Insider Threat*), dovuta a dipendenti o lavoratori di ditte locali.

3.1.3.2 Suddivisione areale della TAOR

Sulla base del concetto operativo, la TAOR della base, per poter assicurare un'aderente difesa contro le minacce precedentemente categorizzate, si suddivide in

---

[31] Il progetto è stato completato nel 2014, si proponeva lo scopo di aumentare la protezione delle base e ridurre il numero di personale impiegato per la loro vigilanza, attraverso l'acquisizione e l'installazione di sistemi integrati di sorveglianza e di reazione nelle FOB e nella FSB nazionali di ISAF RC West.

[32] Per la categorizzazione della minaccia è stato preso a riferimento l'ambiente operativo "non permissivo", quale condizione più sfavorevole per le unità in Te. Op.

specifici settori concentrici che individuano sul terreno le seguenti principali **Aree Funzionali per la Difesa di una base** (**AFD**):

- area "interna" (**AI**);
- area "perimetrale" (**AP**);
- area "di osservazione diretta" (la cui distanza è funzione dei mezzi e sistemi di osservazione a disposizione), cioè prospiciente l'istallazione (*Within Line of Sight* - **WLOS**);
- area "non osservabile direttamente", cioè oltre la visuale dell'istallazione (*Beyond Line of Sight* – **BLOS**).

Lo scopo della definizione delle succitate aree (fig. 8) è quello di:

- schematizzare e settorializzare le funzioni operative che devono svolgere gli assetti integrati della difesa;
- individuare la più idonea localizzazione di tali assetti nell'ambito della TAOR per poter fronteggiare efficacemente ciascun tipo di minaccia incombente contro ciascun settore.

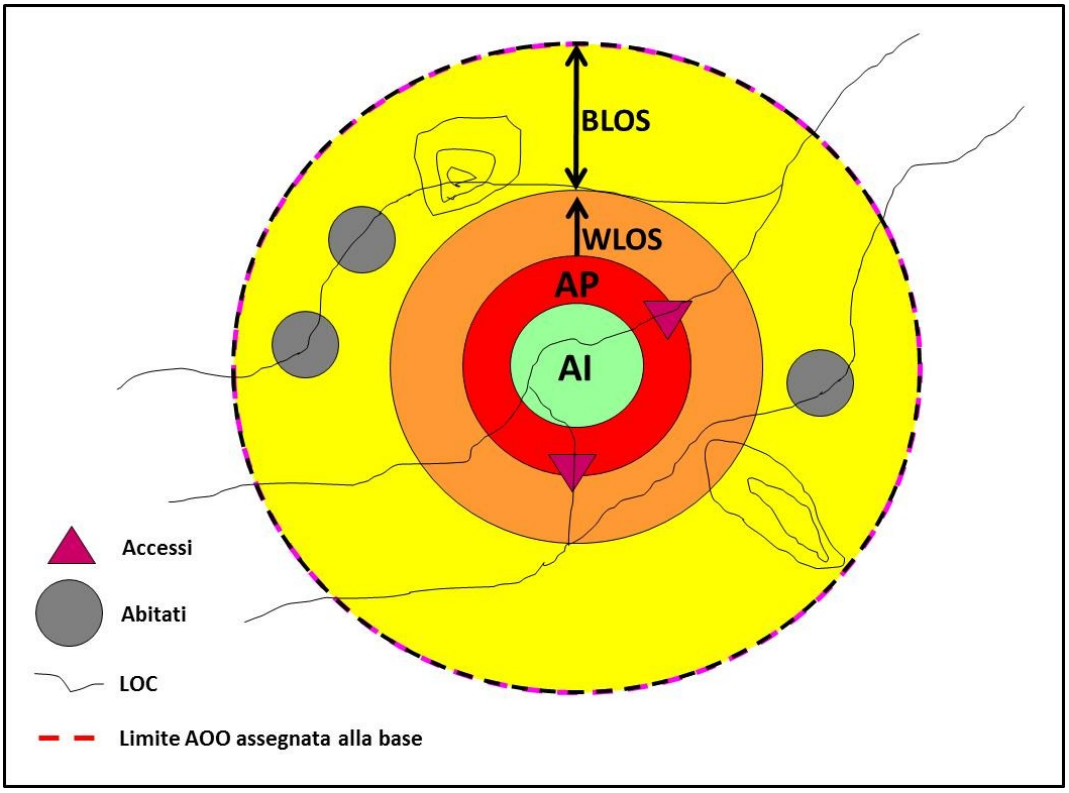


Figura 8: Aree funzionali per la difesa (AFD)

Lo sviluppo dimensionale (ampiezza) di ciascuna area è definito in funzione della rispettiva categoria di minaccia individuata dal S/G2 (come già indicato, nell'ambito del *Threat Assessment*).

Se necessario, possono essere individuate anche ulteriori sub-aree funzionali, qualora lo impongano la particolare variabilità della minaccia, ulteriori specifiche esigenze difensive del momento o la particolare morfologia del terreno.

3.1.3.3 Moduli Funzionali per la Difesa (MFD)

I moduli funzionali per la difesa di una base si sviluppano nell'ambito delle succitate AFD e devono essere considerati come dei contenitori di "assetti" e "misure" per la protezione. Infatti, nell'ambito della loro definizione, comprendono tutti i necessari sistemi, materiali e personale della vigilanza per l'attuazione delle misure di FP della base individuate nel "piano di difesa" e nella "pianificazione di contingenza". Gli MFD sono così articolati:

- **Modulo Comando e Controllo (MC2)**:
  - Tactical Operations Center (TOC)/Base Defense Operations Center (BDOC);
  - sistemi per la gestione integrata;
  - sistemi per i collegamenti e la diffusione dell'allarme.
- **Modulo Protezione (MP)**:
  - Protezione della fascia perimetrale (recinzioni, ingressi, postazioni osservazione/allarme e difensive, sensori antintrusione);
  - Protezione aree interne della base (ricoveri per la protezione collettiva, protezione di aree/elementi critici, protezione di alloggi/luoghi di lavoro e compartimentazione di aree della base e luoghi ad alto indice di affollamento).
- **Modulo Sorveglianza (MSO)**:
  - sistema di sorveglianza interna alla base, fino all'area di sicurezza perimetrale;
  - sistema di sorveglianza ad ampio raggio, oltre il perimetro;
  - sistema per il rilevamento di sorgenti di fuoco.
- **Modulo Reazione Remotizzata (MRR)**:
  - sistema di reazione su torretta amovibile;
  - sistema UGV.

3.1.3.4 Componenti e funzioni operative

A ciascun MFD sono assegnate funzioni di FP, necessarie ad assicurare il controllo e la difesa della TAOR, i relativi componenti/assetti per lo sviluppo delle attività operative di tali funzioni, nonché la loro dislocazione nelle sub aree della TAOR e la zona operativa di interesse ():

MFD	FUNZIONI FP	COMPONENTI SIPROB	AFD	ZONA OPERATIVA
MC2	Comando e Controllo	Posto Comando (BDOC)	AI	TAOR
	Gestione integrata dei sistemi di sorveglianza, controllo, intervento del personale e del fuoco	Sistemi per la gestione	AI	TAOR
	Comunicazioni, diffusione allarme	Sistemi collegamento	AI	TAOR
MP	Anti-intrusione e protezione	Recinzione perimetrale	AP	AP-WLOS
	Sorveglianza e controllo	Ingressi istallazione	AP	AP
	Sorveglianza, scoperta, identificazione, reazione e ingaggio	POA/Postazioni Difensive	AP	AP-WLOS
	Scoperta	Sensori	AP	AP-WLOS
MSO	Sorveglianza, scoperta e identificazione	Sistema video sorveglianza interna (TVCC)	AI-AP	AI-AP
		Sistema integrato video sorveglianza	AI	WLOS
	Scoperta	Sistema acustico localizzazione sorgenti fuoco	AP	BLOS
	Sorveglianza, scoperta e identificazione	UAV	AI	TAOR
MRR	Sorveglianza, scoperta, identificazione, reazione e ingaggio	UGV	AI-AP	AP-WLOS
		Sistemi d'arma remotizzati	AP	AP-WLOS

Figura 9: Schema componenti e funzioni operative degli MFD

3.1.4 Schema funzionale[33]

L'organizzazione del "Sistema Integrato per la Protezione delle Basi Militari" (SIPROB) in operazioni (fig. 10):

- dipende dal Comandante della Base;
- si compone di una struttura ad hoc per il Comando e Controllo delle attività di FP (*Base Defense Operations Center* - BDOC) e di alcuni assetti operativi alle dirette dipendenze o, qualora richiesto, assegnati in rinforzo da altre unità. Qualora una base sia utilizzata per azioni limitate nel tempo o da un complesso tattico del livello compagnia o plotone (base di modeste dimensioni), al fine di assicurare l'economia delle forze ed un impiego razionale delle limitate risorse, fatte salve diverse direttive del Comandante superiore, il BDOC può coincidere con il *Tactical Operations Center* (TOC) dell'unità che, oltre a gestire le operazioni correnti nella TAOR assegnata, provvede anche alla gestione della difesa della base ed al controllo della TAOR stessa.

[33] L'organizzazione delineata dallo schema è da ritenersi solo una struttura di base da prendere a riferimento quale *Minimum Military Requirement*. Essa va adattata, di volta in volta, alle esigenze operative ed alle linee guida di FP dei Comandanti nelle varie TAOR dei Teatri di Operazione.

In particolare:

3.1.4.1 Assetti/sistemi per l'attività di vigilanza

Deputati al controllo ed alla reazione nelle varie AFD:

- AI, AP e WLOS: POA, pattuglie, sentinelle, postazioni difensive perimetrali e ingressi, UGV, sensori e sistemi di allarme anti intrusione e videosorveglianza a corto (TVCC), medio e lungo raggio (elettro-ottiche e radar);
- BLOS: pattuglie, *check point*, UAV, aeromobili e velivoli per ETT, sistemi di videosorveglianza a lungo raggio (elettro-ottiche e radar), sensori acustici.

3.1.4.2 Assetti per il rinforzo e pronto impiego: QRF, aeromobili e velivoli per il trasporto tattico.

3.1.4.3 Assetti specialistici: nu. radar, mortai/artiglierie, UAV, RCP, EOD/IEDD, EDD/MDD, CBRN.

3.1.4.4 Assetti per l'emergenza: PM, SAR, MEDEVAC, nuclei sanità, VF, nu. atz. sp. del genio.

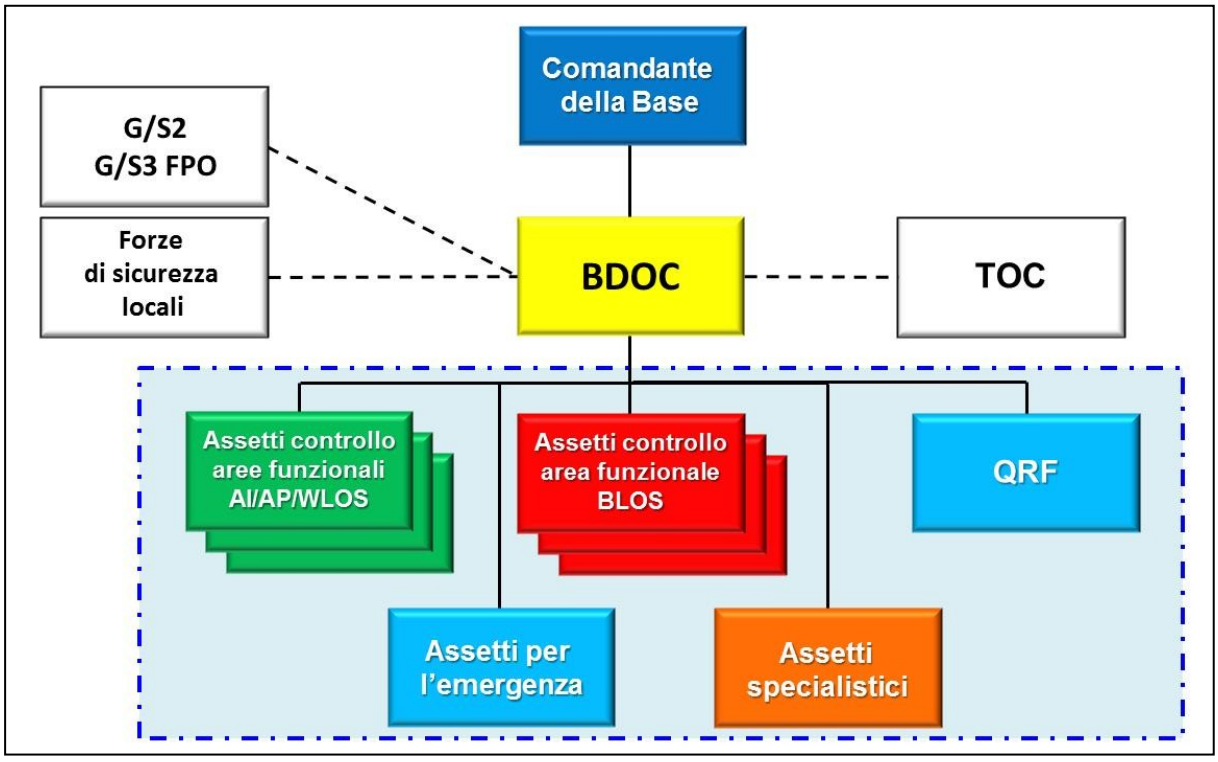


Figura 10: Organizzazione SIPROB

3.2 ESIGENZE OPERATIVE PER IL CONTROLLO E LA PROTEZIONE DI UNA BASE MILITARE

3.2.1 Esigenze di carattere generale

3.2.1.1 Scelta di un sito di adeguate dimensioni

Il sito deve assicurare:

- la possibilità di realizzare una base idonea a contenere tutte le aree funzionali previste per l'accantonamento della/e unità senza dipendere dalle risorse locali;
- le adeguate distanze di sicurezza (*stand off*) nei confronti delle minacce plausibili valutate dal S/G2;
- l'espansione in funzione delle possibili future esigenze operative;
- il diradamento dei dispositivi;
- idonei collegamenti con le LOC.

3.2.1.2 Approntamento di una difesa "concentrica" e in "profondità"

Deve consentire di realizzare:

- la più estesa sorveglianza della base, sia diretta sia con sistemi di videosorveglianza;
- l'integrazione degli assetti di FP in termini di difesa attiva, passiva e sorveglianza[34] ();
- una protezione perimetrale che impedisca l'accesso di mezzi e personale non autorizzato, inibisca l'osservazione, il tiro diretto e l'impiego degli IEDs.

3.2.1.3 Identificazione dei necessari sistemi di FP integrati

Devono assicurare, nel più breve tempo possibile, la scoperta della minaccia, l'immediata diffusione dell'allarme e l'ingaggio.

3.2.1.4 Definizione dell'organizzazione di Comando e Controllo

deve assicurare il funzionamento del SIPROB e le attività di Comando e Controllo con adeguati collegamenti.

[34] Le distanze indicate sono orientative e vanno adattate all'ambiente operativo.

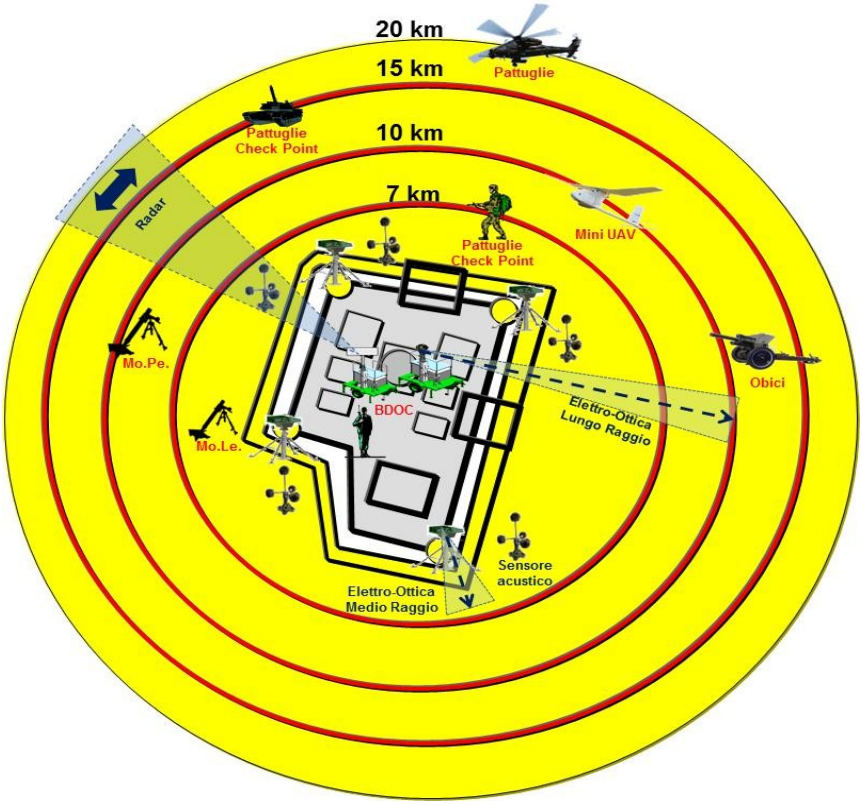


Figura 11: Schema di struttura di Difesa Integrata

3.2.1.5 Studio del perimetro della base e definizione delle migliori posizioni difensive.

Devono essere idonee per la realizzazione delle torri di osservazione idonee ad assicurare adeguati campi di vista e tiro (anche attraverso la rimozione e sgombero di ostacoli presenti) e la "saldatura" dei settori, che assicurino:

- il mutuo intervento;
- campi di tiro sovrapposti;
- sistemi per la sorveglianza a medio e lungo raggio in ogni tempo;
- sistemi di comunicazione e diffusione dell'allarme in tutta la base.

3.2.1.6 Controllo della viabilità intorno alla base e valutazione del numero e della tipologia degli ingressi da realizzare

In funzione della minaccia tenendo presente che per una base sono necessari almeno un ingresso principale ed uno secondario; qualora gli stessi non assicurino l'accesso a mezzi speciali o eccezionali dovrà essere realizzato anche un ingresso dedicato alle colonne logistiche).

3.2.1.7 Valutazione della vulnerabilità delle strutture della base

Orientata agli effetti delle minacce al fine di poter definire le più appropriate misure di protezione strutturale o, in caso di instabilità strutturale insanabile, la loro demolizione.

3.2.1.8 Definizione delle strutture per la limitazione dei danni

Effettuata sulla base della minaccia, per definire le caratteristiche dei muri anti esplosioni (*blast wall*), delle strutture di contenimento degli effetti e di rinforzo strutturale.

L'organizzazione di dettaglio del BDOC e l'impiego dei sistemi di FP sono delineate sulla Pubblicazione 6368 "Impiego dei sistemi integrati di FP per la protezione delle basi militari" (PTE 3.14.1), edizione 2014.

3.2.2 Esigenze di carattere specifico

3.2.2.1 Sicurezza Fisica

- Redazione di un piano flessibile di vigilanza e difesa della base contro le possibili minacce in modo da ridurre le possibilità di sabotaggio.
- Scelta del livello/tipologia di unità da impiegare per la vigilanza e la QRF adeguate ad intervenire contro le minacce, in aderenza ai contenuti del piano di difesa (i compiti principali devono assicurare essenzialmente: sostegno alla vigilanza in caso di emergenza, rinforzo delle attività di pattugliamento esterno, assistenza nel controllo della folla, attività di scorta convogli e VIPs).
- Definizione dei limiti ed assegnazione dei settori di difesa alle varie unità dipendenti o comunque alloggiate in maniera permanente, a qualunque titolo, nella base. Predisposizioni dell'intervento anche per eventuali unità in transito che sostano nella *staging area*.
- Adozione di adeguate procedure di controllo e registrazione del personale che accede ed esce dalla base (modalità e sistemi per la scansione e l'ispezione manuale o con cinofili ai pedoni; in particolare, per il personale femminile, religioso e VIPs).
- Adozione di adeguate procedure per il controllo e la registrazione dei veicoli che accedono ed escono dalla base (modalità e sistemi per la scansione e l'ispezione manuale o con cinofili ai veicoli ed ai conducenti).
- Applicazione di procedure, sistemi e tecniche contro il contrabbando.
- Definizione delle modalità per il pattugliamento interno ed esterno, tempistiche, rotazioni, sistemi di identificazione, modalità per la diffusione dell'allarme e per l'intervento della QRF, relative consegne da applicare, equipaggiamenti e armamento da impiegare.
- Identificazione e segnalazione delle aree con accesso classificato.
- Definizione delle misure antintrusione e di controllo dell'accesso.

3.2.2.2 *Force Protection Engineering*

- Progettazione e realizzazione delle misure di protezione passiva delle aree ad uso collettivo (mensa, PX, bar, ecc.) e di quelle critiche ai fini dell'operatività e sopravvivenza della base (Posto Comando, centro trasmissioni, deposito

munzionii, depocel, viveri ed acqua di emergenza, produzione di energia elettrica e potabilizzazione dell'acqua, ecc.).

- Identificazione delle misure per il rinforzo delle strutture e per il contenimento dei danni dovuti agli effetti della minaccia identificata.

3.2.2.3 Protezione sanitaria

- Definizione delle misure per il controllo sanitario.
- Definizione dei controlli sull'igiene dei cibi e dell'acqua.

3.2.2.4 *Consequence Management*

- Redazione dei piani di contingenza per la prevenzione e gestione delle emergenze.
- Predisposizione dei piani e delle misure per il ripristino della capacità operative post emergenza.

3.2.2.5 *Intelligence – Counter Intelligence*

- Definizione degli elementi informativi per la FP necessari ad integrare le attività di ricerca delle informazioni.
- Emanazione delle misure di coordinamento tra gli assetti Humint e la struttura di C2 della FP.

3.2.2.6 Sicurezza dell'area perimetrale

- All'esterno del perimetro:
  - focalizzazione del pattugliamento sul controllo delle LOC adiacenti alla base, per prevenire il movimento di elementi ostili e l'osservazione delle attività delle forze (sia agli ingressi che nelle aree critiche);
  - integrazione degli ordini di pattugliamento con gli obiettivi informativi necessari ad aggiornare la minaccia;
  - utilizzazione dei sistemi di rilevamento in dotazione per localizzare le aree di fuoco diretto e indiretto;
  - tendere a creare un ambiente favorevole per la forza nell'ambito della TAOR aumentando la percezione di sicurezza della popolazione degli agglomerati compresi in essa attraverso la pianificazione di attività integrative dei nuclei CIMIC e PSYOPS;
  - verifica che il personale delle pattuglie sia addestrato nell'aero-cooperazione.
- Lungo il perimetro:
  - prevenzione dell'osservazione;
  - realizzazione di ostacoli contro il movimento di veicoli esterni a ridosso del perimetro per assicurare un'idonea area di sicurezza;
  - attuazione di misure supplementari (variare le disposizione dei rallentatori e incanalatori di traffico di fronte agli ingressi e lungo le rotabili ad alto traffico,

accensione fuori routine delle luci perimetrali, variazione frequente degli orari di accesso alla base, cambio delle procedure di controllo, ecc.);

- pianificazione del C-IED;
- definizione ROE e diramazione di ordini chiari per il personale delle torri di vigilanza;
- identificazione dei settori d'intervento e dei sistemi di protezione attiva e passiva adeguati;
- variazione degli orari di cambio o del personale della vigilanza.

– All'interno del perimetro:

- definizione delle procedure e degli assetti necessari per il controllo del personale che muove all'interno della base con orari e procedure differenti;
- definizione delle procedure e degli assetti necessari per il controllo dei veicoli e del personale che accede all'infrastruttura;
- pianificazione ed effettuazione di esercitazioni contro atti di sabotaggio, tentativi di intrusione e *Mass Casualties*;
- realizzazione di un'adeguata viabilità di pattugliamento per favorire il controllo ed il rapido intervento della vigilanza o della QRF;
- definizione delle procedure per il controllo e la movimentazione dei veicoli all'interno della base e lungo il perimetro.

3.2.2.7 Addestramento del personale

Tutto il personale della vigilanza viene:

– messo a conoscenza:

- degli stati di allertamento in vigore e le relative misure da applicare;
- della minaccia corrente;
- del piano di difesa e relative misure da attuare in caso di emergenza;
- delle caratteristiche e prestazioni dei sistemi di FP installati;
- dei codici in vigore per il riconoscimento amico/nemico;
- segnali per la diffusione dell'allarme;
- tipologie dei collegamenti in vigore e relativi codici;
- caratteristiche del settore di controllo assegnato;

– addestrato:

- all'uso e manutenzione dell'arma in dotazione personale e di reparto (installato sul mezzo o sulla postazione da occupare);

- all'uso e manutenzione delle stazioni radio (portatili e veicolari) e dei CID[35] in dotazione;
- sulle procedure per diffondere l'allarme e riportare le informazioni necessarie al BDOC per pianificare e coordinare l'intervento degli altri assetti;
- a saper chiedere e coordinare l'intervento del fuoco terrestre ed aereo (in quanto sussiste la possibilità che solo il personale di vigilanza di una specifica posizione sia in condizione di poter dirigere il fuoco di supporto contro un obiettivo solo a lui visibile in quel dato momento);
- sulle tecniche e procedure per il controllo del personale e degli autoveicoli (*Person & Vehicle Search*);
- procedure per il controllo dei documenti, l'uso dei sistemi biometrici e la consegna dei passi.

3.3 PROCEDURE PER LA VERIFICA DEL SISTEMA DI PROTEZIONE DELLA BASE ADOTTATO

La verifica del SIPROB adottato, attraverso l'esame dell'impiego del BDOC, può avvenire a seguito di un evento/incidente o sulla base di controlli preventivi.

3.3.1 A seguito di evento/incidente

La revisione delle predisposizioni e procedure di FP, pianificate ed attuate attraverso lo sviluppo del ciclo delle misure di FP, è una fase fondamentale per assicurare l'adeguamento dell'organizzazione di sicurezza all'evoluzione della minaccia.

Al riguardo, il Comandante della difesa, ovvero il S/G3 FPO, in sede di FPWG, ed il Capo del BDOC provvedono a:

- esaminare l'evento in dettaglio;
- analizzare le capacità di reazione della Forza: tempistiche dei sistemi di rilevamento e sorveglianza, modalità diffusione allarme e di risposta della vigilanza, utilizzazione delle procedure standardizzate;
- aggiornare i dati inerenti la minaccia (sulla base delle informazioni ricevute dal S/G2);
- pianificare eventuali simulazioni ed esercitazioni;
- adeguare piani e SOP, emanando le necessarie disposizioni integrative.

3.3.2 Controlli preventivi

I controlli preventivi vengono invece effettuati dal Capo Centro BDOC sulla base di specifiche *check list* che sono redatte per individuare le criticità dell'organizzazione e minimizzare le vulnerabilità riscontrate.

[35] *Combat Identification Device*: sistemi per il riconoscimento di unità amiche tipo teli colorati, ecc..

Le predette *check list* possono essere anche utilizzate in sede di pianificazione per delineare, a priori, lo sviluppo delle attività da approfondire durante l'applicazione del "Ciclo delle misure di FP".

Tale *check list* (Allegato "D") si basano sul concetto di "autovalutazione", al fine di:

- fornire al Comandante della base un quadro di situazione quanto più ampio e dettagliato in merito alle criticità dell'organizzazione della difesa;
- assicurare:
  - l'individuazione delle criticità dell'organizzazione e l'analisi dei rischi in seno all'unità addetta alla difesa della base, definendo quali di queste possono essere risolte con le risorse locali a disposizione (ovvero con la predisposizione di misure integrative o di mitigazioni adottabili nell'ambito dell'organizzazione adottata);
  - la valutazione dei rischi che non possono essere gestiti dall'unità ma che necessitano del supporto del Comando superiore.

3.4 ATTIVITÀ/COMPITI CONNESSI CON LA PROTEZIONE

Al fine di assicurare una protezione delle basi militari ad ampio spettro, le seguenti misure di protezione specifiche sono state definite principalmente per contrastare una minaccia di tipo "ibrida", che prevede la presenza nel contempo sia di forze ostili regolari sia irregolari. Ai fini delle operazioni tradizionali, l'applicazione delle predette misure, principalmente orientate alle operazioni di stabilizzazione, dovrà tenere conto delle diverse esigenze operative e dei ritmi legati allo sviluppo sia della manovra terrestre sia della 3^ Dimensione. Pertanto, sarà cura dei Comandanti ai vari livelli adattare le misure di protezione di seguito illustrate allo specifico contesto operativo.

3.4.1 Difesa aerea e antimissile

La minaccia aerea e missilistica è definita come la possibilità di una forza ostile di effettuare, in Area di Operazioni, azioni offensive contro le forze amiche/ alleate, particolari Critical Vulnerabilities, i territori e la popolazione, utilizzando le diverse tipologie di vettore operanti nella terza dimensione. Tale minaccia è caratterizzata da:

- vasta tipologia ed elevato raggio d'azione;
- mobilità, furtività e rapidità d'intervento;
- accuratezza, flessibilità e persistenza,

e può essere classificata in termini di:

- piattaforme pilotate (aerei ed Elicotteri da Esplorazione e Scorta – EES - e da trasporto, ecc.);

- sistemi a pilotaggio programmato (*Drone*) e aeromobili a pilotaggio remoto (RPAS)[36];
- missili balistici a traiettoria prefissata (*Tactical Ballistic Missile* – TBM) a corta o media gittata[37], a portata intermedia[38] e intercontinentali[39], missili antiradiazione (*Anti Radiation Missile* – ARM), munizionamento stand-off[40] aria-superficie (*Air-to-Ground Missile* – AGM), guidato da vari tipi di sensori[41], 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)[42] e *balloons*;
- sistemi improvvisati, quali deltaplani, gli ultra-leggeri o gli *Small Unmanned Aerial Vehicles* (mini/micro-UAV).

L'ampia gamma di sistemi offensivi operanti nella terza dimensione determina l'esigenza di disporre di misure e mezzi di protezione adeguati.

3.4.1.1 Deterrenza

Le forme di reazione alla minaccia proveniente dalla terza dimensione comprendono predisposizioni di Autodifesa, Difesa Aerea (nazionale) e Difesa Aerea e Missilistica Integrata (NATO). In particolare:

- **Autodifesa Controaerei**

  Comprende l'insieme delle predisposizioni e azioni attuate da tutte le unità della Forza Armata per la protezione :

---

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

[37] *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.

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

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

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

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

[42] Termine coniato dall'US Army, ma d'origine britannica, ambito nel quale i LEMV vengono denominati chiamati *Hybrid Air Vehicle* (HAV).

- da attacchi diretti alle basse e bassissime quote, allo scopo di annullare la minaccia aerea, al fine di abbattere i sistemi in volo o quanto meno disturbarne l'azione e impedirne lo sviluppo della missione;
- delle basi, anche avanzate, situate nei vari teatri operativi dalla minaccia del tipo *Rockets Artillery & Mortars* (RAM)[43],

e anche al fine di ampliare l'attività informativa e di contro reazione dei Contingenti.

Ciascun Comandante è responsabile della organizzazione e condotta dell'autodifesa C/A e in base all'armamento adottato l'autodifesa è definita:

- specifica, quando condotta con armi destinate al tiro controaerei (missili terra-aria portatili, cannoni automatici, mitragliere e mitragliatrici), oppure che dispongono di congegni di puntamento caratteristici del tiro controaerei o che debbano essere integrate, come nel caso dei sistemi C-RAM, nell'organizzazione della difesa aerea;
- immediata, quando condotta mediante l'impiego a massa delle armi automatiche o semiautomatiche individuali e di reparto non specificatamente organizzate per effettuare il tiro contraerei.

- **Difesa Aerea (nazionale)**

  Consiste nella protezione degli spazi aerei nazionali ed è, come noto, di responsabilità dell'Aeronautica Militare[44]. In tale contesto, l'Esercito dispiega, tuttavia, strutture di Comando e Controllo e unità specialistiche in grado di intervenire nei diversi ambienti, integrandosi in complessi di forze (*Joint e/ o Combined*); esigenza particolarmente evidente nel segmento capacitivo della *Missile Defence* (MD) integrata nella NATO, un ambito che richiede elevata sinergia tra le varie componenti che la costituiscono.

- **Difesa Aerea e Missilistica Integrata (NATO)**

  Prevede la capacità di contrastare una minaccia di tipo aerodinamico, o balistico, diretta contro assetti geopolitici vitali e/o forze nazionali, alleate o di coalizione impiegate in un teatro operativo. Può coinvolgere basi o infrastrutture critiche di particolare rilievo. Per quanto precede, tale capacità di difesa può estendersi su un'area geografica ampia, in linea di massima maggiore del territorio di una

[43] Gli assetti C-RAM fanno parte dei sistemi di difesa aerea GBAD e, pertanto, la loro azione va integrata nell'organizzazione della Difesa Aerea.

[44] Cfr. D.P.R. 15 mar. 2010, n. 90 – "Testo Unico delle disposizioni regolamentari in materia di ordinamento militare", art. 99.

singola Nazione[45] e presupporre la disponibilità di specifiche architetture di difesa[46], nelle quali, in ambito Forze Armate, operano :

- assetti di sorveglianza, come i *radar*, e *Combat Management Systems* (CMS);
- attuatori, come i *Medium Range Surface to Air Missile* (MRSAM)[47] dell'Esercito;
- strutture di simulazione distribuita nazionale-NATO[48].
- In particolare, al fine di contrastare la minaccia militare, e non militare, portata dall'aria, l'Esercito dispiega, in tali contesti:
- strutture di Comando e Controllo;
- unità specialistiche dotate di un articolato mix di sistemi controaerei[49].

Tali sistemi di gestione e/ o di fuoco, schierati a protezione di diverse unità/ basi a grande distanza tra loro, sottostanno ad un'unica organizzazione di Comando e Controllo, grazie all'integrazione con le agenzie deputate alla gestione dello spazio aereo e sono dotati di effettive capacità di identificazione (non solo procedurale, ma anche elettronica) dei velivoli.

---

[45] La minaccia balistica può infatti derivare da missili balistici intercontinentali che, per capacità e portata, possono essere associati a veicoli di lancio spaziale, come gli *Intercontinental Ballistic Missiles* (ICBM) con gittata fino a 5500 km.

[46] In particolare, per quanto concerne la *Theatre Ballistic Missile Defence* (TBMD).

[47] La definizione MRSAM è incentrata sulla portata (*range*), mentre quella di *High Altitude Missile Air Defence* (HIMAD) sulla quota (*altitude*).

[48] Tra le quali il sito del COMACA impiegato per effettuare, tramite tecniche di *Modelling & Simulation* (M&S), analisi preventive delle capacità dei sistemi missilistici; verificare integrazione e interoperabilità tecnica/ operativa e valutarne le prestazioni; cooperare nella definizione di concetti d'operazione, dottrina e procedure, e addestrare nel *network* di difesa della NATO.

[49] Come descritto nella PIE-3.30 "Impiego dell'Artiglieria Controaerei", 2015.

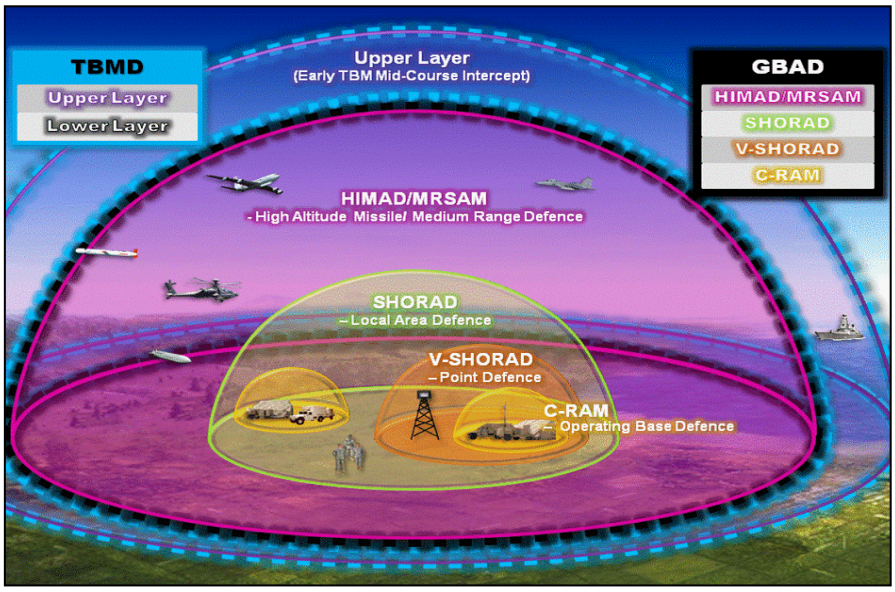


Figura 12: Schema di difesa aerea delle basi

In proposito, la dottrina della NATO[50] prende in considerazione la difesa delle basi, operata prevalentemente da sistemi V/SHORAD e C-RAM, ma integrandola in tale ampio contesto ().Il Controllo Tattico può certamente essere delegato, entro limiti di tempo e di spazio, ai Comandanti delle forze terrestri; non di meno, l'impiego della terza dimensione implica la necessità di dotazioni specifiche (radar, sistemi di comando e controllo), la correlazione con le Agenzie responsabili del controllo dello spazio aereo, e la gestione coerente di procedure (ordini di Controllo Tattico[51], misure di controllo dello spazio aereo[52]).

3.4.1.2 Prevenzione

Il Comandante terrestre, generalmente, dispone di un'organizzazione difensiva specifica, in grado di contrastare la minaccia proveniente dalla terza dimensione. Tale organizzazione garantisce anche il coordinamento della terza dimensione. Lo spazio aereo sovrastante l'Area di Operazioni viene infatti impiegato da un elevato e diversificato numero di sistemi amici, pilotati e non pilotati, che svolgono missioni di appoggio aereo, ricognizione o trasporto, ma anche dalle unità di combattimento organizzate, equipaggiate e addestrate a manovrare nella terza dimensione (come le aviotruppe e le unità aeromobili[53]), nonché dagli assetti deputati alla protezione delle basi.

---

[50] NATO. *Air and Missile Defence Capstone Document*, Sep. 2011, para. 1.2 e 1.4.

[51] Per l'esecuzione degli ingaggi e si classificano in Stati di Controllo delle Armi (*Weapons Control Status* - WCS) e Ordini di Controllo del Fuoco (*Fire Control Orders* - FCO).

[52] *Airspace Control Means* (ACM).

[53] Cfr. SME, ND *La manovra delle forze terrestri nella terza dimensione*, Ed. 2014.

L'utilizzo dello spazio aereo, anche alla basse e bassissime quote, se non adeguatamente coordinato, può condizionare sfavorevolmente la manovra terrestre e incidere negativamente sull'esito delle misure di difesa destinate non solo alla protezione delle forze amiche/ alleate, ma anche a quella di particolari infrastrutture e /o installazioni critiche (più in generale, le *Critical Vulnerability*) e anche, nel caso, della popolazione civile[54].

Di conseguenza, il Comandante terrestre, generalmente, dispone di sistemi in grado di erogare fuoco per annullare/ ridurre l'efficacia di attacchi aerei e balistici avversari, convenzionali e non, condotti alle medie, basse e bassissime quote, in ambienti operativi ad alta intensità, anche integrandosi in sistemi di difesa aerea nazionali, NATO e di teatro, al fine di garantire la difesa delle forze amiche/ alleate, e delle basi, impiegando, a tal fine, assetti idonei e appropriati.

3.4.1.3 Sicurezza attiva

L'Esercito dispiega, al fine di realizzare idonee misure di sicurezza/difesa attiva:

- assetti controaerei peculiari (radar controfuoco, sistemi di allerta, cannoncini e mitragliatrici di autodifesa) disponibili, generalmente, in esigua quantità;
- unità specialistiche dedicate che dispongono di assetti di difesa specifici, come i sistemi:
  - MRSAM;
  - SHORAD;
  - V/SHORAD;

ma anche unità C-RAM e/ o di allerta schierate a protezione di unità/ basi.

L'insieme di tali assetti esplicita, nel quadro di un agile e flessibile esercizio del C2, le capacità di combattimento necessarie per sopprimere, neutralizzare o distruggere le sorgenti di fuoco indiretto.

3.4.1.4 Difesa passiva

La minaccia militare, e non militare, portata dall'aria può essere contrastata non solo attraverso i processi di avvistamento/scoperta ma anche grazie a idonee misure di mascheramento, mimetizzazione, inganno. Tali predisposizioni impongono al nemico l'impiego di un maggior numero di assetti ISTAR per scoprire le posizioni amiche. In particolare, il proliferare di sistemi improvvisati operanti nella terza dimensione (quali deltaplani, ultra-leggeri o i micro-UAV) rappresenta una minaccia crescente, tale da imporre sempre più accurate misure di difesa controaerei passiva.

[54] Cfr. NATO, AJP 3.3.1 *Allied Joint Doctrine for Counter–Air*.

3.4.1.5 Mitigazioni

- Assicurare la disponibilità di un mix di predisposizioni di difesa attiva, difesa passiva e capacità di ingaggio nel quadro di un agile e flessibile sistema di C2;
- garantire la gestione della terza dimensione in coordinamento con le Agenzie del Comando e Controllo responsabili della gestione dello spazio aereo (*deconfliction*).

3.4.2 Recupero del personale

Insieme delle predisposizioni e misure (militari, diplomatiche e civili) atte al recupero e reintegrazione in sicurezza del personale isolato/disperso/catturato attraverso operazioni pianificate. Le operazioni di recupero si sviluppano in un quadro complesso di fattori ambientali che determinano la loro natura. Non si tratta di missioni separate ma devono essere previste all'interno della pianificazione di tutte le missioni, di qualsivoglia genere esse siano. I Comandanti dovranno pianificare tali operazioni di recupero in base alle potenzialità esprimibili, valutando la propria capacità sulla base dell'ambiente operativo, delle capacità amiche e nemiche e del fattore popolazione locale.

3.4.2.1 Deterrenza

Adeguata cornice di sicurezza durante le varie attività operative.

3.4.2.2 Prevenzione

- Conoscenza da parte di tutto il personale militare e civile delle norme di comportamento da tenere durante le varie attività, delle procedure di sicurezza durante il movimento e delle procedure per il recupero del personale isolato/disperso/catturato;
- definizione delle misure di recupero durante la pianificazione delle attività esterne.

3.4.2.3 Sicurezza attiva

Predisposizioni di adeguate misure di sicurezza durante il movimento (scorta convogli, impiego UAV, ecc.) e l'effettuazione delle attività esterne (servizio di vigilanza, *Guardian Angel*, ecc.).

3.4.2.4 Difesa passiva

- Adozione dei dispositivi di protezione per il personale ed i mezzi;
- realizzazione di opere di protezione temporanee durante lo sviluppo delle attività (apprestamenti/postazioni difensive, *check point*, muri protettivi, ecc.).

3.4.2.5 Mitigazioni

Applicazione delle previste procedure e TTPs.

3.4.3 Fuoco fratricida

Il fuoco amico, o fratricida, può essere definito come il coinvolgimento di proprio personale, mezzi o materiali in azioni di fuoco erogate da unità nazionali o della

coalizione (*Blue on Blue*) oppure ritenute amiche (*Green on Blue*). Può portare al ferimento o addirittura alla perdita di personale, mezzi o materiali, appartenenti alle unità stesse. Il fuoco amico, o fratricida, è da ritenersi accidentale e, di solito, deriva da un errore, o da una serie di errori di valutazione da parte di un comandante, del suo staff e/o di un singolo nell'ambito della redazione di specifiche SOP.

3.4.3.1 Deterrenza

Nihil.

3.4.3.2 Prevenzione

La prevenzione dal fuoco amico viene di solito conseguita attraverso un piano di protezione o prevenzione, incentrato su due aree fondamentali :

- **Piena conoscenza della situazione operativa, *Shared Situational Awarness* (SSA):** è l'immediata e aggiornata conoscenza di tutte le operazioni, condizioni ed attività che insistono nella propria area di competenza, anche da un punto di vista temporale e geografico. Include la conoscenza in *"near real-time"* della posizione, delle attività e delle intenzioni delle proprie unità, delle unità amiche, nemiche, neutrali e non combattenti che agiscono nella "*Joint Operational Area (JOA)"*, nel settore e/o nella zona di competenza, ovvero nelle loro immediate vicinanze.
- **Pianificazione, selezione e validazione degli obiettivi:** è il ciclo di selezione e validazione degli obiettivi sul campo di battaglia, siano essi amici o nemici. Il conseguimento degli effetti potrà essere ricercato solo dopo che tutti i criteri di ingaggio siano stati soddisfatti. La probabilità di fuoco fratricida può aumentare a seguito delle condizioni in atto sul campo di battaglia e del cambiamento della situazione operativa. La presenza di non combattenti nella JOA complica ancor di più il "*Battle Space Management"*. Semplicità e chiarezza sono da prediligere rispetto ad un piano complesso e dettagliato, al fine di ridurre il più possibile la possibilità di incidenti derivanti da fuoco amico.

3.4.3.3 Sicurezza attiva

Nihil.

3.4.3.4 Difesa passiva

Nihil.

3.4.3.5 Mitigazioni

Conoscenza da parte di tutto il personale delle misure di riconoscimento amico-nemico, dei codici in vigore e dell'uso dei *Combat Identification Devices* (CID)

3.4.4 Sicurezza dell'area delle operazioni della base (TAOR *Control*)

La dottrina NATO sulla Protezione delle Forze (già cit. AJP 3.14) definisce la TAOR (*Tactical Area of Responsibility*) come quell'area che viene stabilita intorno ad una base militare in operazioni al fine di prevenire, attraverso il suo controllo e dominio, gli attacchi diretti ed indiretti condotti contro le infrastrutture ed il personale. Le

dimensioni della TAOR sono generalmente sufficientemente ampie (sino a 10 km dal perimetro della base e fino anche a 15 km per i sedimi aeroportuali) per identificare la minaccia il più lontano possibile dal perimetro della base e, per i sedimi aeroportuali, poter escludere qualsiasi tipo di minaccia e di attacco contro i velivoli, siano essi parcheggiati o in volo durante le delicate fasi di decollo ed atterraggio.

Il dominio della TAOR, ovvero dell'area di operazioni assegnata ad una base, per essere efficace richiede l'applicazione di misure "stratificate" che comprendono:

- l'istituzione di posizioni di fuoco difensive da disporre quanto più vicino possibile agli assetti ed elementi critici da difendere;
- il pattugliamento interno ed esterno della Base;
- la ricognizione terrestre ed aerea (incluso l'uso di assetti ISTAR);
- la costituzione di Forze di Riserva per il Pronto Intervento;
- l'istituzione di posti di osservazione (*Observation Post* - OP) e di Fuoco di precisione anche esterni al perimetro della Base (*Close Precision Attack - Snipers*).

3.4.4.1 Deterrenza

Consiste nell'applicazione di procedure e misure di controllo delle aree visibili e non visibili della TAOR della base al fine di evidenziare alle forze potenzialmente ostili:

- uno spiccato atteggiamento proattivo e offensivo;
- un idoneo stato di prontezza;
- l'impiego di adeguate misure e capacità di controllo.

3.4.4.2 Prevenzione

Consiste nella predisposizione ed attuazione di piani:

- per la sorveglianza della TAOR che prendano in considerazione l'impiego coordinato dei sistemi:
  - integrati di FP (radar terrestri, elettro-ottiche, ecc.) idonei ad assicurare il controllo dell'area perimetrale e quella visiva dell'AOO della base,
  - ISTAR (UAV, PSS, ecc.), idonei ad assicurare il controllo di aree non visive della TAOR della base;
- di difesa che comprendano:
  - il pattugliamento ed il controllo dell'area sia interna che esterna della base, con pattuglie o posti di controllo (mobili o fissi);
  - la difesa del perimetro e degli elementi critici della base;
  - l'immediata reazione di personale in pronto impiego.

3.4.4.3 Sicurezza attiva

Consiste nella predisposizione e attuazione delle misure per prevenire e ridurre l'efficacia delle azioni ostili legate alla minaccia aerea (*Counter-Surface to Air Fire* e

Counter-Surface to Surface Fire), minaccia terrestre (tiro diretto, indiretto, IEDs, ecc.), ricognizione e osservazione, intrusione e attacco alla base.

3.4.4.4 Difesa passiva

Consiste nella realizzazione strutture di protezione per il supporto delle attività di sicurezza attiva e la salvaguardia dei sistemi di sorveglianza della base.

3.4.5 Sicurezza ed antiterrorismo

La sicurezza coincide con tutta quella serie di predisposizioni, accorgimenti, approntamenti e procedure tesi a tutelare e salvaguardare l'apparato militare, soprattutto nelle fasi più critiche della sua attività operativa (attività tattiche,, trasporti, circolazione stradale, comunicazioni, ecc.). In particolare, l'attività di sicurezza ed antiterrorismo per le basi militari, intese come ogni luogo militare o di interesse militare, tende a garantirne l'inviolabilità, o la possibilità di accesso selettivo e la salvaguardia da ogni tipo di offesa, fisica, morale o informativa. Essa riguarda la programmazione delle attività di difesa contro i tentativi di accesso non autorizzato, azioni ostili contro le infrastrutture o il personale di vigilanza da parte di elementi legati al terrorismo o alla delinquenza locale e si focalizza sul *Risk Management*, sulla pianificazione della difesa della base, integrando il piano di difesa terrestre, attività addestrative ed esercitazioni.

La pianificazione delle misure di sicurezza ed antiterrorismo prevede anche il supporto dell'intelligence per contribuire ad un'adeguata valutazione della minaccia, nonché la valutazione degli aspetti legali legati all'operazione ed agli accordi con la HN.

3.4.5.1 Deterrenza

Prevede l'integrazione delle procedure e misure di controllo agli accessi alla base con quelle antiterrorismo in modo da evidenziare verso l'esterno:

- uno spiccato atteggiamento proattivo;
- un idoneo stato di prontezza;
- l'impiego di adeguate misure di controllo.

Attraverso la percezione di efficienza e di concreta resistenza del sistema ad attacchi o attentati si può radicare negli aggressori la considerazione che la loro eventuale azione risulterà poco remunerativa, inefficace, inutile, o – addirittura – dannosa e controproducente per loro stessi.

3.4.5.2 Prevenzione

Prevede l'integrazione dei compiti assegnati alle unità e delle misure di FP con quelle sull'antiterrorismo al fine di anticipare gli eventi/incidenti, individuando la minaccia in congruo anticipo ed il più lontano possibile dalla base, sviluppare per tempo le necessarie contromisure e mitigare gli effetti di tali eventi/incidenti, condurre attività di *Incident Recovery.*

In particolare, è necessario:

- redigere un programma di misure antiterrorismo per ridurre le vulnerabilità dell'organizzazione della difesa della base;
- raccogliere, analizzare e disseminare le informazioni sull'evoluzione della minaccia;
- aggiornare la valutazione della minaccia e valutare le vulnerabilità senza soluzioni di continuità;
- pianificare le misure per l'adozione degli stati di allertamento necessari all'evoluzione della minaccia;
- predisporre il piano di difesa terrestre della base;
- stabilire le procedure per il controllo degli accessi, il rilascio dei pass e la pianificazione dei movimenti dei veicoli all'interno della base;
- stabilire le procedure per il controllo e l'autorizzazione all'accesso dei lavoratori locali, compreso il processo di verifica dei requisiti per l'assunzione;
- stabilire le procedure per il rilascio delle tessere di riconoscimento individuale;
- stabilire le procedure per le attività di controllo biometrico agli ingressi.

3.4.5.3 Sicurezza attiva

Prevede di:

- integrare le misure di controllo sia agli accessi sia all'interno della base (personale e veicoli, lavoratori locali, ecc.) e quelle di controllo dell'AOO circostante con quelle riguardanti specificatamente l'antiterrorismo;
- attuare le misure di stati di allertamento adeguati alla minaccia locale.

3.4.5.4 Difesa passiva

Consiste nell'integrare le misure di sicurezza passiva con quelle necessarie a ridurre la vulnerabilità in caso di eventi terroristici.

3.4.5.5 Mitigazioni

Consistono in misure per:

- assicurare la conoscenza del fenomeno e sviluppare programmi informativi;
- predisporre attività addestrative (formazione di base, avanzata, condotta di esercitazioni);
- formare dei Comandanti (*Key Leaders Awareness*);
- integrare ed aggiornare i piani di FP con le misure antiterrorismo in aderenza alla minaccia;
- stabilire misure di coordinamento con la HN in merito ad aspetti informativi ed alla sicurezza esterna della base.

3.4.6 Protezione e sopravvivenza

Le misure per la protezione e la sopravvivenza hanno lo scopo di assicurare:

- la protezione fisica e strutturale delle basi/installazioni/infrastrutture[55], siano esse temporanee o permanenti, riducendo l'efficacia delle azioni di forze ostili o di calamità/emergenze complesse (naturali o antropiche);
- il mantenimento della capacità operativa nonostante il verificarsi di eventi/incidenti tendenti, in maniera diretta o indiretta, a limitarla o annullarla.

In particolare, tendono a:

- impedire la distruzione, l'osservazione o il sabotaggio delle installazioni militari;
- assicurare la resistenza delle infrastrutture vitali di un'installazione;
- proteggere fisicamente il personale, i mezzi e i materiali;
- consentire lo svolgimento delle normali attività operative e logistiche al riparo dagli effetti delle armi a tiro teso e curvo e dalle esplosioni;
- contrastare l'accesso alla base da parte di elementi ostili;
- contenere o limitare i danni causati da attività operative convenzionali e non convenzionali, sviluppate da forze ostili, da calamità naturali o da errore umano;
- assicurare l'utilizzazione delle risorse necessarie ai fini della vita all'interno delle basi e la condotta delle operazioni (produzione e distribuzione di energia elettrica e di acqua, disponibilità di munizioni, carburanti, viveri, materiali ed attrezzature critiche ai fini del Comando e Controllo, attività sanitarie e CBRN).

Per tali attività, vengono considerati elementi di situazione quali:

- livelli di protezione standardizzati da adottare in funzione della minaccia[56];
- unità da ospitare e attività da svolgere all'interno dell'infrastruttura militare;
- tipologia di manufatti/materiale per realizzare le strutture di protezione e modalità per il loro reperimento (Madrepatria, *Host Nation*, libero mercato, ecc.).

Il Comandante, sulla base dei livelli di minaccia e dei possibili rischi derivanti da attacchi o azioni ostili, avvalendosi del *Force Protection Engineering Officer* (S3/G/J-Eng), definisce le priorità in termini di attività per la protezione degli assetti chiave e delle infrastrutture. Fissate tali priorità, viene avviata la fase relativa alla quantificazione ed alla progettazione delle strutture di protezione fisica, in relazione a specifici *standards* e al processo di FP *Engineering* delineato nella già cit. PID-O 3.14[57].

---

[55] Cfr. già cit. PID-O 3.14, Cap. II, para 3.c.

[56] Cfr. NATO, STANAG 2280 MC LSB MILENG WG *Design threat levels and handover procedures for temporary protective structures*, Ed. 2 del 2015. La pubblicazione continene la definizione, la realizzazione e l'applicazione delle misure e delle opere di protezione (che prendendo a base diverse tipologie di minacce, fornisce indicazioni per il calcolo e la realizzazione delle misure di *Force Protection*).

[57] Realizzazione delle opere di protezione (Annesso 2, paragrafo 6).

3.4.6.1 Deterrenza

Prevede la:

- realizzazione di barriere (in termini di controlli successivi e recinzioni composte da diversi elementi quali area perimetrale di sicurezza, fossato antiveicolo, muri perimetrali) e postazioni difensive;
- disponibilità di adeguati mezzi e sistemi in dotazione alla vigilanza che ne assicurino la protezione e la capacità d'intervento;
- predisposizione di misure di controllo che evitano attività di controllo consuetudinarie.

3.4.6.2 Prevenzione

Prevede la disponibilità di sistemi di sorveglianza a lungo raggio (radar ed elettro-ottiche, UAV, PSS, ecc.), sensori perimetrali e sistemi per la diffusione dell'allarme.

Consiste nell'attuazione di:

- attività permanente di analisi e scambio informativo sulla minaccia locale;
- misure protettive individuali;
- attività di contro sorveglianza: mascheramento e inganno.

3.4.6.3 Sicurezza attiva

Prevede la disponibilità di personale per la vigilanza (pattuglie, sentinelle, addetto ai controlli nei vari ingressi, QRF) addestrato all'uso delle armi e dei sistemi in dotazione, all'applicazione delle procedure per il controllo, alle reazioni automatiche immediate (appiedate ed a bordo dei mezzi), all'applicazione delle procedure per il riconoscimento di personale amico e di diramazione dell'allarme, informato sulle PTT dell'avversario.

Consiste nell'attuazione di:

- Effettuazione di attività di controllo delle aree esterne ed interne legate a specifiche PTT;
- misure di sicurezza predisposte dalla HN coordinate con la FP.

3.4.6.4 Difesa passiva

- **Scelta di adeguate aree di sedime:**
  - in località baricentrica all'AOO assegnata (supporto più aderente alle operazioni) e non soggetta ad eventi naturali (terremoti, frane, alluvioni, ecc.);
  - in posizione dominante (ampi campi di vista e tiro) e ventilata (evitare ristagni di acque meteoriche);
  - con strade di accesso preesistenti già utilizzabili o di facile ripristino;
  - con infrastrutture utilizzabili attraverso lavori rapidi e di modesta entità;

- preferibilmente dotate di strutture che diano la possibilità di avere appoggio reciproco tra i vari fabbricati e disponibilità di postazioni di tiro alternative in caso di difesa della base.

– **Adeguata organizzazione funzionale delle basi:**
  - progettazione della zonizzazione aderente a supportare le operazioni ed al livello di minaccia (diradamento);
  - adeguata dislocazione degli elementi critici della base (diradamento delle scorte, dislocazione in più punti delle stazioni di energia, stoccaggi differenziati di carburante e munizioni, ecc.);
  - definizione delle misure di igiene campale.

– **Realizzazione di strutture di protezione fisica quali:**
  - barriere (recinzioni e ingressi);
  - postazioni difensive;
  - compartimentazioni di aree esterne (aree alloggiative, Area Cdo, ecc.) o all'interno di infrastrutture (locali mense, negozi, bar, ecc.);
  - barriere protettive perimetrali (per la protezione degli elementi critici della base quali PC, depocel, depomuni, stazioni di energia, viveri emergenza, acqua, ecc.);
  - ricoveri collettivi (bunkers) adiacenti ai luoghi di lavoro ed ad alta densità di affollamento.

3.4.6.5 Mitigazioni

– **Strutture protettive,** che siano:
  - funzionali all'organizzazione di difesa e relative procedure attuative (una struttura deve supportare lo sviluppo di un'azione e non esserne di impedimento);
  - realizzate inizialmente con caratteristiche di tipo campale (materiale di rafforzamento e del genio previsto in sede di pianificazione), con materiali di adeguate caratteristiche e specifiche tecniche (resistenza, durabilità, antincendio, ecc.);
  - definite mediante l'analisi preliminare:
    - della situazione operativa;
    - della tipologia delle forze e del relativo compito assegnato;
    - dell'organizzazione funzionale dell'infrastruttura;
    - degli *standard* e normative tecniche in vigore, laddove possano essere applicate;
    - della morfologia del terreno (che può vincolare in tutto o in parte la scelta delle tipologie costruttive e delle caratteristiche delle protezioni);

- delle condimeteo locali.

- **Predisposizioni per l'emergenza sanitaria e CBRN** (aree sicure per l'attività di *Mass Casualities,* dislocazione di materiale sanitario in più punti della base, aree e sistemi di decontaminazione):
  - predisposizioni per il ripristino della capacità operativa a seguito di evento/incidente[58];
  - predisposizioni antincendio.

3.4.7 Protezione sanitaria

Le misure di protezione sanitaria in ambito Nazionale ed Internazionale rivestono un ruolo fondamentale nel ridurre la vulnerabilità delle forze schierate nei confronti di minacce e rischi sanitari dovuti sia ai diversificati ambienti nella quale si va ad operare sia alle condizioni ambientali ostili.

Le misure di protezione hanno lo scopo di assicurare:

- preparazione sanitaria, pre-impiego e valutazione medica di base;
- funzioni di supporto all'impiego rapido del personale sanitario;
- monitoraggio sanitario dopo l'impiego;
- sorveglianza degli stati morbosi e report dei feriti;
- Pianificazione delle *Mass Casualties* e piano di intervento
- risposta alle minacce sanitarie in ambiente CBRN;
- igiene alimentare e controllo delle acque;
- medicina veterinaria, compreso il monitoraggio delle zoonosi trasmissibili.

3.4.7.1 Deterrenza

- Informazione ed educazione sanitaria del personale;
- conoscenza della situazione epidemiologica dell'aerea di operazioni;
- conoscenza delle patologie connesse al territorio nel quale si opera, compresa la conoscenza delle zoonosi trasmissibili;
- conoscenza delle norme generali di igiene sanitaria individuale e collettiva.

3.4.7.2 Prevenzione

- Attuazione dei protocolli vaccinali redatti in base alle aree geografiche di interesse (al fine di prevenire l'insorgenza di patologie connesse all'impiego in zona di operazioni e/o ridurre la possibile insorgenza delle stesse;
- integrazione dei succitati protocolli in base all'area geografica ed al periodo

[58] Ridondanze di materiali e sistemi per attività di C2 e sorveglianza, QRF, materiali di riserva per le attività di FP, intervento di unità del genio/ditte civili per la ricostruzione di strutture danneggiate (ingressi, recinzioni, posizioni difensive, ecc.).

stagionale di interesse, con misure profilattiche e vaccinali mirate al ridurre l'insorgenza di patologie presenti solo in determinati periodi dell'anno;

- esecuzione di tutte le norme igieniche fondamentali in ambienti dove vi è una precarietà di condizioni igienico/sanitarie per ridurre l'insorgenza di patologie legate all'ambiente circostante.

3.4.7.3 Sicurezza attiva

- Disponibilità di personale sanitario adeguatamente formato per le esigenze del teatro di operazioni. Nella fattispecie particolare attenzione riveste il personale formato in ambito traumatologia di guerra e nel trattamento delle emergenze da utilizzare in determinati contesti operativi;
- disponibilità di mezzi idonei a svolgere il soccorso adeguati all'area di operazioni e nel più breve tempo possibile;
- disponibilità di materiali sanitari, presidi, dispositivi e tutto quanto necessario per intervenire sui possibili incidenti in operazioni: incidenti stradali, ferite d'arma da fuoco, esplosioni di IED, ma anche contromisure sanitarie per morsi di serpenti, scorpioni e ragni, ecc.;
- disponibilità immediata di trauma kit al seguito di unità e di personale formato nell'autosoccorso e nel primo soccorso.

3.4.7.4 Difesa passiva

- Utilizzo dei Dispositivi di Protezione individuale atti a ridurre i rischi di contatto e di contagio per patologie trasmissibili;
- sorveglianza sanitaria dell'acqua e degli alimenti;
- utilizzo di sistemi idonei per l'allontanamento di insetti ed artropodi, possibili mezzi di contagio di patologie altamente contagiose, compreso misure di bonifica e sanificazione, nonché l'utilizzo di dispositivi idonei all'isolamento del personale.

3.4.7.5 Mitigazioni

- Predisposizioni per l'emergenza sanitaria e CBRN, con particolare attenzione alla gestione delle aree di accesso alle strutture sanitarie e di bonifica;
- trattamento sanitario specializzato atto a:
  - limitare il numero di ulteriori vittime con cure tempestive (morti precoci);
  - ottimizzare il trattamento e la degenza dei pazienti per ridurre i tempi di recupero e/o l'insorgenze delle così dette "morti tardive";
  - ottimizzare i piani di gestione sanitaria dei pazienti, logistica e comunicazioni;
  - ripristinare le capacità operative del personale dopo un evento/incidente anche nella componente psico-fisica (*Combat-Stress , Post Traumatic Stress Disorder*).

3.4.8 Protezione CBRN

Per protezione CBRN s'intende il complesso di 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 operazioni condotte in presenza di pericoli CBRN, determinano l'adozione di misure di protezione che limitano la libertà di movimento nell'area di operazione con riduzione della capacità operativa e conseguente impatto negativo sulle operazioni.

Le misure di protezione CBRN si distinguono in:

- **Protezione individuale**: viene assicurata con l'equipaggiamento di protezione in distribuzione individuale a tutto il personale (maschera, filtro, indumento protettivo, cartine rivelatrici, dosimetro individuale, corredo per l'autosoccorso e polveri decontaminanti). In caso di presenza di sostanze di origine industriale la dotazione potrebbe non essere sufficientemente idonea a garantire la permanenza se non integrata da disponibilità di filtri/indumenti di uso industriale precedentemente individuati in sede di valutazione della minaccia. In particolare, l'indossamento prolungato[59] dei dispositivi di protezione, comporta uno stress psicofisico tendente a ridurre le capacità operative del personale, in relazione anche al carico di lavoro e alle condizioni ambientali, che obbliga i comandanti a stabilire opportuni cicli di lavoro, disponendo opportuni periodi di svestizione, riposo e reidratazione, all'interno di predisposte strutture di protezione collettiva.
- **Protezione collettiva (COLPRO):** essenziale per la condotta di operazioni che richiedono una lunga permanenza in aree contaminate è assicurata per permettere:
  - la permanenza all'interno di strutture dedicate a funzioni peculiari come quelle sanitarie (posti di medicazione, ospedali ecc.), Posti Comando di G.U., strutture logistiche e di mantenimento, fondamentali per il supporto operativo alle unità (officine, posti manutenzione ecc.) o ad assetti specialistici dell'unità NBC, preposti alla decontaminazione approfondita per usufruire dei necessari turni di riposo;
  - la rimozione a tutto il personale dei dispositivi di protezione individuale per consentire il riposo e il recupero delle condizioni fisiche in ambiente protetto.

  I sistemi COLPRO, secondo il tipo di struttura e dispiegamento, si distinguono in:
  - fisso, ovvero integrale ad infrastrutture preesistenti;
  - mobile, generalmente tipico di mezzi terrestri, navali, aerei, ecc.;

---

[59] NATO, STANAG 2499 - ATP-65(B) *The effect of wearing CBRN individual protective equipment on individual and unit performance during military operations*, Ed. 2013.

- trasportabile, generalmente disponibile per il dispiegamento in previsione dell'occorrenza nell'area di operazioni. Normalmente non offrono una protezione balistica, tuttavia possono essere posti all'interno di strutture in grado di garantirla (shelters, tende).

In fase di individuazione del sistema più idoneo da schierare, si dovrà tenere conto sia dei principi che delle procedure d'impiego[60].

I comandi delle forze di manovra che normalmente utilizzano i sistemi COLPRO in dotazione possono, per motivi di contingenza, essere supportati dal rgt. difesa NBC che fornisce le strutture e il personale necessario.

Pertanto, idonee procedure operative dovranno essere redatte e ogni sistema COLPRO sarà gestito da un *team* di personale misto, tratto da unità specialistiche CBRN e da altre unità dipendenti per il supporto logistico (non specialistiche). Il controllo operativo (OPCON) sarà di norma dell'unità alla quale il COLPRO è asservito, ma in ogni caso, dovrà essere assicurato il collegamento con il centro di difesa CBRN, per l'attività di consulenza e supporto tecnico.

- **Protezione equipaggiamento e materiali:** consente di evitare il contatto diretto con gli agenti CBRN. In particolare, può essere realizzata utilizzando strutture in muratura mantenendo porte e finestre chiuse e/o coprendo i materiali con teli resistenti alla penetrazione di sostanze pericolose (*Cover Material Chemical Proof*).

  I veicoli dovranno stazionare sotto tettoie e ripari oppure, se in aree boschive, sotto alberi. In caso di eventuale attacco nucleare, deve essere previsto l'interramento, la copertura e l'ancoraggio dei materiali anche con mezzi di circostanza.

  Infine, si dovrà ridurre al minimo la penetrazione degli impulsi elettromagnetici nucleari (*Electromagnetic Pulse* - EMP) e l'effetto transitorio delle radiazioni nella strumentazione elettronica (*Transient Radiation Effects on Electronics* - TREE) e la strumentazione non in uso dovrà essere spenta, disconnessa e adeguatamente riposta.

3.4.8.1 Deterrenza

- Disponibilità di mezzi e materiali atti all'individuazione, identificazione e monitoraggio della contaminazione CBRN;
- capacità di decontaminazione, fino al livello operativo, esprimibile direttamente dall'unità interessata e rivolta a personale, mezzi e materiali;
- disponibilità di assetti dell'unita specialistica CBRN (responsabile nell'AOO) per lo

[60] NATO, STANAG 2515 - ATP-70 *Collective protection in a chemical, biological, radiological and nuclear environment (CBRN- COLPRO)*, Ed. 2014.

svolgimento di decontaminazione a livello approfondito;

- capacità di campionamento periodico/aperiodico all'interno del sedime della base a cura dell'assetto specialistico CBRN.

3.4.8.2 Prevenzione

- Disponibilità di sistemi di rilevamento a lungo raggio (stand off di tipo "fisso" oppure a bordo di automezzi), monitoraggio perimetrale con remote detectors in collegamento diretto con un sistema di CBRN *Warning and Reporting*;
- disponibilità di dispositivi di protezione individuale per tutto il personale della base in aggiunta a quelli già in distribuzione;
- disponibilità di sistemi di protezione collettiva (COLPRO) di natura adeguata alla tipologia di base.

3.4.8.3 Sicurezza attiva

- Impiego dei veicoli blindati da ricognizione CBRN (VBR NBC PLUS) per l'effettuazione delle specifiche attività previste di individuazione, identificazione e monitoraggio sia all'interno che nelle aree esterne e perimetrali;
- Effettuazione di attività di campionamento CBRN con cadenza periodica o al bisogno con lo scopo di verificare ed eventualmente confermare, se precedentemente rilevata dai strumenti di individuazione, la presenza di contaminazione CBRN.

3.4.8.4 Difesa passiva

La scelta del sedime deve tenere in considerazione alcune variabili che concorrono a minimizzare i tempi necessari all'attuazione delle misure difensive in caso di contaminazione CBRN come di seguito riportato:

- disponibilità di risorse idriche che garantiscano la fruibilità di acqua necessaria all'effettuazione delle attività di decontaminazione in sito;
- adeguata distanza da eventuali industrie presenti in loco al fine di ridurre i rischi derivanti da eventuali TIM;
- adeguato posizionamento della base in relazione a:
  - morfologia/orografia del territorio al fine di evitare l'amplificazione degli effetti derivanti da contaminazione CBRN (come ad esempio avvallamenti che favoriscono la permanenza di aggressivi chimici di tipo persistente);
  - situazione dei venti dominanti con lo scopo di evitare le zone che risultino sottovento rispetto ai potenziali rilasci TIM o alle aree ritenute più idonee per un incidente di tipo CBRN.

3.4.8.5 Mitigazioni

A seguito di contaminazione CBRN le azioni immediate volte alla mitigazione degli effetti da essa derivanti vedono prioritariamente:

- l'adozione immediata di sistemi di protezione individuale che possono poi essere

sostituiti/integrati, per il personale che debba operare in posti comando, da sistemi di protezione collettiva;

- l'identificazione dell'agente contaminante, in termini qualitativi e quantitativi, al fine di definirne la natura e stabilire l'adeguatezza della protezione adottata, nonché l'individuazione delle misure di decontaminazione più efficaci;
- la decontaminazione da effettuarsi quanto prima su personale, mezzi e materiali volta a ridurre/contenere il livello di contaminazione, nonché la contestuale gestione dei residui derivati dalla predetta attività.

3.4.9 *Operations Security* (OPSEC)

L'*Operation Security* è vitale per proteggere le informazioni. Si sviluppa attraverso un processo analitico di natura ciclica denominato Ciclo OPSEC, necessario per:

- identificare gli elementi essenziali dell'organizzazione delle informazioni amiche e le attività da svolgere per garantire la Sicurezza delle Operazioni;
- impedire che le forze ostili possano acquisire le informazioni amiche e ritardare, prevenire o annullare le attività pianificate dal Comandante di una base.

In tale processo si confrontano la minaccia e le proprie vulnerabilità con le esigenze di sicurezza del dispositivo amico, al fine di giungere ad un Piano ovvero a delle Direttive OPSEC.

L'OPSEC coinvolge un gran numero di personale (Comandanti, *staff* e specialisti) e di unità (da combattimento, per il supporto al combattimento e logistiche), esercitando un ruolo preminente nell'ambito della Protezione delle Forze sia nella fase di pianificazione sia in quella condotta, individuando e implementando le misure necessarie ad assicurare la sicurezza delle operazioni, attraverso l'attività dell'intelligence, della polizia militare, degli specialisti del genio, delle comunicazioni e della guerra elettronica.

3.4.9.1 Deterrenza

Applicare adeguate misure di controllo delle informazioni in modo da evidenziare all'esterno un elevato e capillare livello di controllo delle stesse.

3.4.9.2 Prevenzione

Identificare le possibili attività di osservazione delle forze ostili (intelligence) e definire le contromisure da adottare per evitare che le stesse possano identificare le seguenti vulnerabilità:

- malfunzionamenti e aree buie nel sistema di controllo perimetrale;
- malfunzionamenti nei cancelli/sbarre dei vari ingressi della base;
- riduzione delle forze addette alla vigilanza;
- vulnerabilità nel sistema di comunicazioni (BDOC-vigilanza, BDOC-TOC);
- vulnerabilità nelle procedure e attività di controllo agli accessi;

- analizzare il sistema di intelligence delle forze ostili e le procedure per la raccolta delle informazioni amiche e definire le contromisure da adottare;
- identificare i rischi e gli aspetti di criticità legati agli elementi essenziali informativi delle operazioni amiche (*Essential Elements Friendly Information* - EEFI) che non devono essere conosciuti dalle forze ostili;
- predisporre le procedure e le misure di sicurezza per il controllo riguardo al personale, alla documentazione (sia classificata che non classificata), ai sistemi ADP e di polizia militare.

3.4.9.3 Sicurezza attiva

Applicazione delle misure di protezione di natura offensiva come il piano d'inganno, il controllo dello spettro elettromagnetico e relative contromisure elettroniche.

3.4.9.4 Difesa passiva

- Definire le misure di protezione fisica per le comunicazioni e per la custodia della documentazione;
- definire le misure di natura difensiva per il personale, le informazioni e l'organizzazione OPSEC.

3.4.9.5 Mitigazioni

Redigere il piano OPSEC e relative SOP al fine di definire ed applicare le misure che possono ridurre o rendere accettabile le vulnerabilità delle attività amiche alla valutazione delle forze ostili.

3.4.10 EOD

Le attività EOD possono essere condotte a favore di installazioni permanenti o semipermanenti, operative o logistiche, porti e aeroporti compresi. Le considerazioni sulle contromisure EOD da applicare per tali installazioni includono:

- misure per la protezione e la sopravvivenza di cui l'installazione è dotata;
- valutazione della minaccia, tipi di EO, effetti e potenziali conseguenze;
- situazione geografica;
- priorità per le OPFOR dell'installazione quale eventuale obiettivo di alto valore.

3.4.10.1 Deterrenza

Applicare adeguate misure organizzative EOD in modo da evidenziare all'esterno un elevata capacità di controllo e di intervento per dissuadere eventuali azioni con l'impiego di esplosivi.

In caso di intervento EOD all'interno e all'esterno dell'installazione, il principale fattore di deterrenza è rappresentato dalle distanze di separazione che le installazioni devono rispettare. Queste, stimate sulla base del peggior evento esplosivo presumibile, insieme alle protezioni disponibili forniscono ai nuclei EOD le condizioni di sicurezza iniziali per mitigare conseguenze non accettabili in caso di fallimento.

3.4.10.2 Prevenzione

Le principali misure di prevenzione sono rappresentate da:

- livello di prontezza e indottrinamento dei nuclei EOD e dei nuclei di pronto intervento o dei supporti;
- necessario addestramento specifico;
- informazione, comunicazioni di tutto il personale che utilizza l'installazione sui rischi di esplosione per fuoco indiretto, mine e UXO rinvenuti e da propagazione degli effetti esplosivi;
- esercitazioni sistematiche su specifiche emergenze.

3.4.10.3 Sicurezza attiva

Per gli EOD la sicurezza attiva si esplica tramite una condotta dell'intervento rispettosa delle procedure previste e tramite un robusto coordinamento con gli altri nuclei di pronto intervento nella gestione delle conseguenze in caso di fallimento totale o parziale.

3.4.10.4 Difesa passiva

Le distanze di separazione, le strutture di protezione e le misure di controllo relative a siti interni pericolosi (riservette, POL, ecc.) che possano partecipare agli effetti esplosivi, rappresentano le principali misure di sicurezza passiva da considerare.

3.4.10.5 Mitigazioni

Le considerazioni sulle mitigazioni possono fondarsi su:

- esistenza di procedure coordinate di gestione del rischio esplosivo relative all'installazione;
- quantità dei nuclei EOD disponibili, loro prontezza operativa ed equipaggiamento disponibile;
- misure di controllo tecniche disponibili a elevata tecnologia;
- risorse ulteriori di pronto intervento;
- distanze e mezzi di proiezione dei nuclei EOD e supporto di fuoco;
- robusto sistema di comando, controllo e comunicazioni in cui i nuclei EOD siano compresi;
- continuo aggiornamento sulla minaccia;
- considerazioni su installazioni particolari (centrali energetiche, depositi munizioni, ecc.).

ALLEGATI

PAGINA INTENZIONALMENTE BIANCA

APPROCCIO SISTEMATICO FP PER LA PROTEZIONE DI UNA BASE MILITARE IN OPERAZIONI

1.1 CARATTERISTICHE

L'approccio sistematico per la FP, da prendere in considerazione per lo sviluppo di un piano di difesa, tiene conto delle seguenti esigenze operative:

1.1.1 Controllare l'AOO

La minaccia di azioni ostili contro una base impone la necessità di stabilire un'area di operazioni (AOO) intorno ad essa allo scopo di prevenire attacchi diretti ed indiretti, convenzionali e non, alle infrastrutture o alle unità ivi accantonate. La dimensione di tale area di operazioni dipende dalla minaccia e dal territorio circostante e delle relative aree che potrebbero essere utilizzate per la preparazione di atti ostili, nonché dalle esigenze di difesa di una base.

L'AOO viene posta sotto il controllo di un unico Comandante, che stabilisce le misure di FP, i compiti e le attività che devono essere attuate per prevenire minacce e rischi ed assicurare un ambiente operativo sicuro per lo svolgimento della missione assegnata. Tale figura, come indicato sul capitolo II, è denominata "Ufficiale addetto alla sicurezza della base" (da non confondere con il FP *Officer*) e può essere ricoperta direttamente dal Comandante della base o da un Ufficiale con specifica delega. Il controllo dell'AOO include le seguenti capacità al fine di assicurare la libertà di movimento, intervento e manovra delle forze amiche ed ostacolare o annullare quella delle forze ostili:

- sorveglianza permanente a lungo raggio;
- difesa e reazione contro il tiro diretto, indiretto (C-RAM);e attacchi non convenzionali (RCIED, SVBIED, attacchi complessi, ecc.);
- C-IED (specie lungo le LOC);
- difesa aerea;
- C-Intelligence;
- attività contro le ricognizioni;
- anti intrusione e difesa perimetrale;
- direzione e controllo della difesa accentrato.

1.1.2 Prevenire un attacco

- Impedire alle forze ostili l'opportunità di condurre ricognizioni intese a ricercare informazioni ed acquisire obiettivi attraverso un'azione di controllo concentrica ed in profondità che utilizzi pattuglie, sistemi di sorveglianza remoti, attività di Intelligence e C-Intelligence;
- ostacolare l'esecuzione di azioni ostili attraverso la predisposizione di adeguate misure di difesa attiva e passiva attivando pattuglie e sistemi di controllo intorno alle possibili postazioni di mortai, posizioni per tiratori o vie di fuga, ecc.

1.1.3 Ridurre gli effetti di un attacco (se la prevenzione fallisce)

- Effettuare la scoperta della minaccia in tempo utile per annullare l'azione ostile o limitare i possibili danni, impiegando sistemi di sorveglianza a medio e lungo raggio, sensori, barriere, ecc.;
- provvedere alla difesa in modo da realizzare una maglia di settori sovrapposti che possano assicurare il mutuo intervento con le armi in dotazione;
- ritardare l'azione delle forze ostili con ostacoli e/o barriere coperte dal fuoco delle armi in modo da fornire alla difesa il tempo per poter intervenire, mantenere/ripristinare l'iniziativa ed attuare una risposta coordinata;
- costituire assetti di vigilanza, appiedati e/o motorizzati, per un intervento cadenzato sulla base dell'esigenza operativa del BDOC (*Base Defense Operations Center*) quali: *Immediate Response Team* (IRT); back up a 5', 10', 15' o 30'; QRF. Tali assetti sono localizzati in posizione baricentrica per poter intervenire in tempi brevi lungo tutto il perimetro;
- realizzare un sistema di difesa concentrico e sviluppato in profondità e suddividendo l'AOO in diverse sub aree di intervento; in ciascuna di esse devono essere definiti assetti, sistemi e misure per l'intervento[1]
- utilizzare tecniche per il mascheramento e l'inganno per annullare/limitare l'osservazione delle forze ostili o focalizzare la loro attenzione su elementi non critici.

1.1.4 Aumentare la resistenza degli obiettivi

- Assicurare il mantenimento della capacità operativa;
- aumentare il livello di resistenza della difesa alle azioni ostili con l'adozione di strutture protettive di supporto ad elevato potere impeditivo intrinseco, ridondanza nelle comunicazioni, dispersione delle risorse, materiale di riserva prontamente disponibile;
- ridurre il tempo per ripristinare la piena capacità operativa dopo un evento;
- adottare misure preventive e post evento (laddove risulti possibile):
  - dispersione degli assetti;
  - duplicazione di infrastrutture di supporto logistico;
  - predisposizione di vie di evacuazione diversificate, aree protette, ingressi alternativi;
  - definizione di misure di supporto con altre basi;
  - definizione di attività MEDEVAC, SAR e relative procedure.

[1] Vds. Capitolo III

1.2 APPROCCIO SISTEMATICO PER LA PROTEZIONE DI UNA BASE

Analogamente allo sviluppo del ciclo delle misure di FP, al fine di rendere l'organizzazione della protezione di una base flessibile ed adeguata alla minaccia individuata, l'approccio sistematico si riferisce a due macro aree di minaccia:

- "calamita naturali/emergenze complesse";
- "forze ostili".

In **Appendice 1** e **Appendice 2** sono riportate le schede riguardanti lo sviluppo dell'approccio sistematico FP per entrambe tali macro aree.

PAGINA INTENZIONALMENTE BIANCA

APPROCCIO SISTEMATICO PER LA FP IN CASO DI MINACCIA DI FORZE OSTILI

Criticità iniziali nell'organizzazione della Fp della base

Capacità forze ostili, TTPs, azioni nel passato, possibili obiettivi ed aree di preparazione/supporto nell'AOO della base

- Caratteristiche degli elementi critici della base
- Criticità nella difesa attiva e passiva

- Analisi dei rischi specifici e loro accadibilità
- Effetti dei rischi residui sulla capacità operativa della base

- Organizzazione antincendio, CBRN and protezione ambientale e relative misure e procedure
- Organizzazione per la gestione delle emergenze (consequence management)
- Organizzazione degli accessi e procedure di controllo

- organizzazione C2 della FP, sistema di sicurezza da attuare, comunicazioni e sistema di notificazione di massa
- Assetti per la difesa, compiti, procedure per l'attivazione e l'intervento, misure di coordinamento
- Sistemi integrati di FP (posizionamento, settori e lineamenti per l'impiego)

PAGINA INTENZIONALMENTE BIANCA

APPROCCIO SISTEMATICO PER LA FP IN CASO DI CALAMITÀ NATURALI O EMERGENZE COMPLESSE

- Organizzazione antincendio, CBRN and protezione ambientale e relative misure e procedure
- Organizzazione per la gestione delle emergenze (consequence management)
- Misure di coordinamento dell'intervento con la HN
- Integrazione della pianificazione dell'intervento per l'emergenza con quella civile
- Assetti, compiti e procedure per l'intervento e relative misure di coordinamento
- Misure per la messa in sicurezza delle aree dell'intervento e delle LOC
- Predisposizione dei materiali per l'emergenza

PAGINA INTENZIONALMENTE BIANCA

APPLICAZIONE DEL CICLO DELLE MISURE DI FP AI FINI DELLA PROTEZIONE DELLE BASI MILITARI

L'ampio spettro di rischi e di minacce dei moderni Teatri di Operazione impone agli specialisti della FP[1] un'analisi della situazione operativa quanto più particolareggiata per poter assicurare la sicurezza delle basi militari nei Te. Op..

A tal fine, lo sviluppo del ciclo delle misure di FP[2] viene attuato secondo un esame comparato dei rischi e delle minacce che possono essere raggruppati in due macro aree di analisi:

- minacce dovute alle azioni di forze ostili;
- rischi occorrenti da calamità ed emergenze complesse.

Il ciclo delle misure di FP (Figura B 1) è lo sviluppo di un'attività ciclica di processi di pianificazione secondo una sequenza temporale ben definita, sviluppata e incentrata sulla valutazione delle criticità, delle vulnerabilità e dei rischi ad esse connessi (Capitolo I).

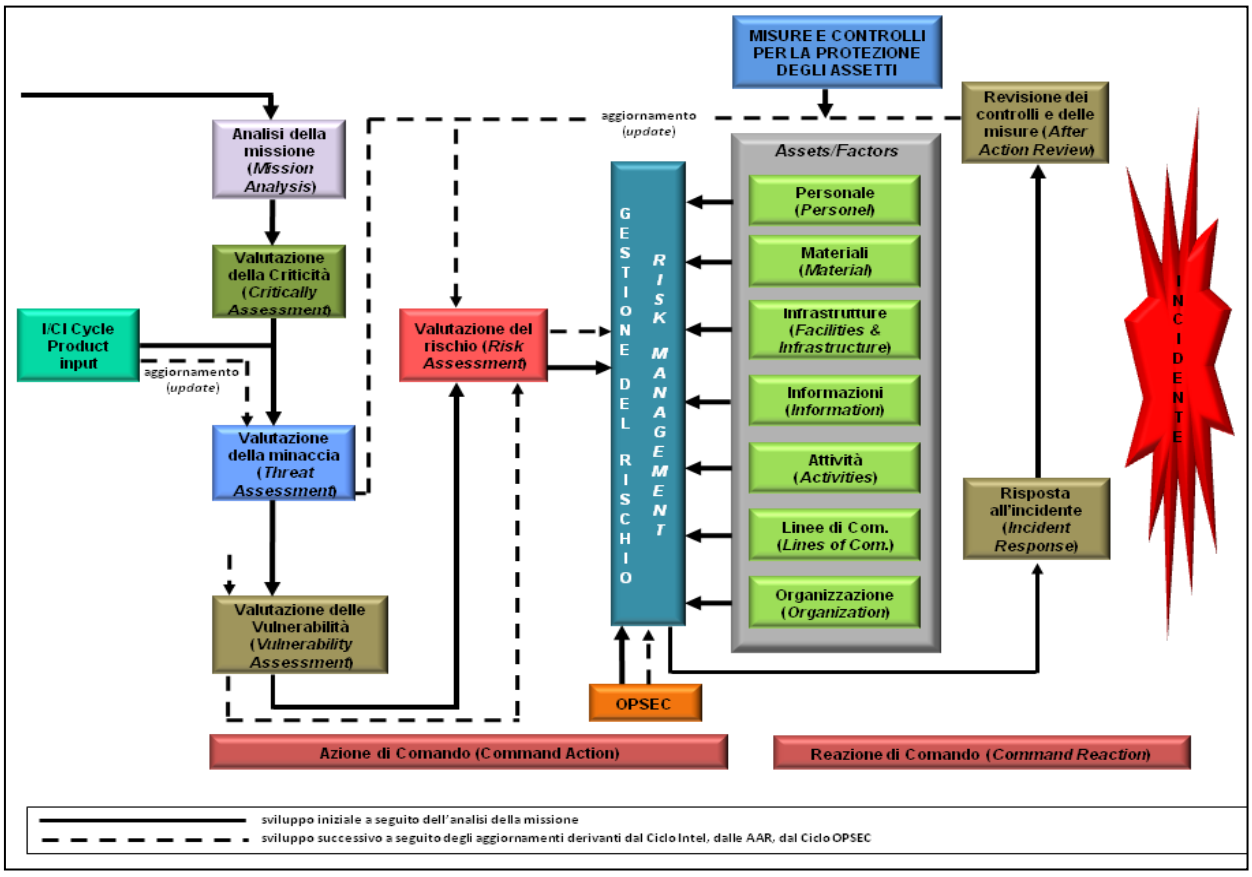


Figura B 1: Ciclo delle misure FP

1 *FP Officer, FP Engineering Officer, FP Working Group.*
2 Capitolo II, Paragrafo2.

L'attività è incentrata sull'esame del rischio residuo[3], cioè quello che non è possibile eliminare nonostante tutte le misure di riduzione applicabili pianificate.

Nell'applicazione del ciclo delle misure di FP alla protezione di ciascuna base militare nel Te. Op., lo Staff dell'unità che gestisce la base sviluppa le varie fasi del ciclo:

- **Analisi della missione (*Mission Analysis*)**
  - Effettuata attraverso l'esame dei seguenti fattori:
  - scopo della missione, compiti assegnati (espliciti e impliciti) e intento del Comandante;
  - tipologia di ambiente operativo;
  - organizzazione funzionale della base e esigenze operative, logistiche e di accantonamento della/e unità ivi alloggiata/e;
  - compiti e settori di impiego della/e unità;
  - vincoli/limitazioni del terreno e delle condimeteo sulle attività amiche;
  - andamento dell'AOO e relativi settori contermini con le altre basi, nonché individuazione delle aree non controllabili con i sistemi in dotazione.
- **Valutazione delle criticità (*Criticality Assessment*)**

  Eseguita con l'identificazione, partendo dagli elementi emersi nel corso dell'analisi della missione, di tutti gli elementi critici relativi alle operazioni, al supporto logistico e dell'organizzazione funzionale dell'accantonamento, dai quali dipende il successo dell'operazione e la sopravvivenza della base.
- **Valutazione della minaccia (*Threat Assessment*)**

  Sviluppata sulla base dell'analisi di:
  - forze ostili:
    - presenza;
    - tipologia;
    - entità;
    - capacità;
    - intenzioni (manifestate o no);
    - azioni svolte nel passato e relative conseguenze;
    - azioni preparatorie o di imminente realizzazione;
    - possibili itinerari di avvicinamento e di esfiltrazione di forze ostili;
    - vincoli/limitazioni del terreno e condimeteo sulle attività nemiche;
  - rischi naturali e antropici:

[3] Potenziale pericolo, impossibile da eliminare o parzialmente eliminato, che può provocare danni se si interviene con metodi, procedure e sistemi non adeguati.

- tipologia;
- caratteristiche e potenzialità;
- incidenti ed emergenze avvenute nel passato, eventuali ciclicità e conseguenze.

– **Valutazione della vulnerabilità (*Vulnerability Assessment*)**

Sviluppata con l'individuazione di tutti quegli elementi e quelle attività della base e della corrispondente AOO che potrebbero essere influenzati negativamente dalle minacce e dai relativi rischi identificati (LOC, varie aree funzionali della base, trasporti, attività di controllo, ecc.).

– **Valutazione del rischio (*Risk Assessment*)**

Realizzata attraverso:

- l'identificazione, tra quelli già individuati come vulnerabili, degli elementi che in funzione della minaccia risultano critici per il raggiungimento della missione;
- la definizione dell'incidenza che il verificarsi della minaccia o dei rischi potrebbero avere sulla sopravvivenza della base.

– **Gestione del rischio (*Risk Management*)**

Effettuata:

- definendo le misure da attuare per eliminare le criticità riscontrate o contenere il rischio al di sotto della soglia che potrebbe compromettere la missione e la sopravvivenza della base;
- predisponendo le attività di controllo e di coordinamento nell'applicazione delle misure correttive definite.

– **Risposta all'incidente (*Incident Response*)**

Tramite l'attuazione delle misure predisposte in pianificazione per la gestione delle attività a seguito di un evento/incidente.

– **Aggiornamento e verifica (*Supervise & Review*)**

Effettuando la revisione ed i controlli sulle misure di FP adottate e l'analisi della risposta all'evento/incidente:

- esame delle procedure attuate a seguito di evento/incidente;
- aggiornamento della minaccia;
- raccolta e diffusione dei dati (caratteristiche, LId, LL, ecc.);
- simulazioni ed esercitazioni;
- adeguamento delle SOP e dei piani predisposti.

Al fine di pianificare un'organizzazione della protezione della base efficace contro tutte le possibili minacce e rischi presenti e potenziali nell'AOO assegnata, ogni fase del ciclo è esaminata nell'ambito delle due citate macro aree di analisi.

I risultati sono successivamente comparati tra di loro al fine di assicurare l'unicità dell'Annesso "J" e dei piani di protezione che vengono redatti al termine dell'applicazione del ciclo delle misure di FP.

1.1 AZIONI DI FORZE OSTILI

1.1.1 *Threat Assessment*

Esame dell'ambiente operativo e delle possibili minacce: osservazione, tiro teso e curvo, attacchi aerei (drone - aerei - missili), mine, trappole, UXO (più gravi se realizzati con sostanze chimiche, batteriologiche, radiologiche), IED (adiacenti alla base o lungo la viabilità limitrofa), possibili itinerari delle LOC lontani dalla base sottoposti a controllo e intervento di centri di fuoco avversari o IEDs.

1.1.2 *Vulnerability Assessment*

- Valutazione della vulnerabilità delle aree e degli edifici, dei luoghi ad alta frequentazione, degli accantonamenti di materiali/viveri, delle centrali tecnologiche per la produzione dell'energia elettrica e dei sistemi per la captazione e la distribuzione dell'acqua potabile;
- valutazione della vulnerabilità del sistema integrato di protezione (sistemi di rilevamento e scoperta, dislocazione e caratteristiche delle postazioni difensive, BDOC4, collegamenti, ecc.), dell'organizzazione sanitaria, CBRN ed antincendio della base.

1.1.3 *Risk Assessment*

- Accertamento dei limiti e delle restrizioni per l'impiego dei sistemi di sorveglianza (disponibilità di campi di vista e tiro, elementi del terreno o condimeteo avverse per i sistemi di rilevamento e scoperta, ecc.);
- identificazione delle criticità in relazione all'organizzazione funzionale degli accessi alla base, delle aree perimetrali e ricoveri;
- valutazione dei limiti d'utilizzazione delle infrastrutture critiche;
- analisi delle risorse e tecnologie disponibili;
- analisi delle criticità in relazione alla possibilità di effettuare/ricevere rifornimenti urgenti/MEDEVAC.

1.1.4 *Risk Management*

- Pianificazione e definizione delle procedure per la difesa attiva e delle esigenze di materiali e sistemi di sorveglianza aereo-terrestre;
- realizzazione delle strutture protettive per la difesa attiva e dei ricoveri;
- attuazione del mascheramento e del piano di inganno;
- definizione delle opere di protezione degli elementi critici e viabilità della base;

[4] Base Defense Operations Center.

- definizione delle opere per il contenimento e la limitazione dei danni dagli effetti del tiro diretto e curvo e dalle esplosioni ravvicinate;
- progettazione delle opere di puntellamento e rinforzo delle strutture critiche;
- definizione delle misure di difesa CBRN;
- definizione delle misure di preservazione dell'ambiente.

1.1.5 *Incident response*

Attuazione delle misure predisposte in pianificazione per la gestione delle attività a seguito di un evento/incidente.

1.1.6 *Supervise e Review*

- Esame delle procedure attuate a seguito di evento/incidente;
- analisi e aggiornamento della minaccia;
- raccolta lezioni identificate, analisi e diffusione dei risultati (sotto forma di LId da sottoporre alle S.A. o lezioni apprese);
- definizione delle necessarie attività di simulazione ed esercitazioni da effettuare;
- adeguamento delle SOP e dei piani già predisposti.

1.2 CALAMITÀ NATURALI/EMERGENZE COMPLESSE

1.2.1 *Threat Assessment*

- Identificazione dei rischi naturali in AOO (terremoti, maremoti, eruzioni vulcaniche, frane, esondazioni, inondazioni, alluvioni, incendi, ecc.);
- individuazione dei rischi antropici in AOO (fughe/depositi di sostanze tossiche, esplosioni di gas, incendi colposi o dolosi, ecc.);
- individuazione delle cause:
  - predisponenti: condizioni geologiche particolari che possono determinare l'evento, condimeteo avverse, ecc.;
  - scatenanti: piccoli eventi che possono determinare l'accadere di altri fenomeni in scala maggiore [5];
  - acceleranti: condizioni o eventi concomitanti che possono accelerare il processo;
- ricerca sugli stati di calamità accaduti nel passato in AOO e relative caratteristiche degli eventi.

[5] Smottamento che causa la distruzione di un impianto di produzione che utilizza materiali infiammabili o chimici scatenando un incendio di grosse proporzioni, esondazione di piccoli torrenti che producono grossi smottamenti lungo le LOC, ecc.

1.2.2 *Vulnerability Assessment*

- Identificazione delle aree dell'AOO interessate dai possibili rischi e studio delle caratteristiche: geologiche e geotecniche, dimensioni, infrastrutture strategiche presenti, popolazione, attività economiche primarie, ecc.;
- individuazione delle attività operative che potrebbero essere influenzate negativamente dai rischi identificati;
- identificazione delle aree vulnerabili delle infrastrutture, dei sistemi di protezione e supporto logistico della base;
- valutazione dell'influenza della pianificazione d'emergenza della *Host Nation* (HN) sulle operazioni e sulle attività della base.

1.2.3 *Risk Assessment*

- Identificazione delle criticità dell'organizzazione funzionale della base in relazione ai rischi ed alle vulnerabilità identificate;
- individuazione delle criticità del territorio e dell'organizzazione per la risposta all'emergenza della HN;
- valutazione delle possibili limitazioni all'utilizzazione della viabilità, delle risorse locali e attuazione dei rifornimenti urgenti;
- analisi delle criticità in relazione alla possibilità della base di intervenire per il soccorso/sostegno di altre basi o della popolazione nell'ambito dell'AOO;
- analisi delle criticità in relazione alla possibilità di soccorso/sostegno da parte di altre basi o dalla popolazione.

1.2.4 *Risk Management*

- Predisposizione dei piani d'intervento e dei SOP;
- definizione della capacità di risposta della base in caso di Major Incident;
- pianificazione degli assetti di pronto impiego e di rinforzo (Immediate Reaction Teams, Back Up, ecc.);
- identificazione degli interventi sulle infrastrutture strategiche (ristrutturazione, rinforzo, demolizione di quelle instabili o pericolanti, ecc.);
- predisposizione dei depositi di materiali per l'emergenza;
- identificazione e mappatura delle aree sicure per l'installazione delle strutture di primo soccorso e della viabilità dedicata ai soccorsi;
- definizione delle attività di coordinamento dei soccorsi con altre basi/organizzazioni nell'AOO;
- identificazione degli assetti specialistici necessari per lo sviluppo dell'intervento durante la fase d'emergenza;
- pianificazione delle esercitazioni con le unità (in genere allargate alla HN, IOs, GOs, NGOs).

1.2.5 *Incident response*

Vds. Sottopara a.

1.2.6 *Supervise e Review*

Vds. Sottopara a.

Per facilitare lo sviluppo delle attività di *Threat* e *Vulnerability Assessment* possono essere impiegati:

- specifici ausili informatici, quali ad es.: sistemi di previsione delle condimeteo;
- programmi che possono simulare gli effetti di esplosioni o incendi, comparando una serie di parametri standardizzati, ecc.);
- varie metodologie di indagini, supportate o meno da attrezzature:
  - analisi preventiva del territorio circostante e delle variazioni apportate dalla popolazione locale;
  - indagini geognostiche;
  - esame delle carte tematiche;
  - indagini storiche.

PAGINA INTENZIONALMENTE BIANCA

MATRICI PER L'ANALISI DEI RISCHI

Le matrici dei rischi disponibili nelle seguenti Appendici n. 1 e 2 sono gli strumenti necessari per il Capo Cellula S/G/J3 FP (ovvero l'FPO) ai fini dell'effettuazione dell'analisi dei rischi connessi alle minacce individuate dal S/G/J2.

Le predette matrici consentono di analizzare tutti i rischi possibili ma sono orientate a fornire, come risultato, elementi di informazione diversi, necessari al Comandante per supportarlo nel suo processo decisionale riguardo all'accettazione dei rischi.

In particolare:

- l'**Appendice 1**: assicura l'analisi dei rischi permettendo di valutare a priori il valore di:
  - grado di probabilità che il rischio si manifesti, sulla base di una minaccia identificata;
  - effetti di ogni singolo rischio ed efficacia delle misure adottate/adottabili;
  - rischio residuo.

  Con tale matrice il Comandante può valutare il valore delle misure adottate per ciascun rischio e la gravità del rischio residuo che deve accettare o trasferire al Comando superiore.
- l'**Appendice 2**: permette di valutare:
  - un'analisi più accurata della minaccia;
  - il grado di accadibilità dei rischi legati a quella minaccia;
  - il valore dell'impatto dei rischi nei confronti di ciascun obiettivo preso in considerazione.

  Con tale matrice il Comandante può valutare il valore dell'impatto dei rischi sull'organizzazione generale della sicurezza ed il grado di accettabilità.

Le Appendici proposte non sono esaustive, ciascun FPO, sulla base della propria esperienza, provvederà ad integrarle sulla base delle specifiche esigenze di analisi.

Gli FPO possono utilizzare qualsiasi altro strumento per l'analisi dei rischi a loro disposizione, o possono crearne di nuovi e personalizzati, purché in linea con le esigenze operative e lo sviluppo del ciclo delle misure di FP.

PAGINA INTENZIONALMENTE BIANCA

MATRICE PER L'ANALISI DEI RISCHI ED IL CALCOLO DEL RISCHIO RESIDUO

1 Tipologia della Minaccia in esame	2 Valore probabilità di avvenimento	3 Valore degli effetti	4 Valore probabilità Di avvenimento moltiplicato per il valore degli effetti	5 Misure di prevenzione dell'avvenimento	6 Valore efficacia	7 Misure di attenuazione effetti dei rischi	8 Valore efficacia	9 Valore complessivo probabilità di avvenimento	10 Valore complessivo effetti	11 Valore rischio residuo (%)
				Media dei valori		Media dei valori				
				Media dei valori		Media dei valori				

VALORI DA INSERIRE NELLE RIGHE DELLA MATRICE

TABELLA I

Probabilità avvenimento	
Altissimo	**10**
Alto	**9**
Significativo	**8**
Medio	**7**
Basso	**6**
Trascurabile	**5**

TABELLA II

Valore degli effetti	
Missione compromessa	**10**
Elevato numero di perdite di vite umane e livello di danni	**9**
Moderato numero di perdite di vite umane e livello di danni	**8**
Modesto numero di perdite di vite umane e livello di danni	**7**
Basso numero di perdite di vite umane e livello di danni	**6**
Feriti e danni riparabili	**5**

TABELLA III

Efficacia delle misure individuate	
Elevatissima – azioni ostili ed incidenti comuni non influenzano lo svolgimento delle operazioni; – capacità operativa forze amiche ripristinata entro 1 ora.	**5**
Elevata – azioni ostili ed incidenti comuni influenzano minimamente lo svolgimento delle operazioni; – capacità operativa forze amiche ripristinata entro 2 ore.	**4**
Media – azioni ostili ed incidenti comuni potrebbero creare disagi alle operazioni limitati nel tempo; – capacità operativa forze amiche ripristinata entro 3 ore.	**3**
Bassa – azioni ostili e ed incidenti comuni creano disagi alle operazioni; – capacità operativa forze amiche ripristinata entro 4 ore.	**2**
Bassissima – azioni ostili e ed incidenti comuni, difficili da prevenire o gestire, compromettono lo svolgimento delle operazioni; – ogni risorsa per il recupero della capacità operativa deve essere dalla conduzione sottratta al sostentamento delle operazioni principali.	**1**
Nulla – l'avversario potrebbe attaccare facilmente equipaggiamenti e personale per le operazioni; – la finalità per l'organizzazione di incidenti è molto alta; – non sono state predisposte misure o piani per il recupero della capacità operativa delle unità amiche.	**0**

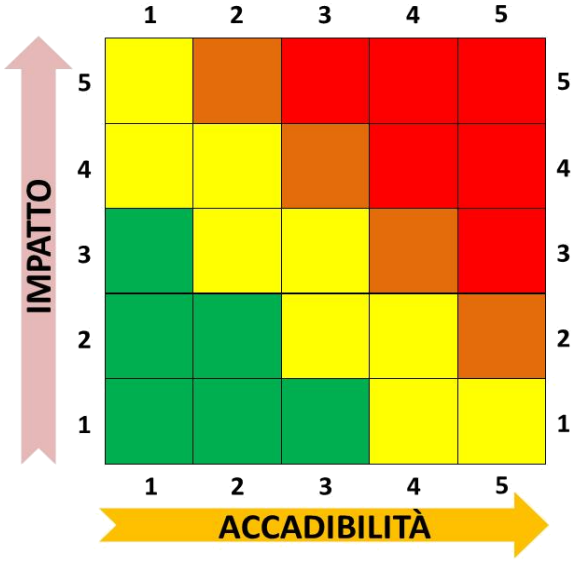
ELEMENTI DA INSERIRE NELLE COLONNE DELLA MATRICE

Nelle colonne della matrice vanno inseriti i seguenti dati:

COLONNA	DATI DA INSERIRE
1	Tipologia della minaccia in esame, individuata dagli organi J/G/S2
2	Valore della probabilità che un incidente/evento legato alla minaccia possa avvenire, definito dai risultati del *Threat Assessment* (J/G/S2). Scegliere uno dei valori della tabella I
3	Valore degli effetti dell'incidente/evento, identificato dalla valutazione tecnica dell'analisi dei risultati del Vulnerability e Risk Assessment. Scegliere uno dei valori della tabella II
4	Valore della probabilità che un incidente/evento legato alla minaccia possa essere moltiplicato per il valore degli effetti. Moltiplicare il valore della colonna 2 x quello della colonna 3
5	Elenco delle misure e predisposizioni ritenute necessarie per la prevenzione dell'incidente/evento, individuate attraverso l'analisi dei risultati del Risk Management.
6	Valutazione dell'efficacia delle misure di prevenzione individuate (colonna 5), definito attraverso una valutazione tecnico-operativa.
7	Scegliere uno dei valori della tabella III
8	Elenco delle misure e predisposizioni ritenute necessarie per la limitazione ed il contenimento degli effetti dell'incidente/evento, individuate attraverso l'analisi dei risultati del Risk Management
9	Valutazione dell'efficacia delle misure di limitazione e di contenimento degli effetti individuate (colonna 7), definito attraverso una valutazione tecnico-operativa. Scegliere uno dei valori della tabella III
10	Valore della probabilità complessiva che un incidente/evento, legato alla minaccia, possa compromettere lo svolgimento delle operazioni. Risultato del valore indicato sulla colonna 2 meno la media dei valori della colonna 6.
11	Valore dell'effetto complessivo che un incidente/evento legato alla minaccia può causare. Risultato dal valore indicato sulla colonna 3 meno la media dei valori della colonna 8.
12	**Valore del rischio residuo**. Viene espresso in % del valore degli effetti indicato sulla colonna 4, dopo l'applicazione delle misure e le predisposizioni per la limitazione ed il contenimento degli effetti (impatto). Risultato dalle seguenti operazioni: 1) calcolo del valore del rischio complessivo: prodotto del valore della colonna 9 per il valore della colonna 10; 2) calcolo del valore del rischio residuo: prodotto del valore del rischio complessivo per 100, diviso il valore della colonna 4.

PAGINA INTENZIONALMENTE BIANCA

MATRICE PER LA VALUTAZIONE DEL VALORE DELL'ACCADIBILITÀ E DELL'IMPATTO DEI RISCHI DI UNA BASE MILITARE



Valutazioni del Comandante della Base in merito ai rischi (COAs)	
	Tollerabile
	Può essere tollerato o trattato
	Deve essere trattato o trasferito
	Deve essere trasferito

Valore potenzialità minaccia	
Alto	5
Medio-Alto	4
Medio	3
Medio-Basso	2
Basso	1

Valore vulnerabilità	
Alto	5
Medio-Alto	4
Medio	3
Medio-Basso	2
Basso	1

Valore frequenza temporale	
Giornaliero	5
1-2 settimane	4
Quadrimestrale	3
Annuale	2
1-5 anni	1

Valore livello compromissione missione	
Strategico	5
Operativo	4
Tattico	3
Locale	2
Minore	1

Valore possibili perdite	
1000 KIA	5
100 KIA	4
10 KIA	3
1 KIA	2
WIA	1

NR	Obiettivo	Minaccia	Intento	Opportunità	Capacità	Valore minaccia	Vulnerabilità	Frequenza	Valore accadibilità	Missione	Perdite	Valore impatto
1												
2												
3												
4												
5												
n												

1-2.1 INDICAZIONI PER LA COMPILAZIONE

- Minaccia: analisi della potenzialità della minaccia: media tra il valore assegnato all'intento, opportunità e capacità di attuare la minaccia;
- accadibilità: probabilità che un evento possa avvenire: pari alla media tra il valore della vulnerabilità e la frequenza temporale;
- impatto: effetti che un evento può avere sull'organizzazione di sicurezza della base: media tra il valore dell'impatto sulla missione e le possibili perdite.

1-2.2 ANALISI DEI RISULTATI

- Riportare il valore dell'accadibilità sulle ascisse e quello dell'impatto sulle ordinate;
- Il colore dell'area di incrocio delle predette ordinate fornirà una valutazione di supporto al processo decisionale del comandante in merito ai rischi e vulnerabilità della sua organizzazione di sicurezza della base.

CHECKLIST PER L'AUTOVALUTAZIONE DELLE MISURE DI FP E DEL SISTEMA DI PROTEZIONE ADOTTATO

BASE MILITARE DI_____

A. Generalità			
Unità:	Sito:		
Comandante:	Tipologia di istallazione:		
Livello di minaccia:	Località (nominativo e coordinate):		
Stato di allertamento:	Indirizzo di posta elettronica:		
B. Punti di contatto	**Telefono**	**Fax**	**E-mail**
Force Protection Officer (FPO):			
Comandante della Difesa:			
Vice Comandante della Difesa (Capo BDOC):			
Capo Centro BDOC:			

C. Verifica FP	
Componenti del Team FP:	
Periodo della verifica FP:	Periodo della precedente verifica FP:
Riassunto della precedente verifica FP[1]:	
Misure attuate per rimuovere le problematiche riscontrate[2]:	

[1] Allegare i documenti esplicativi a corredo se ritenuto necessario.

[2] Allegare i documenti esplicativi a corredo se ritenuto necessario.

1. Documenti FP	
1. Esiste l'Annesso "J" all'OPORDERer? ☐ Si ☐ No Quando è stato aggiornato?	2. Esiste un piano della difesa della base? ☐ Si ☐ No È correlato con l'Annesso J all'OPORDERer? ☐ Si ☐ No Quando è stato aggiornato?
3. Esiste un SOP sulla FP? ☐ Si ☐ No Quando è stato aggiornato?	4. Esistono documenti per la definizione e l'attivazione degli stati di allertamento? ☐ Si ☐ No Vengono applicate le procedure? ☐ Si ☐ No
5. _____	6. _____
Annotazioni:	

2. Informazioni	
1. Come il BDOC riceve le informazioni sulla minaccia?	2. Quali strumenti operativi vengono utilizzati?
3. Esiste una ridondanza nel sistema di comunicazione? ☐ Si ☐ No	4. Sono state individuate delle deficienze organizzative? ☐ Si ☐ No
5. Esiste un coordinamento efficace tra il FPO e il BDOC? ☐ Si ☐ No	6. Esiste un coordinamento efficace tra la cellula G/S2 e il BDOC? ☐ Si ☐ No
7. _____	8. _____
Annotazioni:	

3. Sicurezza Fisica	
1. Le misure di protezione fisica sono aderenti alle direttive Nazionali e NATO? ☐ Si ☐ No	2. È stata attuata una sicurezza in profondità con organizzazione concentrica? ☐ Si ☐ No
3. Sono state stabilite delle procedure per il controllo degli accessi? ☐ Si ☐ No	4. Il sistema perimetrale della base è composto da tutti gli elementi previsti? ☐ Si ☐ No
5. Vengono condotte periodicamente le Mission Essential Vulnerable Assessment (MEVAs)? ☐ Si ☐ No Quando sono state effettuate le ultime?	6. La base è localizzata vicino a rifiuti tossici o aree a rischio che potrebbero essere dannose per l'ambiente o moltiplicare gli effetti di attacchi non convenzionali? ☐ Si ☐ No
7. Le misure intraprese per ridurre i rischi ambientali sono risultate idonee? ☐ Si ☐ No	8. Le misure di sicurezza del sistema sono risultate commisurate ai rischi ed alle vulnerabilità individuate? ☐ Si ☐ No
9. Sono stati istallati sistemi di sorveglianza, rilevamento e diffusione di allarme? ☐ Si ☐ No	10. Esiste un SOP per il loro impiego? ☐ Si ☐ No Quando è stato effettuato l'ultimo test?
11. Il sistema generale è risultato ridondante? ☐ Si ☐ No	12. Il personale è addestrato a reagire prontamente all'allarme? ☐ Si ☐ No
13. Sono stati localizzati in maniera idonea i sistemi di attivazione dell'allarme?	14. Qual è il tempo intercorso tra l'avvistamento e la diffusione dell'allarme?
15. Chi può attivare l'allarme? Con quali sistemi?	16. Sono state condotte attività di addestramento sull'uso dei sistemi di allarme? ☐ Si ☐ No utto il personale è stato addestrato ed è in grado di impiegarli? ☐ Si ☐ No
17. Sono state evidenziate delle lezioni apprese?	18. Sono state corrette eventuali deficienze riscontrate?
19. _____	20. _____
Annotazioni:	

4. Sicurezza delle Informazioni	
1. La documentazione classificata è custodita in contenitori/armadi regolamentari? ☐ Si ☐ No	2. I documenti classificati vengono distrutti quando non più necessari o alla scadenza della loro validità? ☐ Si ☐ No
3. Le combinazioni delle serrature sono cambiate regolarmente? ☐ Si ☐ No	4. Viene verificato il possesso di adeguato nulla osta di sicurezza prima di consegnare la documentazione? ☐ Si ☐ No
5. Viene verificato il possesso di adeguato security clearance certificate prima di far accedere il personale nelle aree riservate? ☐ Si ☐ No	6. _____
Annotazioni:	

5. Addestramento FP	
1. L'addestramento FP viene effettuato per tutto il personale? ☐ Si ☐ No	2. Le esercitazioni di FP vengono condotte per verificare la risposta del personale di vigilanza e QRF, le procedure di evacuazione di edifici, l'idoneità di aree di raccolta e strutture di ricovero collettivo? ☐ Si ☐ No Quando è stata condotta l'ultima esercitazione?
3. L'attività viene regolarmente documentata? ☐ Si ☐ No	4. Sono state evidenziate delle lezioni apprese? ☐ Si ☐ No
5. Le procedure vengono attuate per addestrare il nuovo personale? ☐ Si ☐ No	6. Le direttive sulla FP sono disponibili e accessibili da tutto il personale? ☐ Si ☐ No
7. _____	8. _____
Annotazioni:	

6. Personale della Security	
1. È stato redatto un SOP per la Security? ☐ Si ☐ No Quando è stata fatta l'ultima revisione?	2. L'equipaggiamento della Security (radio, binocoli, CID, dotazioni NBC e sanitarie, ecc.) è risultato adeguato allo svolgimento del compito? ☐ Si ☐ No
3. Il personale di vigilanza viene designato con specifico ordine del giorno? ☐ Si ☐ No	4. Le postazioni sono risultate idonee ad assicurare il servizio di vigilanza (posizione, quota, visibilità, ecc.)? ☐ Si ☐ No
5. Le postazioni sono risultate idonee in merito alle caratteristiche costruttive ed alle dotazioni (sistema diffusione allarme, collegamenti, CID, fari illuminazione, campo di vista e tiro, ecc.) per fronteggiare la minaccia? ☐ Si ☐ No	6. Le turnazioni consentono il recupero fisico del personale impiegato? ☐ Si ☐ No
7. Il personale è risultato addestrato sulle procedure da attuare? ☐ Si ☐ No	8. L'attività risulta documentata? ☐ Si ☐ No
9. Il personale nuovo assegnato è addestrato secondo le succitate procedure? ☐ Si ☐ No	10. Sono stati pianificati e predisposti gli assetti e sistemi in caso d'innalzamento del livello di allertamento? ☐ Si ☐ No
11. _____	12. _____
Annotazioni:	
7. *Quick Reaction Force* (QRF)	
1. È stata designata una QRF nell'ambito del servizio di Security? ☐ Si ☐ No	2. Esiste un SOP per l'impiego della QRF? ☐ Si ☐ No Quando è stato aggiornato?
3. Il personale è addestrato sulle procedure previste dal SOP? ☐ Si ☐ No	4. La QRF è risultata adeguatamente equipaggiata? ☐ Si ☐ No

5. Quando è stata effettuata l'ultima esercitazione per la QRF? Sono state evidenziate lezioni apprese? ☐ Si ☐ No Sono state corrette le deficienze riscontrate? ☐ Si ☐ No	6. Il personale nuovo assegnato è addestrato sulle citate procedure? ☐ Si ☐ No
7. L'addestramento è documentato? ☐ Si ☐ No	8. _____
Annotazioni:	

8. Armamento	
1. L'armamento in dotazione risulta idoneo a contrastare la minaccia individuata? ☐ Si ☐ No	2. Il personale è addestrato al suo impiego? ☐ Si ☐ No Quando sono state effettuate le ultime lezioni di tiro?
3. Il munizionamento è risultato sufficiente? ☐ Si ☐ No	4. Il personale ha azzerato la propria arma? ☐ Si ☐ No
5. L'armamento è risultato adeguatamente manutenzionato? ☐ Si ☐ No	6. _____
Annotazioni:	

9. Armi non letali	
1. Sono disponibili armi non letali? ☐ Si ☐ No	2. Se non sono disponibili, l'unità potrebbe ricevere tale armamento in caso di necessità? ☐ Si ☐ No
3. Il personale è stato addestrato al loro impiego? ☐ Si ☐ No	4. L'addestramento è documentato? ☐ Si ☐ No
5. _____	6. _____

Annotazioni:	
10. Regole d'Ingaggio	
1. Sono state stabilite delle Regole di Ingaggio (ROE)? ☐ Si ☐ No	2. Il personale è stato addestrato sulla loro applicazione? ☐ Si ☐ No
3. Il personale nuovo assegnato è addestrato sulle citate procedure? ☐ Si ☐ No	4. L'addestramento è documentato? ☐ Si ☐ No
5. _____	6. _____
Annotazioni:	
11. Supporto Medico	
1. Il supporto medico (personale, materiali e procedure) è risultato adeguato alle esigenze operative? ☐ Si ☐ No	2. È disponibile un supporto medico/MEDEVAC per le pattuglie all'esterno della base? ☐ Si ☐ No
3. Sono stati previsti accordi con la HN in merito al supporto sanitario e sull'utilizzazione di strutture sanitarie locali? ☐ Si ☐ No	4. Esiste un SOP per l'intervento in caso di Mass Casualties (MC) o Major Incident (MI)? ☐ Si ☐ No
5. L'unità ha condotto esercitazioni di MC e MI? ☐ Si ☐ No Quando è stata effettuata l'ultima esercitazione? Sono state evidenziate lezioni apprese? ☐ Si ☐ No Sono state corrette le deficienze riscontrate? ☐ Si ☐ No	6. Il personale ha ricevuto addestramento di primo soccorso o BLS? ☐ Si ☐ No L'attività è stata documentata? ☐ Si ☐ No

7. Sono state previste misure e procedure per prevenire la contaminazione dell'acqua? ☐ Si ☐ No Sono in linea con quanto definito dalla normativa NATO e nazionale? ☐ Si ☐ No	8. Sono state previste misure e procedure per prevenire la contaminazione degli alimenti? ☐ Si ☐ No Sono in linea con quanto definito dalla normativa NATO e nazionale? ☐ Si ☐ No
9. _____	10._____
Annotazioni:	

12. NBC	
1. Nel piano di difesa sono state presi in considerazioni attacchi terroristici con armi WMD? Attacco chimico? ☐ Si ☐ No Attacco biologico? ☐ Si ☐ No Attacco nucleare/radiologico? ☐ Si ☐ No	2. Il personale ha al seguito la maschera NBC? ☐ Si ☐ No Il personale è addestrato nel suo impiego? ☐ Si ☐ No L'addestramento è stato documentato? ☐ Si ☐ No
3. Il personale ha al seguito il corredo NBC? ☐ Si ☐ No Il personale risulta addestrato al suo impiego? ☐ Si ☐ No L'addestramento è stato documentato? ☐ Si ☐ No	4. Sono disponibili sistemi di decontaminazione individuali? ☐ Si ☐ No Il personale risulta addestrato al loro impiego? ☐ Si ☐ No L'addestramento è stato documentato? ☐ Si ☐ No

5. Sono disponibili sistemi di decontaminazione collettiva? ☐ Si ☐ No Il personale risulta addestrato al loro impiego? ☐ Si ☐ No L'addestramento è stato documentato? ☐ Si ☐ No	6. Quando è stata effettuata l'ultima esercitazione? Sono state evidenziate lezioni apprese? ☐ Si ☐ No Sono state corrette le deficienze riscontrate? ☐ Si ☐ No
7. _____	8. _____
Annotazioni:	

13. Supporto della Host Nation	
1. Sono state siglate intese e accordi con la HN in merito allo svolgimento delle attività di vigilanza della Base e del territorio circostante da parte delle Forze Amiche e delle Forze di Sicurezza locali? ☐ Si ☐ No	2. Sono disponibili un adeguato numero di interpreti per coordinare le attività con la HN? ☐ Si ☐ No
3. Sono state pianificate attività di cooperazione tra le Forze e la HN in merito a: – Eventi di pubblica crisi? ☐ Si ☐ No – Fenomeni naturali e antropici? ☐ Si ☐ No – Attività di controllo al di fuori della Base? ☐ Si ☐ No	4. È stato coordinato l'intervento degli assetti della HN in caso di: – Incendi nella Base? ☐ Si ☐ No – Attacchi contro la Base? ☐ Si ☐ No – Situazioni di Mass Casualties? ☐ Si ☐ No
5. _____	6. _____
Annotazioni:	

14. Pianificazione dell'intervento in caso di emergenze	
1. Il processo di risk management è stato attuato per redigere la pianificazione degli interventi in caso di emergenze? ☐ Si ☐ No	2. Sono state pianificate tutte le misure di intervento contro le possibili emergenze in AOR? ☐ Si ☐ No
3. Sono state pianificate esercitazioni in merito alla valutazione delle procedure in caso di emergenza? ☐ Si ☐ No Quando è stata effettuata l'ultima esercitazione?	In particolare: – antincendio? ☐ Si ☐ No – incidenti stradali? ☐ Si ☐ No
4. È stata sviluppata la pianificazione antincendio? ☐ Si ☐ No Quando è stata effettuata l'ultima esercitazione antincendio?	– incidenti a persone? ☐ Si ☐ No
5. I risultati dell'esercitazione hanno evidenziato un'adeguata capacità? ☐ Si ☐ No Sono state evidenziate lezioni apprese? ☐ Si ☐ No Sono state eliminate le deficienze riscontrate? ☐ Si ☐ No	6. È stata effettuata la valutazione di vulnerabilità per tutti gli edifici ed aree della Base? ☐ Si ☐ No
7. _____	8. _____
Annotazioni:	

15. Ulteriori informazioni
Valutazione finale:
Elenco Allegati:

Il Capo Cellula FP

PAGINA INTENZIONALMENTE BIANCA

ABBREVIAZIONI E SIGLE

ACRONIMO	SIGNIFICATO
AD	*Allied Directive* (Direttiva Alleata).
AFD	Area funzionale per la difesa della base
AI	Area Interna (*Internal Area*)
AJP	*Allied Joint Publication* (Pubblicazione Alleata).
AMD	*Air & Missile Defense* (Difesa aerea ed antimissile)
AOO	*Area of Operations* (Area di Operazioni).
AOR	*Area of Responsibility* (Area di responsabilità)
AP	Area Perimetrale (*Perimeter Area*)
APOE/D	*Airport of Embarkation/Debarkation* (Aeroporto di imbarco/sbarco)
BDA	– *Battlefield Damage Assessment* (Accertamento dei risultati). – *Bomb Damage Assessment* (Accertamento dei danni a seguito di esplosione).
BDOC	*Base Defense Operations Center* (Centro Operativo per la Difesa della Base – ovvero anche Posto Comando FP).
BFI	*Bulk Fuel Installation.*
BLOS	*Beyond Line of Sight* (Area non osservabile direttamente)
C.A.I.	Centro Amministrativo d'Intendenza.
CBRN	*Chemical Biological Radiological Nuclear* (Nucleare, Biologico, Radiologico e Chimico).
C/C (AT)	Controcarri (*Anti Tank*).
C-IED	*Countering Improvised Explosive Devices* (Contrasto agli Ordigni esplosivi improvvisati)
CID	*Combat Identification Device* (Dispositivo di identificazione da combattimento)
CIMIC (COCIM)	*Civil Military Cooperation* (Cooperazione Civile-MIlitare).
CIS	*Communication and Information System* (Sistema di comunicazioni e informazioni)
CND	*Computer Network Defence* (Sicurezza Informatica)
COMSEC	*Communication Security* (Sicurezza delle comunicazioni).
COMPUSEC	*Computer Security* (Sicurezza informatica).
C-RAM	*Counter Rocket Artillery & Mortar*
CRO	*Crisis Response Operations* (Operazioni di risposta alle crisi)
CSAR	*Combat Search and Rescue* (Ricerca e soccorso di combattimento)
DAMRA	*Defence Against Mortar and Rocket Attack* (Difesa contro mortai e razzi)
dep.cel./depocel (BFI)	Deposito carbo-lubrificanti (*Bulk Fuel Installation*).

dep.mu./depomuni	Deposito munizioni (*Ammunition Depot*).
ECM	*Electronic Counter measures* (Contromisure elettroniche).
EDD	*Explosive detection Dog* (Cane abilitato alla ricerca di esplosivi).
EO	Elettro Ottica (*Electro-Optic*)
EOD	*Explosive Ordnance Disposal* (Bonifica di ordigni esplosivi).
EOR	*Esplosive Ordnance Reconnaissance* (Riconoscimento ordigni esplosivi).
EPO	*Environmental Protection Officer* (Ufficiale Addetto alla Protezione Ambientale).
ESO	*Explosive Safety Officer* (Ufficiale Addetto alla Sicurezza del Munizionamento).
ESMRM	*Explosive Safety Munition Risk Management.*
FOB	*Forward Operating Base* (Base Operativa Avanzata).
FP	*Force Protection* (Protezione delle Forze).
FPE	*Force Protection Engineering (Supporto del Genio alla Force Protection).*
FPEO	*Force Protection Engineering Officer (Ufficiale del Genio Addetto alla FP).*
FPEPM	*Force Protection Engineering Project Management (Gestione del Processo di FPE).*
FPO	*Force Protection Officer (Ufficiale Addetto alla FP).*
FPWG	*Force Protection Working Group (Gruppo di Lavoro sulla Force Protection).*
FRAGO	*Fragmentary Order (Pacchetto d'ordini)*
FSB	*Forward Support Base (Base di supporto avanzata)*
GCS	*Ground Control Station (Stazione di controllo terrestre)*
GO	*Government Organizations (Organizzazione Governativa).*
HEAT	*High Esplosive Anti Tank (alto esplosivo controcarri - proietto)*
HME	*Home Made Explosive (Esplosivo di circostanza/fatto in casa).*
HN	*Host Nation (Nazione Ospitante).*
HNS	*Host Nation Support (Supporto della Nazione Ospitante).*
HNSF	*Host Nation Security Forces (Forze di Sicurezza della Nazione Ospitante).*
IDS	*Intrusion Detection System (Sistemi per la scoperta di intrusione).*
IED	*Improvised Explosive Device (Ordigno Esplosivo Improvvisato).*
IEDD	*Improvised Explosive Device Disposal (Bonifica di Ordigni Esplosivi Improvvisati).*
IFF	*Identification Friend-or-Foe (Identificazione*

	amico/nemico)
INFO OPS	*Information Operations (Operazioni dell'informazione)*
INFOSEC	*Information Security (Sicurezza delle informazioni)*
IO	*International Organization (Organizzazione Internazionale).*
IR	*Infra-Red (Infrarossi).*
IRT	*Immediate Response Team (Nucleo di pronto impiego).*
ISTAR	*Intelligence Surveillance Target Acquisition and Reconnaissance (Intelligence, Sorveglianza, Acquisizione di Obiettivi e Ricognizioni)*
JOC	*Joint Operational Center (Centro Operativo Interforze)*
LI	*Lessons Identified (Lezione Identificata)*
LL	*Lessons Learned (Lezione Appresa)*
LOC	*Line of Communication (Linee di comunicazione-viabilità)*
MASCAL	*Mass Casualties (Particolare situazione di emergenza medica)*
MC2	*Modulo Comando e Controllo FP (MFD del SIPROB)*
MEDAD	*Medical Advisor (Consulente Medico).*
MEDEVAC	*Medical Evacuation (Sgombero sanitario)*
M&B	*NATO Military Budget (Fondi Militari della NATO).*
MFD	*Moduli funzionali per la difesa*
MILENG	*Military Engineering (Genio Militare).*
MMR	*Minimum Military Requirement (Requisito Minimo Militare).*
MoU	*Memorandum of Understanding (Protocollo d'intesa)*
MP (PM)	*Military Police (Polizia Militare).*
MP	*Modulo Protezione (MFD del SIPROB)*
MRR	*Modulo Reazione remotizzata (MFD del SIPROB)*
MSO	*Modulo Sorveglianza (MFD del SIPROB)*
MRSAM	*Medium Range Surface to Air Missile*
NGO	*Non Governmental Organization (Organizzazione Non Governativa).*
NSIP	*NATO Security Investment Programme (Programma di investimento della NATO per la Sicurezza).*
OPSEC	*Operations Security (Sicurezza delle Operazioni).*
PBIED	*Person Born IED (Ordigno esplosivo improvvisato trasportato da persona).*
PC (CP)	*Posto Comando (Commad Post).*
POA (OP)	*Posto di osservazione e allarme (Observation Post).*
POC	*Progettazione Operativa di Contingenza (Field Engineering).*
POL (cel)	*Petroleum Oils and Lubricants (Carburanti e Lubrificanti).*
PSYOPS	*Psychological Operations (Operazioni psicologiche)*
PSO	*Peace Support Operations (Operazioni di sostegno alla*

	pace)
PVAB	*Portable Vehicle Arresting Barrier (Barriera di arresto contro veicoli di tipo portatile)*
QRF	*Quick Reaction Force (Forza di Reazione Rapida).*
RA	*Risk Assessment (Valutazione del rischio)*
RCIED	*Radio Control IED (Ordigno Esplosivo Improvvisato radiocomandato).*
RCS	*Remote Control Station.*
RM	*Risk Management (Gestione del Rischio)*
ROE	*Rules of Engagements (Regole di Ingaggio).*
RPG	*Rocket Propelled Grenade*
SAR	*Search and Rescue (Ricerca e soccorso)*
SHORAD	*Short Range Air Defense*
SIBCRA	*Sampling and Identification of Biological, Chemical and Radiological Agents*
SIED	*Suicide IED (Ordigno esplosivo improvvisato attivato da un terrorista con l'intenzione di uccidere se stesso come parte dell'attacco o impedire la sua cattura).*
SIFP	*Sistema Integrato di FP*
SIPROB	*SIstema Integrato di PROtezione Basi militari*
SITREP	*SITuation REPort (Rapporto di situazione).*
SPOE/D	*Seaport of Embarkation/Debarkation (Porto di imbarco/sbarco)*
SOFA	*Status of Forces Agreement (Accordo sullo statuto delle forze)*
SOI	*Standing/Standard Operating Instructions (Istruzioni Operative Standard)"*
SOP	*Standing/Standard Operating Procedures (Procedure Operative Standard).*
STANAG	*Standardization Agreement (Accordo di Standardizzazione)*
SVIED	*Suicide Vest IED (Attentatore suicida con giubbotto esplosivo).*
SVBIED	*Suicide Vehicle Borne IED (Ordigno esplosivo improvvisato all'interno di un veicolo attivato dal conduttore o da uno degli occupanti).*
TA	*Threat Assessment (Valutazione della minaccia).*
TAOR	*Tactical Area of Responsibility (Area di responsabilità Tattica).*
Te. Op. (T.O.)	*Teatro Operativo/Teatro di Operazioni (Theatre of Operations).*
TIM	*Toxic Industrial Material (Materiale Tossico Industriale).*
TOC	*Tactical Operation Centre (Sala Operativa Tattiche).*
TTPs	*Tactics, Techniques and Procedures (Tattiche, Tecniche e Procedure).*
TVCC	*Sistema di sorveglianza elettronica perimetrale o interna di una base militare attraverso l'impiego di telecamere a*

	circuito chiuso.
UAV	*Unmanned Aerial Vehicle (Velivolo a pilotaggio remoto).*
UGV	*Unmanned Ground Vehicle (Veicolo a pilotaggio remoto).*
WLOS	*Within Line of Sight (Area di osservazione diretta).*
WLR	*Weapon Location Radar.*
VBIED	*Vehicle Born Improvised Explosive Device (Autobomba).*
VA	*Vulnerability Assessment (Valutazione della vulnerabilità).*
V/SHORAD	*Very Short Range Air Defense*
ZAE (HLZ)	*Zona Atterraggio Elicotteri (Helicopter Landing Zone).*

PAGINA INTENZIONALMENTE BIANCA

GLOSSARIO

I termini contrassegnati con * sono da considerare di nuova introduzione ad integrazione e completamento delle seguenti pubblicazioni che ne risultano mancanti:

- Pub. SMD-G-016A-2 "Glossario nazionale delle abbreviazioni e sigle militari", ed. 2012;
- Pub. SMD-G-024 "Glossario dei Termini e delle Definizioni", ed. 2007 – Aggior. 1 –2009;
- Pub. 5867 "Abbreviazioni e sigle di uso autorizzato nell'Esercito", ed. 2000;
- Pub. 5985 "Nomenclatore Militare", ed. 1998.

Tali termini sono stati redatti utilizzando le seguenti pubblicazioni/direttive NATO, Nazionali (sia militari che Vigili del Fuoco), USA ed ONU:

- AAP-06 "NATO *Glossary of Terms and Definitions*", ed. 2013 (**AAP-06**);
- AAP-15 "NATO *Glossary of Abbreviations used in NATO Documents and Publications"*, ed. 2011 (**AAP-15**);
- AAP-19 (D) "NATO *Combat Engineer Glossary*", ed. 2003 (**AAP-19**);
- AJP 3.14 (A) "*Allied Joint Doctrine for Force Protection*", ed. 2014 (**AJP 3.14**);
- AJP 4.10 (B) "Allied Joint Medical Support Doctrine", ED. 2015 (**AJP 4.10**);
- AEmedP-13 (A) "NATO Glossary of Medical Terms and Definitions", ed. 2011 (**AEmedP-13**);
- ATP-3.12.1.1 *Allied Tactical Doctrine for Military Search*, ed. 2015 (**STANAG 2283**);
- AD 80-25 "ACO FP Directive", ed. 2009 (**AD 80-25**);
- PID-O 3.14 "La protezione delle forze", ed. 2012 (**PID-O 3.14**);
- Nota Dottrinale "Il contrasto alla minaccia interna (*Insider Threat – Green on Blue*), SME, ed. 2013 (**ND-IT**);
- Pub. 5985 "Nomenclatore Militare", ed. 1998 (**PUB. 5985**);
- Pub. 6365 "Impiego del Genio", ed. 2015 (**PUB. 6365**);
- Pub. 6838 "Lineamenti d'impiego dei sistemi integrati di *Force Protection*", ed. 2014 (**PTE-SIFP**);
- SOP "Tecniche e procedure per la progettazione di contingenza di opere del genio", ed. 2014 (**SOP POC**);
- SOP "Protezione di persone, attività e beni in caso di detonazione in campo aperto di ordigni esplosivi ed esplosivi in genere", ed. 2014 (**SOP PROT-EOD**);

- "*Joint Forward Operations Base Force Protection Handbook*", U.S. *Center* for *Army Lessons Learned*, ed. 2007 (**JFOB**);
- Dispensa "Prevenzione Incendi", Ministero dell'Interno - Dipartimento dei Vigili del Fuoco del Soccorso Pubblico e della Difesa Civile - Direzione Centrale per la Formazione - Area I – Coordinamento e Sviluppo della Formazione, ed. 2010 (**VV.F.**);
- "*Guidelines on the Use of Military and Civil Defence Assets to Support United Nations Humanitarian Activities in Complex Emergencies*", ed. March 2003 (**UN-MCDA**).

Per ciascuna definizione, oltre alla determinazione dei significati, è stato posto tra parentesi il documento di riferimento tra quelli precedentemente indicati:

- in cui il termine viene riportato ufficialmente (es: **AAP-06**);
- dal quale è stata tratta la nuova definizione (es: **di nuova introduzione-PID-O 3.14**).

Alcuni termini, per meglio comprenderne il significato, sono stati riportati anche con più definizioni attualmente ufficialmente approvate con i vari documenti in parola e/o di nuova introduzione.

TERMINE	SIGNIFICATO
Analisi della missione (*Mission Analysis*),	Passo del ciclo delle misure di FP che ne avvia lo sviluppo identificando chiaramente l'intento dei Comandanti superiori, il Concetto d'azione del proprio Comandante, i compiti espliciti e quelli impliciti, nonché i possibili vincoli (**PID-O 3.14**).
Area di Operazioni (*Area of Operations*)	Porzione di un'area necessaria per la condotta delle operazioni militari (**PUB. 5895**).
Area di Responsabilità Tattica *(Tactical Area of Responsibility – TAOR)*	Area che viene stabilita intorno ad una base militare in operazioni al fine di prevenire, attraverso il suo controllo e dominio, gli attacchi diretti ed indiretti condotti contro le infrastrutture ed il personale (**AJP 3.14**).

TERMINE	SIGNIFICATO
Area di Sicurezza Perimetrale* (*Perimeter Security Area*)	– Area perimetrale necessaria per prevenire che personale non autorizzato possa accedere ad una installazione NATO (**AJP 3.14**). – Zona intorno ad una sorgente di rischio nell'ambito della quale si può assicurare che un livello di rischio non possa aumentare (**AAP-19**). – Porzione di area perimetrale, denominata anche striscia perimetrale, di adeguata profondità, recintata e libera da ostacoli che possano limitare o impedire il controllo e l'azione di fuoco delle armi della difesa perimetrale (**di nuova introduzione-SOP POC**).
***Base Defense Operations Center* – BDOC**	Centro di Comando e Controllo della difesa di una base militare (ovvero Posto Comando FP) che ha il compito di pianificare e coordinare le misure per la vigilanza e la protezione della base e della relativa Area di Responsabilità (TAOR/AOO) assegnata (**PTE SIFP, JFOB**).
Base Militare (Military *Base*)	– Una zona dalla quale hanno inizio o sono appoggiate le operazioni (**PUB. 5895**). – Un'area o località contenente installazioni che provvedono al supporto logistico o altra tipologia di supporto (**AAP-06**).
Base Militare Tattica* (*Field Base*)	Accampamenti o installazioni che utilizzano solo equipaggiamenti ed attrezzature in dotazione alle unità. La loro utilizzazione è legata allo sviluppo dell'operazione con possibili frequenti cambiamenti di localizzazione dovuti alle azioni di combattimento nelle immediate vicinanze e di alta intensità. Per gli standard previsti, consentono il supporto alle operazioni fino a 2 mesi consecutivi (**di nuova introduzione-SOP POC**).
Base Militare Provvisoria* (*Provisional Base*)	Accampamenti o installazioni caratterizzati dalla temporaneità degli alloggiamenti, servizi infrastrutturali essenziali e possibili frequenti cambiamenti di localizzazione dovuti alle azioni di combattimento nelle immediate vicinanze di media-alta intensità. Per gli standard previsti, consentono il supporto alle operazioni fino a 6 mesi consecutivi (**di nuova introduzione-SOP POC**).

TERMINE	SIGNIFICATO
Base militare Temporanea* (*Temporary Base*)	Accampamenti o installazioni provvisti di strutture shelterizzate e/o di prefabbricazione leggera che assicurano ottimali *standard* abitativi e servizi infrastrutturali completi. Non sono presenti azioni di combattimento nelle immediate vicinanze o, tuttalpiù, di bassa o bassissima intensità. Per gli standard previsti, consentono il supporto alle operazioni da 6 fino a 12 mesi consecutivi (**di nuova introduzione-SOP POC**).
Base Militare Permanente* (*Permanent Base*)	Accampamenti o installazioni provvisti di infrastrutture in prefabbricato leggero ed opere di urbanizzazione che assicurano elevati standard abitativi. Consentono l'impiego in operazioni per lunghi periodi di tempo (**di nuova introduzione-SOP POC**).
Base Operativa Avanzata* (*Forward Operating Base* - FOB)	Infrastruttura temporanea e/o permanente concepita per supportare le attività di C2 e di sostegno logistico a favore di unità che assolvono compiti/missioni particolari o in profondità (**di nuova introduzione – JFOB**).
Campo di Tiro (*Field of Fire*)	Zona nell'ambito della quale un'arma o un gruppo di armi, dislocate in determinata posizione, sono in grado di intervenire efficacemente con il fuoco (**PUB. 5895**).
Campo di vista (*Field of vision*)	Angolo solido che delimita lo spazio visibile del tiratore dalla sua postazione di osservazione (**PUB. 5895**).
Camp Site Manager*	Ufficiale del genio militare, appartenente al settore infrastrutturale, responsabile della gestione delle infrastrutture utilizzate dal Contingente Nazionale o che ricadono sotto la responsabilità nazionale. È inquadrato nell'ambito dello Staff del Comando di Contingente Nazionale e risponde, in linea tecnico/operativa, al COI (**di nuova introduzione-SOP POC**).
Ciclo delle Misure di FP (*FP Model*)	Attività ciclica del processo di pianificazione, secondo un ordine temporale ben definito. Detta sequenza di attività deve comunque essere sviluppata e imperniata alla luce di una preventiva valutazione delle vulnerabilità (*vulnerability assessment*) e dei rischi (*risk assessment*) correlati (**PID-O 3.14**).
Controllo dell'Area di Responsabilità Tattica (*TAOR Domination*)	Include tutte le azioni che assicurano il controllo della situazione operativa su tutta la TAOR in modo che le forze amiche abbiano libertà di manovra nelle operazioni al contrario dell'avversario (**AJP 3.14**).

TERMINE	SIGNIFICATO
Controllo del personale (*Person Search*)	Procedura di controllo delle *military search* tendente all'ispezione approfondita del personale, ivi compresi pacchi e bagagli al seguito, al fine di scoprire armi, esplosivi, materiale di contrabbando e altri materiali di interesse ai fini dell'*intelligence* (**STANAG 2283**).
Controllo dei veicoli (*Vehicle Search*)	Procedura di controllo delle *military search* tendente all'ispezione approfondita dei veicoli, ivi compresi conducente, passeggeri, pacchi e bagagli trasportati, allo scopo di scoprire il trasporto di terroristi, ordigni esplosivi improvvisati (VBIEDs), risorse legate al crimine e altri materiali di interesse ai fini dell'*intelligence* (**STANAG 2283**).
Deterrenza (*Deterrence*)	Capacità di convincere un potenziale aggressore che le conseguenze dell'atteggiamento di minaccia e del conflitto armato potrebbero oltrepassare i potenziali ricavi. Richiede il mantenimento di una capacità militare adeguata, una strategia credibile ed una chiara determinazione politica (**PUB. 5895**).
Difesa Attiva (*Active Defence*)	– Misure attive prese contro le forze nemiche per impedire, annullare o ridurre l'efficacia di una qualsiasi forma di attacco nemico (**SMD-G-024**). – Misure e predisposizioni tese a prevenire, annullare e ridurre l'efficacia di qualsiasi forma di offesa da parte di elementi ostili (**PID-O 3.14**).
Difesa CBRN (*CBRN Defence*)	Tutte le misure che debbono essere adottate allo scopo di difendersi contro attacchi condotti con armi CBRN e contro tutti i pericoli derivanti dal rilascio nell'ambiente di sostanze tossiche di origine industriale (*Toxic Industrial Materials* - TIM), inclusi atti terroristici (**PID-O 3.14**).
Difesa Passiva (*Passive Defence*)	Misure e predisposizioni da adottare per assicurare la sicurezza fisica, la protezione del personale, delle infrastrutture e delle attrezzature essenziali e ridurre l'efficacia delle azioni di elementi ostili (**AAP-06**).
Dissuasione (*Deterrence*)	Percezione di efficienza e di concreta resistenza del sistema ad attacchi o attentati che viene a radicarsi negli aggressori, i quali considereranno la loro eventuale azione poco remunerativa, inefficace, inutile, o – addirittura – dannosa e controproducente per loro stessi (**PID-O 3.14**).

TERMINE	SIGNIFICATO
Distanza di sicurezza* (*Stand Off*)	– Distanza minima che deve intercorrere tra un elemento della base ed il possibile punto di esplosione di una carica esplosiva, posizionata lungo il suo perimetro esterno, al fine di assicurarne l'integrità fisica e strutturale e la sopravvivenza del personale dislocato al suo interno (**di nuova introduzione - SOP PROT-EOD**). – In termini di guerra terrestre, la distanza dalla sorgente di rischio la quale assicura che uno specifico grado di rischio non aumenti (**AAP-19**).
Emergenza complessa (*Complex Emergency*)	Crisi umanitaria in uno stato, regione o società dove c'è una considerabile mancanza di autorità a causa di conflitti interni o esterni e che richiede una risposta internazionale che va oltre il mandato o la capacità di un singolo e/o di un programma regionale dell'ONU in corso di svolgimento (**UN-MCDA**).
Gestione delle Emergenze (*Consequence Management* - CM)	– L'insieme delle azioni intraprese per mantenere o ripristinare i servizi essenziali, nonché gestire ed attenuare i danni derivanti da calamità e/o catastrofi (naturali o accidentali), o causati da eventi provocati deliberatamente quali ad esempio attentati terroristici (**PID-O 3.14**). – Azione intrapresa per mantenere o ripristinare i servizi essenziali e per mitigare gli effetti di disastri naturali o provocati dall'uomo (**AAP-06**). – L'impiego di misure reattive per mitigare gli effetti distruttivi di un attacchi, incidenti, terrorismo o disastri naturali (**AEmedP-13**).
Gestione del Processo di FPE* (*Force Protection Engineering Project Management* - FPEPM)	Analisi qualitativa e quantitativa delle esigenze di supporto del genio alla FP (**di nuova introduzione - Pub. 6365**).

TERMINE	SIGNIFICATO
Gestione del Rischio (*Risk Management* - RM)	– Passo del Ciclo delle misure di FP necessario per: • verificare che l'eventuale gap, determinatosi dal confronto esigenze/possibilità, non superi i limiti fissati dal Comandante nella sua direttiva per la pianificazione, tenendo, altresì, conto degli esiti del ciclo *Operations Security* (OPSEC); • individuare e predisporre i controlli e le relative misure per la FP (**PID-O 3.14**). – Processo di identificazione, valutazione e controllo dei rischi derivanti da fattori operativi e decisione delle misure che bilanciano i costi dei rischi con i benefici della missione (**AAP-06**).
Identificazione (*Identification*)	Processo di ottenimento di un' accurata definizione di un entità scoperta da ogni tipo di azione o dispositivo così che si possano prendere decisioni attendibili in tempo reale, incluso l'ingaggio a fuoco. (**AAP-06**).
Infiltrazione (*Infiltration*)	– Procedimento operativo avente lo scopo di introdurre in maniera occulta, elementi o piccoli gruppi, forze di diversa entità all'interno di una base militare (PUB. 5895). – Avviene anche quando un elemento dell'insurrezione, si arruola sotto mentite spoglie nelle HNSF, seguendo l'iter di selezione previsto (**ND-IT**).
Ingaggio (*Engagement*)	– Azione intrapresa contro forze ostili con l'intento di danneggiarle o neutralizzarle (combattimento) (**PUB. 5895**). – Nel contesto delle regole d'ingaggio, azione presa contro forze ostili con l'intento di dissuaderle, danneggiarle o neutralizzarle (**AAP-06**).
Inganno (*Deception*)	Complesso di misure intese a fuorviare il nemico mediante la manipolazione, la distorsione o la falsificazione di elementi o circostanze reali e ad ostacolarne la corretta valutazione della situazione operativa (**PUB. 5895**).
Mass Casualty (MASCAL)	– Qualsiasi numero di vittime causato in tempi relativamente brevi che supera la capacità di supporto medico e logistico disponibile (**AAP-06**). – Forma estrema di un *Major Incident* dove la *Host Nation* non ha la capacità di gestire l'emergenza ed il numero delle vittime e degli sfollati risulta oltremodo elevato (**PID-O 3.14**). – Situazione nel quale esiste una eccessiva disparità tra le vittime e la capacità medica localmente disponibile per la loro gestione (**AMedP-13**).

TERMINE	SIGNIFICATO
Matrice dei rischi*	Strumento per l'analisi dei rischi connessi a specifiche minacce ai fini della valutazione del valore dei rischi residui e del loro impatto sull'organizzazione della sicurezza di una base militare (**di nuova introduzione – AD 80-25**).
Minaccia (*Threat*)	– La minaccia è il prodotto di capacità e di intenzione di arrecare danno da parte di un avversario. Entrambi i fattori dovranno essere presenti allo scopo di rendere credibile una minaccia (**PID-O 3.14**). – Percezione di essere in un certo grado di pericolo sulla base di una valutazione generale della situazione, che prende in considerazione le proprie capacità e quelle dell'avversario, le sue precedenti azioni, le intenzioni ostili, ecc.. Possono esistere minacce esterne ed interne in ambienti considerati sicuri come installazioni o FOB (**AJP 3.14**).
Minaccia interna (*Insider Threat*)	Fenomeno degli attacchi o azioni violente perpetrate contro le Forze Armate o di Sicurezza operanti in *partnership* nell'ambito di una operazione militare, da parte di elementi interni alle forze di sicurezza della nazione ospitante (**ND-IT**).
Misure Protettive (*Protection Measures*)	Azioni per incrementare la sopravvivenza delle forze da una minaccia NBC, terrestre/aerea diretta o indiretta. Generalmente è espressa in termini di livelli progressivi individuali e collettivi (**AAP-19**).
Nazione Ospitante (*Host Nation* -HN)	Una nazione che, da accordi: – riceve forze e materiali dalla NATO o da altre nazioni operanti al suo interno o in transito attraverso il suo territorio; – consente a materiali e/o organizzazioni NATO di essere dislocati sui suoi territori; – provvede al supporto per tali scopi. (**AAP-06**).
Nucleo Progettazione Operativa di Contingenza (nu. POC)	– Nucleo di personale qualificato nella progettazione campale, inquadrato nei reggimenti genio del supporto generale, che ha il compito di supportare in Te. Op. la progettazione e la realizzazione di accampamenti/basi militari, viabilità e opere/strutture di FP (**PUB. 6365**). – Ufficiali e Sottufficiali del genio altamente qualificati nella Field Engineering ed inquadrati nei Reggimenti genio (**PID-O 3.14**).

TERMINE	SIGNIFICATO
Piano di Difesa (*Defence Plan*)	Documento esecutivo rispecchiante tutte le predisposizioni per l'organizzazione e la condotta della difesa. È costituito da un piano di base, normalmente integrato da piani complementari che trattano aspetti parziali dell'organizzazione quale il piano di fuoco, piano dell'ostacolo, piano dei lavori, ecc. (**di nuova introduzione – PID-O 3.14**).
Piano di Emergenza (*Consequence Management Plan*)	Pianificazione che deve contenere tutte le procedure da mettere in atto nel caso in cui si verifichi un evento dannoso. Nel particolare, la pianificazione di emergenza prende in esame le possibili tipologie di eventi di pericolo (naturali, meteorologiche o connesse con le attività svolte dall'avversario), che per loro natura ed estensione territoriale, richiedono normalmente un intervento coordinato (**PID-O 3.14**).
Piano d'Inganno (*Deception Plan*)	Documento complementare che definisce le predisposizioni ed i provvedimenti di carattere tattico e tecnico diretti a creare situazioni fittizie a schermo di situazioni reali, per fuorviare l'attenzione del nemico e conseguire la sorpresa (**PID-O 3.14**).
Posto di guardia* (*Guard Post*)	Struttura altamente protetta per alloggiare il personale addetto alla gestione del controllo/difesa della base o dell'ingresso ed il personale in pronto intervento (**di nuova introduzione – JEEP**).
Prevenzione* (*Prevention*)	Impedire e ostacolare l'intrusione nella base per l'effettuazione di atti ostili attraverso l'integrazione dell'organizzazione funzionale con ostacoli vari, procedure di controllo variabili e adeguatezza delle risorse (**di nuova introduzione – PID-O 3.14**).
Protezione Antincendio* (*Fire Protection*)	– Insieme delle misure finalizzate alla riduzione dei danni conseguenti al verificarsi di un incendio, attraverso interventi che si suddividono in misure di protezione attiva o passiva in relazione alla necessità o meno dell'intervento di un operatore o dell'azionamento di un impianto (**di nuova introduzione – VV.F.**). – Include la progettazione e la realizzazione di sistemi di prevenzione e soppressione di incendi per le infrastrutture. Include lo sviluppo, il potenziamento ed il monitoraggio di un programma di sicurezza per le basi che può includere anche l'addestramento. Il supporto del genio include capacità di risposta antincendio in coordinamento con altre capacità logistiche e competenze funzionali di FP (**AJP 3.14**).

TERMINE	SIGNIFICATO
Protezione Fisica* (*Physical Protection*)	Combinazione di misure di sicurezza attiva e passiva quali il controllo del perimetro e degli accessi, attività di mascheramento e inganno, controllo del personale e approntamento di unità per l'emergenza, destinate a rilevare e annullare la minaccia di elementi ostili contro le installazioni (**di nuova introduzione – PID-O 3.14**).
Protezione delle Forze (*Force Protection* - FP)	Insieme di misure e mezzi per ridurre al minimo la vulnerabilità del personale, delle installazioni, dei mezzi e delle operazioni rispetto a qualsiasi minaccia ed in ogni circostanza, al fine di preservare la libertà di azione e l'efficienza operativa delle forze (**PID-O 3.14**).
Protezione delle Infrastrutture (*Infrastructure Protection*)	Comprende i possibili provvedimenti atti a garantire l'incolumità del personale ed aumentare così la credibilità del Contingente e, di riflesso, quella della Nazione e dell'Alleanza (**PID-O 3.14**).
Protezione Perimetrale* (*Perimeter Protection*)	– Predisposizioni di sicurezza intese ad impedire l'accesso di mezzi e personale non autorizzato, inibire l'osservazione, il tiro diretto e l'impiego degli IEDs (**di nuova introduzione – PID-O 3.14**). – Provvedere alla difesa contro attacchi da armi a distanza attraverso la selezione di barriere perimetrali che ostacolano l'osservazione: schermi oscuranti, infrastrutture non critiche, piante e arbusti (**di nuova introduzione – JFOB**).
Protezione Sanitaria (*Force Health Protection* – FHP)	– La risultante degli sforzi per ridurre o eliminare l'incidenza di malattie e lesioni da incidenti per accrescere la prontezza operativa sanitaria e l'efficacia in combattimento (**AJP 3.14**). – La somma di tutti gli sforzi volti a ridurre o eliminare l'incidenza generale delle malattie (con esclusione di quelle connesse con la traumatologia di guerra), al fine di migliorare la prontezza e l'efficienza operativa delle proprie Forze" (**PID-O 3.14**).
Protezione Strutturale* (*Structural Protection*)	Combinazione di opere di FP, sistemi di rinforzo e lavori di fortificazione destinate ad assicurare la resistenza di elementi sensibili di un'installazione contro il tiro diretto e indiretto, il contenimento degli effetti di esplosioni ravvicinate e gli effetti/danni causati da eventi naturali e antropici (**di nuova introduzione – PID-O 3.14**).

TERMINE	SIGNIFICATO
Recupero della capacità operativa (*Recuperation*)	Predisposizioni necessarie ai Comandi e alle forze dipendenti per riprendersi dagli effetti di un attacco avversario, ristabilire i servizi essenziali e, dove appropriato, fare in modo che le operazioni militari continuino col minimo disservizio possibile (**PID-O 3.14**).
Revisione dei controlli e delle misure *(Supervise & Review/Update)*	– Passo del Ciclo delle misure di FP che prevede l'esame comparato dell'incidente/evento occorso e delle relative capacità di reazione messe in atto, ovvero l'aggiornamento degli elementi di conoscenza sulla minaccia (**PID-O 3.14**). – Indipendentemente dall'avvenimento dell'incidente, la supervisione e l'esame dell'accaduto sono necessari per convalidare l'efficacia della pianificazione FP al fine di identificare i necessari aggiustamenti, per assicurare che il controllo dei rischi venga accresciuto ed applicato agli standard e che i meccanismi di revisione siano attuati (**AJP 3.14**).
Rischio (*Risk*)	– Eventualità di subire un danno (più incerto di quello implicito di "pericolo" (**PID-O 3.14**). – La probabilità e severità di una potenziale perdita legata a pericoli e minacce (**AJP 3.14**). – La combinazione della probabilità che un evento possa accadere e le sue conseguenze negative (**UN-MCDA**).
Rischi di incendi* (*Fire risks*)	Probabilità che sia raggiunto il livello potenziale di accadimento di un incendio e che si verifichino conseguenze dell'incendio sulle persone presenti (**di nuova introduzione - VV.F.**).
Rischi naturali (*Natural Hazards*)	Processo naturale o fenomeno che può causare la perdita della vita, ferimento o altri impatti sulla salute, danno alla proprietà, perdita di mezzi di sostentamento e servizi, degrado sociale ed economico, o danno ambientale (**UN-MCDA**).

TERMINE	SIGNIFICATO
Risposta all'incidente *(Incident Response)*	– Passo del ciclo delle misure di FP indispensabile per attuare tutte le misure necessarie al fine di limitare/prevenire gli effetti causati da un incidente/evento. Comprende l'insieme delle misure tese a prevenire, neutralizzare e/o contenere gli effetti di uno specifico evento, che intenda danneggiare ovvero abbia colpito elementi tangibili e non della Forza militare (**PID-O 3.14**). – Comprende l'insieme delle misure tese a neutralizzare, isolare, contenere e o risolvere una specifica minaccia o mitigare i suoi effetti contro il successo della missione, individui, unità ed installazioni (**AJP 3.14**).
Scoperta (*Detection*)	– Individuare, monitorare e valutare una potenziale minaccia prima che possa essere attuata (**di nuova introduzione – PID-O 3.14**). – La scoperta di qualsiasi segnale della presenza di persone, fenomeni obiettivi o potenziale importanza militare (**APP-06**).
Sicurezza (*Security*)	– Condizione che si realizza quando le informazioni, il materiale, il personale, le attività e le installazioni sono protette contro lo spionaggio, il sabotaggio, la sovversione e il terrorismo, nonché contro l'eventuale smarrimento e la divulgazione non autorizzata. – Insieme delle misure necessarie a garantire la protezione contro lo spionaggio, il sabotaggio, la sovversione e il terrorismo, nonché contro l'eventuale smarrimento e la divulgazione non autorizzata. – Organi responsabili della protezione contro lo spionaggio, il sabotaggio, la sovversione e il terrorismo, nonché contro l'eventuale smarrimento e la divulgazione non autorizzata. (**PID-O 3.14**).

TERMINE	SIGNIFICATO
Sicurezza fisica (*Physical Security*)	– Controlli e misure tese ad impedire la distruzione, l'osservazione o il sabotaggio delle installazioni e garantire l'accessibilità e la percorribilità delle linee di comunicazione (**PID-O 3.14**). – Aspetto della sicurezza che riguarda le predisposizioni intese a salvaguardare il personale, ad impedire l'accesso non autorizzato ad impianti, materiali e documenti, ed a proteggerli da eventuali danni, furti, azioni di spionaggio e sabotaggio (**SMD-G-024**). – Parte della sicurezza concernente con le misure fisiche designate a salvaguardare il personale, prevenire accessi non autorizzati ad equipaggiamenti, installazioni, materiali e documenti e tutelarli contro lo spionaggio, sabotaggio, danneggiamenti e sottrazioni (**AAP-06**).
Sicurezza delle operazioni (*Operations Security* - OPSEC)	Complesso di misure volte a creare le necessarie condizioni di sicurezza per una operazione o esercitazione militare, utilizzando mezzi passivi o attivi per impedire che il nemico venga a conoscenza del dispositivo, dei mezzi e delle intenzioni delle forze amiche. (**PID-O 3.14**)
Sicurezza strutturale* (*Structural Security*)	– Controlli e misure tese a garantire la resistenza delle infrastrutture vitali contro offese di diversa natura e la resistenza di punti chiave delle linee di comunicazione contro attacchi di diversa natura e pericoli ambientali (**PID-O 3.14**). – Insieme delle misure tese ad assicurare la resistenza delle infrastrutture vitali di una installazione (**di nuova introduzione – PID-O 3.14**).

TERMINE	SIGNIFICATO
Sistema Integrato di FP* (*Integrated FP System*)	Il complesso di *hardware* e *software* che forniscono al personale della *Force Protection* (FP), operante nell'ambito delle aree decisionali (TOC[69] o BDOC[70]), gli elementi necessari per effettuare un'analisi ed una verifica delle informazioni ricevute dai sensori (Elettro-Ottico, radar etc.) che, monitorizzando le aree d'interesse della TAOR della base militare, consente di ottenere le informazioni necessarie (dati e video) per scoprire (*detection*), identificare le possibili minacce (*identification*) e di conseguenza, operare la reazione ritenuta più opportuna (**di nuova introduzione – PTE SIFP**).
Sistema Integrato di Protezione Basi Militari* (SIPROB)	Insieme integrato di assetti, misure, strutture e procedure di FP che interagiscono tra di loro per la difesa delle basi militari nei Teatri di Operazione (**di nuova introduzione – PTE SIFP**).
Sorveglianza (*Surveillance*)	Osservazione sistematica di zone aeree, terrestri, marittime, sottomarine, di località, di persone o di cose, effettuata, a scopo informativo, con mezzi ottici, elettronici, fotografici o altri. La sorveglianza si realizza con determinate modalità (palese, occulta, sistematica, saltuaria, permanente, mirata), al fine di poter anche individuare/prevenire qualsiasi forma di attività/evento ostile, o potenzialmente ostile, al fine di poter eventualmente attivare la catena di allertamento e/o di allarme e predisporre, o far attivare, le previste azioni di reazione e contrasto della minaccia (**PID-O 3.14**).
Sorveglianza Armata*	Forma ibrida che individua tre diverse tipologie di attività: – il personale di sorveglianza (disarmato) si può rapidamente armare in caso di necessità con tempistiche determinate dall'assetto difensivo in vigore; – il personale di sorveglianza (disarmato) è comunque integrato con alcuni elementi armati in modo da poter garantire comunque una reazione immediata; – il mezzo con cui si attua la sorveglianza non si può fisicamente separare dall'armamento, quali ad es. autoblindo, motovedetta, ecc. (**PID-O 3.14**).

[69] *Tactical Operations Center*

[70] *Base Defense Operations Center*

TERMINE	SIGNIFICATO
Supporto del Genio alla FP (*Engineer support to FP – FP Engineering - FPE*)	Insieme delle attività tecniche del genio necessarie per la protezione e la sopravvivenza delle forze in operazioni, ovvero l'insieme di misure e mezzi per ridurre al minimo la vulnerabilità del personale, delle installazioni, dei mezzi durante le operazioni rispetto qualsiasi minaccia ed in ogni circostanza, al fine di preservare la libertà di azione e l'efficienza operativa delle forze" (**PUB. 6365**).
Supporto della nazione ospitante (*Host-Nation Support* - HNS)	Assistenza civile e militare resa in pace, crisi o guerra da una nazione alla NATO e/o altre forze ed organizzazioni NATO che sono dislocate al suo interno, operano all'interno ed all'esterno di esso, o in transito (**AAP-6**).
Ufficiale addetto alla FP* (*Force Protection Officer* - FPO)	Ufficiale delle Varie Armi e Corpi qualificato nella FP e inquadrato nella Cellula S/G/J3 (**di nuova introduzione – AJP 3.14**).
Ufficiale del genio addetto alla FP* (*Force Protection Engineering Officer*- FPEO)	Personale del genio qualificato nella FP inquadrato nella J-Eng o G3-Eng Cell del Comando del Contingente/G.U., ovvero anche in posizione di Advisor FPE del Comandante (**PID-O 3.14**).
Ufficiale addetto alla Sicurezza (*Security Officer*)	Soggetto al quale è attribuito il compito di sovrintendere, coordinare e controllare, nell'ambito dell'Ente, tutte le attività che riguardano la sorveglianza e la sicurezza (**PID-O 3.14**).
Ufficiale Addetto alla Sicurezza del Munizionamento e degli Esplosivi (*Explosive Safety Officer*)	Ufficiale responsabile di fornire consulenza al Comandante su tutte le questioni inerenti alla sicurezza nel settore del munizionamento e degli esplosivi. Deve assicurare in modo efficace, efficiente e sicuro la gestione e l'impiego di munizionamento ed esplosivi presente, a qualsiasi titolo, all'interno dell'installazione ed, ove possibile, ricondurre il relativo rischio a livelli accettabili (**ALP-16, AASTP-5**)
Ufficiale Addetto alla Protezione Ambientale (*Environmental Protection Officer*)	Consulente del Comandante per la Protezione Ambientale (**SMDL-015**).

TERMINE	SIGNIFICATO
Valutazione delle criticità (*Criticality Assessment*)	– Passo del ciclo delle misure di FP che, partendo dagli elementi emersi nel corso dell'analisi della missione, identifica gli elementi critici propri (tangibili e non), dai quali dipende il successo dell'operazione (**PID-O 3.14**). – Passo del ciclo delle misure di FP che, partendo dagli elementi emersi nel corso dell'analisi della missione, identifica gli elementi critici propri (tangibili e non), dai quali dipende il successo dell'operazione: l'identificazione degli assetti/elementi (riferiti al personale, alle infrastrutture, ai materiali, alle informazioni, alle attività, alle linee di comunicazione e all'organizzazione) che sono ritenuti critici per il conseguimento del successo della missione. Essi sono individuati dall'analisi della missione, dalle *assumptions* e dalla linea d'azione scelta. La valutazione delle criticità è, nello stesso tempo, anche una stima e un inventario, quantitativo e qualitativo, degli assetti individuati e ponderati, in termini di importanza (per gli effetti che ci consentono di conseguire) e di possibilità o capacità di protezione (**di nuova introduzione - PID-O 3.14**).
Valutazione della minaccia (*Threat Assessment*)	– Passo del ciclo delle misure di FP necessario per identificare gli assetti e le capacità del nemico, nonché i fattori ambientali che possono ostacolare o influire negativamente sull'azione delle unità amiche, indicando anche le probabilità che questi eventi negativi possano verificarsi (**PID-O 3.14**). – Valutazione che scaturisce dallo sviluppo del ciclo di *intelligence* e del processo di sviluppo cognitivo (*Knowledge Development*), afferisce alle minacce e ai rischi che possono verificarsi sui propri assetti in una area geografica definita. Tale valutazione, include anche l'analisi effettuata dagli specialisti di *counter intelligence*, *counter* IED e di CBRN (**PID-O 3.14**).

TERMINE	SIGNIFICATO
Valutazione del rischio (*Risk Assessment*)	– Passo del ciclo delle misure di FP necessario per: • verificare se tra gli elementi di vulnerabilità dell'organizzazione vi siano quelli già individuati come "critici" e/o quelli che possono condizionare questi ultimi; • stimare quale incidenza può avere sul successo della missione la neutralizzazione, anche parziale, di tali elementi. (**PID-O 3.14**). – Identificazione e valutazione dei rischi come parte delle prime due fasi del processo di gestione dei rischi (**AJP 3.14**).
Valutazione della vulnerabilità* (*Vulnerability Assessment*)	– Passo del ciclo delle misure di FP necessario per definire, comparando gli esiti della valutazione della minaccia con gli elementi (tangibili e non) del proprio dispositivo, quali elementi possono essere realmente influenzati negativamente dalle minacce e dai rischi identificati (**PID-O 3.14**). – Processo di comparazione tra le criticità (elementi tangibili e non), definite durante la valutazione della minaccia, e i rischi individuati ma anche di stima delle possibili conseguenze che il verificarsi di tali rischi sulle singole criticità possono avere sull'intera missione. Maggiori sono gli effetti, tanto più tali elementi sono definibili punti deboli del Contingente. Esistono tre categorie di valutazione delle vulnerabilità: • non-tecnica, condotta da teams di valutazione multidisciplinari ed effettuata a livello operativo; • tecnica, condotta da personale del genio e tecnici specialistici che valutano le vulnerabilità nell'ambito delle rispettive competenze specialistiche; • dinamica, condotta da teams di valutazione multidisciplinari che esaminano la vulnerabilità degli assetti impiegati (**di nuova introduzione – PID-O 3.14**).

TERMINE	SIGNIFICATO
Vigilanza	Attività di sorveglianza con la specifica capacità di poter attuare una reazione, un'azione di contrasto immediato nei confronti di un atto ostile o di una minaccia manifesta con l'impiego delle armi a disposizione. La vigilanza può essere fissa (il personale staziona nella posizione assegnata), mobile (il personale si può muovere per effettuare attività di pattugliamento, controllo e verifica) o dedicata (l'attività di pattugliamento, controllo e verifica è indirizzata unicamente a determinati punti o aree considerate sensibili/critiche/vitali). In tal senso, il servizio di vigilanza, inteso generalmente come attività dissuasiva o di deterrenza, è attuato da personale armato (**PID-O 3.14**).

RIFERIMENTI

PUBBLICAZIONI/NORMATIVE NATO

AJP-3 (B) "*Allied Joint Doctrine for the conduct of Operations*", ed. 2009;
AJP 3.14 (A) "*Allied Joint Doctrine for Force Protection*", ed. 2015;
AJP-3.2 (B) "*Allied Joint Doctrine for Land Operations*", ed. 2011;
AJP 3.3.1 "*Allied Joint Doctrine for Counter–Air*", ed. 2011.
AD 70-1 "ACO *Security Directive*" Edizione 7 gennaio 2008.
AD 80-25 "ACO *Force Protection*", ed. 2009;
Bi-SC 85-1 "*Capability Package Directive*", ed. 2013;
ATP 3.2.2 "*Command and Control of Allied Land Forces*", ed. 2009;
ATP 3.12.1 "*Allied tactical Doctrine for Military Engineering*", ed. 2015;
ATP-3.12.1.1 *Allied Tactical Doctrine for Military Search*, ed. 2015;
STANAG 2122 "*Medical training in first aid, basic hygiene ajd emergency care*" – AemedP-79, ed. 2012;
STANAG 2136 "*Minimum Standards of Water Potability during Field Operations and in Emergency Situation*"-AEmedP-18, ed. 2014;
STANAG 2280 "*Design threat levels and handover procedures for temporary protective structures*", ed. 2015;
STANAG 2409 " NATO Glossary of Medical Terms and Definitions"- AEmedP-13 (A), ed. 2011
STANAG 2561 "*Allied Joint Medical Force Health Protection Doctrine*" - AJMedP-4, ed. 2011;
STANAG 2617 – "ALP-16/*Allied Logistic Publication*" – "*Explosives Safety And Munitions Risk Management* (ESMRM) *in NATO Planning, Training, and Operations*" , Ed. 2015;
STANAG 2618 "*Allied Operational Level Doctrine for Ground Based Air Defence*" - ATP-82(A);
STANAG 4440 "*Allied Ammunition Storage and Transport Publication* AASTP-1 "*Manual of* NATO *Safety Principles for Storage of Military Ammunition and Explosives*", Ed. 2015;
STANAG 4657 "*Allied Ammunition Storage and Transport Publication* -AASTP-5 "NATO *Guidelines for the Storage, Maintenance and Transport of Ammunition on Deployed Missions or Operations*", Ed. 2015;
STANAG 7141 Ed. 5 "Joint NATO *Doctrine For Environmental Protection During* NATO *Led Military Activities*" Ed. 2008;
NATO "*Air and Missile Defence Capstone Document*", ed. 2011;
PFP(NAAG-LCG/7)D(2008)0001 "*Field Accommodation Guide*", ed. 2008.

PUBBLICAZIONI/NORMATIVE NAZIONALI

D.P.R. 15 marzo 2010, n. 90, "Testo Unico delle disposizioni regolamentari in materia di ordinamento militare";
Legge di conversione del 14 luglio 2016 n. 131 del Decreto Legge 16 maggio 2016, n. 67- Proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione, nonché misure urgenti per la sicurezza. Proroga del termine per l'esercizio di delega legislativa;
D.Lgs 152/2006 'Norme in materia ambientale' (Testo Unico Ambiente.);

D.M. 06 Marzo 2008 Individuazione, ai sensi dell'articolo 184, comma 5-bis del decreto legislativo 3 aprile 2006, n. 152, dei sistemi d'arma, dei mezzi, dei materiali e delle infrastrutture direttamente destinati alla difesa militare e alla sicurezza nazionale;
D.M. Difesa 22 Ottobre 2009 Gestione dei materiali e dei rifiuti e la bonifica dei siti e delle infrastrutture direttamente destinati alla difesa militare e alla sicurezza nazionale;

Decreto Ministeriale del 10/03/1998 "Criteri generali di sicurezza antincendio e per la gestione dell'emergenza nei luoghi di lavoro";
Codice Ordinamento militare (D.Lgs 15 Marzo 2010, Titolo VII, Capo II, Ambiente);
Pub. SMD-G-014 - "Manuale di Diritto Umanitario", ed. 1991;
Pub. SMD-L-104 -"La politica, il programma e le direttive ambientali della Difesa", ed. 2001;
Pub. SMD L-015 'La politica, i programmi e la direttiva ambientale della difesa' (Ed.2011);
PID-O 3.14 "La Protezione delle Forze", SMD III CID, ed. 2012;
Nota Dottrinale "Il contrasto alla minaccia interna (*Insider threat – Green on Blue*), SME, ed. 2013;
Direttiva sulla sicurezza delle installazioni militari, SME, ed. 2000;
Pub. PIE 3.30 "Impiego dell'Artiglieria Controaerei", ed. 2015;
Pub. 6365 "Impiego del Genio", ed. 2015;
Pub. 6450 "Impiego del plotone e della squadra di fanteria", ed. 2015;
Pub. 6461 "Manuale per l'impiego delle minori unità al combattimento nei centri abitati", ed. 1991;
Pub. 6560 "Le pattuglie" ed. 1996;
Pub. 6622 "Impiego della squadra e nuclei tiratori scelti", ed. 2015;
Pub. n. 6838 "Lineamenti d'impiego dei sistemi integrati per la protezione delle basi militari", edizione 2014;
Pub. 6838 "Lineamenti d'impiego dei sistemi integrati di *Force Protection*", ed. 2014;
Concetto d'Impiego *Mission Need Urgent Requirement* "Incremento del livello di protezione delle FOB/FSB nel Te. Op. Afghanistan" – SME, 2011;
ILE-NL-4130-0028-12-00B01 Norme e procedure relative al servizio sanitario in corso di operazioni.
SOP "Tecniche e procedure per la progettazione di contingenza di opere del genio", ed. 2014;
SOP "Protezione di persone, attività e beni in caso di detonazione in campo aperto di ordigni esplosivi ed esplosivi in genere", ed. 2014;
Vademecum sulle misure di protezione del personale contro rischi di natura ambientale e CBRN", ed. 2009.

BIBLIOGRAFIA

ATTP 3.39-32 "*Physical Security*", U.S. Army HQ, ed. 2010;
FM 3-37 "Protection", US Army HQ, ed. 2009;
FM 3.37.2 "Antiterrorism", ed. 2011;
ATTP 3.39-32 "Physical security", U.S. Army HQ, ed. 2010;
"*Reference manual to mitigate potential terrorist attacks against buildings*", US Department of Homeland Security, ed. 2003;
"*Vehicle Bomb Mitigation Guide*", US Air Force Handbook, ed. 2006;
"*Joint Forward Operations Base (JFOB) Force Protection Handbook*", U.S. Center for Army Lessons Learned, ed. 2007;

"*Base Defense, Tactics, Techniques and Procedures*", U.S. Center for Army Lessons Learned, ed. 2007;
"*Building Vulnerability in Relation to Terrorist Attacks with Explosives*", Istituto Ricerche Esplosivistiche di Parma, ed. 2008;
"Afghanistan: rischi sanitari e misure di prevenzione", 1° Reparto Centro Studi e Ricerche di Sanità e Veterinaria dell'Esercito;
"Linee guida per la programmazione dell'educazione Sanitaria in ambito Esercito Italiano";
"*Guidelines on the Use of Military and Civil Defence Assets to Support United Nations Humanitarian Activities in Complex Emergencies*", ed. March 2003.

PAGINA INTENZIONALMENTE BIANCA

M_D E25200 REG2017 0008103 08-03-2017

COMANDO PER LA FORMAZIONE, SPECIALIZZAZIONE E DOTTRINA DELL'ESERCITO

SM – Ufficio Dottrina

Indirizzo telegrafico: COMFORDOT DOTTRINA - ROMA

Prot. n. MD_E 25200/ /D.CSCSS/1.3
Allegati: 1

00143 Roma,
Ten.Col. A. D'Agostino ☎ 105.6630
casezdotcscss@comfordot.esercito.difesa.it

OGGETTO: PSE[1] 3.14.05.02 "La Protezione delle basi militari in operazioni" – Ed. 2017.

ELENCO INDIRIZZI IN ALLEGATO

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

Rif.:

a. Circolare 7005 "Modalità di sviluppo del corpo dottrinale dell'Esercito Italiano", Ed. 2016 di SME;
b. Circolare 1001 "Modalità per l'approntamento delle pubblicazioni dell'Esercito Italiano", Ed. 2016 di SME;

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

1. Questo Comando, in qualità di Ente Editore delle PSE, ha approvato la versione 2 della pubblicazione in oggetto, disponibile per la consultazione sul sito Istituzionale[2].
2. La pubblicazione:
   - abroga e sostituisce la:
     - PSE 3.14.1 "La Protezione delle basi militari in operazioni", Ed. 2015;
     - N. 6712 Manuale sulla protezione delle infrastrutture e delle basi militari nell'ambito delle *Crisis Response Operations*, Ed. 2012;
   - recepisce le linee guida della recente pubblicazione NATO, AJP 3.14 (A) vers. 1 *Allied Joint Doctrine for Force Protection*, Ed. 2015;
   - fornisce i principi e i concetti generali per organizzare la protezione di qualsiasi base militare in operazioni attraverso l'applicazione del processo di *risk management* (gestione del rischio);
   - illustra le forme di protezione da adottare per definire le azioni e misure necessarie per fronteggiare le minacce e i pericoli identificati;
   - è applicabile in qualunque contesto operativo.
3. Al fine di consentire la più ampia diffusione della citata pubblicazione, si chiede:
   - allo Stato Maggiore dell'Esercito, III RPG SM – Ufficio Dottrina e Lezioni Apprese, di inserirla sul proprio portale e, data la spiccata "valenza interforze" del documento[3],

---

1 Pubblicazione di Supporto Dell'Esercito.

2 http://www.sme.esercito.difesa.it/siti/comfordot/Pagine/PUBBLICAZIONI-DOTTRINA.aspx?RootFolder=%2Fsiti%2Fcomfordot%2FPUBBLICAZIONI%2FPSE%20%28Pubblicazioni%20di%20Supporto%20dell%27Esercito%29&FolderCTID=0x01200022D4852F9713B646803C3DACC19530B5&View=%7b3B8C2

Digitally signed by MICHELE PELLEGRINO
Date: 2017.03.08 14:13:01 CET

di darne comunicazione allo Stato Maggiore della Difesa, segnalando l'abrogazione della pub. n. 6712 "Manuale sulla protezione delle infrastrutture e delle basi militari nell'ambito delle *Crisis Response Operations*";

– ai Comandi in indirizzo di diramarla a tutti gli Enti dipendenti.

d'ordine
IL CAPO DI STATO MAGGIORE
(*Gen. D. Michele PELLEGRINO)*

[3] La PSE 3-14.05.02, in aderenza a quanto riportato nella già cit. PID-O 3.14, rappresenta il nuovo documento di riferimento, a livello tattico-operativo, per la realizzazione delle opere di protezione delle basi militari semipermanenti/permanenti, delle basi operative avanzate e degli accampamenti nelle operazioni di risposta alle crisi fuori dal territorio nazionale.

ELENCO INDIRIZZI

A STATO MAGGIORE DELL'ESERCITO
III RPG– Ufficio Dottrina e Lezioni Apprese — ROMA

COMANDO FORZE OPERATIVE TERRESTRI - COE — ROMA

COMANDO LOGISTICO DELL'ESERCITO — ROMA

COMANDO MILITARE DELLA CAPITALE — ROMA

COMANDO FORZE OPERATIVE NORD — PADOVA

COMANDO FORZE OPERATIVE SUD — NAPOLI

COMANDO TRUPPE ALPINE — BOLZANO

COMANDO FORZE OPERATIVE TERRESTRI DI SUPPORTO — VERONA

NRDC-ITA — SOLBIATE OLONA

COMANDO PER LE FORZE SPECIALI DELL'ESERCITO — PISA

COMANDO PER LA FORMAZIONE E SCUOLA DI APPLICAZIONE DELL'ESERCITO — TORINO

CENTRO DI SIMULAZIONE E VALIDAZIONE DELL'ESERCITO — CIVITAVECCHIA

COMANDO SCUOLA DI FANTERIA — CESANO DI ROMA

COMANDO SCUOLA DI CAVALLERIA — LECCE

COMANDO SCUOLA INTERFORZE PER LA DIFESA NBC — RIETI

COMANDO SCUOLA DI COMMISSARIATO — MADDALONI

COMANDO SCUOLA DI SANITA' E VETERINARIA — ROMA

COMANDO COMPRENSORIO "CECCHIGNOLA" — ROMA

COMANDO GENIO — ROMA

Diramazione interna:

UFFICIO DEL COMANDANTE

UFFICIO DEL CAPO DI STATO MAGGIORE

UFFICIO DEL SOTTOCAPO DI SM OPERATIVO

UFFICIO DEL SOTTOCAPO DI SM SUPPORTO

SM – UFFICIO LOGISTICO

SM – UFFICIO ADDESTRAMENTO E STUDI

SM – UFFICIO FORMAZIONE E SPECIALIZZAZIONE

SM – UFFICIO SICUREZZA

SM – UFFICIO PERSONALE

SM – UFFICIO AFFARI GENERALI

SZ. – PIANIFICAZIONE PROGRAMMAZIONE E BILANCIO