



# STATO MAGGIORE DELLA DIFESA

## III REPARTO

### Centro Innovazione della Difesa



## PID/O-3.14

## LA PROTEZIONE DELLE FORZE

## ANNESI

## Edizione 2012



# **ANNESSI**



## PREMESSA

La complessità dello scenario internazionale e l'instabilità di alcune aree geografiche, specialmente quelle nel cosiddetto Mediterraneo Allargato, richiedono sempre più frequentemente il coinvolgimento diretto delle Forze Armate italiane, inserite in Alleanze o Coalizioni, chiamate a pianificare e condurre operazioni che assumono sempre più spesso il carattere *expeditionary*. La crescente aspettativa della società italiana di veder concretizzato il cosiddetto "rischio zero" nell'impiego dei propri uomini e donne in operazioni militari pone in primo piano l'importanza e la complessità di come proteggere i propri assetti impiegati. La *Protezione delle Forze* è divenuta, *de facto*, una capacità fondamentale atta ad impedire all'avversario di minacciare direttamente quello che, nella maggioranza dei casi, è individuabile quale il Centro di Gravità (*Centre of Gravity*) per eccellenza, cioè la "capacità di mantenere il consenso e l'unitarietà degli intenti alle Forze della Coalizione".

Il presente documento intende, quindi, definire gli elementi essenziali della funzione operativa *Protezione delle Forze*, contestualizzandone i contenuti al moderno ambiente operativo e, in tal modo, costituire il riferimento dottrinale per i Comandanti e i loro *staff* per la pianificazione, l'organizzazione e lo sviluppo delle attività afferenti alla funzione in parola. Esso è coerente con le linee guida e le direttive strategiche della Difesa<sup>1</sup>, si ispira alla dottrina generale della NATO<sup>2</sup> nonché alla specifica dottrina NATO relativa all'argomento<sup>3</sup>.

Tenuto conto delle innumerevoli attività che concorrono alla *Protezione delle Forze* e degli attuali e futuri ambienti operativi<sup>4</sup> nei quali i contingenti nazionali sono o saranno chiamati ad operare, il documento è stato redatto in forma "non classificata controllata" allo scopo di consentirne un'ampia diffusione e una più facile consultazione. Per lo stesso motivo è da considerarsi come un *living document*. Esso è stato strutturato in:

- un testo principale riguardante i concetti generali, il ciclo di protezione delle forze quale metodo di riferimento, gli aspetti relativi al Comando e Controllo con le connesse responsabilità da parte della figura del Comandante;
- diversi annessi e appendici relativi allo sviluppo di particolari aree di capacità e secondo specifiche esigenze di Componente, che rappresentano le sottofunzioni di supporto alla funzione operativa interforze Protezione delle Forze (Tutela amministrativa del Segreto di Stato e delle informazioni classificate, Supporto del Genio alla Protezione delle Forze, Protezione delle Infrastrutture/Controaviazione Difensiva, Protezione Sanitaria e Ambientale, Gestione delle emergenze - *Consequence Management* - Difesa CBRN e Protezione dell'Ambiente Cibernetico).

Le Lezioni Apprese, maturate attraverso le esperienze in Teatro Operativo da parte dei

<sup>1</sup> "Direttiva Ministeriale in merito alla politica militare per l'anno 2013", Nota aggiuntiva allo stato di previsione per la Difesa per l'anno 2013" Ed. ottobre 2012, "Il Concetto Strategico del Capo di SMD" Ed. 2004-2006, e "La Dottrina Militare italiana" (PID/S-1) Ed. 2011, che inquadrano la "Sopravvivenza e la Protezione delle Forze" tra le capacità operative fondamentali.

<sup>2</sup> AJP-01(D) "*Allied Joint Doctrine*"; AJP-02 "*Allied Joint Doctrine for Intelligence*"; AJP-3(B) "*Allied Joint Doctrine for the conduct of Operations*"; AJP-5 "*Allied Joint Doctrine for Operational Level Planning*"; ACO "*Force Protection Directive 80-25*".

<sup>3</sup> AJP-3.14 "*Allied Joint Doctrine for Force Protection*".

<sup>4</sup> "Le implicazioni militari dei futuri ambienti operativi" – *Capstone Concept 001*, III Reparto dello Stato Maggiore della Difesa, Centro Innovazione della Difesa, edizione 2012.

Contingenti nazionali sia da quelli alleati, costituiscono la base principale per il tempestivo e continuo processo di aggiornamento della presente pubblicazione.

**INDICE**

<b>Premessa</b> .....	<b>V</b>
<b>Indice delle figure</b> .....	<b>XIV</b>
<b>Annesso “1”- Tutela amministrativa del segreto di Stato e delle informazioni classificate</b> .....	<b>1</b>
1. Premessa.....	1
2. Organizzazione di sicurezza.....	2
a. Strutture di Sicurezza.....	2
b. Responsabilità e competenze per la Sicurezza .....	3
c. Campo di applicazione .....	3
3. Pianificazione e programmazione della attività volte alla tutela amministrativa del segreto di Stato e delle informazioni classificate .....	3
a. I Piani di Sicurezza .....	4
b. Regolamento Interno di Sicurezza.....	4
c. Regolamento Interno di Sicurezza EAD di Ente (eventuale) .....	5
d. I Piani di Emergenza.....	5
e. Indottrinamento.....	6
4. La sicurezza del personale.....	6
a. Premessa .....	6
b. Attribuzioni, competenze, responsabilità .....	6
5. Sicurezza fisica.....	7
a. Premessa .....	7
b. La sicurezza fisica per le Informazioni classificate.....	8
c. Responsabilità e compiti.....	10
d. Misure di Sicurezza materiale specifiche ed attrezzatura approvata .....	10
6. Sicurezza delle comunicazioni, della cifra e dei sistemi EAD (INFOSEC) .....	11
a. Premessa .....	11
b. Obiettivi .....	11
c. Sicurezza della documentazione e gestione dei supporti EAD removibili.....	13
d. Norme per la conservazione e utilizzo dei supporti EAD removibili.....	13
e. Distruzione dei mezzi di supporto EAD.....	14
<b>Appendice “1” all’Annesso “1” - Il contributo dell’Arma dei Carabinieri alla dimensione sicurezza</b> .....	<b>15</b>
1. L’ambiente operativo tipico nella dimensione <i>security</i> .....	15
2. Principi e fattori delle operazioni nella dimensione <i>security</i> .....	16
a. Generalità.....	16
b. L’attività informativa.....	16

c. L'attività di dissuasione .....	17
d. La prevenzione della conflittualità .....	17
3. Criteri generali per l'applicazione delle misure di <i>Force Protection</i> .....	17
a. Generalità.....	17
b. Le forze di sicurezza.....	18
c. La componente di soccorso .....	18
d. La protezione .....	18
4. Applicazione del modello <i>Force Protection</i> nella dimensione <i>Security</i> .....	18
a. Capacità .....	18
b. Capacità tipiche della dimensione <i>security</i> .....	19
c. Il Comando e Controllo della FP per le operazioni nella dimensione <i>security</i> .....	20
d. Elementi generali di <i>security</i> nella FP dei luoghi militari .....	21
<b>Annesso "2" - La <i>Force Protection Engineering</i> e la protezione delle infrastrutture - Controaviazione difensiva .....</b>	<b>23</b>
<b>Parte I – Principi e caratteristiche .....</b>	<b>23</b>
1. Premessa.....	23
2. Generalità .....	23
3. Campi di applicazione .....	24
4. Obiettivi.....	24
5. Requisiti.....	25
6. Pianificazione .....	25
7. Criteri.....	30
<b>Parte II – Funzionalità di componente.....</b>	<b>.....</b>
<b>Sezione I – Esercito.....</b>	<b>33</b>
1. Generalità .....	33
2. Organizzazione di Comando e Controllo della FP .....	34
3. Sistema di protezione delle forze .....	34
4. Il supporto del Genio .....	36
5. L'impiego delle specialità del Genio.....	39
a. Guastatori.....	39
b. Pionieri.....	39
c. Pontieri e Ferrovieri .....	40
6. La realizzazione delle opere di protezione .....	40
<b>Sezione II – Marina .....</b>	<b>45</b>
1. La "minaccia ibrida" contro le forze marittime.....	45
a. Minaccia subacquea.....	46
b. Minaccia di superficie.....	46



## INFORMAZIONI NON CLASSIFICATE CONTROLLATE

c. Minaccia proveniente da terra .....	46
d. Minaccia proveniente dall'aria .....	47
e. Minaccia di tipo "stand off" .....	47
f. Minaccia di tipo "CBRN" .....	47
g. Minaccia per le "Information operations/C2" .....	48
2. Principi fondamentali per la FP in ambito Marina .....	48
a. Sicurezza Preventiva .....	48
b. Difesa Attiva .....	49
c. Difesa Passiva .....	49
d. Capacità di Recupero .....	49
3. Livelli di responsabilità .....	50
4. Organizzazione <i>Force Protection</i> di bordo .....	50
<b>Sezione III - Aeronautica .....</b>	<b>53</b>
1. Generalità .....	53
2. Principali capacità della protezione delle forze per le operazioni aeree .....	53
a. Sicurezza Protettiva .....	54
b. Difesa Attiva .....	54
c. Difesa Passiva .....	57
d. Recupero della Capacità Operativa .....	58
3. Altre capacità essenziali .....	59
<b>Appendice "1" all'Annesso "2" – Ciclo delle attività per la realizzazione delle opere di FPE .....</b>	<b>60</b>
<b>Appendice "2" all'Annesso "2" – Attribuzioni di competenze e responsabilità nella realizzazione di opere di FPE .....</b>	<b>61</b>
<b>Appendice "3" all'Annesso "2" - La minaccia IED.....</b>	<b>63</b>
1. Introduzione.....	63
2. Obiettivi strategici del C-IED.....	64
3. Il C-IED nell'ambito della forza <i>Joint</i> .....	65
4. Elementi per un efficace approccio C-IED .....	65
5. Protezione delle forze e della popolazione.....	66
6. Fattori abilitanti C-IED .....	66
<b>Annesso "3" - La protezione sanitaria delle forze .....</b>	<b>71</b>
1. Introduzione.....	71
a. Generalità.....	71
b. Definizione .....	71
2. Processo di protezione sanitaria della forza .....	71
a. Generalità.....	71
b. Fasi del processo di Protezione Sanitaria della Forza .....	72

INFORMAZIONI NON CLASSIFICATE CONTROLLATE

## INFORMAZIONI NON CLASSIFICATE CONTROLLATE

3. Comando e Controllo .....	74
a. Responsabilità.....	74
b. Comandi schierati .....	74
c. Sistemi di comunicazione e informazione.....	74
4. Aspetti specifici della protezione sanitaria della forza.....	75
a. Sorveglianza Sanitaria ed epidemiologica.....	75
b. Misure di medicina preventiva .....	77
c. Misure di igiene campale, alimentare, idrica e di medicina veterinaria .....	80
d. Attività di promozione della salute.....	81
e. Minacce di carattere chimico, biologico, radiologico e nucleare (CBNR).....	82
f. Rischi sanitari occupazionali, ambientali ed industriali .....	82
5. Formazione e addestramento .....	83
a. Formazione e addestramento individuale .....	83
b. Formazione e addestramento del personale “chiave” .....	83
c. Formazione e addestramento di <i>Staff</i> .....	83
d. Formazione e addestramento collettivo .....	83
<b>Annexo “4” - La protezione dell’ambiente .....</b>	<b>85</b>
1. Premessa.....	85
2. Generalità .....	86
3. La politica ambientale .....	87
a. Precedenti storici .....	87
b. La politica ambientale nazionale .....	88
c. Terminologia di riferimento .....	89
<b>Sezione I – Esercito.....</b>	<b>91</b>
1. La protezione dell’ambiente.....	91
a. Generalità.....	91
b. La valutazione dell’impatto ambientale.....	91
2. La protezione dell’ambiente in guarnigione.....	93
a. Generalità.....	93
b. La protezione dell’ambiente in guarnigione .....	93
3. La protezione dell’ambiente in addestramento ed in esercitazione.....	94
a. Generalità.....	94
b. Predisposizioni afferenti alla protezione dell’ambiente in addestramento ed in esercitazione .....	94
4. La protezione dell’ambiente in operazioni .....	97
a. Generalità.....	97
b. La protezione ambientale in operazioni.....	97

## INFORMAZIONI NON CLASSIFICATE CONTROLLATE

5. La protezione dell'ambiente in attività logistiche .....	100
a. Generalità.....	100
b. Emissione di gas nell'atmosfera .....	101
c. Contaminazione di acque.....	101
d. Rilascio di sostanze e rifiuti (tossici e non).....	101
e. Spargimento di carburanti e lubrificanti .....	102
6. Aspetti connessi con la protezione dall'ambiente .....	102
a. Protezione da eventi naturali .....	102
<b>Appendice "1" all'Annesso "4" - Sezione Esercito - Decalogo ambientale del militare</b>	<b>109</b>
<b>Appendice "2" all'Annesso "4" - Sezione Esercito - Lista di controllo per l'occupazione di un'area addestrativa .....</b>	<b>111</b>
<b>Appendice "3" all'Annesso "4" - Sezione Esercito - Schema per la stesura dell'Allegato "Tutela ambientale" all'ordine di operazione .....</b>	<b>113</b>
<b>Appendice "4" all'Annesso "4" - Sezione Esercito - Scheda notizie poligono/area addestrativa.....</b>	<b>115</b>
<b>Appendice "5" all'Annesso "4" - Sezione Esercito - Norme pratiche per la realizzazione di un deposito carburanti e lubrificanti in campagna.....</b>	<b>117</b>
<b>Appendice "6" all'Annesso "4" - Sezione Esercito - Norme per la realizzazione di un deposito temporaneo di rifiuti in campagna .....</b>	<b>119</b>
<b>Appendice "7" all'Annesso "4" - Sezione Esercito - Norme per la raccolta e trattamento degli oli e dei grassi vegetali ed animali esausti in campagna .....</b>	<b>121</b>
<b>Sezione II - Marina .....</b>	<b>123</b>
1. Generalità .....	123
2. Quadro giuridico: "Normativa antinquinamento" .....	123
3. La Marina Militare a difesa dell'ambiente marino - L'attività delle Capitanerie di Porto .....	125
4. La Marina Militare a difesa dell'ambiente marino - La gestione dei rifiuti sulle navi militari .....	126
a. Certificazione MARPOL .....	127
b. La tipologia dei rifiuti .....	127
c. Lo scarico dei rifiuti all'interno delle acque territoriali e nelle acque portuali .....	133
<b>Sezione III - Aeronautica .....</b>	<b>135</b>
1. Generalità .....	135
2. Idrocarburi alogenati e HALONS .....	135
a. Generalità.....	135
b. Principali riferimenti normativi .....	136
c. Adempimenti e obblighi .....	136
3. Rumore .....	137
a. Generalità.....	137

## INFORMAZIONI NON CLASSIFICATE CONTROLLATE

b. Valori Limite (Zonizzazione) .....	137
c. Criterio differenziale.....	138
d. Principali adempimenti ed obblighi.....	139
4. Gestione materiali pericolosi, agenti chimici, serbatoi e cisterne interrate.....	139
a. Agenti pericolosi e agenti chimici .....	139
b. Serbatoi e cisterne interrate .....	140
c. Procedure in caso di incidente/inconveniente.....	141
<b>Annexo “5” - La gestione delle emergenze (<i>Consequence Management</i>) .....</b>	<b>143</b>
1. Premessa.....	143
2. Generalità .....	143
3. Il piano di emergenza CM .....	144
a. Scenari degli eventi attesi .....	145
b. Modello di intervento .....	146
4. Gestione del rischio .....	146
5. Realizzazione del piano di emergenza CM .....	147
a. Impatto e conseguenze.....	147
b. Risorse richieste.....	147
c. Addestramento ed esercitazioni.....	148
6. Gestione degli effetti di un evento disastroso (risposta all’incidente) .....	148
a. Fase 1 – Valutazione e preparazione .....	148
b. Fase 2 – Assistenza immediata.....	149
c. Fase 3 – Operazioni di CM a lungo effetto.....	149
7. Revisione dei controlli e delle misure .....	149
8. Il Comando e Controllo.....	150
<b>Annexo “6” - La Difesa CBRN.....</b>	<b>151</b>
1. Introduzione.....	151
2. Componenti della Difesa CBRN .....	152
a. Individuazione, identificazione e monitoraggio ( <i>Detection, Identification and Monitoring - DIM</i> ) .....	152
b. Preavviso e segnalazione CBRN ( <i>CBRN Warning &amp; Reporting</i> ).....	152
c. Protezione fisica ( <i>Physical Protection</i> ) .....	152
d. Gestione del Pericolo ( <i>Hazard Management</i> ) .....	152
e. Sostegno sanitario e contromisure di natura sanitaria ( <i>Medical Countermeasures and Support</i> ).....	153
3. Rischio CBRN.....	153
a. Armi chimiche .....	154
b. Armi biologiche.....	154
c. Armi radiologiche.....	155

## INFORMAZIONI NON CLASSIFICATE CONTROLLATE

d. Armi nucleari .....	155
e. Sostanze tossiche di origine industriale .....	155
4. Principi di <i>Force Protection</i> e componenti della difesa CBRN .....	158
a. Principi di <i>Force Protection</i> applicati alla difesa CBRN .....	158
b. Componenti della difesa CBRN .....	158
5. Livelli di difesa CBRN (individuale/unità/unità specialistiche) .....	163
a. Individuale .....	163
b. Unità operativa.....	163
c. Unità specialistica NBC.....	164
6. Aspetti legati all'ambiente navale ed aereo.....	164
a. Ambiente Navale .....	164
b. Ambiente Aereo.....	166
7. Elementi di particolare interesse per la condotta di operazioni in ambiente CBRN...	167
a. Livelli di minaccia .....	167
b. Attivazione della rete di segnalazione e preavviso.....	168
c. Sorveglianza CBRN.....	168
d. Gestione dell'esposizione ai pericoli CBRN .....	168
e. Sostegno logistico .....	170
<b>Annesso "7" - La protezione dell'ambiente cibernetico.....</b>	<b>173</b>
1. Introduzione.....	173
2. Elementi dello spazio cibernetico.....	173
3. Gestione operativa.....	175



## INDICE DELLE FIGURE

<b>Figura 1</b> <i>Organizzazione di Sicurezza</i> .....	3
<b>Figura 2</b> <i>Analisi del rischio</i> .....	10
<b>Figura 3</b> <i>Il processo di revisione delle misure di FP</i> .....	25
<b>Figura 4</b> <i>La pianificazione FPE</i> .....	27
<b>Figura 5</b> <i>La Valutazione della vulnerabilità</i> .....	28
<b>Figura 6</b> <i>I passi del piano di FP</i> .....	29
<b>Figura 7</b> <i>Composizione JOA</i> .....	35
<b>Figura 8</b> <i>Aree funzionali per la difesa</i> .....	36
<b>Figura 9</b> <i>Capacità della protezione delle forze per le operazioni aeree</i> .....	59
<b>Figura 10</b> <i>Integrazione del FHP nell'ambito del modello FP</i> .....	72
<b>Figura 11</b> <i>L'iceberg delle malattie</i> .....	76
<b>Figura 12</b> <i>Azioni in caso di incidente con carbolubrificanti</i> .....	142





## TUTELA AMMINISTRATIVA DEL SEGRETO DI STATO E DELLE INFORMAZIONI CLASSIFICATE<sup>5</sup>

### 1. Premessa

Il presente annesso stabilisce i principi fondamentali in materia di sicurezza che gli Enti devono applicare per garantire un comune livello di protezione alle informazioni classificate ed assicurare, di riflesso, anche la necessaria ed opportuna protezione delle forze schierate.

Il concetto di *Security* verrà trattato non come singolo prodotto o soluzione, bensì come un processo che coinvolge, in ogni suo aspetto, l'organizzazione della Difesa, quale struttura chiamata ad applicare misure e procedure protettive secondo la normativa nazionale o internazionale (prevalentemente NATO). Quanto sopra per impedire e/o scoprire l'eventuale perdita delle informazioni classificate, ricercando soprattutto l'adozione delle necessarie precauzioni per escludere il ripetersi di simili eventi.

La tutela delle informazioni, in particolar modo di quelle classificate, è diventata un elemento cruciale delle operazioni correnti e, di conseguenza, assume una rilevanza strategica sia la protezione dei luoghi, sia dei sistemi e delle persone che a qualsiasi titolo trattano o gestiscono dati classificati.

Tale protezione assume, in generale, uguale rilevanza per la trattazione di dati su formato cartaceo e per l'*Information and Communication Technology* (ICT), dove le informazioni vengono gestite in forma digitale. In entrambi i casi, è necessaria la scrupolosa applicazione di procedure operative che riescano a prevenire dannose conseguenze qualora tali informazioni dovessero entrare in possesso di persone malintenzionate o compromesse.

È palese che gli scenari in cui opera lo strumento militare sono caratterizzati da un elevato numero di rischi diversificati per tipo, dimensioni, punti di applicazione e provenienza. Pertanto, al fine di garantire alla propria struttura una cornice di tutela informativa “sicura”, la ricerca di forme idonee a valutare l'entità della minaccia avversaria<sup>6</sup> diventa il *focal point* dell'intero sistema.

Nel merito della categorizzazione della minaccia, si dovrà, altresì, tenere conto sia di azioni esterne alla propria organizzazione - derivanti da spionaggio, terrorismo, sabotaggio, crimine organizzato - ma anche da quelle provenienti da errori accidentali, compiuti da appartenenti all'organizzazione stessa, che comportano il rilascio non autorizzato dell'informazione.

La “minaccia”, relazionata alla “vulnerabilità”, determina, di fatto, il “rischio” per l'intera organizzazione laddove la prima costituisce un parametro fisso, rappresentato dall'incombente forma di pericolo proveniente da un altro attore (Stato, coalizione o gruppo ostile, soggetti, ecc.), mentre la seconda riguarda la debolezza propria della struttura e, quindi, un parametro su cui è possibile porre delle modifiche. La variazione di quest'ultima, in particolare, avrà

---

<sup>5</sup> Nel contesto del DPCM in data 22 luglio 2011, è definita “sicurezza delle informazioni”: “la salvaguardia e la continua e completa protezione delle informazioni classificate o coperte da segreto di Stato, attraverso l'adozione di norme e procedure, organizzative ed esecutive, nei settori delle abilitazioni di sicurezza, della sicurezza fisica, della tecnologia delle informazioni e delle comunicazioni”. Nel contesto del presente annesso, si è preferito evitare l'utilizzo del termine “sicurezza delle informazioni” per evitare fraintendimenti con la specificità delle attività INFOSEC.

<sup>6</sup> Sotto questo punto di vista, la valutazione dell'entità della minaccia avversaria è orientata a identificare forme di pericolo reale o potenziale che, nel caso si concretizzassero, produrrebbero un grave danno al patrimonio informativo.

un’incidenza diretta sul rischio. L’organizzazione di sicurezza dovrà, pertanto, adoperarsi al fine di contenere il “livello di rischio” entro un valore che risulti accettabile per il Comandante, individuando tutte quelle contromisure necessarie a rendere le informazioni impenetrabili e sicure in funzione della situazione operativa contingente.

Per assicurare che le contromisure individuate possano realmente essere efficaci, è indispensabile integrare la struttura organizzativa esistente con una rete di responsabilità specifiche sulla sicurezza e condividere una serie di principi e regole che devono essere conosciute da tutti i membri dell’organizzazione.

## **2. Organizzazione di sicurezza**

Ogni Comandante, che ha la necessità di trattare informazioni classificate/qualificate, ha l’obbligo di dotarsi di un’organizzazione finalizzata alla protezione del patrimonio informativo, quest’ultima configurata in ottemperanza alla normativa applicabile per la specifica missione (Nazionale/NATO/UE/di coalizione, ecc.).

In sostanza, si tratta di un’architettura composta da singoli soggetti e da strutture organizzative, ordinata in base ad un’articolazione gerarchica che, attraverso livelli ordinativi intermedi, giunge sino all’Organo Centrale di Sicurezza (OCS)<sup>7</sup> il cui obiettivo è garantire il pieno e costante rispetto delle normative afferenti alla tutela delle informazioni classificate. Nelle operazioni, la trattazione di documenti e materiale classificato deve essere effettuata secondo procedure organizzative ed esecutive opportunamente integrate da idonee misure di protezione fisica<sup>8</sup>.

Di massima, si dovrà provvedere alla:

- individuazione di misure di sicurezza, a prescindere dall’impiego del singolo Ente/Comando, in linea con la “missione istituzionale della Difesa”;
- definizione di ruoli e responsabilità degli elementi organizzativi che compongono la struttura di sicurezza operanti all’interno dell’Ente;
- indicazione delle procedure per la protezione delle informazioni classificate/qualificate;
- creazione di un sistema documentale che consenta di garantire la continuità operativa dei processi vitali dell’Ente, tenendo conto del parametro “sicurezza”.

### **a. Strutture di Sicurezza**

L’organizzazione per la Sicurezza, o *Information Security Management System*, rappresenta un insieme di responsabilità, ruoli organizzativi, modalità operative, istruzioni e sistemi che consentono l’operatività di un Ente e si concretizza nell’attività combinata di strutture articolate sia in funzione del proprio livello ordinativo, sia della tipologia e della qualità delle informazioni trattate. Tali strutture rappresentano, pertanto, i gangli attraverso i quali si realizza il sistema gestionale per la tutela amministrativa del segreto di Stato e delle

---

<sup>7</sup> È il complesso costituito – a livello di un Ministero, Forza o Ente – dall’Ufficiale alla Sicurezza, dal Capo della Segreteria Principale di Sicurezza, dall’Ufficiale COMSEC, dall’Ufficiale alla Sicurezza EAD, dall’Ufficiale alla Sicurezza Fisica, dalla Segreteria Principale di Sicurezza, dal Centro e dal Custode del materiale CIFRA.

<sup>8</sup> DPCM 22 luglio 2011, Direttiva PCM-ANS 6/2006 e per i Teatri Operativi “Direttiva per la protezione e tutela delle informazioni classificate nei Teatri Operativi” (SMD RIS SIC 002) Ed. 2008.

informazioni classificate, principalmente individuati nell’Organo Centrale di Sicurezza (OCS) ed Organo Periferico di Sicurezza (OPS)<sup>9</sup>.

**b. Responsabilità e competenze per la Sicurezza**

Ciascun organo sopraccitato applica i correlati principi normativi, attribuendo determinate responsabilità agli individui selezionati dal Comandante, sulla base dei criteri di affidabilità

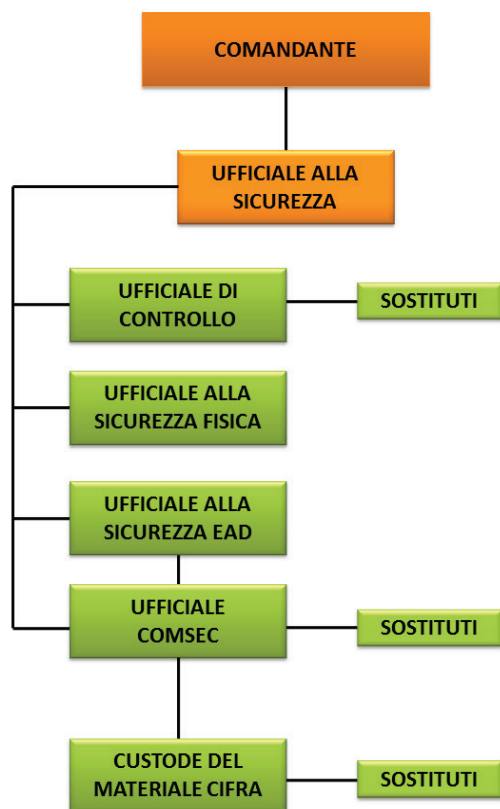


Figura 1 Organizzazione di Sicurezza

delle informazioni classificate”. Tale normativa costituisce il quadro normativo di riferimento base applicabile a tutte le missioni in cui lo strumento militare è chiamato ad operare e dove sussiste la necessità di ricevere/ trattare/partecipare informazioni classificate. Per le strutture esecutive di sicurezza schierate nei Teatri Operativi la dipendenza risale allo SMD-RIS per il tramite del COI DIFESA, quando il controllo Operativo è delegato al COI.

**3. Pianificazione e programmazione della attività volte alla tutela amministrativa del segreto di Stato e delle informazioni classificate**

L’architettura di un sistema gestionale per la tutela amministrativa del segreto di Stato e delle informazioni classificate, si realizza attraverso un processo analitico che, in armonia con le Direttive emanate dall’OCS, è finalizzato all’adeguamento delle proprie componenti, secondo

e di competenza in materia di sicurezza, a fronte dell’autorizzazione rilasciata dal proprio Organo Centrale di Sicurezza.

In particolare, il Comandante, per l’espletamento delle proprie funzioni nello specifico settore, può avvalersi di un delegato, Ufficiale alla Sicurezza designato, consulente tecnico, il cui compito è quello di dirigere, coordinare e controllare tutte le attività che riguardano la protezione e la tutela delle informazioni, dei documenti e dei materiali classificati. A lato, si riporta uno schema di organizzazione di sicurezza, il cui dimensionamento è funzione della complessità del Comando (Figura 1).

**c. Campo di applicazione**

L’organizzazione di sicurezza è disciplinata dal DPCM 22 luglio 2011 n. 4 “Disposizioni per la tutela amministrativa del segreto di Stato e

<sup>9</sup> È il complesso costituito – presso le articolazioni dei Ministeri, delle Forze Armate o degli Enti – dall’Ufficiale alla Sicurezza designato, dall’Ufficiale COMSEC designato, dall’Ufficiale alla Sicurezza EAD designato, dall’Ufficiale alla Sicurezza Fisica designato, dal Capo della Segreteria di Sicurezza, dal Centro CIFRA, dal Custode del materiale CIFRA e dalla Segreteria di Sicurezza.

un meccanismo di revisione continua, a fronte dell'individuazione della minaccia esterna e delle vulnerabilità delle strutture organizzative.

In tale ottica, le azioni essenziali che riguardano la pianificazione di sicurezza, dovranno individuare gli elementi più sensibili, le procedure per la loro protezione e le contromisure da adottare, attraverso un percorso aperto che si estrinseca di massima in quattro fasi:

- la prima in cui definire le linee guida della Sicurezza in generale, l'individuazione delle competenze nel sistema di gestione dell'informazione rispetto all'intera organizzazione e lo sviluppo di un piano per il trattamento dei rischi;
- la seconda prevede la realizzazione delle strategie necessarie per gestire i rischi attraverso misure di prevenzione;
- la terza, nel controllare l'efficacia delle misure adottate, individua lo scostamento tra i processi in uso e la natura del rischio;
- l'ultima fase prevede l'individuazione delle cause che hanno originato i rischi e i correttivi da adottare al fine di ridurre gli effetti delle criticità sull'intero sistema.

Il risultato finale di tale processo genera gli elementi fondamentali per la stesura o verifica dei Piani di Sicurezza.

**a. I Piani di Sicurezza**

I Piani di Sicurezza costituiscono i documenti di riferimento, in cui sono riportate tutte le norme e le procedure di sicurezza necessarie a preservare il patrimonio informativo del Comando di appartenenza.

Le norme prescritte devono essere necessariamente divulgate a tutto il personale e, in particolare, a quello inserito nell'organizzazione di sicurezza, ma devono anche essere contestualizzate e attagliate alle singole realtà.

Tutto il personale deve essere costantemente aggiornato sulle normative di sicurezza e deve poter fare affidamento su disposizioni particolari che, discendendo dalle direttive di riferimento, stabiliscono esattamente i compiti e le responsabilità in ogni situazione.

A premessa di qualsiasi tipo di operazione, assume una fondamentale importanza la fase dell'indottrinamento del personale, nella quale dovranno essere trattati i riferimenti e i principi basilari per la protezione dei dati classificati. Sarà dovere del responsabile della sicurezza verificare che quanto comunicato nella fase di istruzione sia stato correttamente recepito dal personale impegnato in operazione.

**b. Regolamento Interno di Sicurezza**

È il documento che ogni Ente della Difesa, legittimato alla trattazione di informazioni classificate, deve predisporre al fine di descrivere in modo funzionale le misure per la tutela delle stesse. Trattasi di un insieme di principi, regole e direttive con le quali si intende proteggere, gestire e utilizzare in sicurezza le risorse e il patrimonio informativo.

In particolare, il Regolamento in questione, viene redatto dall'Ufficiale alla Sicurezza designato che, avvalendosi delle altre figure dell'Organizzazione di sicurezza, dovrà:

- delineare le generalità dell'Organizzazione costituita (cfr. **Figura 1**);
- stabilire e dettagliare i compiti e le conseguenti responsabilità di tutto il personale impiegato in incarichi connessi con la Sicurezza;
- definire quel complesso di regole e procedure particolari tese a regolamentare nel proprio ambito l'applicazione delle norme di carattere generale;

- esprimere la liceità delle azioni e dei comportamenti consentiti;
- stabilire le sanzioni per i comportamenti illeciti.

Il documento deve essere approvato dalla massima autorità dell'Ente, va portato a conoscenza di tutto il personale dell'Organizzazione e deve rappresentare l'argomento da trattare nel corso delle istruzioni periodiche alla sicurezza.

**c. Regolamento Interno di Sicurezza EAD di Ente (eventuale)**

In funzione del numero e della tipologia di sistemi EAD classificati in uso, ogni Comando/Ente organizzativo/Articolazione funzionale valuta l'opportunità di elaborare un Regolamento Interno di Sicurezza (RIS) EAD, al fine di fornire indicazioni generali per gli aspetti EAD ed a cui dovranno fare riferimento i RIS EAD specifici dei sistemi in uso presso il Comando/Ente organizzativo/Articolazione funzionale (ad esempio NS WAN, JDISS, BICES, ecc.).

Nel citato documento devono essere focalizzati gli aspetti relativi a:

- Sicurezza Fisica;
- Responsabilità e controlli;
- Sicurezza Personale;
- Sicurezza della documentazione;
- Sicurezza tecnica dell'installazione;
- Sicurezza *hardware*;
- Sicurezza *software*;
- Terminali remoti;
- Guida per l'utente.

In linea generale, si rammenta che, per poter trattare informazioni classificate, un sistema EAD deve essere abilitato (approvato ed omologato) dall'Autorità Nazionale per la Sicurezza (ANS), sulla base di un processo commisurato al livello di classifica dei dati che si vuole vengano trattati e secondo quanto previsto dalla PCM ANS TI-001 (ed.1995) "Procedura nazionale per l'omologazione di sistemi/reti EAD militari<sup>10</sup>" dal DPCM 22 luglio 2011 n. 4 recante "Disposizioni per la tutela amministrativa del segreto di stato e delle informazioni classificate" e relative Direttive discendenti. Particolari esigenze operative possono determinare l'adozione di procedure "ad hoc" da concordare con l'Organo Centrale di Sicurezza di riferimento che interesserà i competenti Organismi nazionali di sicurezza.

**d. I Piani di Emergenza**

In caso di calamità naturali o attività ostili, il Comandante dell'Ente è responsabile della redazione e dell'aggiornamento dei piani per la protezione e la distruzione di materiali classificati (Piani di Emergenza).

I criteri di base per l'organizzazione dei Piani di Emergenza devono prevedere che tutto il personale coinvolto sia a conoscenza degli aspetti operativi.

In relazione al tipo di emergenza dovranno essere compilati i piani di evacuazione e di distruzione.

Il Piano di Evacuazione dovrà prevedere:

---

<sup>10</sup> Tale Direttiva descrive la documentazione e le procedure per l'omologazione di sicurezza dei sistemi militari destinati a trattare dati classificati.

- elenco dei materiali da sgomberare;
- contenitori o imballaggi da impiegare;
- personale responsabile dell'attuazione e del controllo delle attività;
- mezzi da impiegare per il trasporto;
- strumenti e metodi di protezione durante il trasporto;
- località da raggiungere (principale o alternativa);
- itinerario da seguire.

Il Piano di Distruzione per Emergenza dovrà prevedere:

- elenco dei materiali da distruggere in base alle priorità;
- strumenti e modalità per la distruzione;
- personale responsabile della distruzione e del controllo delle attività;
- tempistica di attuazione.

**e. Indottrinamento**

La verifica della congruità e della completezza delle misure preventive di sicurezza delle informazioni rappresenta una costante esigenza che si concretizza in attività programmatiche, finalizzate al controllo dell'efficacia dell'Organizzazione Sicurezza. In tale ottica i Comandanti dovranno addestrare il proprio personale in diverse circostanze, sia mediante istruzioni teoriche che mediante esercitazioni pratiche.

**4. La sicurezza del personale**

**a. Premessa**

L'insidia alle informazioni classificate si potrebbe manifestare nelle forme più subdole, tra le quali si citano la corruzione, il ricatto, ma soprattutto lo sfruttamento delle debolezze o negligenze di chi custodisce, conosce e trasporta documenti e materiali riservati.

L'esperienza ha evidenziato che, nella ricerca illegale di notizie, il metodo normalmente seguito è quello di individuare il personale che tratta informazioni classificate e di esercitare su di esso ogni possibile forma di pressione.

Per le ragioni che precedono, la trattazione di informazioni classificate è consentita esclusivamente a coloro che hanno necessità di conoscerle per lo svolgimento del proprio incarico, funzione o attività e che siano a conoscenza delle misure poste a tutela delle stesse e delle connesse responsabilità. Inoltre, in conformità alle esigenze dettate dall'OCS, è necessario che vi sia un criterio di certezza relativo alla lealtà, onestà ed affidabilità di tutte le persone cui è consentito l'accesso alle informazioni classificate o le cui funzioni possano richiederlo. Tale personale, oltre a possedere capacità e professionalità richieste dall'incarico di attribuzione, abbisogna, per la trattazione di informazioni classificate RISERVATISSIMO, SEGRETO o SEGRETISSIMO, stante la necessità di conoscere, del possesso del NOS, in corso di validità per tutta la durata dell'accesso a tale tipo di informazioni.

**b. Attribuzioni, competenze, responsabilità**

Al fine di soddisfare il criterio di certezza sopra menzionato, il rilascio del NOS è subordinato al favorevole esito di un preventivo procedimento di accertamento soggettivo sulla base delle disposizioni riportate nel DPCM 22 luglio 2011 ed in particolare nella pubblicazione "PCM-ANS /2006" e successive varianti legislative.

Il rilascio del NOS, dell'abilitazione temporanea e l'accesso ad informazioni classificate "RISERVATO" è accompagnato dall'istruzione alla sicurezza. Se il NOS o l'abilitazione temporanea riportano anche una o più qualifiche di sicurezza, detta istruzione è estesa alle relative disposizioni internazionali o comunitarie.

Quindi, anche al personale che tratta informazioni con classifica non superiore a RISERVATO per il quale non è richiesta alcuna abilitazione di sicurezza, è necessario che gli vengano forniti tutti gli strumenti dottrinali per la valorizzazione della propria coscienza informativa allo scopo di rammentare i rischi per la sicurezza derivanti da:

- conversazioni indiscrete con persone che non hanno necessità di conoscere;
- relazioni con i mezzi di informazione;
- minaccia costituita dai servizi informativi avversari, ecc.

In tale ottica, è responsabilità delle Organizzazioni di Sicurezza, ai vari livelli ordinativi:

- identificare gli incarichi che richiedono il Nulla Osta di Sicurezza;
- autorizzare l'accesso alle informazioni classificate secondo il principio del *need to know*;
- assicurare l'osservanza di criteri stabiliti per la sicurezza del personale;
- sensibilizzare il proprio personale secondo appositi piani di formazione in funzione dei ruoli e delle responsabilità attribuite.

Le credenziali di sicurezza ricevute e scambiate con le autorità militari competenti (OCS) dovranno essere tenute aggiornate al fine di garantire l'impiego del personale senza soluzioni di continuità. La validità, il rinnovo del NOS e i casi particolari per la concessione di una proroga alla sua scadenza sono disciplinate dall'art. 31 e 33 del DPCM 22 luglio 2011.

## 5. Sicurezza fisica

### a. Premessa

La Sicurezza fisica deve basarsi su di un sistema di "difesa in profondità", che utilizzi una combinazione di misure materiali coordinate con provvedimenti procedurali tesi alla riduzione della vulnerabilità del personale, dei documenti, delle comunicazioni, degli apparati informatici e di tutti quegli elementi vitali che garantiscono la libertà d'azione e l'efficienza operativa di un Comando.

I Comandanti o suoi delegati sono responsabili di pianificare tali misure di sicurezza interna attraverso la valutazione e adozione di quanto di seguito indicato:

- identificazione delle sedi che necessitano di protezione;
- creazione di provvedimenti di sicurezza a più livelli rispondenti a una difesa in profondità e a fattori di disturbo;
- definizione dell'area protetta e impedimento all'accesso non autorizzato;
- modalità di rilevazione dei tentativi di accesso o accesso non autorizzato e di allertamento del personale di vigilanza;
- creazione di ostacoli sufficienti all'accesso di intrusi al fine di "coprire" interamente i tempi di reazione e di intervento del personale di vigilanza (l'impedimento creato dagli ostacoli deve essere direttamente proporzionale ai tempi di intervento efficace del personale di vigilanza).

L'efficienza ed il rendimento dell'organizzazione della sicurezza devono essere garantite

attraverso la manutenzione dei sistemi e da periodiche valutazioni della loro singola efficacia, anche tramite la messa in pratica di piani di reazione all'incidente. È opportuno che la gestione dei rischi di sicurezza per la compensazione delle vulnerabilità, attraverso la combinazione di misure protettive, per essere ritenuta nel contempo economicamente efficace venga esaminata in sede di definizione dei requisiti di sicurezza fisica durante la pianificazione.

Appare evidente che tale sistema non potrà mai derivare dall'implementazione di un unico tipo di misura di sicurezza, in quanto nessuna di questa potrà mai fornire la garanzia di assoluta efficacia. Nella selezione delle misure da adottare occorrerà quindi scegliere un'opportuna combinazione di esse, individuando quelle che possano colmare le lacune intrinseche delle altre e possano garantire sia un'adeguata prevenzione dello Spionaggio e Sabotaggio sia la protezione delle installazioni e del personale da atti di Terrorismo e Crimine Organizzato.

Tali misure dovranno concretizzarsi in un sistema di protezione che rappresenti il risultato di un processo metodologico di individuazione, valutazione e confronto delle risorse da preservare, delle fonti di minaccia e della vulnerabilità dell'organizzazione; in particolare esso ha ad oggetto l'individuazione del bene da proteggere, la valutazione delle tipologie e livelli di minacce che insistono sul sistema, l'analisi delle misure di sicurezza da adottare e il calcolo delle vulnerabilità intrinseche e residue del sistema.

L'esito di tale analisi determinerà la pianificazione, l'organizzazione, la direzione, il controllo delle risorse e la progettazione delle infrastrutture al fine di assicurare che il rischio rimanga entro limiti accettabili in base al rapporto costo/efficacia.

Al Comandante è conferito il compito di verificare l'idoneità del profilo di sicurezza del sistema implementato, riducendo, ove necessario, le vulnerabilità residue attraverso l'adeguamento delle misure protettive materiali delle aree sensibili.

Il sistema di protezione che verrà individuato non potrà quindi prescindere dalla costante interazione di tre elementi fondamentali:

- Misure fisiche di protezione;
- Norme procedurali;
- Misure di eliminazione della minaccia.

**b. La sicurezza fisica per le Informazioni classificate**

Le misure di protezione dovranno essere basate sul concetto di Area di sicurezza con i livelli di protezione diversificati in funzione della sensibilità del bene da proteggere. Secondo l'articolo 66 del DPCM 22 luglio 2011, le aree dove vengono trattate informazioni classificate a livello RISERVATISSIMO o superiore, sono organizzate e strutturate in modo da corrispondere ad una delle seguenti tipologie:

- **I classe**: l'ingresso consente di poter accedere direttamente alle informazioni classificate;
- **II classe**: aree protette con controlli predisposti internamente, contro l'accesso di persone non autorizzate e in cui non si ha accesso diretto alle informazioni, poiché le stesse sono conservate in contenitori di sicurezza.

Tali aree presentano le seguenti caratteristiche:



- protezione con idonei sistemi di allarme e con dispositivi elettronici per il rilevamento delle intrusioni<sup>11</sup>;
- perimetro definito e protetto, tutte le entrate/uscite controllate;
- sistema controllo accesso peraltro rivolto a persone adeguatamente abilitate ed espressamente autorizzate.

Inoltre, in seno all'articolo 67 del citato DPCM le informazioni classificate con livello non superiore a RISERVATO possono essere trattate in:

**Aree controllate** ovvero aree in prossimità delle aree di I e II classe, con perimetro chiaramente delimitato e dotate di misure di protezione minime tali da consentire l'accesso alle sole persone autorizzate per motivi attinenti al loro impiego, incarico o professione.

Gli standard minimi per la custodia dei documenti classificati sono descritti al paragrafo 5 della Pubblicazione "Misure di sicurezza materiale per la salvaguardia delle informazioni classificate" (PCM ANS 6/2006).

I Comandanti dovranno prevenire l'accesso non autorizzato alle aree riservate tramite l'implementazione di adeguate misure fisiche in relazione all'impiego di procedure di sicurezza personale. In particolare l'accesso andrà controllato sia da personale di sorveglianza qualificato, sia dallo scambio di credenziali che certificano oltre la *clereance* necessaria al predetto accesso, la necessità di conoscere l'informazione.

L'accesso alle informazioni classificate, in particolare, dovrà essere determinato sulla base dei seguenti principi:

- accertamento sul possesso di credenziali in funzione del livello di classifica e qualifica delle informazioni da trattare;
- verifica del reale *need-to-know* in funzione dell'incarico/mansione da svolgere;
- minaccia valutata localmente proveniente dai servizi di *intelligence* (sabotaggio, terrorismo, attività sovversive o altre attività criminali);

e tramite l'adozione di adeguate misure fisiche di sicurezza al fine di:

- impedire l'accesso forzato o clandestino;
- impedire le azioni messe in atto da personale sleale;
- accertare per tempo le violazioni alla sicurezza.

**c. Responsabilità e compiti**

Il personale preposto alla realizzazione delle misure di sicurezza materiale, specifiche per contrastare la minaccia e ridurre le vulnerabilità delle strutture dove le informazioni classificate sono trattate e custodite, si identifica con l'Ufficiale alla Sicurezza designato o con l'Ufficiale alla sicurezza fisica designato, ove così disposto dalla massima Autorità dell'Ente. A tale persona è deputata "**l'analisi del rischio**", uno studio aperto che è riassunto nella seguente illustrazione (**Figura 2**).

La matrice dei requisiti minimi, la lista delle misure di sicurezza e le disposizioni particolari per effettuare l'analisi del rischio sono contenute e descritte nei documenti PCM ANS 6/2006 e SMD RIS SIC 001 08.

---

<sup>11</sup> Articolo 68 DPCM 22 luglio 2011.

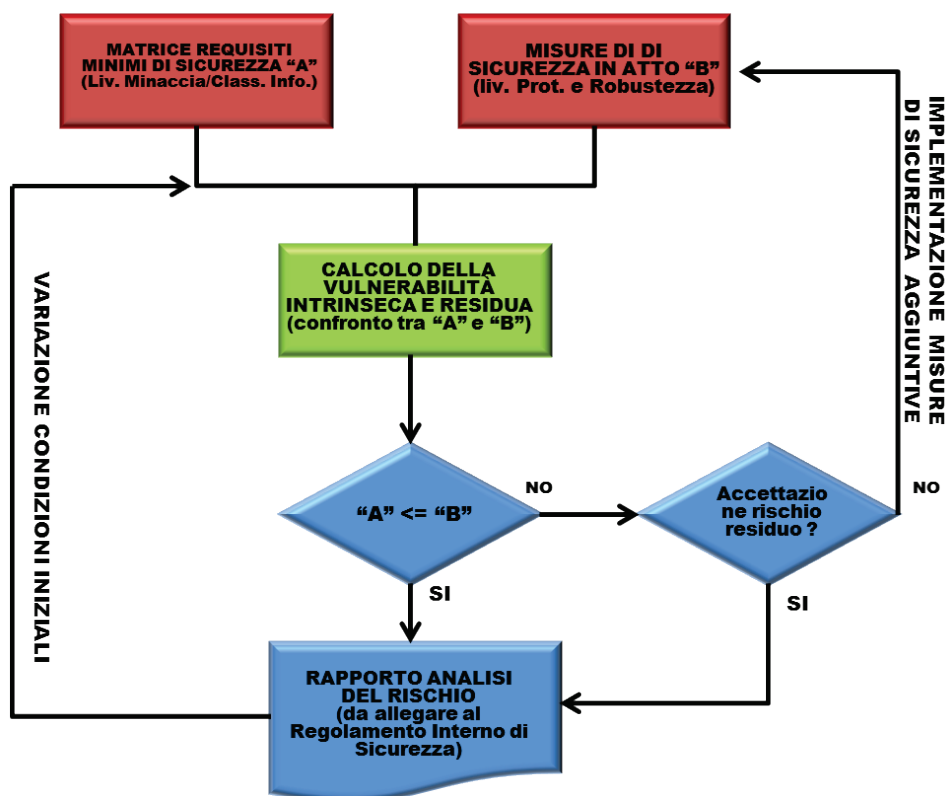


Figura 2 Analisi del rischio

d. **Misure di Sicurezza materiale specifiche ed attrezzatura approvata**

Le modalità particolari e la descrizione delle misure di sicurezza a disposizione, di seguito elencate, sono trattate nella Pubblicazione “Misure di sicurezza materiale per la salvaguardia delle informazioni classificate” (PCM ANS 6/2006):

- barriere perimetrali;
- sistemi d'illuminazione;
- sistemi di rilevazione ed anti intrusione;
- servizi di vigilanza e sorveglianza;
- sistemi di videosorveglianza;
- sistemi di controllo accessi;
- sistemi di controllo accessi personale in servizio;
- sistemi di controllo accesso visitatori;
- controllo dei fornitori e del personale per la manutenzione e la pulizia;
- controllo degli automezzi;
- controllo delle chiavi e delle combinazioni;
- apparati di continuità e di segnalazione guasti;
- mezzi per la distruzione dei documenti classificati;
- regolamento interno di sicurezza;
- protezione contro gli attacchi di tipo tecnico (ascolto clandestino).

**6. Sicurezza delle comunicazioni, della cifra e dei sistemi EAD (INFOSEC)****a. Premessa**

L'implementazione di sistemi informatici avanzati per la gestione delle informazioni classificate, l'esplosivo sviluppo tecnologico e l'inasprimento della minaccia telematica, rende necessario un costante adeguamento sia delle procedure che dei sistemi da impiegare, al fine di garantire una minore permeabilità della struttura gestionale per la tutela amministrativa del segreto di Stato e delle informazioni classificate.

In tale ottica, l'INFOSEC, si delinea come disciplina di riferimento finalizzata a proteggere le informazioni elaborate, archiviate o trasmesse da sistemi di comunicazione, di informazione o da altri mezzi elettronici, contro la perdita di riservatezza, integrità o disponibilità, accidentale o intenzionale, nonché a proteggere l'integrità e la disponibilità dei sistemi stessi, attraverso la messa in opera di azioni rivolte a:

- prevenire la deliberata o involontaria acquisizione, manipolazione, modifica o perdita di informazioni classificate ricevute, memorizzate, elaborate e trasmesse elettronicamente;
- verificare che l'uso dei sistemi informatici, che trattano informazioni classificate, siano utilizzate secondo quanto previsto dalla normativa vigente;
- impedire a persone non autorizzate di dedurre informazioni classificate dallo studio delle emissioni compromettenti (TEMPEST);
- garantire l'autenticità delle comunicazioni.

**b. Obiettivi**

Lo scopo principale dell'INFOSEC è quello di garantire un accesso pratico e razionale alle risorse del sistema e alle informazioni, unicamente a soggetti legittimamente autorizzati, provvisti di appropriata abilitazione di sicurezza ed opportuna necessità di conoscere, secondo quanto già esposto al precedente paragrafo 4. – "Sicurezza del Personale" –, contrastando al contempo ogni azione o evento, sia casuale che doloso, diretto ad impedire l'utilizzo dei servizi forniti dal sistema stesso.

Al fine di sopperire a tale esigenza, il Comandante o responsabile della Sicurezza dell'Ente dovrà avvalersi di un'organizzazione, configurata in ottemperanza alla normativa applicabile per la missione (Nazionale/NATO/UE/di coalizione, ecc.), costituita da un insieme di responsabilità, ruoli organizzativi, modalità operative, istruzioni e sistemi che si concretizza nell'attività combinata di strutture articolate sia in funzione del proprio livello ordinativo sia della tipologia e della qualità delle informazioni trattate – vedasi paragrafo 2. "Organizzazione di Sicurezza".

Allo scopo di garantire la riservatezza, l'integrità e la disponibilità delle informazioni e dei sistemi che trattano informazioni classificate, si devono applicare misure di sicurezza fisica, tecnica, personale e procedurale, che devono essere stabilite sulla base di fattori oggettivamente determinabili, quali:

- il livello di classifica delle informazioni da proteggere;
- la tipologia delle informazioni da proteggere (supporti cartacei, supporti informatici);
- la tipologia della struttura nella quale le informazioni classificate vengono trattate ed il grado di vulnerabilità alle minacce (spionaggio, sabotaggio o qualsiasi altra forma di criminalità).

Al riguardo, l'individuazione dei requisiti di sicurezza è necessaria per:

- prevenire la deliberata o involontaria divulgazione, manipolazione, modifica o perdita di informazioni classificate ricevute, memorizzate, elaborate e trasmesse elettronicamente;
- impedire a persone non autorizzate, la possibilità di dedurre informazioni classificate attraverso lo studio delle emissioni compromettenti (TEMPEST);
- prevenire l'accesso non autorizzato ai sistemi informatici che trattano informazioni classificate;
- garantire ai soggetti autorizzati l'autenticità delle informazioni, implementando misure di sicurezza logica e fisica, contro tentativi di modifica e distruzione delle stesse;
- garantire ininterrottamente, ai soggetti autorizzati, la disponibilità delle informazioni, anche in presenza di tentativi di sabotaggio o di fenomeni non controllabili (disastri naturali, incendi, ecc..).

Per conseguire gli obiettivi descritti nel precedente paragrafo si applicano i seguenti principi di sicurezza:

- gestione del rischio: devono essere installati solo i servizi, le funzioni e gli applicativi necessari per conseguire la missione operativa assegnata;
- privilegio minimo: agli utenti del sistema devono essere attribuite solo le autorizzazioni necessarie all'espletamento dei compiti istituzionali;
- autoprotezione del nodo: inizialmente ogni sistema deve considerare non fiduciosi tutti gli altri sistemi ed implementare misure di sicurezza per il controllo dello scambio di informazioni con essi;
- difesa in profondità: per quanto possibile, le misure di protezione devono essere implementate su più componenti del sistema in modo che la protezione non debba dipendere da un'unica linea di difesa;
- trasparenza: le misure di sicurezza devono essere trasparenti per l'utente ovvero non devono comportare un aggravio di lavoro;
- addestramento: tutto il personale deve essere addestrato ad applicare i principi di sicurezza ed a tenere sotto controllo la loro efficace implementazione;
- verifica dell'implementazione della sicurezza: l'applicazione di questi principi e la conseguente implementazione delle specifiche contromisure devono essere verificate dalle Autorità responsabili della sicurezza, inizialmente attraverso un rigoroso iter di certificazione dei sistemi e loro autorizzazione all'impiego operativo (omologazione) e poi, periodicamente, tramite apposite attività ispettive e conseguenti ri-omologazioni.

La sicurezza si evolve dinamicamente durante il ciclo di vita di una rete/sistema classificato, pertanto, i suoi requisiti ed i suoi effetti devono essere rivisti nel corso degli anni al fine di contrastare in modo efficace ed economico le nuove minacce e le vulnerabilità emergenti.

L'analisi del rischio deve valutare l'impatto delle minacce e delle vulnerabilità sul raggiungimento degli obiettivi di sicurezza. Il suo scopo è quello di consentire l'individuazione di misure di sicurezza che siano un buon compromesso tra funzionalità, costi e rischio residuo, nella consapevolezza che non tutte le minacce possono essere contrastate e le vulnerabilità eliminate.

**c. Sicurezza della documentazione e gestione dei supporti EAD removibili**

Come descritto in premessa, l'incremento esponenziale della documentazione classificata trattata in formato elettronico, insieme con la necessità di contrastare la possibile minaccia proveniente dall'interno, cioè da utenti legittimati all'impiego di sistemi classificati della Difesa, rendono necessaria l'adozione di misure, procedurali e tecniche, per ridurre il rischio di compromissione delle informazioni classificate.

In tale quadro, deve essere assicurato il rispetto di specifiche norme di sicurezza, tra cui:

- gli output di stampa devono riportare l'adeguata classifica/qualifica di segretezza ed essere registrati sull'apposito Registro degli Output. Qualora detta documentazione sia solo propedeutica alla realizzazione di copie cartacee di documenti consolidati, dovrà essere apposta, in rosso, la dicitura "BOZZA DI LAVORO - DA DISTRUGGERE ENTRO IL \_\_\_\_\_". Tali documenti devono essere custoditi secondo le vigenti norme e saranno considerati "Bozza di lavoro" purché vengano distrutti entro 30 giorni. Oltre tale termine, i documenti che si ritiene necessario conservare devono essere considerati come documenti finali ed essere registrati dall'Organo Esecutivo di Sicurezza dell'Ente e custoditi secondo le vigenti norme;
- se non operativamente necessari, i dispositivi per la lettura/scrittura di CD, DVD e i supporti di memorizzazione USB devono essere disabilitati a livello di sistema operativo. In ogni caso, per ridurre il rischio di diffusione di *virus/malware*, non è autorizzato l'impiego di Pen-Drive USB a meno dell'adozione di specifiche misure di sicurezza tecnica, approvate dallo SMD-RIS, che consentano di circoscrivere l'impiego dei supporti EAD removibili alle sole workstation classificate autorizzate.
- ogni supporto EAD rimovibile inizializzato dall'Ente dedicato alla trattazione di informazioni classificate deve essere rilasciato dal PCN, dopo esser stato appositamente etichettato e contabilizzato sul "Registro dei mezzi di supporto EAD". E' assolutamente vietato utilizzare supporti EAD che non siano stati preventivamente numerati e registrati dal PCN;
- i documenti classificati, fatta eccezione dei documenti memorizzati ai fini di back-up, non devono essere memorizzati nel supporto EAD rimovibile per un periodo superiore a 30 giorni.
- la riproduzione di supporti EAD contenenti documentazione classificata deve essere effettuata a fronte di una motivata richiesta/specifica procedura.

**d. Norme per la conservazione e utilizzo dei supporti EAD removibili**

Tutti i supporti EAD removibili devono essere registrati e custoditi in base alla massima classifica e qualifica dei dati in essa memorizzati. Le modalità di conservazione dei mezzi di supporto EAD sono identiche a quelle applicate per la documentazione cartacea di pari classifica, significando che presso le Aree Riservate EAD istituite presso il Reparto dove sono installati terminali classificati, possono essere conservati i supporti EAD in accordo alle vigenti normative.

La verifica della conservazione e della custodia dei supporti EAD contenenti dati classificati viene, normalmente, effettuata dall'Ufficiale / Sostituto Ufficiale alla sicurezza EAD.

I supporti, destinati a contenere dati classificati, devono essere utilizzati solo su PC omologati. Inoltre, devono essere seguite le seguenti procedure minime di sicurezza:

- cancellare i file contenenti i dati da eliminare;
- formattare i supporti di memorizzazione EAD se la cancellazione dei dati contenuti è totale.

A riguardo, si evidenzia che:

- per i supporti che contengono informazioni fino al livello RISERVATO, la cancellazione dei dati e la formattazione del supporto debbono avvenire a mezzo dell'utilità del sistema operativo;
- per i supporti in cui sono memorizzati dati classificati SEGRETO o RISERVATISSIMO, con o senza qualifiche di sicurezza, la cancellazione dei dati e la formattazione del supporto debbono avvenire per mezzo di quattro successivi cicli di scrittura nella sequenza zero, uno, zero e un carattere alfanumerico, fermo restando che detti supporti non possono essere utilizzati all'esterno dell'area riservata EAD.

**e. Distruzione dei mezzi di supporto EAD**

Nel caso in cui si debba procedere alla distruzione di mezzi di supporti EAD contenenti dati classificati<sup>12</sup>, questa dovrà essere eseguita, ove possibile, dopo la cancellazione dei *file* con i seguenti metodi, in accordo alle disposizioni della Direttiva PCM-ANS 5/2006:

- i nastri magnetici e dischi flessibili devono essere tritati o distrutti mediante incenerimento;
- i dischi rigidi devono essere distrutti meccanicamente;
- le memorie a stato solido (CD, USB) devono essere distrutte meccanicamente.

Detta operazione deve essere eseguita dal personale del PCN alla presenza del Sostituto Ufficiale alla Sicurezza EAD ed annotata sugli specifici Registri dei supporti EAD.

Per la distruzione di supporti EAD classificati si applicano, sotto il profilo della verbalizzazione o meno, le stesse disposizioni concernenti la distruzione dei documenti classificati (PCM ANS 1/2006).

---

<sup>12</sup> I CD/DVD utilizzati per uso interno all'Ente (per finalità di bozze di lavoro o messaggistica per il centro trasmissioni di Reparto devono essere distrutti entro 180 giorni dalla data della loro inizializzazione se contenenti dati di alta classifica. Diversamente, non è necessario distruggere i suddetti CD/DVD dedicati alla trattazione di dati fino a RISERVATO.

## IL CONTRIBUTO DELL'ARMA DEI CARABINIERI ALLA DIMENSIONE SICUREZZA

### 1. L'ambiente operativo tipico nella dimensione security

La sicurezza militare, ovvero la difesa da atti ostili diretti contro lo Stato ad opera di soggetti esterni allo stesso<sup>1</sup>, si identifica nella salvaguardia e conservazione del complesso apparato di difesa militare, ricorrendo anche all'adozione di idonee misure di *Force Protection* per consentire alle Forze Armate di assolvere al proprio ruolo istituzionale<sup>2</sup>.

A livello più ampio, la sicurezza militare 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 e nei suoi beni essenziali. Basti pensare alla disciplina dei trasporti, della circolazione stradale militare, delle comunicazioni, delle operazioni militari terrestri, navali e aeree. In tal modo la sicurezza militare coinvolge pienamente l'Arma dei Carabinieri che potrà fornire il proprio contributo per pianificare le misure di *Force Protection* nei seguenti ambiti:

- sicurezza delle infrastrutture militari, anche nella fase di realizzazione<sup>3</sup>, intese come ogni luogo militare o di interesse militare di cui deve essere garantita l'inviolabilità, o la possibilità di accesso selettivo e la salvaguardia da ogni tipo di offesa, fisica, morale o informativa;
- sicurezza degli stabilimenti militari o comunque collegati alla produzione di interesse militare, con le stesse finalità di salvaguardia previste per le infrastrutture militari;
- sicurezza dei beni militari, mobili ed immobili, di cui deve essere garantita l'integrità materiale da offese esterne, l'eventuale segretezza e l'efficace utilizzo da parte dell'organizzazione militare;
- sicurezza del personale militare, di cui deve essere garantita l'integrità fisica e morale da qualsiasi tipo di offesa. La sicurezza del personale riguarda anche l'aspetto dell'affidabilità del personale ai fini della sicurezza e della tutela del segreto e delle informazioni riservate;
- sicurezza delle informazioni, intese nel senso più ampio possibile, cioè non solo come documenti e notizie segrete, ma anche come tutti quei dati ed elementi di informazione utili all'attività istituzionale delle FF.AA. e di cui deve essere garantita almeno la riservatezza, per divulgazioni o comunicazioni non autorizzate, e l'integrità da offese esterne volte a carpirne il contenuto;

---

<sup>1</sup> "La Dottrina Militare italiana" (PID/S-1), Ed. 2011.

<sup>2</sup> Il ruolo istituzionale delle Forze Armate trova compiuta definizione nel Codice dell'ordinamento militare che, ispirandosi al dettato costituzionale, sancisce per le Forze Armate il compito:

- prioritario, "di difesa dello Stato";
- sussidiario, "di operare al fine della realizzazione della pace e della sicurezza, in conformità alle regole del diritto internazionale ed alle determinazioni delle organizzazioni internazionali delle quali l'Italia fa parte";
- ulteriore, "di concorso alla salvaguardia delle libere istituzioni". Ibid.

<sup>3</sup> Infatti, nel più ampio contesto della tutela della riservatezza delle opere destinate alle FF.AA. per le attività connesse ai compiti d'Istituto, la vigente normativa sui lavori pubblici prevede la possibilità di ricorrere alla dichiarazione di "segretezza" ovvero di "opera eseguibile con speciali misure di sicurezza". Tale declaratoria consente di evitare la divulgazione del progetto della realizzanda opera, procedendo all'affidamento degli appalti pubblici in deroga alle disposizioni ordinarie.

- sicurezza delle comunicazioni e delle reti telematiche della difesa;
- sicurezza dei movimenti e dei trasporti, come necessità di garantire l'integrità dello strumento militare nello svolgimento di attività che statisticamente presentano possibilità di danno ed offese esterne;
- sicurezza nelle operazioni militari, per le quali gli assetti *Multinational Specialised Unit* (MSU) o *Stability Policing* (SP) in ambito NATO, le *Integrated Police Unit* (IPU) in ambito UE, le *Formed Police Unit* (FPU) in ambito ONU e gli assetti di Polizia Militare (ciascuno nel proprio ambito di riferimento) costituiscono un elemento di sistema per l'ottimale riuscita e il raggiungimento del successo operativo.



## 2. Principi e fattori delle operazioni nella dimensione security

### a. Generalità

Una delle componenti essenziali della *Force Protection* nella dimensione sicurezza è costituita dall'insieme delle attività preventive svolte dagli assetti schierati dell'Arma dei Carabinieri. Tra le più importanti attività preventive poste in essere si segnalano quella informativa, che impegna organi appositamente costituiti, quella dissuasiva che esprime una caratteristica dell'efficienza dell'intero sistema di sicurezza, e quella di prevenzione.

### b. L'attività informativa

Un efficiente sistema di *Force Protection* nella dimensione *security* non può prescindere da un'efficace attività informativa. Le informazioni di natura criminale, terroristica ed eversiva rappresentano un elemento fondamentale per decidere, pianificare ed intervenire nel modo più corretto per fronteggiare efficacemente la minaccia, ma soprattutto per la predisposizione di idonee misure di *Force Protection*. L'informazione è necessaria per individuare minacce e rischi, la loro potenzialità lesiva, provenienza e struttura interna. Essenziale, allora, diventa l'insieme delle attività di ricerca, individuazione, raccolta, elaborazione, tutela, custodia ed utilizzazione delle stesse informazioni. Il sistema informativo per la *Force Protection* è fondato sull'attività preventiva e di intervento attraverso lo svolgimento della funzione di polizia per la quale bisogna effettuare una distinzione che riguarda l'ambito in cui essa è esercitata. Infatti, in teatro di operazioni, gli assetti dell'Arma operanti in unità di Polizia militare svolgono la propria attività nella



compagnie militare, mentre quelli che svolgono le loro funzioni a favore delle unità MSU/SP/IPU/FPU sono proiettabili nella società civile dell'area di operazioni, in relazione a specifici obiettivi informativi individuati ed assegnati. La cultura dell'informazione deve essere coltivata e sviluppata come capacità di osservazione critica dell'ambiente circostante, di valutazione



ponderata di persone, eventi e situazioni ai fini della predisposizione di misure adeguate di *Force Protection*.

**c. L'attività di dissuasione**

Gli assetti dell'Arma schierati, svolgono anche un'importante azione dissuasiva. L'efficacia dissuasiva è costituita dalla 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. La dissuasione, però, non è soltanto un effetto statico del sistema, ma si sviluppa e potenzia anche in relazione ad una specifica attività.

Gli assetti MSU/SP/IPU/FPU attraverso l'espletamento delle loro funzioni di polizia nella società civile, all'interno dell'area di responsabilità assegnatagli, svolgono un'azione dissuasiva nei confronti di minacce rappresentate ad esempio dalla criminalità organizzata e da organizzazioni terroristiche.

La Polizia Militare svolge la sua attività anche in funzione dissuasiva, nel contribuire all'efficienza dello strumento militare schierato.

**d. La prevenzione della conflittualità**

La conflittualità sociale è una costante minaccia per le Forze schierate, anche quando non coinvolge direttamente gli interessi nazionali o non sia sviluppata ad un livello tale da compromettere le esigenze di sicurezza del Contingente Nazionale. La capacità di prevenire la conflittualità sociale si basa prevalentemente sulle capacità di gestione della folla, terreno privilegiato di impiego degli assetti MSU/SP/IPU/FPU.

La conflittualità può svilupparsi anche nel contingente nazionale. In tale situazione la PM sarà un assetto pregiato a disposizione del Comandante del contingente per prevenire l'insorgere di tale fenomeno, o ricondurlo ad un alveo di normalità.



**3. Criteri generali per l'applicazione delle misure di Force Protection**

**a. Generalità**

All'atto della minaccia o al verificarsi del rischio preventivato, il sistema di *Force Protection* attiva la sua componente reattiva per gli interventi ritenuti più adeguati alla situazione. La componente di intervento è in realtà un complesso ed articolato insieme di forze che, ai vari livelli, con diversa intensità e con differenti funzionalità innescano un meccanismo di difesa estremamente flessibile e proporzionato agli obiettivi da conseguire. Se la minaccia si sviluppa ad un livello di intensità basso, che comporta il perturbamento dell'ordine pubblico o situazioni d'insicurezza pubblica fronteggiabili con gli assetti MSU/SP/IPU/FPU, la reazione si mantiene ad un corrispondente livello di normalità istituzionale, per il quale intervengono eventualmente in concorso le Forze Armate e la responsabilità dell'attività di contrasto spetta alle autorità locali.

Se la minaccia si sviluppa ad un livello di intensità alto, la reazione aumenta, pertanto intervengono prioritariamente le FF.AA. e la responsabilità delle operazioni spetta alle autorità militari (principio della *green box* e *blue box*<sup>4</sup>).



**b. Le forze di sicurezza**

Sono denominate forze di sicurezza tutte quelle organizzazioni che hanno capacità operativa di intervento per contrastare le minacce alla sicurezza. Nelle forze di sicurezza, in un'accezione ampia, possiamo

ricomprendere le Forze di polizia, quindi gli assetti MSU/SP/IPU/FPU, le FF.AA. e i Servizi di Informazione e Sicurezza.

**c. La componente di soccorso**

Prima del verificarsi di situazioni conflittuali, il Contingente Nazionale deve predisporre un sistema di soccorso capace di tutelare e salvaguardare le risorse umane, materiali (beni, ambiente e territorio) e morali.

Gli assetti dell'Arma dei Carabinieri sono in grado di prestare soccorso, quando vengano arrecati danni, e di ripristinare situazioni (umane, materiali e morali) deteriorate dalle eventuali offese, avendo cura di preservare lo stato dei luoghi a successivi fini investigativi.

**d. La protezione**

La protezione si basa sullo svolgimento di:

- attività di previsione e prevenzione della varie ipotesi di rischio;
- azioni di soccorso;
- ogni altra necessaria ed indifferibile attività diretta a superare l'emergenza derivante dagli eventi.

**4. Applicazione del modello *Force Protection* nella dimensione *Security***

**a. Capacità**

La Polizia Militare ha il compito di realizzare condizioni di sicurezza ed ordinata convivenza nelle aree d'intervento nel quadro delle operazioni per il mantenimento ed il ristabilimento della pace e della sicurezza internazionale.

MSU/SP/IPU/FPU esercitano una nuova ed originale funzione militare che possiamo definire "di polizia ordinaria". Infatti sono assetti con competenza di polizia da schierare in Teatro d'Operazioni.

Il Legislatore ha anche attribuito all'Arma il compito di concorrere ad "assicurare il contributo nazionale alle attività promosse dalla comunità internazionale o derivanti da

---

<sup>4</sup> Nell'ambito delle operazioni per il mantenimento dell'ordine pubblico e della sicurezza pubblica (operazioni per il controllo della folla), il Comandante di Settore responsabile stabilisce, intorno alla località di interesse, una Zona di Controllo Sicurezza (*Security Control Zone* - SCZ), chiamata anche "*green box*", al fine di garantire la sicurezza del complesso minore MSU/SP operante. Il Comandante di Settore individuerà anche l'Area di Responsabilità Tattica (TAOR) o "*blue box*" nella quale il complesso minore MSU/SP condurrà le operazioni. L'accesso e l'uscita dalla TAOR saranno controllati dalle forze nazionali o NATO/UE nella Zona di responsabilità del Comandante di Settore (SCZ).

accordi internazionali, volte alla ricostituzione ed al ripristino dell'operatività dei corpi di polizia locali nelle aree di presenza delle Forze armate, assolvendo compiti di addestramento, consulenza, assistenza e osservazione". È questo un altro compito militare che, sebbene di norma riconducibile a missioni di polizia internazionale dell'ONU o di Organizzazioni regionali, anche MSU/SP, IPU ed FPU possono agevolmente svolgere in completamento e contestualmente alle altre attività, in particolare a quelle sostitutive di imposizione della legge, quale attività preparatoria alla cessione di autorità e responsabilità di polizia alle forze locali, cui naturalmente spettano.

**b. Capacità tipiche della dimensione security**

I compiti di Polizia Militare di sicurezza riguardano essenzialmente:



- la vigilanza e la protezione di determinate installazioni militari o di interesse militare, con la correlativa disciplina e controllo degli accessi;
- il controllo della circolazione stradale militare e degli itinerari ad essa connessi, con i relativi servizi di viabilità e di scorta;
- la scorta alle autorità militari;
- il concorso all'attuazione delle misure concernenti la sicurezza e la protezione del segreto e delle comunicazioni riservate;
- l'attività informativa di prevenzione e di specifico interesse, anche d'iniziativa;
- il concorso alla tutela dell'integrità fisica e morale del personale militare, con riguardo anche alla sicurezza nei luoghi di lavoro;
- il concorso alla sicurezza delle operazioni militari, con particolare riguardo alla sicurezza nelle retrovie (anche se i moderni scenari operativi tendono a non avere una chiara distinzione del campo di battaglia), nei porti e negli aeroporti militari e dei movimenti di forze militari;
- il concorso nelle operazioni di polizia di frontiera, anche delle basi aeroportuali e portuali, militari e civili, in caso di invio o rientro di personale o di reparti per o da attività all'estero;
- la vigilanza sulle persone non militari autorizzate a seguire le forze militari o a svolgere attività al loro interno;
- la disciplina delle evacuazioni della popolazione dalla zona di combattimento e il controllo degli sbandati e dei profughi;
- il mantenimento e, qualora necessario, il ristabilimento dell'ordine e della legalità;
- l'attuazione di misure di prevenzione dei crimini, soprattutto per quel che concerne il saccheggio, la busca e le requisizioni illegali;
- la protezione di personalità ad alto livello di rischio;



- la consulenza sul trattamento dei prigionieri di guerra e le attività di scorta, sorveglianza e custodia degli stessi;
- il concorso nelle attività di cooperazione civile-militare;
- l'intervento in caso di incidente informatico.

Nel settore dell'Ordine e Sicurezza Pubblica si colloca l'assetto MSU/SP, a livello di Brigata o di Reggimento. Esso è composto da forze di polizia a status militare e dispone dell'addestramento, dell'esperienza e della capacità per soddisfare tali esigenze ed affrontare le problematiche relative alla polizia ordinaria, al fine di creare un ambiente sicuro per le forze militari schierate nell'ambito della propria Area di Responsabilità durante le "operazioni di risposta alle crisi non articolo 5 della NATO" o nelle cosiddette "missioni di Petersberg" dell'Unione Europea.

Le IPU, pur agendo in ambito civile, hanno gli stessi compiti e la medesima struttura delle MSU/SP, rapidamente schierabili, flessibili ed interoperabili, costituiscono l'aspetto innovativo del catalogo delle capacità che l'Europa può esprimere.

L'FPU, invece, ha il compito di garantire la sicurezza e la protezione del personale, delle installazioni e dell'equipaggiamento delle Nazioni Unite, può agire in auto difesa e per difendere i civili esposti a imminente pericolo di vita. Nelle missioni con mandato esecutivo le FPU supportano l'attività della polizia locale.

Il ruolo dell'assetto dell'Arma potrebbe variare in relazione al mandato internazionale da un minimo consistente nelle attività di pattugliamento areale, di raccolta di informazioni/operazioni di *intelligence* criminale, e di collegamento con le Autorità civili locali, fino al monitoraggio ed assistenza alle forze di polizia (*Local Police* – LP), alle indagini sui crimini di guerra ed all'imposizione della legge. In quest'ultimo caso, lo scopo è quello di trasferire la responsabilità per l'imposizione della legge alle forze di Polizia Locale non appena possibile.

Gli assetti MSU/SP/IPU/FPU dovranno garantire un ambiente sicuro per le forze schierate nel Teatro di Operazioni attraverso operazioni/attività d'intervento preventive. Per adempiere la missione, è necessario che compiano ogni sforzo affinché si instauri nella popolazione e nelle Autorità civili locali un sentimento positivo verso le forze nazionali, l'ONU, la NATO e l'UE.

**c. Il Comando e Controllo della FP per le operazioni nella dimensione *security***

Il sistema di comando e controllo, che assume un'importanza cruciale in funzione della sensibilità dei flussi e dei contenuti informativi, delle esigenze di manovra nell'area di responsabilità, della collocazione dell'Unità a livello di Teatro, rispetta i seguenti principi<sup>5</sup>:

---

<sup>5</sup> Per ulteriori approfondimenti sull'argomento vds:

- AJP-3.2.3.3 "*Allied Military Police Doctrine*";
- "*Guidelines for rapid deployment of Integrated Police Units – IPUs – and other Police elements in the initial stage of an EU-led substitution mission and interoperability of IPUs and Police Headquarter*". Documento del Consiglio dell'Unione Europea;
- "*The United Nations Formed Police Units Doctrine Paper*" e "*Guidelines for Formed Police Units on assignment with Peacekeeping Operations*". DPKO – Police Division dell'ONU.

- il Comandante dell'MSU/SP/IPU dipende direttamente dal Comandante della missione di cui è il consigliere per le operazioni in materia di ordine e sicurezza pubblica e per le connesse problematiche nei rapporti con l'autorità giudiziaria e di polizia locali;
- il Comandante della missione, quando lo ritenga necessario, delega, con riferimento al vincolo del tempo ed all'assolvimento del compito, l'impiego dell'assetto di MSU/SP/IPU al Comandante nella cui area di responsabilità opera;
- il segretario delle Nazioni Unite nomina il *Police Commissioner (PC)* o il *Senior Police Advisor (SPA)* designato per la missione da svolgere. Il PC o l'SPA sono i dirigenti della componente di Polizia e come tali sono responsabili della implementazione del mandato. Loro è il compito di fissare un quartier generale unificato di Polizia all'interno del Comando della Missione, espletando funzioni direttive delle componenti di polizia dipendenti assegnate alla missione (FPU od osservatori di polizia);
- il *Provost Marshal* è il consulente del Comandante e dello Stato Maggiore in materia di Polizia Militare, inoltre potrebbe svolgere contemporaneamente l'incarico di Comandante dell'assetto di PM. Il *Provost Marshal* svolge funzione di coordinamento sugli assetti di PM e di collegamento con le autorità e le forze di Polizia Locali responsabili della sicurezza, in assenza di un assetto MSU/SP/IPU. Quando una MSU/SP/IPU è costituita, il *Provost Marshal* e il Comandante di MSU/SP/IPU devono cooperare efficacemente al fine di evitare aree di sovrapposizione e migliorare lo scambio d'informazioni e la continuità del risultato.

**d. Elementi generali di security nella FP dei luoghi militari**

La principale misura di *security* nella *Force Protection* volta a garantire la sicurezza dei luoghi militari viene primariamente garantita dall'attività di sorveglianza, cioè dal controllo assiduo e diretto a scopo cautelare, di custodia e di difesa. Il sistema di sorveglianza viene predisposto soprattutto per respingere nell'immediatezza minacce fronteggiabili con il personale addetto alla vigilanza e per attivare l'intervento di forze superiori qualora la minaccia sia di gravità maggiore.

Responsabile della sicurezza delle installazioni militari è il Comandante, cioè l'autorità militare di più alto rango gerarchico nel luogo militare considerato. In particolare, nel settore della sicurezza, è responsabile:

- dell'organizzazione dei servizi di vigilanza e sorveglianza;
- della pianificazione ed attuazione della difesa dell'infrastruttura e delle operazioni di allertamento;
- dell'organizzazione del servizio antincendio.

La pianificazione delle misure di *Force Protection* deve tenere in considerazione che la sicurezza dei luoghi militari viene anche garantita dalla normativa disciplinare che detta particolari doveri dei militari.

Per la sicurezza dei luoghi militari è fondamentale l'attività di controllo degli accessi.





La persona autorizzata ad accedere non è anche autorizzata a circolare liberamente all'interno dell'installazione militare, ma può recarsi – se necessario accompagnata – solo per la destinazione richiesta e per la quale è stata autorizzata.

Il Comandante dell'installazione militare può disporre l'adozione, da parte degli organi di servizio, di controlli al personale in uscita e in entrata per impedire che sia asportato materiale o che sia introdotto materiale che possa nuocere al singolo o alla comunità. La PM contribuisce alla sicurezza agli accessi effettuando controlli di polizia.

Il personale militare è il bene più prezioso dell'amministrazione e come tale va tutelato e salvaguardato. Per tale ragione, come soggetto primario della sicurezza, il personale militare deve garantire la necessaria affidabilità.

La Polizia Militare ha un particolare dovere di vigilanza nei confronti del personale fornito di Nulla Osta di Segretezza, al fine di verificare la permanenza delle condizioni di affidabilità stabilite dalla normativa vigente, inoltre la sua azione per tale finalità investirà i doveri di tutela morale dell'istituzione militare, di tutela dei beni militari.

Il personale militare può essere oggetto di specifica attività offensiva che può aggredire lo stesso sentimento di fedeltà alle istituzioni repubblicane o l'integrità fisica o morale del militare. Questa forma di offesa è particolarmente insidiosa e virulenta nei periodi di impiego in Area di Operazioni e in situazioni apertamente conflittuali, ma può essere recata anche in scenari stabilizzati o a scopo di orientamento ideologico. Le offese all'integrità fisica e morale del militare non differiscono nella sostanza dalle altre forme di aggressione alla persona previste e punite dalla legge penale, per tale ragione la PM orienta la propria azione verso la prevenzione\repressione di:

- propaganda disfattista e sovversiva;
- violazioni doganali.

La sicurezza dei luoghi militari è, pertanto, un obiettivo prioritario dell'attività di Polizia Militare, a cui concorrerà l'assetto MSU/SP/IPU/FPU, contribuendo con altri assetti ad individuare le misure di *Force Protection* più idonee a individuare i rischi e le minacce. Tali misure comprendono anche la tutela garantita dalla sfera penale ai luoghi militari. In tale cornice le attività investigative condotte autonomamente o in supporto della Polizia Locale, saranno sempre svolte di concerto con le competenti AA. GG. Internazionali, nazionali e del Paese ospite.

La Polizia Militare pone particolare attenzione verso le minacce derivanti da:

- spionaggio;
- sabotaggio;
- atti dimostrativi;
- attività informativa-offensiva, da cui discende quella controinformativa, che si basa su una serie di provvedimenti di carattere precauzionale, preventivo e repressivo di competenza della Polizia Militare.

# **LA FORCE PROTECTION ENGINEERING E LA PROTEZIONE DELLE INFRASTRUTTURE - CONTROAVIAZIONE DIFENSIVA**

## **PARTE I PRINCIPI E CARATTERISTICHE**

### **1. Premessa**

La *Force Protection Engineering* (FPE) comprende una serie di attività contraddistinte da una lunga tradizione storica che può essere fatta risalire almeno all'epoca romana. Compito del Genio era, infatti, quello di fornire adeguato supporto tecnico alle unità combattenti nella progettazione e realizzazione degli accantonamenti, nel movimento (strade e ponti) e nelle operazioni di assedio (macchine da assedio, rampe, terrapieni e delimitazione dell'area di assedio).

In particolare, con riferimento al *Castrum*<sup>1</sup>, occorre evidenziare come la sua progettazione e la direzione dei relativi lavori fosse affidata ad un *praefectus fabrum* e a un gruppo di genieri (*architecti*) che utilizzavano il lavoro manuale dei legionari per la costruzione di quanto progettato.

La scelta del sito dove impiantare il *Castrum* veniva effettuata dal *metador* che precedeva l'esercito in marcia. Subentravano, poi, due ulteriori figure professionali il *librator* con il compito di assicurare l'orizzontalità dell'accantonamento e il *mentor* che aveva il compito di definire l'esatta collocazione di ogni struttura in seno al *Castrum*.

Da evidenziare, infine, come il cuore dell'accantonamento, in senso sia geometrico sia operativo, fosse nelle strutture destinate al Comando e Controllo della Legione e come le strutture meno sensibili fossero meno baricentriche ma comunque a distanza di sicurezza, anche dal tiro indiretto, da eventuali aggressori esterni. Tale zona di sicurezza costituiva, peraltro, anche via per il transito dei reparti in afflusso e deflusso dall'accantonamento.

Come è possibile desumere da quanto sopra, i principi organizzativi posti a base del *Castrum* rimangono tuttora validi. Ciò che cambia sono le modalità organizzative, legate all'evoluzione tecnologica sia per l'attacco sia per la difesa. Non viene meno, però, né la necessità di pianificare e progettare con rigore la scelta del sito né una scelta logica e funzionale della dislocazione di ogni struttura all'interno del *Castrum*.

Oggi, come allora, le perdite dovute ad attività diverse dal combattimento devono tendere al minimo. Il singolo militare è un bene prezioso, preparato per operare e combattere, che necessita di ricondizionare sé stesso e il proprio equipaggiamento in condizioni di sicurezza.

La presente pubblicazione nella sua descrizione del FPE e del Concetto di Supporto allo Schieramento, risponde ai principi generali appena descritti.

### **2. Generalità**

La FPE è un'area di applicazione della *Force Protection* che comprende tutte le attività tecniche

---

<sup>1</sup> Vds. Polibio (Libro VI, 27-42) “Descrizione di un Campo Romano” e Pseudo Igino “De Munitionibus Castrorum”.

del genio necessarie per la protezione e la sopravvivenza delle forze durante lo svolgimento delle operazioni.

La 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<sup>2</sup>.

### 3. Campi di applicazione

Principalmente la FPE prende in esame la trattazione delle problematiche connesse con i seguenti ambiti di applicazione:

- protezione delle infrastrutture;
- antincendio;
- EOD<sup>3</sup>, IEDD<sup>4</sup>;
- mine e campi minati, trappole e rischi dovuti ad esplosioni di IED;
- *military search*;
- *route & area clearance*;
- mascheramento e inganno;
- C-IED.

Deve però ritenersi correlata ed indispensabile in caso di:

- gestione delle emergenze (*Consequent Management*) laddove, specialmente nel caso di un MASS CASUALTIES (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), sono necessari interventi mirati alla rimozione di macerie, alla messa in sicurezza di edifici pericolanti (o loro demolizione), all'individuazione di aree sicure per la realizzazione di tendopoli o ospedali da campo, al ripristino della viabilità per i soccorsi o attività tecniche mirate a contenere frane, esondazioni, etc.;
- definizione delle attività connesse con la protezione delle infrastrutture (*Area & Infrastructures Protection*), ad integrazione delle predisposizioni della vigilanza e specificatamente al fine di valutare la sicurezza fisica e strutturale attraverso l'esame della vulnerabilità di edifici e di aree critiche delle basi militari, nonché le necessarie opere o strutture da realizzare.

### 4. Obiettivi

Le attività della FPE sono indirizzate al raggiungimento di due importanti obiettivi:

- contribuire ad aumentare la sicurezza delle infrastrutture, integrando e potenziando le misure della difesa attiva (*security*) ed attuando tutte le opere di difesa necessarie (*field fortifications*);
- salvaguardare il personale, i mezzi ed i materiali dall'osservazione, dal tiro indiretto e diretto di elementi nemici e da attacchi non convenzionali (*physical & fire protection*).

---

<sup>2</sup> Pub. Ispettorato per la formazione e la specializzazione dell'Esercito n. 6712 "Manuale sulla protezione delle infrastrutture e delle basi militari nell'ambito delle *Peace Support Operations*", ed. 2011.

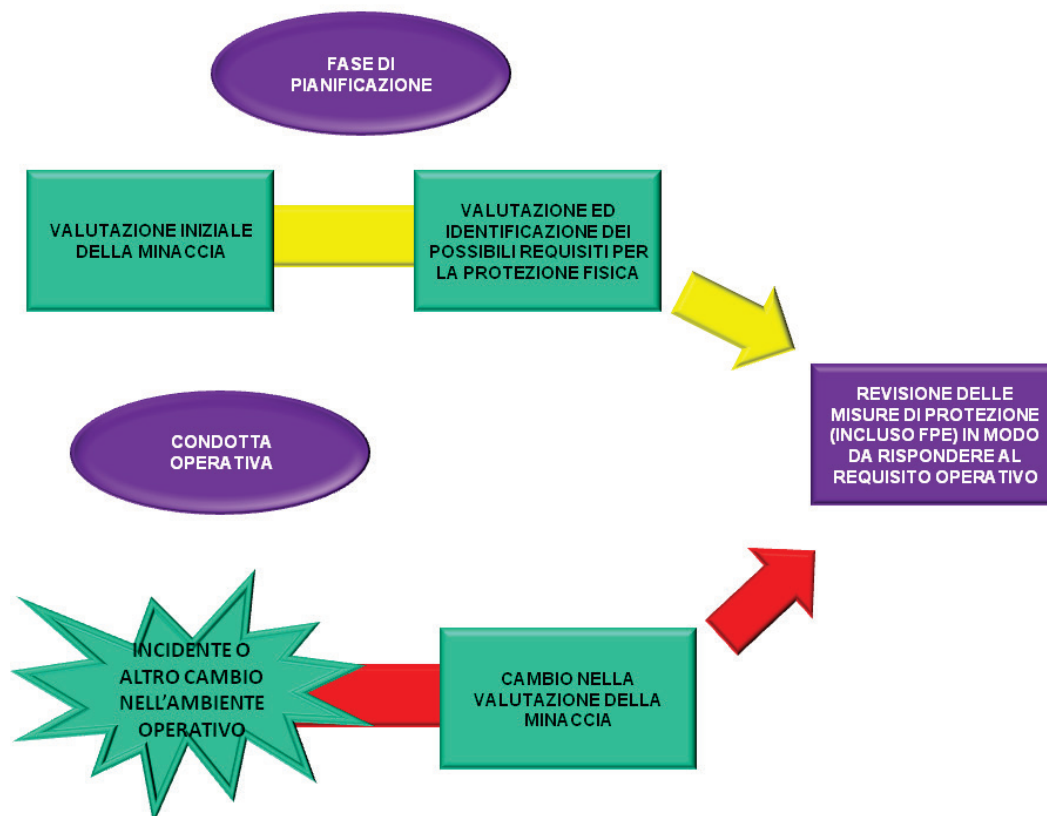
<sup>3</sup> *Explosive Ordnance Disposal (EOD)*.

<sup>4</sup> *Improvised Explosive Device Disposal (IEDD)*.



## 5. Requisiti

Il livello qualitativo e quantitativo delle opere di protezione per la FPE da realizzare può derivare sia dalla valutazione iniziale del rischio insito nell'operazione che in risposta a variazioni nell'ambiente operativo intervenute operazione durante (**Figura 3**).



**Figura 3** Il processo di revisione delle misure di FP

In entrambi i casi si giunge ad una valutazione o ad una revisione delle misure di protezione della forza nel complesso, delle quali la FPE è solamente un sottoinsieme. In base alla valutazione di rischio il Comandante della Forza supportato dal *Chief J-Eng* determina le opere da realizzare sulla base dei requisiti minimi (*Minimum Military Requirements*) indicati dalle normative vigenti in ambito NATO, UE, UN e nazionali.

Riguardo a quest'ultime, la loro applicazione è da ritenersi prioritaria qualora risultino più restrittive rispetto a quelle NATO UE o UN.

## 6. Pianificazione

I generi forniscono le indicazioni ed i suggerimenti in merito alle misure protettive e, alla fine, mettono in atto le misure fisiche per garantire il livello di FP richiesto. Qualsiasi tipo di pianificazione si faccia, nello sviluppo di un piano per garantire la protezione fisica di una forza, esistono un certo numero di ruoli funzionali:

- Identificazione della minaccia. Lo *staff* e gli specialisti *intelligence* sono i responsabili dell'effettuazione di una valutazione del rischio.

- Determinazione della rilevanza delle perdite. Il personale delle operazioni deve contribuire alla determinazione della rilevanza delle perdite, del contesto operativo e dei limiti posti allo sviluppo di un piano di protezione.
- Gestione delle infrastrutture. Lo *staff* operativo che è preposto alla gestione ed all'utilizzo delle infrastrutture, deve avere un ruolo significativo nella valutazione degli investimenti da adottare nel settore specifico.
- Consulenza degli specialisti. Nel processo di pianificazione si dovrà tenere conto di eventuali suggerimenti di altre componenti specialistiche dello *staff* (comunicazioni, CIMIC ecc.).
- Accettazione dei rischi. Il Comandante, avendo la responsabilità ultima del piano operativo, deve determinare quale sia il livello di rischio da considerare accettabile.

Per quanto concerne la metodologia di pianificazione dei mezzi protettivi, è possibile seguire diverse strade. Possono essere usati dei valori "tabulati" per ogni livello di sicurezza che permettono di monetizzare il beneficio ottenuto in termini di sicurezza e raffrontarlo con i costi dei lavori necessari. Questo fornirà un apprezzamento costo/efficacia in meri termini economici<sup>5</sup>. Altri approcci prendono in considerazione i valori assegnati al rischio, agli assetti da proteggere ed ai livelli di protezione da garantire per poi ottenere un valore costo/efficacia ponderato<sup>6</sup>. Tutte queste tecniche hanno in comune il fatto di dipendere dalla scelta soggettiva di valori ponderali pre-tabulati e quindi, in definitiva, di essere soggettive e dipendenti dalle valutazioni individuali.

Inoltre questi metodi sono maggiormente indicati per ambienti permissivi, sono focalizzati sul costo in meri termini di risorse economiche e non consentono di tenere facilmente conto dell'impatto sulla libertà di manovra e concedono poco spazio per inserire correttivi derivanti dall'assunzione di determinati livelli di rischio.

Un ulteriore limite di questi sistemi è costituito dal fatto che essi focalizzano l'attenzione sugli assetti vulnerabili e sui lavori esterni per fronteggiare la minaccia. Non contribuiscono all'intrinseca promozione di un approccio sistematico integrato alla sopravvivenza.

Misure di protezione efficaci non possono fare affidamento su una singola tecnica o azione, ma derivano dalla combinazione bilanciata di misure attive e passive che formino un sistema coerente e flessibile.

La **Figura 4**, illustra un processo tipico che, tenendo in considerazione vari aspetti, anche non meramente monetari, permette un approccio più flessibile alla pianificazione FPE.

I vari passi forniscono un metodo di pianificazione che può essere facilmente implementato in teatro.

Di seguito si analizzano i singoli passi del processo:

- Chiarificazione dei requisiti operativi. È importante determinare chiaramente quali siano i risultati da ottenere, una cosa è la protezione di un AOD (*Airport of Debarkation*) dal fuoco indiretto, altra è il contenimento delle vittime in un *checkpoint* permanente. La determinazione deve essere fatta in termini di *effetti da ottenere* e non in termini di mezzi da impiegare o misure da prendere. È altresì importante che il livello di protezione richiesto

<sup>5</sup> Approccio USA nel TM 5-853.

<sup>6</sup> Approccio UK nella pubblicazione JSP 440.

non comprometta la funzionalità della struttura o ne limiti indebitamente l'efficienza operativa. In questa fase del processo vengono individuati i criteri di successo del piano.

- Valutazione della minaccia. 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. Lo scopo di questo passo del processo di pianificazione è la valutazione, la più esatta possibile, della effettiva presenza di un avversario, della sua capacità operativa e delle sue reali intenzioni di arrecare danno. Questo allo scopo di valutare l'entità della minaccia, i potenziali effetti e l'impatto che gli stessi possono avere sulle nostre forze.

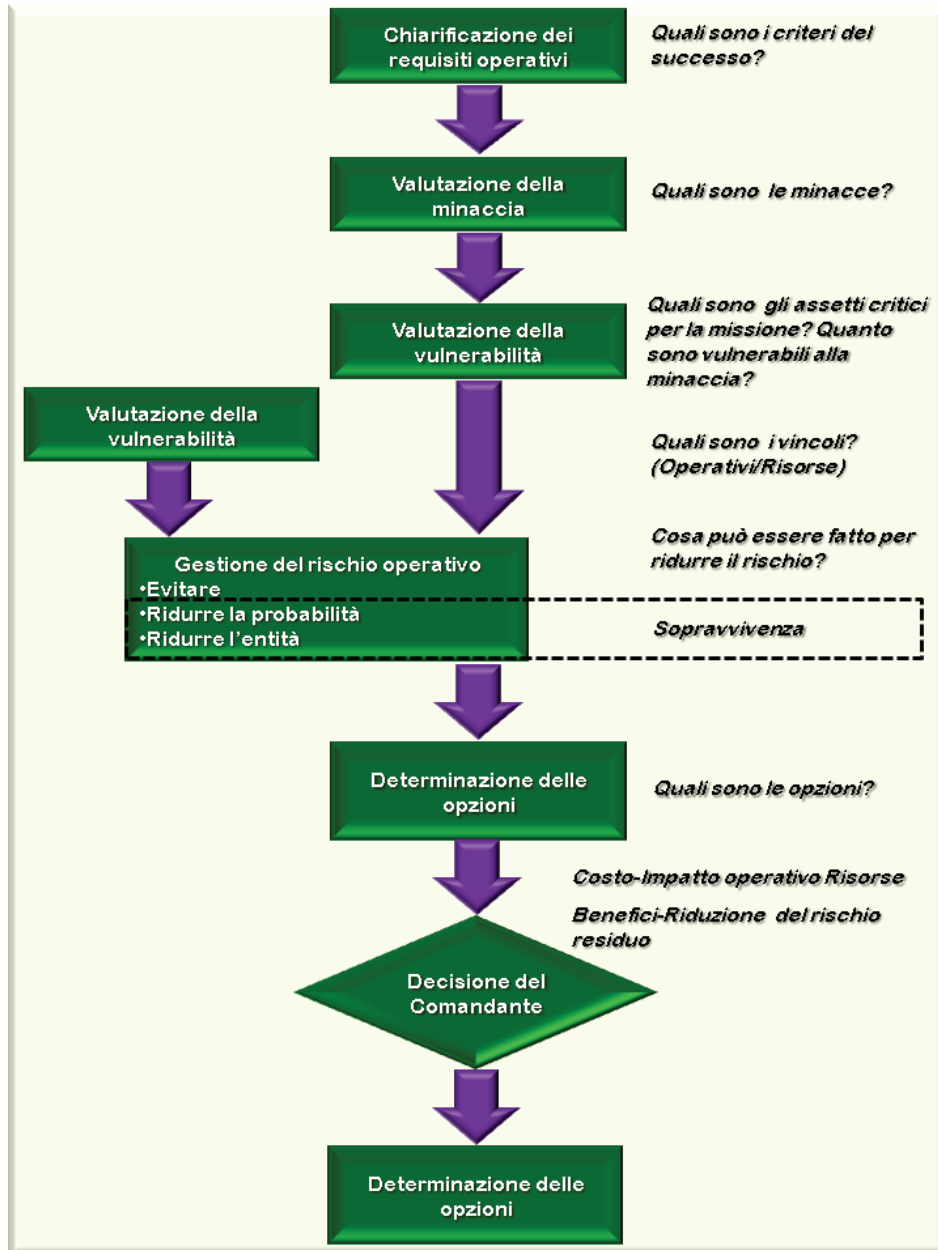


Figura 4 La pianificazione FPE

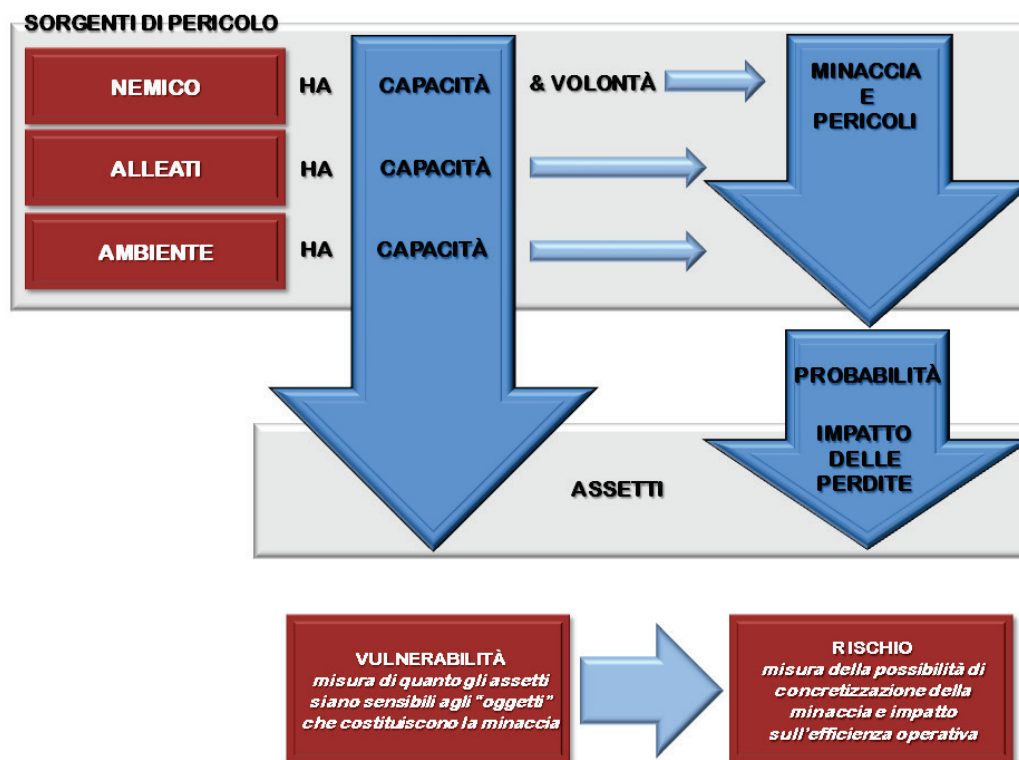
- Valutazione della vulnerabilità. La valutazione della vulnerabilità è un processo congiunto fra lo staff delle operazioni e personale della FP. Deve essere valutata la sensibilità alle minacce che possono essere portate dal nemico, da

potenziali eventi causati da forze amiche o dall'ambiente stesso. Il tutto, messo a sistema come in **Figura 5**, permetterà di ottenere una concreta ed attendibile valutazione del rischio e delle possibili ripercussioni sulla operatività delle nostre forze.

- Identificazione dei vincoli. Parallelamente alla valutazione della minaccia e della vulnerabilità devono essere individuati i vincoli del piano operativo.

Questi vincoli possono essere:

- *Operativi*. È probabile che ci siano vincoli di ordine operativo, politico o mediatico che limitano le possibili misure da porre in essere per contrastare la minaccia. L'atteggiamento e l'impronta che si vuol dare alla forza ed i limiti imposti dalla *Host Nation*, in particolare influenzeranno in maniera sensibile le possibili soluzioni pianificate.
- *Risorse*. Il tempo, il costo e la disponibilità di materiali da costruzione e di personale pongono chiaramente dei vincoli alle possibili soluzioni da implementare. La loro influenza è variabile in tutto lo spettro delle operazioni, per cui le opzioni disponibili mutano sia all'interno del teatro che nel tempo.

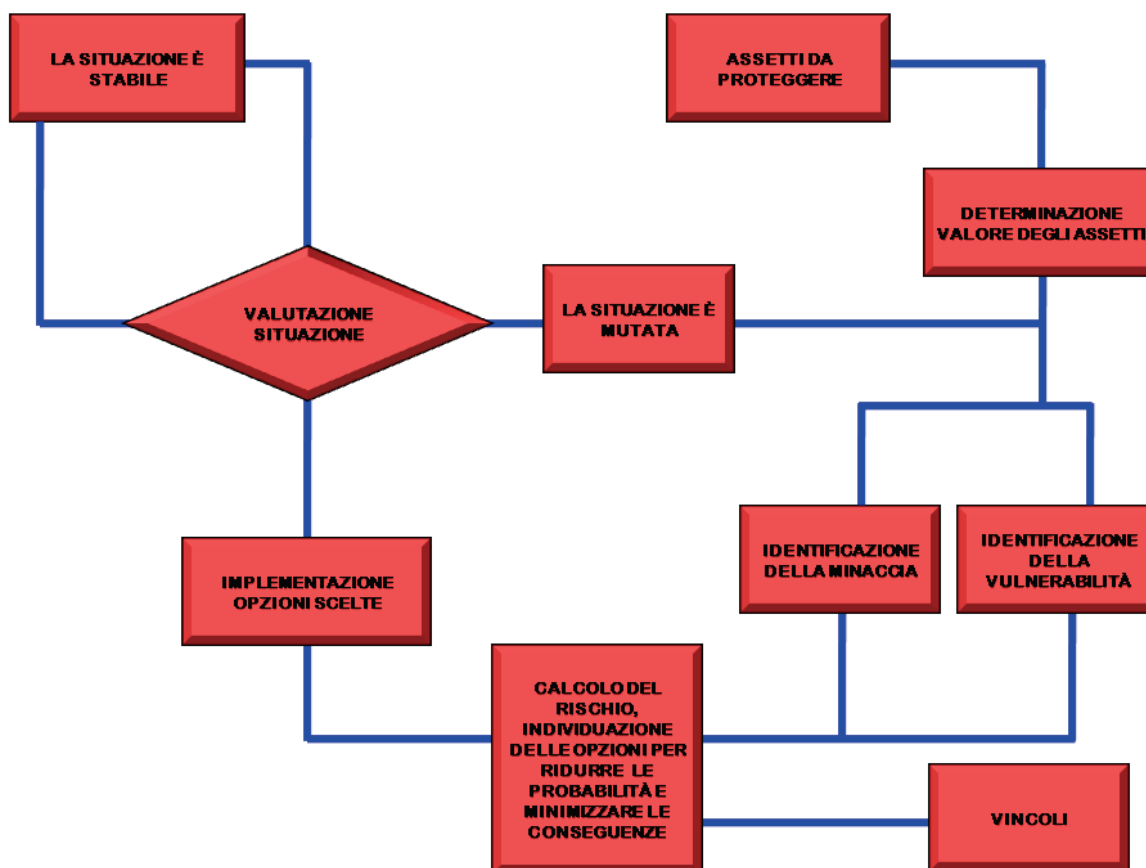


**Figura 5** La Valutazione della vulnerabilità

- Gestione del rischio. Una volta individuati sia le possibili sorgenti di pericolo che gli eventuali punti deboli del nostro sistema di protezione, assodato che è poco pratico (se non impossibile) eliminare tutti i possibili rischi, diventa importante individuare le migliori opzioni che consentano sia di ridurre le probabilità di concretizzazione della minaccia sia, al contempo, di minimizzare il numero di perdite e l'impatto sull'operatività della forza nel caso di concretizzazione di una minaccia. La decisione sul livello di rischio e sulle conseguenze ritenuti accettabili è propria del Comandante.

- Selezione delle opzioni ed implementazione del Piano di protezione. Al termine di tutte le valutazioni si sarà in presenza di un piano di protezione della forza, o più probabilmente diversi piani corrispondenti a diverse opzioni. È essenziale che gli stessi siano espressi in termini di costi e benefici, dove i benefici sono rappresentati dalla riduzione del rischio.

In **Figura 6** è illustrato graficamente il succedersi dei passi di realizzazione del piano di FP.



**Figura 6** I passi del piano di FP

A seconda delle circostanze operative verrà quindi determinato l'appropriato COA. Perché le misure di protezione della forza siano pienamente efficaci, esse dovranno avere effetto sia sul piano della protezione fisica del personale che sul piano del morale. Il personale che deve fare affidamento sulle misure di protezione scelte, deve avere confidenza sulla qualità delle stesse ma deve essere conscio anche dei limiti che le stesse hanno. Questo contribuirà sia a ridurre gli aspetti negativi generati dall'ansia di conoscere con esattezza le capacità di protezione, sia l'impatto sul morale una volta che eventuali minacce si concretizzassero e causassero delle perdite limitate a quanto valutato nella fase di assunzione dei rischi.

Una volta che il piano è stato implementato, con l'evolversi della Campagna muteranno le situazioni di contorno, e lo stesso dovrà costantemente essere confrontato con la situazione operativa in atto ed eventualmente modificato in accordo con il mutare della ambiente operativo. Quindi il ciclo sin qui visto verrà sviluppato reiterativamente in modo da avere un piano di FP sempre aggiornato con l'evolversi della situazione e della possibile minaccia.

## 7. Criteri

Per la progettazione e la realizzazione delle opere di FPE devono essere presi in considerazione i seguenti criteri operativi:

- campalizzazione: realizzazione di strutture secondo specifiche campali con tipologie già collaudate nel passato e l'impiego della prefabbricazione;
- defilamento e occultamento:
  - sfruttamento della conformazione naturale del terreno;
  - evitare, per quanto possibile ed in funzione di esigenze operative, l'uso di strutture protettive sporgenti al di sopra del piano di campagna;
- orientamento:
  - orientamento in senso longitudinale alla prevedibile direzione di provenienza della minaccia;
  - utilizzazione di posizioni dominanti per evitare l'azione erosiva delle strutture da parte delle acque sotterranee (o il ristagno delle acque meteoriche) ed implementare i campi di vista ed i settori di tiro;
- difesa da aggressivi chimici:
  - realizzazione di:
    - › pareti sigillate con infissi a tenuta stagna ed apposizione di filtri nelle varie aperture di accesso;
    - › camere di bonifica;
    - › impianti di pressurizzazione o aerazione con filtri NBC;
    - › ventilazione forzata per l'eliminazione di aggressivi ancora persistenti;
  - predisposizione materiale per la bonifica di urgenza e l'intervento sanitario;
  - orientamento o utilizzazione di strutture orientate sul terreno in posizione dominante per evitare i ristagni o l'azione di acque sotterranee;
  - defilamento di ingressi dall'azione erosiva degli aggressivi movimentati secondo la direzione del vento dominante locale;
- interramento:
  - profondità degli scavi proporzionata in funzione della tipologia della minaccia e degli schermi artificiali utilizzabili e/o realizzabili;
  - protezione dal tiro diretto al personale seduto a terra ed al tiratore in piedi;
- protezione:
  - impiego di strutture e schermi protettivi di adeguato spessore per contrastare la minaccia individuata;
  - realizzazione di ricoveri di piccola capacità, di rapida accessibilità da ogni punto dell'accampamento; separazione dei ricoveri in serie da strutture di contenimento onde d'urto ad elevata capacità di assorbimento;
  - aperture di comunicazione o di ingresso/uscita ridotte al minimo indispensabile ed in direzione opposta a quella della minaccia;

- integrazione delle opere di difesa e protezione con camminamenti defilati;
- antincendio:
  - costruzione di barriere o elementi di tenuta realizzati con materiale antincendio o trattato con intumescenti;
  - definizione delle opportune distanze di sicurezza dagli stoccaggi di materiale infiammabile;
  - realizzazione di protezioni che impediscano alle sostanze incendiarie di penetrare lungo le pareti inclinate dei ricoveri.





## PARTE II FUNZIONALITÀ DI COMPONENTE

### SEZIONE I – ESERCITO

#### 1. Generalità

I Comandanti delle forze terrestri nell'elaborazione delle linee guida sulla FP del concetto di azione devono tenere presente le seguenti priorità:

- gravitazione degli sforzi;
- scoperta e ingaggio alla massima distanza;
- profondità del dispositivo;
- flessibilità dell'organizzazione della difesa attiva;
- possibilità di mutuo soccorso;
- solidità delle opere di protezione;
- sicurezza strutturale delle infrastrutture;
- possibilità impiego di riserve;
- disponibilità materiali per la sopravvivenza;
- efficace struttura di comando e controllo dedicata alla FP.

Gli *staff* devono integrare le capacità esprimibili nell'ambito delle disponibili funzioni di supporto alla FP nello sviluppo dei piani d'intervento delle seguenti aree di preminente interesse operativo per la F.A.:

- difesa integrata: impiego integrato di unità per la vigilanza, sistemi di fuoco (mortai, artiglierie, UGV, torrette di fuoco remotizzate, ecc.) con sistemi di sorveglianza aerei (aerei, elicotteri, UAV, satelliti, ecc.) o terrestri (pattuglie, *check points*, ecc.), di rilevamento (sensori, ottiche, ecc.), opere di protezione passiva e difesa delle informazioni;
  - risposta alle emergenze complesse: predisposizione di SOPs, piani di contingenza base-base e base-HN, dislocazione preventiva di risorse per la sopravvivenza o materiali per lavori di contingenza, definizione degli assetti per l'intervento (unità del genio e materiale campale per la realizzazione di accampamenti temporanei o interventi sulla viabilità, assetti EOD/IEDD, antincendio, SAR, strutture sanitarie campali, trasporti);
- capacità di recupero dell'efficienza operativa: ripristino dei servizi essenziali e della capacità operativa a seguito di un evento o incidente occorso in una delle TAOR (*Tactical Area of Responsibility*) del Contingente.



## 2. Organizzazione di Comando e Controllo della FP

Per assicurare lo sviluppo della pianificazione della FP e delle relative attività i Comandanti devono approntare una adeguata struttura di Comando e Controllo che preveda:

- nell'ambito degli *staff*:
  - la costituzione di una Cellula dedicata alla FP (livello Comando Contingente o G.U. El., nell'ambito della Cellula J3/G3) o Ufficiale addetto alla FP (livello rgt./btg., nell'ambito della Cellula S3);
  - l'individuazione di personale incaricato di gestire gli aspetti di interesse di FP in ciascuna Cellula dello *staff*;
  - la costituzione di gruppo di lavoro permanente sulla FP (FPWG), coordinato dal Capo Cellula FP, a livello Comando Contingente/G.U. El.;
- nell'ambito dell'organizzazione di Comando di ciascuna base militare:
  - un Comando della difesa.

## 3. Sistema di protezione delle forze

L'ampio spettro di rischi e di minacce dei moderni Te. Op. necessita da parte dello *staff* del Comando di Contingente di un'analisi accurata della situazione operativa per poter assicurare la sicurezza delle Forze nei Te. Op.. Pertanto, la Cellula FP del J3/G3 (ovvero il FPO della Cellula S3) deve provvedere a sviluppare il ciclo delle misure di FP esaminando in dettaglio due macro aree di analisi dei rischi:

- azioni di forze ostili;
- calamità ed emergenze complesse.

In particolare, nell'applicazione del predetto ciclo alla protezione delle basi militari in Te. Op. (FOB, FSB, PRT, APOD/SPOD, ecc.) ed alla sicurezza delle relative LOCs, la cellula FP deve assicurare, senza soluzione di continuità, lo sviluppo di uno studio comparato che prenda in esame i rischi e le minacce presenti in ciascuna TAOR delle basi nelle varie fasi del ciclo ed in entrambe le citate macro aree.

Nella considerazione che la TAOR di una base militare è in genere caratterizzata da elevate estensioni, compartimentazioni e differenze di quota, anche repentine, le unità dovranno ricorrere alla “dispersione” del proprio dispositivo sul terreno per poter garantire il controllo del territorio e contrastare efficacemente l'azione condotta dalle forze ostili.

Tale contesto operativo impone alle basi militari l'adozione di un sistema “integrato” di protezione composto da:



- unità incaricata della sorveglianza ed assetti specialistici di supporto tattico e logistico;
- un sistema informatizzato che consenta di effettuare l'analisi e la verifica di tutte le informazioni ricevute dalle aree controllate, permettendo di visualizzare tutte le informazioni (dati e video) ricevute dai sensori, sistemi e mezzi non pilotati integrati nel sistema di *Force Protection*;

organizzato "concentricamente" che deve:

- tenere conto della variabilità della minaccia;
- articolarsi in profondità comprendendo:
  - aree controllabili visivamente con personale di sorveglianza;
  - aree controllabili visivamente con sistemi di video sorveglianza;
  - aree non controllabili visivamente, compreso le LOCs a supporto delle attività della base (operative e logistiche) e delle eventuali aree ed abitati da tenere sotto controllo a mezzo pattuglie, *check point* (fissi o mobili), sorveglianza con elicotteri o UAV, ecc.;
- assicurare l'unitarietà di Comando degli assetti di FP.

La profondità e l'andamento di ciascuna TAOR delle basi militari, nell'ambito delle AOR assegnate alle unità del Contingente che compongono la JOA (*Joint Area of Operations*), dovrà essere definita in funzione della minaccia individuata dal J2/G2/S2 e delle capacità di controllo/intervento/combattimento delle varie unità; inoltre, si dovrà tenere conto dell'andamento del terreno, degli effetti delle condimeteo e dovranno essere sempre assicurate aree contermini di sovrapposizione al fine di assicurare il mutuo controllo ed il reciproco soccorso (**Figura 7**).

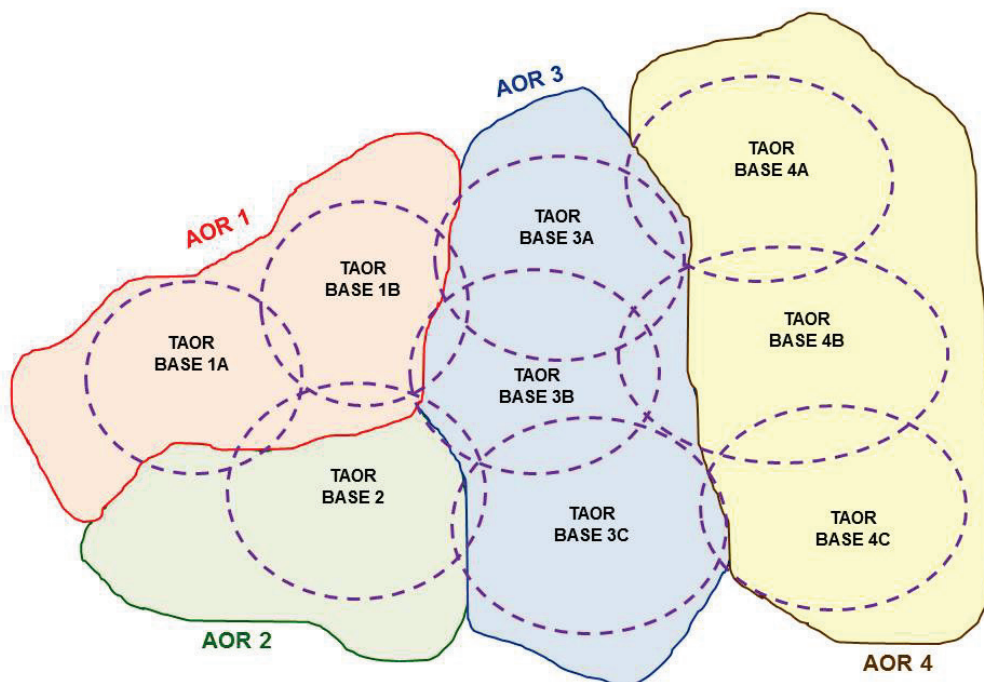


Figura 7 Composizione JOA

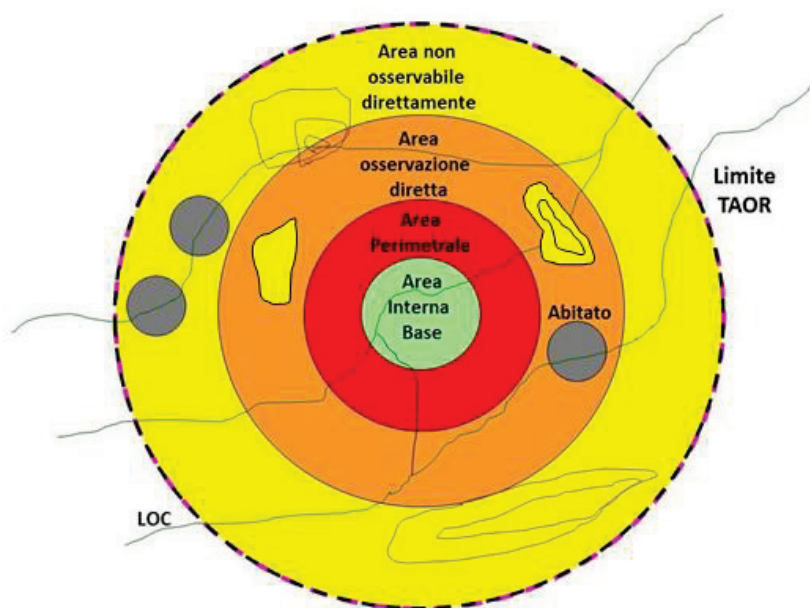
Allo scopo di dislocare in maniera più favorevole gli assetti della difesa integrata di una base e delle relative LOCs, la TAOR deve essere divisa in settori concentrici che individuano sul terreno le seguenti principali aree funzionali della difesa (**Figura 8**):

- area interna della base;
- area perimetrale;
- area di osservazione diretta;
- area non osservabile direttamente.

Qualora la situazione operativa lo richieda, potranno essere definite ulteriori sub-aree funzionali.

Inoltre, dovranno essere definite le misure di coordinamento necessarie con la *host nation* (HN) al fine di:

- raccogliere e scambiare le informazioni sulle attività di forze ostili per la redazione dei piani di contingenza comuni e l'intervento coordinato degli assetti disponibili;
- definire le misure di controllo del territorio e delle zone di confine;
- stabilire le modalità per l'uso ed il controllo degli aeroporti, porti e delle LOCs;
- definire il supporto alla formazione delle forze della HN.



**Figura 8** Aree funzionali per la difesa

#### **4. Il supporto del Genio**

Tutte le unità delle Forze Armate sono responsabili per la loro auto protezione e pertanto dovrebbero possedere le capacità (in termini di professionalità e materiali) per porre in essere delle misure minime di protezione collettive al fine di dare avvio all'attività operativa in tempi ridotti. Questo vale in maniera particolare per tutte quelle unità che, per compiti istituzionali e per peculiari modalità di dispiegamento (es. truppe anfibie, aviotruppe), si trovano a dover



condurre operazioni del tipo *expeditionary*, che prevedono l’inserimento in ambiente ostile, incerto o permissivo, svolgendo la funzione di *Initial Entry Force*.

L’intervento del genio aumenterà e potenzierà le possibilità di sopravvivenza entro i limiti imposti dalle risorse disponibili e dalle priorità fissate dal Comandante Tattico.

Le misure di protezione iniziano con lo sfruttamento di tutta la copertura ed il riparo naturale disponibile, seguite da interramenti e postazioni per l’osservazione ed il combattimento.

Il sostegno del genio consisterà essenzialmente in azioni, pianificate e specializzate, realizzabili unicamente con i mezzi tecnici e peculiari propri dell’Arma del genio. Le predisposizioni di protezione collettive realizzate dalle unità del genio devono essere pianificate e condotte nel quadro del supporto generale allo schieramento ed a premessa della realizzabilità dei piani operativi e tattici predisposti per tutta la durata della missione. Le capacità del genio esprimibili



ai vari livelli ordinativi vanno configurate sulla base di due criteri fondamentali:

- il supporto diretto: in grado di “generare” strutture di Comando e Controllo a livello reggimento con capacità modulari assemblate sulla base dello scenario operativo di riferimento;
- il supporto generale: sia per un impiego unitario sia quale “serbatoio” di capacità specialistiche da inserire a ragion veduta nelle *task force* del supporto diretto.

Pertanto, i reggimenti guastatori sono decentrati in ogni singola G.U. elementare (o assegnati a quelle Brigate o JTF in operazioni che non hanno in organico le unità del genio) essendone l’unità organica di supporto al combattimento, mentre il reggimento pionieri, analogamente ai reggimenti ferroviari e pontieri, è posto alle dipendenze del Comando Genio quale serbatoio specialistico per l’impiego dell’Arma.

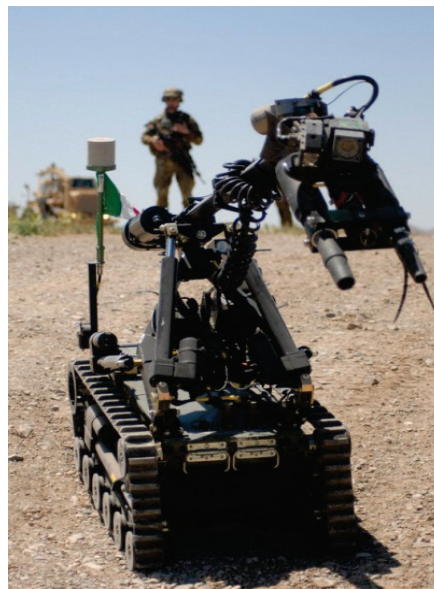


Il concorso del genio ai fini della FPE deve essere eseguito in aderenza alla situazione operativa ed alla fase della missione in corso di svolgimento (“schieramento”, “condotta” o “proseguimento”, che prevedono diversi livelli qualitativi di intervento) e deve essere funzionale alle prescrizioni operative del Comandante dell’unità.

Le unità del genio devono essere impiegate dal Comandante del Contingente

principalmente per le seguenti opere di protezione:

- progettare e realizzare gli ingressi e la viabilità annessa alla base, le aree o le strisce di sicurezza perimetrali e le relative recinzioni;
- progettare e realizzare gli apprestamenti e le posizioni difensive da realizzare lungo la recinzione o gli ingressi precedentemente determinati;
- potenziare le postazioni difensive approntate dall’unità dell’Arma Base durante la realizzazione del campo all’atto del dispiegamento;
- incrementare l’ampiezza del settore di intervento delle armi, attraverso lo sgombero preventivo del campo di vista e di tiro;
- costruire le strutture necessarie per la limitazione ed il contenimento degli effetti delle esplosioni ravvicinate o a contatto;
- realizzare gli ostacoli indispensabili per la protezione contro le azioni condotte da aeromobili con caratteristiche tali da non permettere assalti provenienti dalla terza dimensione, da collocare in aree idonee all’atterraggio o sui tetti degli edifici;
- mettere in opera il mascheramento necessario per impedire l’individuazione di particolari elementi o localizzazioni pregiate della base;
- effettuare attività di *route* ed *area clearance* delle aree in prossimità e di pertinenza della base sottoposte a minaccia da mine, UXO<sup>1</sup> ed IED<sup>2</sup>;
- costruire i simulacri per l’attuazione del piano di inganno della base;
- installare i sistemi di rilevazione ed allarme intrusione, i congegni ed artifici di allarme di varia tipologia;



<sup>1</sup> *Unexploded Explosive Ordnance (UXO)*, ordigno inesplosivo: quel munizionamento preparato, spolettato, armato o altrimenti disposto all’uso e usato che, per varie motivazioni, non è detonato (Cfr. “Direttiva SMD sull’attuazione del Prot. 5 alla Convenzione per la proibizione o restrizione di Certe Armi Convenzionali”, Ed. 2010).

<sup>2</sup> *Improvised Explosive Device (IED)*.

- rinforzare le infrastrutture esistenti e gli elementi sensibili all'interno della base;
- suggerire al Comandante e realizzare le misure di protezione volte a salvaguardare la tutela ambientale ed a prevenire i rischi di incendio.

## 5. L'impiego delle specialità del Genio

### a. Guastatori

Oltre ad essere in grado di assolvere i compiti del genio nei settori della mobilità e contro mobilità, nello specifico campo della protezione delle forze rappresentano lo strumento in grado di fornire una cooperazione di aderenza all'Arma Base.

Elementi caratteristici:

- spiccata attitudine a cooperare in stretta aderenza di tempo e di spazio con le pedine base della Brigata d'appartenenza, anche mediante inserimenti diretti nelle rispettive formazioni di movimento e nei dispositivi di combattimento;
- capacità di assolvere anche compiti imprevisi in situazioni di limitata sicurezza e disponibilità di tempo e con ridotta possibilità di spiegamento di mezzi tecnici;
- capacità di attuare le demolizioni pianificate e non pianificate di particolare complessità ed importanza;
- struttura organica idonea a soddisfare le normali esigenze di decentramento, garantendo nel contempo sia l'assolvimento dei compiti generali a carattere prioritario, sia la capacità di ricevere e gestire rinforzi;
- leggerezza delle attrezzature e delle dotazioni che ne elevano la capacità operativa e d'intervento.

### b. Pionieri

Sono in grado di assolvere tutti i compiti fondamentali del genio, operando prevalentemente con attività tecnico-tattiche e lavori per il ripristino di itinerari e delle infrastrutture, nonché di reperire, produrre e distribuire le risorse idriche ed elettriche. Riguardo alla FPE posseggono nel proprio organico tutte le capacità (*costruzioni orizzontali e verticali*) per potenziare le opere di protezione realizzate in aderenza dai reggimenti genio guastatori o costruire strutture protettive complesse che richiedono elevata competenza, perizia tecnica e materiali complessi (strutture portanti in cemento armato, opere metalliche, strutture miste, prefabbricazione pesante, ecc.).

L'Esercito ha da tempo individuato la necessità di garantire la disponibilità di unità specialistiche dotate di capacità tecniche (progettazione ed esecuzione di lavori d'ingegneria) equipaggiate con mezzi e materiali idonei a realizzare nell'ambito dell'attività di supporto alla schieramento, ad esempio, le opere necessarie a garantire l'opportuna cornice di sicurezza dei Contingenti dispiegati nei vari Te. Op.

In tale quadro, la F.A. si è dotata di un'unità del genio pionieri assegnata al supporto generale, identificata dall'appellativo CAMPALGENIO<sup>3</sup>.

Tale unità, in particolare, è dotata di specializzazione tale da garantire, in autonomia, la

---

<sup>3</sup> L'appellativo CAMPALGENIO trae origine dalla denominazione delle unità del Genio operativo della AM, in grado di ideare ed eseguire l'intero processo di realizzazione di lavori d'ingegneria (progettazione-esecuzione) sia sul territorio nazionale, sia a supporto dei propri reparti di volo schierati nei vari Te. Op.

completa gestione del processo progettuale/esecutivo tipico dei lavori d'ingegneria, caratteristico della realizzazione di opere infrastrutturali anche a spiccato contenuto tecnico, ossia dove sono richieste la competenza tecnica di personale specialistico e la disponibilità di adeguati mezzi ed attrezzature del genio, di norma non disponibili presso i rgt. guastatori (idonei invece a fornire il supporto diretto alle unità “*combat*”).

Elementi caratteristici:

- attitudine ad assolvere con sistematicità compiti di notevole impegno tecnico, durata e complessità;
- maggior mole delle attrezzature e delle dotazioni, che conferisce loro una particolare attitudine di versatilità.

Il reggimento pionieri dispone anche di ponti da interruzione, mezzi, materiali e attrezzature per l'esecuzione di lavori campali di gran mole connessi con la viabilità, il funzionamento e la protezione dei Comandi e degli organi logistici.

### c. Pontieri e Ferrovieri

Benché trattasi di unità specialistiche ad elevata connotazione tecnica e quindi non costituite per le specifiche esigenze di FPE come i pionieri, possono comunque esprimere alcune capacità per il supporto generale idonee per la realizzazione di opere di protezione complesse, anche se in misura minore rispetto al reggimento pionieri.

## 6. La realizzazione delle opere di protezione

Le opere di FPE rientrano nell'ambito della “*progettazione di opere campali*” a favore delle Unità impiegate nelle operazioni all'estero, in operazioni o attività addestrative particolari sul territorio nazionale o in zone colpite da calamità naturali.

La progettazione delle opere di protezione è incentrata su opere di cemento armato, strutture per le quali risulti conveniente l'utilizzazione della prefabbricazione pesante e leggera, opere in legno, metalliche e comprende tutte le tipologie di lavori in terra.

Sia la progettazione sia la realizzazione delle opere di FPE devono essere effettuate con celerità e coinvolgono diversi livelli di personale altamente qualificato:

- Ufficiale Addetto alla Force Protection Engineering (FPE), quale personale del genio qualificato nella FPE inquadrato nella *J-Eng* o *G3-Eng Cell* del Comando del Contingente ovvero anche in posizione di *Advisor* FPE del Comandante:
  - individua le prime esigenze di FPE sulla base dell'analisi del compito delle unità del Contingente, della situazione operativa nel Teatro di Operazioni e delle caratteristiche delle zone di dislocazione nell'AOR assegnata e del livello qualitativo e quantitativo di opere di protezione definite dal Comandante del Contingente;
  - predisporre le linee guida per la realizzazione degli interventi necessari già sin da prima dell'effettuazione delle ricognizioni in Zona di Operazioni;
  - definisce le caratteristiche operative di impiego e le specifiche tecniche dei materiali da utilizzare sulla base degli standard minimi fissati dagli STANAGs NATO, dai documenti EUMS<sup>4</sup>, dalle pubblicazioni nazionali e manuali tecnici del genio in vigore;

<sup>4</sup> *European Military Staff* (EUMS).



- predisporre il programma degli interventi di FPE per il successivo esame da parte del personale della Catena di Comando responsabile per l’approvazione (*Chief J-Eng*, Comandante di Contingente o COI Difesa) sulla base dei fondi stanziati o eventualmente da assegnare/integrare;
- “Nuclei Progettazione Operativa di Contingenza” (Nuclei POC), composti da Ufficiali e Sottufficiali del genio altamente qualificati nella *Field Engineering* ed inquadrati nei Reggimenti genio:
  - effettuano le ricognizioni in Zona di operazioni;
  - definiscono compiutamente gli interventi da effettuare attraverso specifici progetti di FPE (scaturiti dalle valutazioni e dagli studi redatti precedentemente in via di approssimazione dall’U. Ad. FPE) al fine di renderli:
    - › rispondenti alle caratteristiche del terreno esaminato;
    - › fattibili, sulla base delle risorse disponibili sul territorio e reperibili dalla madre patria;
    - › in linea con i compiti assegnati al Contingente;
    - › aderenti alla minaccia individuata dagli organi del servizio informazioni;
  - forniscono il concorso nella FPE ai *Camp Site Manager* delle basi militari dislocate fuori area, sulla base delle direttive emanate dalle *J-Eng/G3-Eng*.
- unità genio (di aderenza o supporto generale): realizzano le opere progettate anche con il concorso di ditte locali, salvo le limitazioni dovute alla classifica ed alla riservatezza delle opere progettate.

In **Appendice 1**, è riportato lo schema di sintesi del ciclo delle attività necessarie per la realizzazione delle opere di FPE.

In **Appendice 2**, sono evidenziate le attribuzioni di competenza e le responsabilità delle diverse figure che partecipano all’*Engineer Project Management* delle opere di FPE.



## SEZIONE II – MARINA

### 1. La "minaccia ibrida" contro le forze marittime

Le unità navali, soprattutto se militari, hanno sempre rappresentato un obiettivo pagante per le azioni di possibili sabotatori o terroristi. Difatti una carica esplosiva relativamente semplice, se ben piazzata a bordo o fissata in maniera occulta sotto carena, può provocare gravi danni strutturali e causare perdite ingenti, anche in termini di vite umane, e sproporzionatamente superiori rispetto allo sforzo organizzativo ed al materiale necessario per compiere l'attentato. Non è difficile immaginare quali danni può provocare un'esplosione su un'unità militare in navigazione lontano dalla costa con tutto il personale, il carburante e le munizioni presenti a bordo.

Esempi recenti ed eclatanti di azioni terroristiche contro unità navali sono stati gli attacchi subiti nell'ottobre del 2002 dalla motonave LIMBURG a largo delle coste yemenite e quello dell'ottobre del 2000 contro la U.S.S. COLE (DDG 67) alla fonda ad Aden, che costò la vita a 17 marinai statunitensi.



Anche se il rischio di attentati ad unità navali è strettamente correlato con le capacità acquisite dai vari gruppi terroristici internazionali di operare in ambiente marittimo, recenti studi *intelligence* tendono a confermare che al Qaeda sia in possesso di unità mercantili acquisite tramite società di navigazione compiacenti o

colluse, in grado di essere utilizzate sia per il traffico occulto di uomini e armi, sia per eclatanti attacchi terroristici che ripropongano, in chiave marittima, quanto accaduto l'11 settembre 2001. Anche qualora non si utilizzi l'arma del terrorista suicida, gli ordigni utilizzabili contro le unità navali, potendo essere posti sotto carena, permettono agli attentatori di avvicinarsi ed operare occultamente contribuendo alla riuscita dell'effetto sorpresa.

Un attacco contro una nave da guerra permette, infine, di ottenere un notevole ritorno mediatico per il gruppo terrorista che lo porta a termine.

I terroristi possono utilizzare un numero pressoché illimitato di metodi per colpire le forze navali italiane o alleate. È quindi di vitale importanza approfondire, grazie alle informazioni dei servizi d'*intelligence*, il tipo ed il potenziale della minaccia con la quale l'unità potrebbe confrontarsi nella sua normale permanenza nei sorgitori nazionali, ma anche e soprattutto nelle dislocazioni fuori area per operazioni o rappresentanza. Dallo studio e dalla valutazione della minaccia "locale" devono quindi scaturire prudenti misure difensive che mirino alla deterrenza, alla prevenzione e all'eventuale contrasto della minaccia, tenendo nel debito conto l'esigenza di

sostenibilità e mantenimento delle capacità di reazione nel tempo.

La principale minaccia a un'unità militare è costituita da attacchi con bombe ad alto potenziale portati nei modi e con i metodi più disparati sia in porto che in navigazione, e da azioni condotte da *sniper* con armi automatiche o lancia razzi anticarro. Gli attacchi con le bombe determinano gravi danni alle strutture, causano la perdita di numerose vite umane, ottengono l'effetto psicologico di dimostrare la vulnerabilità del mezzo seppur tecnologicamente molto avanzato e soprattutto attraggono e polarizzano l'attenzione dei media.

Quella che segue costituisce una lista, assolutamente non esaustiva, di quelle che possono essere le forme con cui si potrebbe manifestare una minaccia di tipo asimmetrico nei confronti di una unità navale da guerra.

**a. Minaccia subacquea**

Le navi sono particolarmente esposte a questo tipo di minaccia che, data la sua natura insidiosa, potrebbe addirittura portare alla perdita dell'unità senza che si abbia alcun tipo d'allertamento o sentore della minaccia stessa. Essa può essere costituita da:

- operatori subacquei che posizionano sotto carena cariche esplosive, mine, I.E.D. o si fanno esplodere in un'azione di tipo suicida;
- Mine convenzionali;
- R.O.U.V. (Remotely Operated Underwater Vehicles), A.U.V. (Autonomous Underwater Vehicles), U.U.V. (Unmanned Undersea Vehicles) o mini sommergibili.



**b. Minaccia di superficie**

Le piccole imbarcazioni cariche d'esplosivo, sia lente sia veloci, potrebbero costituire una vera e propria arma d'assalto contro un'unità militare (vedi il caso dell'U.S.S. Cole – foto alla pag. precedente) oppure essere usate come piattaforma dalla quale condurre un attacco di tipo "stand-off" tramite armi spalleggiate di vario tipo. Altre tipologie di minaccia asimmetrica di superficie sono:

- motoscafi-bomba radiocomandati;
- moto d'acqua o windsurf utilizzati per attacchi suicidi;
- imbarcazioni, barche o piccole navi mercantili utilizzate per abbordare le unità militari alla fonda od ormeggiate in porti scarsamente sorvegliati<sup>1</sup>.

**c. Minaccia proveniente da terra**

Il principale mezzo d'attacco asimmetrico terrestre è costituito da bombe ad alto potenziale.

<sup>1</sup> Allo scopo di contrastare efficacemente tale tipologia di minaccia è opportuno adottare la cosiddetta "Sicurezza portuale" definita come le predisposizioni orientate alla "salvaguardia di naviglio, porti, scali portuali, attrezzature portuali e carichi da minacce interne quali: distruzione, perdite, danni causati da atti di sabotaggio o da altre azioni sovversive, incidenti, furti o altre cause di analoga natura" (SMD G-024). Per approfondimenti sulla tematica in ambito NATO si rimanda al documento "Allied Maritime Force Protection Against Asymmetric Threats in Harbour and Anchorage" ATP-74 (STANAG 1468).



Questo tipo di minaccia si può materializzare attraverso veicoli imbottiti d'esplosivo che possono essere "scagliati" ad alta velocità contro la nave o semplicemente parcheggiati in banchina anche prima dell'arrivo in porto dell'unità. Non va poi sottovalutata, soprattutto quando in sosta in sorgitori non militari, la possibilità di un attacco portato da kamikaze che potrebbero salire a bordo spacciandosi

per fornitori di merci e servizi, lavoratori del porto, ecc.

La minaccia asimmetrica proveniente da terra può quindi manifestarsi attraverso:

- attacchi con bombe autobomba (con o senza attentatori suicidi);
- attacchi con armi automatiche o lanciagranate portati da cecchini occultati all'interno d'installazioni portuali prospicienti il posto d'ormeggio;
- il rapimento o l'attentato/aggressione di membri dell'equipaggio a scopo propagandistico o di ricatto nei confronti della politica estera del Governo;
- dimostrazioni o proteste non pacifiche;
- intrusione occulta di estranei a bordo.

**d. Minaccia proveniente dall'aria**

Può comprendere:

- aerei di linea dirottati, aerei turismo o velivoli ultraleggeri pilotati da terroristi kamikaze;
- aeromodelli radiocomandati o velivoli tipo U.A.V. (*Unmanned Aerial Vehicles*);
- palloni aerostatici o mongolfiere.

**e. Minaccia di tipo "stand off"**

I moderni arsenali militari comprendono una gran varietà di armi di tipo "stand off" potenzialmente utilizzabili da gruppi estremistici per attacchi di tipo asimmetrico. Tra queste vale la pena menzionare i sistemi missilistici controcarro portatili o i sistemi antiaerei spalleggiabili. Le armi di questo tipo, oltre a poter essere utilizzate direttamente contro unità navali, possono costituire una grave minaccia per gli aeromobili imbarcati durante le operazioni di volo condotte in prossimità di costa.

**f. Minaccia di tipo "CBRN"**

Esistono al momento prove circostanziate che fanno ritenere probabile che alcuni gruppi terroristici di spicco stiano cercando la maniera di entrare in possesso di agenti biologici o chimici da utilizzare sotto forma di liquidi o aerosol da disperdere nell'ambiente nonché di materiale radioattivo con il quale poter costruire bombe radiologiche "sporche".

La minaccia CBRN dunque va considerata come sempre presente e possibile anche in territorio nazionale e pertanto attuabile a bordo di unità dislocate in taluni particolari scenari operativi fuori dagli stretti.



**g. Minaccia per le "Information operations/C2"**

La società occidentale è oggi fortemente dipendente dall'uso della "information technology". Questa dipendenza può rivelarsi una condizione di vulnerabilità sfruttabile da potenziali avversari.

L'intercettazione d'informazioni scambiate via e-mail o di conversazioni telefoniche a mezzo cellulare può fornire preziose informazioni sui movimenti dell'unità, risultando di grande ausilio nella pianificazione di attacchi di tipo asimmetrico.

**2. Principi fondamentali per la FP in ambito Marina**

La FP copre un vasto spettro d'azioni e misure inerenti la sicurezza passiva, la difesa attiva e la protezione delle forze. In tempo di pace le misure di FP generalmente implementate sono essenzialmente quelle inerenti la sicurezza protettiva (*protective security*) e quelle garantite dai servizi d'emergenza (ad esempio polizia, pompieri, soccorso medico ecc.). Al crescere della tensione, di pari passo col crescere dell'approntamento operativo delle forze, le necessità di FP evolvono verso capacità più prettamente tecnico-militari. In ambito marina, vengono quindi identificate quattro aree di interesse operativo:



- Sicurezza preventiva (*Pro-Active security*);
- Difesa Attiva (*Active Defence*);
- Difesa Passiva (*Passive defence*);
- Capacità di Recupero (*Recuperation*).

**a. Sicurezza Preventiva**

La Sicurezza preventiva è definita come "il sistema organizzato di misure difensive messo in atto e mantenuto, a tutti i livelli di comando, con lo scopo di raggiungere e mantenere la cosiddetta *Security*. La *Security* (sicurezza degli uomini, dei mezzi e delle infrastrutture), a sua volta, si articola nelle seguenti sotto aree: la *General Security* (norme generali di sicurezza), la *Operational Security* (sicurezza operativa), la *Physical Security* (sicurezza di mezzi e strutture), la *Personnel Security* (sicurezza del personale) e la *Information Security* (INFOSEC). Queste sotto aree della *security* sono a loro volta direttamente collegate ed interagenti con le misure volte a garantire la sicurezza antincendio, il rispetto della legge (*Law Enforcement*), la salute e la prevenzione degli infortuni (*Health & Safety*), la sicurezza degli spostamenti e del tempo libero (*Road/Traffic and Recreational Safety*).

La *Safety* e la *Security* nei confronti dell'intero spettro di minacce e pericoli ipotizzabili per il personale militare, rimangono responsabilità sia collettiva (in pratica a carico dei Comandi) che individuale (cioè a carico del singolo militare).

**b. Difesa Attiva**

La sicurezza attiva include tutte quelle misure necessarie a scoraggiare, prevenire, impedire o ridurre l'efficacia di un attacco nemico, incluse la difesa contro i mezzi di superficie, subacquei e la difesa antimissile.

La difesa attiva è quindi volta a togliere l'iniziativa all'aggressore sia negandogli la possibilità di nuocere sia neutralizzando la sua capacità di attaccare o di porre in essere una minaccia. La difesa attiva include, pur non limitandosi a questo, la *Offensive Counter Air* (OCA), le operazioni d'interdizione, la difesa anti aerea e anti missile balistico, le capacità di combattimento terrestre e navale, il dominio della Area di Responsabilità Tattica (TAOR), le capacità di coordinamento con le forze amiche adiacenti ed il controllo degli accessi alle installazioni militari.

Per le forze dislocate in aree d'operazione all'estero che si trovano ad operare in una area di possibile minaccia di tipo CBRN, tutte le funzioni di difesa attiva devono poter essere svolte in ambiente contaminato senza che ciò pregiudichi la tempestività delle operazioni e l'efficacia in combattimento.

**c. Difesa Passiva**

La difesa passiva si riferisce alle misure necessarie per proteggere unità e formazioni militari dalle conseguenze operative, tattiche, psicologiche e politiche derivanti dall'uso avverso di armi convenzionali e di tipo CBRN.

La possibilità di avere notizie di *intelligence* dell'imminente attacco convenzionale o non convenzionale contro comandi o unità militari è da considerarsi un fattore chiave per aumentare la capacità di sopravvivenza, così come la capacità di mettere in atto una preventiva ed efficace organizzazione di difesa passiva.

I Comandi superiori/centrali (CINCOMNAV, NAVISPELOG, MARISTAT in ambito Marina) devono, inoltre, far sì che il personale potenzialmente esposto agli effetti d'armi convenzionali o di tipo CBRN abbia in dotazione il necessario equipaggiamento in accordo alle direttive NATO e nazionali in vigore e sulla base dell'effettivo rischio valutato presente nel teatro operativo di dislocazione.

La difesa passiva include, senza esserne limitata, la protezione fisica del personale e del materiale da ogni genere d'attacco.

Tutte le forze dislocate in teatri d'operazione all'estero e quelle che si trovano in zone di potenziale pericolo di tipo CBRN devono poter continuare ad operare in ambiente contaminato garantendo le necessarie capacità di comando e controllo e di difesa CBRN.

**d. Capacità di Recupero**

La capacità di recupero copre tutte le misure 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. I comandi e le forze dipendenti devono riuscire a possedere un'effettiva capacità di recupero a seguito dei danni causati da:



- un attacco avversario;
- una contaminazione dovuta a materiale tossico di origine industriale (*Toxic Industrial Material*, TIM).

Le funzioni di recupero possono includere, senza esserne limitate, il *Damage Control* (DAMCON), la ricognizione e valutazione post attacco (PAR), la ricerca e brillamento di ordigni inesplosi (EOR/EOD), la lotta antincendio, la gestione ed il soccorso dei feriti e, qualora necessario, la decontaminazione.

Per le forze dislocate in aree d'operazione all'estero, tutte le funzioni di ricupero devono poter essere assicurate anche in ambiente CBRN.

Per quanto riguarda, infine, l'organizzazione FP di bordo, essa è strutturata in modo da poter supportare il Comandante nella sua funzione di comando nello specifico argomento, basandosi quindi su un organo consultivo (Consiglio di FP) che supporti il Comandante nel prendere le sue decisioni e su un organo esecutivo (*FP Management Group*) che si occupi di metterle in pratica.

### 3. Livelli di responsabilità

I livelli di responsabilità inerenti la *Force Protection* di un'Unità Navale sono una funzione di Comando di Unità isolata o di dispositivo navale (più navi in porto sotto lo stesso Comando complesso).

L'organizzazione FP di una nave si compone degli elementi necessari a valutare il rischio; gestire il rischio; rispondere in maniera efficace in caso di incidente; gestire le fasi del post incidente; mantenere aggiornate le procedure e i piani di FP di Bordo; curare l'addestramento del personale addetto alla FP e sensibilizzare l'equipaggio alla minaccia asimmetrica.

L'organizzazione FP deve essere semplice, versatile ma soprattutto ben conosciuta e ben testata in modo da potersi adattare alle varie situazioni operative ed alle varie missioni in cui una Unità od una Forza navale può essere chiamata ad assolvere.

L'organizzazione, infine, deve essere sostenibile (anche in termini economici) e deve risultare efficace ed attuabile anche in caso di operazioni con marine alleate o dispositivi multinazionali.

### 4. Organizzazione Force Protection di bordo

Per poter rispondere ai sopraccitati requisiti, l'organizzazione FP deve essere strutturata in modo da poter supportare il Comandante nella sua funzione di Comando rispetto allo specifico



argomento. Il Comandante si avvale di un organo consultivo di FP, denominato Consiglio di FP, che è composto dalle figure di preminente importanza di bordo.

Il Consiglio di FP si riunisce in concomitanza dell'assegnazione di una missione all'Unità, al variare delle condizioni di allertamento o quando ritenuto necessario dal comando di Bordo in base al modificarsi della situazione

in atto.

La responsabilità del coordinamento delle misure scaturite dal processo di valutazione del rischio condotto dal consiglio di FP è devoluta al Comandante in 2<sup>a</sup>, che si avvale del personale



preposto al *FP Management Group*.

Il Comandante in 2<sup>a</sup> è anche responsabile dell'attuazione del dispositivo di FP, della sensibilizzazione dell'intero equipaggio verso tutti gli aspetti inerenti la FP e in questa situazione si avvale del *FP Responce Group*.

L'organizzazione di FP si articola sui seguenti livelli funzionali che si identificano con gli elementi di organizzazione di fianco indicati:

- Livello Comando      Comandante (con l'ausilio del Consiglio di FP);
- Coordinamento      Comandante in 2<sup>a</sup> (con l'ausilio del *FP Management Group*);
- *Reaction & Recovery Responce Group*.

A sua volta il *Responce Group* si compone di:

- *Reaction team (RT)*;
- *Safety team*;
- *Security team*;
- *Information team*;
- *C3 team*;
- *Medical team*;
- *Logistic team*;
- *Under water team*.

L'organizzazione deve essere attagliata per i casi di porto o navigazione mantenendo a fattore comune la forza di deterrenza che ha lo scopo di scoraggiare azioni offensive nei confronti dell'Unità mediante la messa in atto di opportune misure dissuasive.

Affrontando la problematica della FP con Unità in navigazione è bene precisare, invece, come tale minaccia debba essere intesa quale particolare manifestazione delle convenzionali tipologie di minaccia altrimenti definite. Pertanto, pur avendo peculiari specificità, la minaccia asimmetrica può essere infatti considerata, in base all'ambiente nel quale si manifesta come un particolare tipo di minaccia convenzionale da affrontare e contrastare nell'ambito della corrispettiva forma di lotta.

#### **a. Unità in porto**

Con Unità in porto la dissuasione e deterrenza si esplicano 24 ore su 24 attraverso il vigile controllo degli accessi all'unità; la presenza palese e ben visibile di personale armato; la diffusione dell'allarme e l'allertamento della forza di reazione in caso di necessità.

La reazione ha lo scopo la gestione di un incidente di tipo simmetrico al suo manifestarsi, o nell'imminenza del suo manifestarsi assicurando la gestione dell'incidente nell'immediato verificarsi dello stesso; le procedure d'intervento delle varie forze a disposizione non ultime quelle di polizia; l'allertamento della catena di Comando e delle Autorità locali.

In questa situazione il *Reaction Team* si compone di tre cellule operative:

- *Detection Force* - DE.FO: con funzione di deterrenza, assicurata dalle misure e predisposizioni previste dall'assetto di guardia in porto.
- *Reaction Force* – RE.FO: con funzione di gestione dell'incidente al suo manifestarsi o nell'imminenza del suo manifestarsi, gestione dell'intervento del supporto interno (SU.PO) e/o esterno (Forze di polizia, Forze specialistiche, Soccorso sanitario), allertamento della catena di Comando e delle Autorità locali.



- *Support Force* – SU.PO: con funzione di supporto alla RE.FO., garantendo la sostenibilità di imprevista e improvvisa implementazione di misure connesse ad elevati livelli di FP che possano richiedersi fuori dall'orario lavorativo, e di attuazione delle misure per assicurare il *recovery* ove possibile.

**b. Livelli di Force Protection con Unità in navigazione**

I livelli di FP variano da 5 ad 1 a seconda dell'incremento di minaccia rilevata o percepita corrispondendo a uno stato delle armi che varia da 3 a 1 che relativamente alla FP corrisponde al ruolo combattimento delle altre forme di lotta.

**c. Normativa**

La normativa specifica edita dal Comando della Squadra Navale dispone nel dettaglio i compiti e le disposizioni attraverso le quali discendono le organizzazioni che ciascuna Unità o ciascuna forza navale si deve dare in relazione alla tipica situazione ed alle forze a disposizione.



**SEZIONE III - AERONAUTICA****1. Generalità**

La peculiarità della componente aeronautica, abbinata ai sistemi indispensabili allo sviluppo della missione aerea (Basi aeree, sistemi di rifornimento, depositi, infrastrutture e servizi per la navigazione, ecc.) impongono l'adozione di particolari misure di FP orientate a garantire



sicurezza e protezione terrestre al personale, ai mezzi e materiali, nonché alle stesse installazioni, assetti e infrastrutture, sia fuori dai confini nazionali che in Patria.

Tale esigenza è sentita soprattutto quando il mezzo aereo è rischierato in Teatri Operativi in cui è chiamato a condurre operazioni aeree da basi estese, spesso sedi di traffico aereo non

militare, sovente scarsamente difese e, quindi, facilmente attaccabili.

L'estrema vulnerabilità degli assetti aerei a terra congiuntamente a tutte le unità di supporto ad essi dedicate ha sviluppato la consapevolezza che la FP è un fattore decisivo e critico per lo sviluppo del Potere Aereo<sup>1</sup>.

**2. Principali capacità della protezione delle forze per le operazioni aeree**

Il documento dottrinale relativo alla Protezione delle Forze per le Operazioni Aeree, seguendo la classica visione NATO di settore, suddivide l'intero spettro delle capacità della FP in quattro aree principali:

- Sicurezza Protettiva;
- Difesa Attiva;
- Difesa Passiva;
- Recupero della Capacità Operativa.

Le capacità da rischierare in una operazione dipendono, ovviamente, dal contesto in cui si opera e sono strettamente correlate al livello di pericolosità dell'ambiente circostante. Tali



capacità sono espresse sia da unità altamente specializzate in FP che da altri elementi che comunque concorrono alla difesa di una Base Aerea.

Alla base del requisito che un dispositivo di FP deve possedere vi è, quindi, un'accurata fase di analisi della situazione logistica e di studio della minaccia.

In tale contesto occorre poi tener presente che le Operazioni Aeree in O.F.C.N. (Operazioni Fuori dai Confini Nazionali) possono essere condotte da una *Well-Found Base*, da una *Austere Base* o da una *Bare Base*, volendo con tali termini indicare, in modo decrescente, il livello di sostegno logistico che è possibile aspettarsi nelle varie situazioni.

<sup>1</sup> Tale considerazione ha spinto la NATO ad elaborare una dottrina specifica di settore: la *Force Protection Doctrine for NATO Air Operation* (STANAG 7217). Il documento, allo stato attuale in fase di studio, costituisce il vero punto di riferimento per la creazione di un credibile strumento di Protezione delle Forze a connotazione "Air".

**a. Sicurezza Protettiva**

La Sicurezza Protettiva è definita come il sistema di misure difensive istituito e mantenuto a tutti i livelli di Comando con lo scopo di raggiungere e mantenere un ambiente operativo sicuro.

Di tale ambito fanno parte tutte le misure di sicurezza fisica, del personale, delle infrastrutture unitamente alla sicurezza antiterrorismo ed a quella delle informazioni (INFOSEC). Si tratta quindi di misure che necessitano di una collaborazione stretta con altri settori dell'organizzazione di una Base Aerea, primo tra tutti quello dell'*Intelligence*.

Al di là del preciso dimensionamento del dispositivo di FP, la Sicurezza Protettiva deve sempre comprendere la capacità di disciplinare l'accesso in Base intesa sia in termini di identificazione certa del personale (*Management* dell'Identità), sia quale capacità di discriminare l'accesso alle aree riservate interne alla Base. Tale capacità deve essere espressa ai massimi livelli e deve basarsi sui più moderni sistemi per la memorizzazione di dati ivi compresi quelli che prevedono il controllo dei dati biometrici del personale.

Ulteriore sviluppo in tale settore è rappresentato dalla capacità di assicurare, tramite assetti dedicati, un servizio di *Close Protection* a favore di personale di rilievo/autorità, nonché quello di Sicurezza anche nelle fasi di trasferimento di uomini e materiali a mezzo di vettori aerei (*Air Marshalling*).

Qualsiasi attività di FP deve tener conto della valutazione della minaccia che, per consentire l'adozione di adeguate misure di protezione, deve essere costantemente aggiornata. A tale scopo un dispositivo di Protezione delle Forze deve essere dotato di una capacità *Intelligence*, abbinata ad un efficace processo di sviluppo cognitivo, in grado di collezionare dati provenienti da varie fonti compresi quelli derivanti dagli assetti di *Human Intelligence* (*Field Humint Teams - FHT*) e quelli provenienti da assetti ISTAR (*Intelligence, Surveillance, Target Acquisition And Reconnaissance*).

**b. Difesa Attiva**

La Difesa Attiva è definita come l'insieme delle misure necessarie per impedire, prevenire, annullare o ridurre l'efficacia di un attacco nemico, inclusa la difesa contro attacchi di superficie, aerei e missilistici.

Le misure di Difesa Attiva includono, tra le altre, le capacità di combattimento terrestre, il dominio della Tactical Area of Responsibility - TAOR (nel recente passato definita anche come *Ground Defence Area*), il controllo degli ingressi e la Controaviazione Difensiva.

**(1) La capacità di combattimento terrestre**

La capacità di combattimento terrestre deve essere sviluppata a mezzo di una unità di manovra particolarmente specializzata nel settore della FP, ben equipaggiata e mantenuta ad un elevatissimo stato di prontezza.

In alcuni compiti di routine può essere impiegato anche personale non particolarmente specializzato nel settore della FP.



Gli assetti dedicati al combattimento terrestre comprendono anche il “*Guard Incident Commander*”, che svolge, tra l’altro, il compito di Comandante sulla scena (*on the spot Commander*) in caso di incidente e le Unità Cinofile (*Military Dogs*).



Le Unità Cinofile, altrimenti denominate “K-9”, vengono, in particolare, definite come “significativo moltiplicatore di forza” che possono essere impiegate isolatamente o come componenti di pattuglie da combattimento. In quest’ultimo caso si ritiene opportuno

che tali Unità posseggano lo stesso livello di *Expertise* degli specialisti della FP.

Le Unità Cinofile possono essere suddivise in tre tipologie principali:

- Explosive Detection Dog (EDD).
- Patrol Dog (PD);
- Force Protection Dog (FPD).

## (2) La “*Tactical Area of Responsibility - TAOR*”

La dottrina NATO della Protezione delle Forze nelle Operazioni Aeree definisce la TAOR come quell’area che viene stabilita intorno ad una *Deployed Operating Base* (DOB) al fine di prevenire, attraverso il suo dominio appunto, gli attacchi diretti ed indiretti condotti contro gli aeroplani, le infrastrutture ed il personale. Le dimensioni della TAOR devono essere sufficientemente ampie (sino a 10 - 15 km dal perimetro aeroportuale) per 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 per essere efficace deve prevedere l’applicazione di misure “stratificate” che comprendono:

- l’istituzione di posizioni di fuoco difensive da disporre quanto più vicino possibile agli assetti da difendere, con la possibilità di essere incrementate mediante l’impiego di assetti GBAD (*Ground Based Air Defence*)<sup>2</sup>, purché gli stessi siano integrati in un sistema C2 interoperabile con quelli aerei deputati ad assolvere tale compito”;
- 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*) e di Fuoco di precisione anche esterni al perimetro della Base (*Close Precision Attack - Snipers*).

## (3) Il controllo degli ingressi

Il controllo degli ingressi è definito di primaria importanza specie in caso di uso di aeroporti commerciali (caratterizzati da un notevole flusso di personale civile locale) per la conduzione delle operazioni aeree militari.

<sup>2</sup> Assetti di artiglieria c/a.

I punti di controllo degli accessi possono essere di due tipi:

- *Permanent Vehicle Checkpoint (PVCP)*;
- *Entry Control Point (ECP)*.

Il personale chiamato ad operare presso un PVCP è particolarmente esposto ad attacchi nemici e, pertanto, deve essere particolarmente addestrato. Quando possibile deve operare congiuntamente alle Unità Cinofile.

Gli ECP sono sempre disposti all'interno del perimetro della Base e consentono l'accesso all'interno di Settori della Base adibiti a particolare attività.

#### (4) La Controaviazione Difensiva

Lo scopo delle operazioni di contro aviazione è di raggiungere il desiderato livello di Controllo dell'Aria, distruggendo o impedendo l'utilizzo del Potere Aereo Avversario. In tale quadro le operazioni di Controaviazione Difensiva (*Defensive Counter Air*) sono volte a proteggere le forze amiche e gli interessi vitali da un qualsiasi attacco aereo e/o missilistico nemico e consistono in tutte quelle misure attive e passive (diradamento,



mascheramento, inganno, uso di *shelter*, ecc.) atte a scoprire, identificare, intercettare e distruggere le forze aeree/missilistiche nemiche o impedire che esse possano colpire, attaccare o penetrare il *battlespace* amico o, quantomeno, ridurne l'efficacia.

La Controaviazione Difensiva, nello specifico la *Ground Based Air Defence (GBAD)*<sup>3</sup>,

deve comprendere la capacità di difesa di punto, di area e di rotta di assetti di alto valore. Essa deve essere capace di scoprire, seguire, riportare, ingaggiare e identificare *target* che attraversano l'area di responsabilità, evitando il fuoco fratricida.

Nel segmento della difesa aerea, si evidenzia un chiaro ampliamento della minaccia, che evolve in maniera sempre più diversificata. Oltre alle tradizionali minacce di tipo aerodinamico (a cui si aggiungono realtà di tipo *unmanned* o *remotely piloted*) devono essere considerate ed efficacemente contrastate soprattutto le minacce dalla tipologia RAM<sup>4</sup>, oltre a quelle balistiche nelle loro diversificate gittate e tipologie. Infatti, le basi aeree nei teatri operativi spesso sono esposte a minacce costituite da razzi balistici/guidati, proiettili d'artiglieria e colpi di mortaio, nei confronti delle quali è necessario consolidare capacità di avvistamento, comando e controllo e contrasto. Il requisito base che sta portando allo sviluppo della capacità *Counter-RAM (C-RAM)* è, dunque, quello di avere un sistema in grado di distruggere proiettili di artiglieria, razzi e

<sup>3</sup> Sono costituite da missili terra-aria (SAM), artiglierie controaerei e associati sistemi C4I.

<sup>4</sup> *Rockets, Artillery, Mortars.*

bombe di mortaio in volo il più possibile lontano dal punto di impatto. L'esigenza capacitiva C-RAM è rilevante anche in ambito NATO e, ancorché sia riconosciuta la necessità di assicurare un ampio margine di autonomia nazionale nell'impiego, stante le peculiarità e le tempistiche reattive particolarmente ristrette, questa capacità deve essere integrata nella più ampia cornice del NATO *Integrated Air and Missile Defence* (IAMD)<sup>5</sup> ovvero nazionale.

L'attuale disponibilità di sistemi C-RAM basati esclusivamente sull'uso di proiettili/intercettori (dunque più facilmente soggetti a problematiche di saturazione), nonché le strettissime tempistiche per il contrasto RAM, ancorché altamente automatizzate, rendono le reali capacità operative di questi sistemi non sempre pienamente rispondenti alle necessità operative. Lo sviluppo e il consolidamento di tecnologie di tipo *Direct Energy Weapon* (DEW) può fornire un considerevole e fondamentale incremento capacitivo. La capacità C-RAM risulta, quindi, complementare alle consolidate capacità GBAD<sup>6</sup> di tipo *Short Range Air Defence* (SHORAD) e *Very Short Range Air Defence* (VSHORAD) e insieme mirano a soddisfare le esigenze di protezione di forze ed equipaggiamenti dislocate su basi aeree da minacce provenienti dalla terza dimensione.

La protezione da minacce missilistiche balistiche di diversa tipologia e gittata è assicurata dalla *Missile Defence*, nella più ampia cornice dell'IAMD, che va ben oltre il *footprint* difensivo della singola installazione. In questo ambito, infatti, la *Theatre Missile Defence* materializza la difesa contro la minaccia portata dai missili di Teatro<sup>7</sup> contro le forze amiche. In particolare, la protezione delle forze amiche schierate in teatro operativo è garantita attraverso la capacità *Active Layered Theatre Ballistic Missile Defence* (ALTBMD).

### c. **Difesa Passiva**

La Difesa passiva è definita l'insieme delle misure necessarie per proteggere le unità dalle conseguenze derivanti dall'uso di armi convenzionali e CBRN. La Difesa Passiva quindi include, ma non solo, la protezione fisica del personale e dei materiali da ogni forma di attacco.

La Difesa CBRN deve comprendere le seguenti capacità:

- rilevazione Biologica (*BW Defence*)<sup>8</sup>;
- Centri di osservazione e segnalazione delle offese CBRN (*CBRN W&R*<sup>9</sup> *Centers*);

<sup>5</sup> Ampio progetto volto alla protezione della popolazione, territorio e delle forze dei paesi dell'Alleanza Atlantica contro la minaccia di missili balistici.

<sup>6</sup> I sistemi c/a sono classificati come segue dalla Pub. di SME n.5910 ed. 2002 "L'impiego dell'artiglieria delle grandi unità Parte II Artiglieria Controaerei":

- sistemi a cortissima portata (*Very SHORt Range Air Defence* - VSHORAD), portata fino a 5km, quota fino a 1500 m.;
- sistemi a corta portata (SHORAD), portata da 5 a 15km, quota fino a 3.000 m.;
- sistemi missilistici a media portata (MSAM), portata da 15 a 50km, quota fino a 15.000 m..

<sup>7</sup> Un missile di Teatro è un missile impiegato per attaccare assetti amici all'interno di un teatro di operazioni, a prescindere della portata del sistema considerato e dal metodo di lancio del missile (AJP-3.3, *Allied Joint Doctrine for Air and Space Operations*).

<sup>8</sup> *Biological Warfare Defence*.

<sup>9</sup> *Warning And Reporting*.

- *staff* per la protezione collettiva (COLPRO<sup>10</sup>);
- ricognizione Chimica e Radiologica;
- decontaminazione;
- Campionamento ed Identificazione di agenti Biologici, Chimici e Radiologici (SIBCRA<sup>11</sup>);

La Difesa Passiva deve poter esprimere, inoltre, capacità di controsorveglianza e cioè:

- mimetizzazione;
- mascheramento;
- dispersione;
- inganno;

così come capacità di protezione fisica attraverso la disponibilità di specialisti in *Force Protection Engineering*.

#### d. **Recupero della Capacità Operativa**

Il Recupero della Capacità Operativa (per brevità definito Ripristino) è definito come l'insieme delle misure necessarie ad una Base Aerea per il recupero dagli effetti di un attacco, per ripristinare i servizi essenziali e consentire la continuazione delle operazioni con la minima interruzione. Il Ripristino include, tra l'altro:

- il controllo dei danni (*Damage Control*);
- la ricognizione post-attacco (*Post-Attack Reconnaissance - PAR*);
- la capacità EOR-EOD e IEDD;
- la capacità antincendio;
- il soccorso;
- il trattamento dei feriti;
- la riparazione delle superfici dedicate alle operazioni aeree, dei servizi essenziali e delle infrastrutture.



Pur nella consapevolezza che le suddette capacità sono tutte essenziali per una buona organizzazione di un dispositivo di FP, l'esperienza maturata dalle nazioni della NATO nelle ultime *Crisis Responce Operation* porta a porre una particolare enfasi sulle necessità di disporre di un efficace dispositivo per il contrasto agli IED (*Improvised Explosive Device*). Tale capacità risulta di particolare importanza

nelle Basi Aeree sia nella difesa degli accessi sia nell'ambito del dominio della "*Tactical Area of Responsibility*". La capacità in parola deve avvalersi, tra l'altro, di misure appartenenti alla Guerra Elettronica (disturbatori C-IED).

<sup>10</sup> COLlective chemical, biological, radiological and nuclear PROtection.

<sup>11</sup> Sampling and Identification of Biological, Chemical and Radiological Agents.



**3. Altre capacità essenziali**

Qualsiasi dispositivo di Protezione delle Forze da rischiare in Teatro di Operazioni deve possedere una capacità di Comando e Controllo dedicata (FP C2).

La complessità della struttura di FP C2 dipende, ovviamente, dalla situazione. Indipendentemente dalla dimensione della unità all’interno della quale opera la struttura di FP, la capacità di C2 fa sì che il Comandante dell’unità possa concentrare la propria attenzione sulla sua missione primaria nella consapevolezza che qualsiasi incidente sarà prevenuto o trattato con efficacia ed efficienza.

Altra capacità indispensabile per la realizzazione di un dispositivo di FP credibile è rappresentata dall’implementazione di misure per la scoperta automatica di intrusioni (Intrusion Detection Systems-IDS) e per la sorveglianza elettronica-TVCC.

Idonei apparati antintrusione e sistemi TVCC (anche con sensori termici – *Thermal Camera*) consentono di ridurre l’apporto di personale dedicato alla Difesa Attiva di una base ed aumentano il livello di sicurezza specie nelle ore notturne.

Sia per garantire un efficace flusso di comunicazioni all’interno della catena di Comando e Controllo del dispositivo di Protezione delle Forze, sia per garantire il buon funzionamento dei sistemi elettronici in dotazione al personale addetto alla FP, ovvero per assicurare il primo intervento tecnico ai sistemi antintrusione e TVCC disponibili, il dispositivo di FP deve possedere un minimo di capacità CIS dedicata.

Le capacità che dovrebbe esprimere un efficace sistema di protezione delle forze sono riassunte nella figura di seguito riportata:

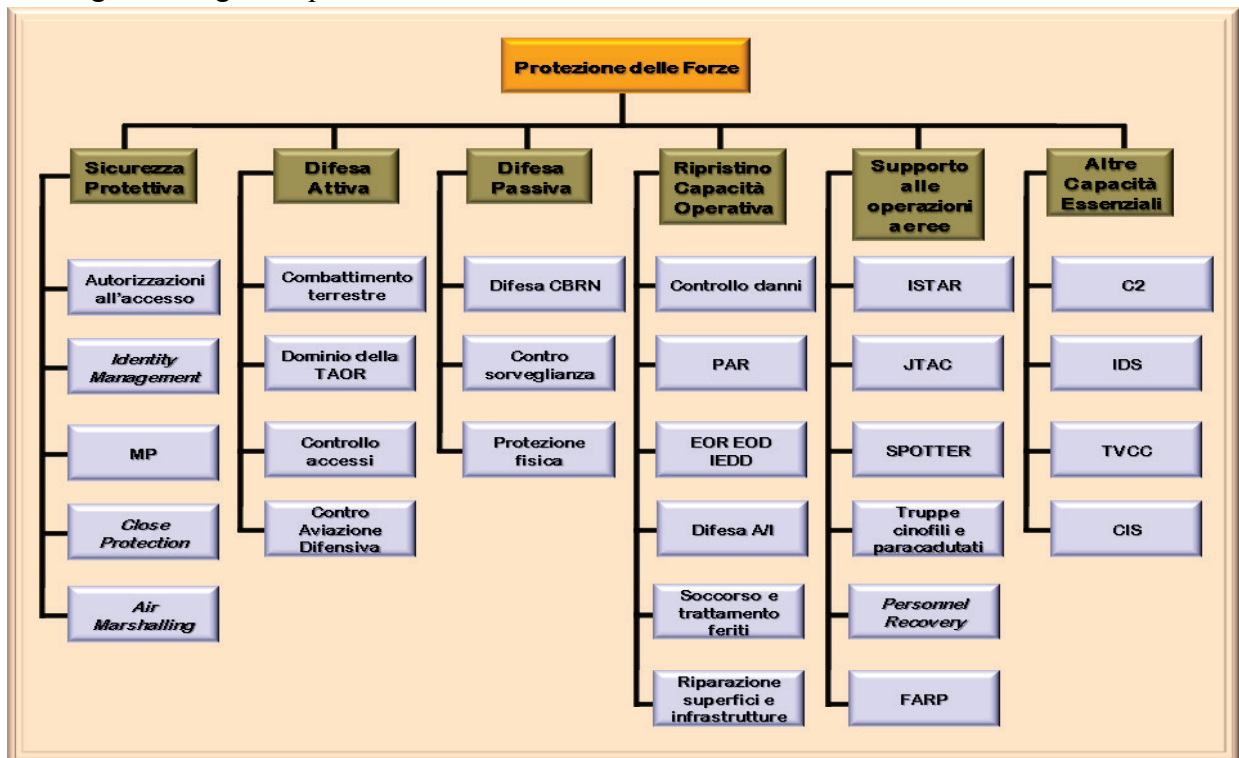


Figura 9 Capacità della protezione delle forze per le operazioni aeree



## ATTRIBUZIONI DI COMPETENZE E RESPONSABILITÀ NELLA REALIZZAZIONE DI OPERE DI FPE

INCARICO RICOPERTO NELL'AMBITO DEL CONTINGENTE	ATTRIBUZIONI E COMPETENZE
Comandante del Contingente	<ul style="list-style-type: none"> <li>· Stabilisce il livello qualitativo e quantitativo delle opere di protezione delle unità del Contingente, sulla base della minaccia individuata dal J-2.</li> <li>· Approva il programma definitivo degli interventi di FPE redatto dalla Cellula/Branca <i>J-Eng</i>.</li> </ul>
Ufficiale Addetto FPE	<ul style="list-style-type: none"> <li>· Individua le esigenze di FPE del Teatro di Operazioni.</li> <li>· Redige il programma di massima (precedente le ricognizioni) e definitivo degli interventi di FPE (al termine delle ricognizioni).</li> <li>· Definisce le caratteristiche operative e le specifiche tecniche dei materiali da impiegare.</li> <li>· Predisporre le linee guida per la realizzazione delle opere di FPE.</li> </ul>
<i>Chief Engineer</i>	<ul style="list-style-type: none"> <li>· Stabilisce i requisiti minimi delle opere di FPE.</li> <li>· Approva il programma di massima degli interventi di FPE.</li> <li>· Emanando gli Ordini necessari per le ricognizioni dei Nuclei POC in Teatro, sulla base del predetto programma.</li> <li>· Approva tecnicamente il programma definitivo degli interventi di FPE.</li> <li>· Approva i progetti di FPE, in funzione del titolo di studio posseduto.</li> <li>· Assegna le priorità d'intervento.</li> <li>· Effettua i collaudi delle opere di FPE realizzate, in funzione del titolo di studio posseduto.</li> </ul>
Nuclei POC ( <i>Point of Contact</i> ) Rgt.Genio	<ul style="list-style-type: none"> <li>· Effettuano le ricognizioni.</li> <li>· Redigono i progetti, in funzione del titolo di studio posseduto.</li> <li>· Controllano i lavori durante la realizzazione.</li> </ul>
Unità del Genio	Realizzano le opere di FPE.



## LA MINACCIA IED

### 1. Introduzione

La minaccia costituita dagli *Improvised Explosive Device* (IED) affonda le proprie radici in reti<sup>1</sup> di soggetti ed organizzazioni di opposizione violenta che spaziano dalle bande criminali agli insorgenti, fino ai terroristi con capacità globale, e che hanno fatto degli IED la loro arma preferita<sup>2</sup>. Tali network-minaccia operano in ambienti caratterizzati dalla generale disponibilità<sup>3</sup> di componentistica a duplice uso (lecito/illecito) e dall’accesso a materiale esplosivo prontamente reperibile a livello locale. Sfruttando la possibilità di ricorrere ai servizi di IED-maker<sup>4</sup> con esperienze di combattimento in aree ove sistemi di governo deboli e corrotti coesistono con condizioni socioeconomiche pressoché disperate, tali organizzazioni di opposizione hanno facile gioco nel creare ed alimentare instabilità politica ed economica e costituiscono una minaccia costante e durevole per le Forze Armate.

Quando l’impiego di ordigni esplosivi improvvisati viene associato a campagne di informazione orchestrate al fine di minare la volontà politica di intervento in specifici teatri operativi, si realizzano condizioni per le quali eventi di natura squisitamente tattica (quali sono le attivazioni di IED) possono produrre vigorosi effetti a livello strategico.

Gli IED sono, peraltro, armi semplici ed economiche, di realizzazione relativamente facile, che si rivelano capaci di costituire, nella realtà dei fatti, una minaccia particolarmente difficile da contrastare<sup>5</sup>. Le contromisure sono sovente generate attraverso processi lenti e particolarmente costosi che difficilmente riescono a prevenire l’approvvigionamento dei materiali componenti da parte degli avversari e che ancor più difficilmente riescono a tenere il passo con la capacità avversaria di cambiare rapidamente metodologie d’azione.

Gli ordigni esplosivi improvvisati sono quindi, sostanzialmente, armi tattiche in grado di produrre effetti a livello strategico; generalmente vengono usate nei confronti di un vasto insieme di obiettivi, tra i quali si possono evidenziare, in aggiunta ai contingenti militari nazionali, la popolazione locale, il governo e le forze di sicurezza locali, agenzie e organizzazioni non governative, strutture ed infrastrutture cariche di significati simbolici, istituzioni commerciali e nodi di flusso economico; le linee di comunicazione marittime, inoltre, unitamente ai relativi passaggi ristretti<sup>6</sup> e alle aree portuali fondamentali, costituiscono un insieme di potenziali bersagli altamente remunerativi per gli avversari. È sempre più evidente, quindi, che gli IED possono essere parimenti impiegati contro i nostri stessi network, creando in tal modo un senso di minaccia dai marcati effetti psicologici. Non deve essere inoltre trascurato il crescente grado di complessità degli attacchi portati a mezzo degli IED, né il devastante

---

<sup>1</sup> Networks.

<sup>2</sup> Per ulteriori approfondimenti sul tema si rimanda ai contenuti dei documenti “*Direttiva strategica interforze per il contrasto della minaccia costituita dagli ordigni esplosivi improvvisati (C-IED)*” (SMD-M-015), versione in Bozza, e redigenda PID/O-3.15 “*La Dottrina Interforze per il C-IED*”.

<sup>3</sup> Attraverso canali commerciali legittimi.

<sup>4</sup> Fabbricatori di ordigni esplosivi improvvisati.

<sup>5</sup> In allegato “B” della “*Direttiva strategica interforze per il contrasto della minaccia costituita dagli ordigni esplosivi improvvisati (C-IED)*” (SMD-M-015), versione in Bozza, viene fornita una descrizione più approfondita degli ordigni esplosivi improvvisati.

<sup>6</sup> Più comunemente noti con il termine inglese *Choke-Point*.

potenziale che deriva dalla possibilità di sfruttarli in combinazione con agenti chimici, biologici e/o radiologici per la costruzione, seppur artigianale, di armi di distruzione di massa.

L’impressione di insicurezza che si genera attraverso l’uso degli IED produce effetti demoralizzanti sulla popolazione locale al punto da danneggiarne sensibilmente la coesione ed il rapporto con il legittimo governo locale. Le conseguenze possono quindi estendersi molto facilmente ben oltre il campo di battaglia fino ad investire persino le relative relazioni internazionali e poiché la tolleranza verso vittime civili e militari nelle attuali società di matrice culturale occidentale è molto bassa, la limitata disponibilità di efficaci contromisure nei confronti degli IED ne innalza inevitabilmente gli effetti, come già accennato, al livello strategico.

Tutto ciò è ben chiaro nella mente degli avversari che, forti di rapidità, adattabilità, flessibilità e reattività normalmente superiori a quelle delle forze schierate in zona di operazioni, riescono a penetrare i nostri cicli decisionali e, ponendosi sovente un passo avanti, mirano essenzialmente a minare la volontà politica del Paese di proseguire nell’impegno concreto nei teatri operativi.

## 2. **Obiettivi strategici del C-IED**

Lo scopo del C-IED è scardinare, disarticolare e smantellare efficacemente l’intero sistema IED, impedire o limitare il ricorso all’uso degli ordigni esplosivi improvvisati da parte dell’avversario allo scopo di proteggere le nostre forze dislocate in zona di operazioni, assicurare loro libertà d’azione e di movimento e, conseguentemente, contribuire al conseguimento degli obiettivi di missione ed al raggiungimento dell’end-state prefissato.

Vengono pertanto individuati i seguenti obiettivi strategici per il contrasto della minaccia IED:

- dotare le Forze Armate delle capacità per neutralizzare gli IED quali strumenti di influenza strategica, avviando e portando a compimento, con efficacia ed efficienza, le necessarie iniziative di sviluppo capacitivo;
- migliorare la capacità di contrastare i network-minaccia attraverso l’adozione del cosiddetto “approccio multidimensionale” (*Comprehensive Approach*): è necessario raggiungere un’efficace e sfruttabile comprensione dell’ampio contesto C-IED e sviluppare una efficace capacità di intervenire sui network per disarticolarlo e renderlo non-operativo. Ciò va ben oltre la semplice interdizione all’impiego degli IED stessi e richiede azioni estese all’intero sistema IED, con particolare riferimento ai Leader, ai pianificatori, ai finanziatori, ai fornitori di materiali, ai fabbricatori di ordigni ed ai collocatori degli stessi;
- migliorare la capacità di lotta all’ordigno: per minimizzare le perdite sul campo e migliorare la capacità di operare efficacemente è fondamentale migliorare la cosiddetta *situational awareness*<sup>7</sup> e preparare il personale e le unità a mitigare i rischi e le conseguenze degli IED già posizionati per l’impiego.

È tuttavia importante comprendere ed accettare il fatto che, per quanto efficace, nessuno sforzo C-IED potrà mai annullare completamente il sistema IED che potrebbe continuare a costituire un problema per le forze di sicurezza e per la popolazione locali dopo il ritiro dei contingenti militari dai teatri operativi.

---

<sup>7</sup> Consapevolezza della situazione.

**3. Il C-IED nell'ambito della forza Joint**

La natura e l'ampiezza dello sforzo C-IED sono strettamente connessi alla dimensione dell'operazione, alla natura del conflitto, all'ambiente strategico ed operativo, la scala delle attività militari e, ovviamente, il livello della minaccia IED. Ad esempio, in operazioni di lunga durata e su vasta scala, caratterizzate da una significativa minaccia e da consistenti disponibilità di specialisti C-IED, la costituzione di una Task Force C-IED appare particolarmente appropriata. Tale struttura organizzativa deve disporre di consulenti<sup>8</sup> (e relativi *staff*) a tutti i livelli ove sussiste l'esigenza di coordinare l'impiego di assetti C-IED specialistici nell'ambito di una o più componenti. Una *Task Force* specificamente dedicata a funzioni di contrasto IED può non essere più necessaria allorché il livello della minaccia è riportato sotto controllo e le forze di sicurezza locali sono in grado di gestire la problematica in proprio.

In operazioni minori e di breve durata, ove gli staff specialistici sono in numero ridotto, può risultare più appropriato inserire lo *staff* C-IED direttamente all'interno delle articolazioni organizzative dei Quartier generali<sup>9</sup> (HQ) già esistenti (ad esempio, negli *staff Intelligence, Operations, Engineering*, ecc.).

Gli *advisor* C-IED ed i relativi *staff* devono essere organizzativamente collocati in modo tale da poter fornire efficace supporto al Comandante ed a tutte le pertinenti funzioni di *staff* lungo tutto l'evolvere della Campagna, dalla inizio della fase di pianificazione, all'approntamento, all'esecuzione delle operazioni, fino alla fase di transizione finale. La costituzione di una articolazione di *staff* C-IED nell'ambito del quartier generale del JFC contribuisce ad assicurare che il necessario equilibrio dell'approccio C-IED sia integrato e sincronizzato lungo l'intero spettro delle componenti e, trasversalmente, a livello multinazionale. In proposito, è importante osservare che lo scopo di un elemento di *staff* C-IED nell'ambito del HQ non è la condotta di specifiche attività C-IED, bensì quello di assicurare che gli aspetti C-IED delle operazioni siano considerati e coordinati nell'ambito del HQ stesso e che l'approccio C-IED sia opportunamente considerato in fase di pianificazione ed esecuzione di tutte le attività: lo sforzo C-IED non può e non deve essere visto in forma isolata, ma deve essere profondamente integrato nelle attività di intelligence, di pianificazione ed operative a tutti i livelli.

**4. Elementi per un efficace approccio C-IED**

Un efficace approccio C-IED mira a distruggere o disarticolare il sistema IED mediante l'adozione di quattro elementi chiave:

- isolamento del sistema IED dalle proprie fonti di supporto esterno;
- interdizione del sistema IED stesso per compromettere la capacità IED avversaria;
- riduzione dell'effetto strategico conseguente all'impiego degli IED, principalmente nel dominio cognitivo;
- attenuazione dei potenziali effetti tattici degli IED e neutralizzazione degli IED già collocati in posizione d'uso (inclusivo degli aspetti di *Force Protection*).

Deve essere osservato, d'altra parte, che l'esigenza di sicurezza delle forze in teatro introduce, a livello sistemico, un paradosso particolarmente meritevole di attenzione. È chiaro, infatti, che nelle operazioni di stabilizzazione il successo ultimo si consegue proteggendo la popolazione e

---

<sup>8</sup> *Adviser*.

<sup>9</sup> *Headquarters*.

non solo le proprie forze. Restando all’interno delle proprie basi protette, le forze godono certamente di significativa protezione, ma perdono il contatto con la popolazione locale e, ancor più grave, concedono all’avversario tale preziosa opportunità. Anche quando il livello di insicurezza è significativo, i Comandanti in zona di operazioni devono trovare il giusto equilibrio tra l’implementazione di misure di *Force Protection* restrittive e l’esigenza di mantenere contatti ravvicinati con i locali, nella consapevolezza che misure di *Force Protection* particolarmente restrittive tendono a generare isolamento e, nel tempo, ad alienare le forze in teatro dalle popolazioni locali e, conseguentemente, a privare i Comandanti della necessaria percezione di cosa accade sul terreno. Sforzi mirati a proteggere la popolazione, di contro, consentono alle forze dislocate in zona di operazioni di guadagnare preziose opportunità di contatto ravvicinato con i locali, di comprenderne le esigenze, i bisogni e, più in generale, di raccogliere preziosi elementi di intelligence. Al tempo stesso, attività di pattugliamento ben organizzate esercitano pressione sugli avversari e ne limitano le possibilità di azione. In sintesi, attività condotte a livello tattico tra la popolazione locale, seppur foriere di più elevati livelli di rischio, manifestano la seria volontà di condividere tale rischio con gli abitanti locali e, conseguentemente, aiuta a guadagnare il loro sostegno per il conseguimento di più ampi obiettivi di Campagna. Deve essere assolutamente evitata la tentazione di focalizzare principalmente gli sforzi sulla neutralizzazione degli ordigni già collocati in posizione d’uso.

## **5. Protezione delle forze e della popolazione**

La capacità di proteggere la popolazione locale e di interagire con essa è fondamentale per il successo dello sforzo C-IED e, più in generale, per un efficace contributo agli obiettivi di stabilizzazione e contro-insorgenza. Ciò può essere conseguito attraverso mirate attività di bonifica integrate da appropriate misure finalizzate ad impedire il collocamento degli ordigni in posizione d’uso; l’ottimale gestione delle limitate risorse C-IED disponibili non può pertanto che derivare da un approccio C-IED globale. La libertà di movimento, d’altra parte, va ben oltre la semplice bonifica delle strade poiché dipende molto dalla fiducia che si ha nei confronti della sicurezza (in termini di minaccia IED) delle vie di comunicazione e, conseguentemente, dipende a sua volta in modo particolarmente significativo dagli effetti delle attività di influenza, che giocano pertanto, ancora una volta, un ruolo chiave.

## **6. Fattori abilitanti C-IED**

In un contesto astratto, si definisce con il termine “fattore” qualsiasi elemento, sia esso interno o esterno ad un sistema, che concorre a produrre un determinato effetto, a conseguire un determinato risultato, o, più in generale, che può esercitare un’azione positiva o negativa sulla condotta di una serie di azioni, sull’esito di una iniziativa o sul conseguimento di un risultato. I fattori abilitanti, in particolare, esercitano influenza positiva e contribuiscono al raggiungimento del successo.

### **a. Capacità di *Route Clearance***

Le attività di *Route Clearance* realizzano, in pratica, quelle condizioni di libertà di movimento che costituiscono, di fatto, l’effetto che lo sforzo C-IED si prefigge di conseguire. Si tratta di attività specialistiche del Genio Militare<sup>10</sup> che sviluppano compiti di

---

<sup>10</sup> *Military Engineering.*



ricognizione, manutenzione, miglioramento e rimozione ostacoli da strade e percorsi in genere in contesti di esposizione a minaccia IED. Da un punto di vista organizzativo si osserva che risulta particolarmente efficace la costituzione in pacchetti capacitivi<sup>11</sup> dedicati inseriti in strutture organizzative più ampie di tipo *all-arms* che ricevono, in tal modo, supporto per la gestione dei percorsi in ambienti operativi sotto minaccia IED. Tali pacchetti possono essere costituiti da opportune combinazioni di veicoli, equipaggiamenti e personale specialistici e non e devono svolgere la fondamentale funzione di individuare occultamenti di IED, munizionamento e depositi temporanei<sup>12</sup> di materiali a potenziale finalità IED unitamente allo sviluppo di attività sistematica di scoperta, eventuale bonifica e deterrenza lungo i percorsi operativamente prescelti. I pacchetti RCP possono essere impiegati sia in contesti di supporto generale (ad esempio mantenendo aperte le principali vie di comunicazione logistica e di rifornimento) che di sostegno diretto ad unità di manovra in circostanze di movimento tattico.

#### **b. Capacità di *Military Search***

La Ricerca Militare è definita<sup>13</sup> come l'applicazione, la gestione e l'utilizzo di procedure sistematiche che, associate ad appropriati equipaggiamenti, consente l'individuazione di specifici obiettivi (risorse, persone e informazioni impiegate da un avversario) in supporto alle Operazioni Militari. Nel quadro dello sforzo C-IED, la ricerca militare rappresenta un efficace strumento per integrare le potenzialità degli assetti disponibili per la condotta di operazioni di natura offensiva (tese a minare le fondamenta sulle quali poggiano le attività e le strutture delle Forze avverse) e difensiva (per incrementare il livello di *Force Protection* delle nostre Forze); in pratica, ha lo scopo di contrastare e/o neutralizzare le capacità IED esprimibili dagli avversari conseguendo la riduzione dell'esposizione delle Forze amiche e della popolazione alle minacce inerenti agli IED, materiali esplosivi, munizioni in genere.

Le *Military Search* sono operazioni condotte su determinati obiettivi (materiali per la costruzione di IED, strutture nelle quali vengono nascosti e/o fabbricati gli ordigni, *bomb makers*, informazioni varie). Le attività sono pianificate dagli *staff* che si avvalgono di personale esperto in *Military Search* (*coordinators, advisors*, ecc.) e sono svolte da *team* specialistici che, di norma, operano all'interno di una cornice di sicurezza. Per rendere efficaci le attività di ricerca, ai *team* di ricerca vengono spesso dati in supporto altri assetti specialistici (assetto cinofili, *team* EOD/IEDD, WIT, polizia militare).

Gli obiettivi della ricerca militare generalmente includono:

- negare all'avversario opportunità e risorse;
- ottenere elementi di informazione utili a fini di intelligence;
- salvaguardare materiale probatorio utile per procedimenti giudiziari;
- proteggere potenziali bersagli.

La capacità di Ricerca Militare è strutturata su tre livelli (Basico, Intermedio ed Avanzato). Il livello di Ricerca Militare viene definito in funzione dell'analisi e della valutazione del rischio che viene condotta su un determinato Ambiente Operativo. Tale analisi tiene conto di

---

<sup>11</sup> *Route Clearance Package* – RCP.

<sup>12</sup> *Caches*.

<sup>13</sup> STANAG 2283, "*Military Search*" - ATP-73 Vol. I.

tre fattori fondamentali: grado della minaccia, rischi ambientali e grado di affidabilità (della ricerca). I tre livelli di Ricerca Militare sono così definiti:

- *Basic Military Search*: è il livello di Ricerca Militare che deve essere posseduto da tutti i Militari. Tale livello si basa sulla consapevolezza del rischio derivante dalla presenza di Ordigni Esplosivi e le Tecniche, Tattiche e Procedure (TTP) da adottare al fine di incrementare il livello di *Force Protection*;
- *Intermediate Military Search*: è la capacità di condurre Operazioni di Ricerca dove esiste un minimo grado di minaccia derivante dalla presenza di Ordigni Esplosivi, dove è accettabile un discreto grado di Affidabilità nella Ricerca e/o dove i rischi correlati al luogo in cui deve essere condotta la ricerca sono di medio livello;
- *Advanced Military Search*: è la capacità di condurre Operazioni di Ricerca dove il Grado di Minaccia derivante dalla presenza di Ordigni Esplosivi è elevato e/o dove sia richiesto un alto grado di affidabilità nel risultato che si intende conseguire con l’attività di Ricerca e/o dove sono certamente presenti rischi legati all’ambiente in cui si opera.

La scelta del tipo e del livello di ricerca da attuare in un determinato contesto dipende dal livello della minaccia (rischio operativo), di sicurezza (certezza che il luogo oggetto della ricerca sia privo di ordigni esplosivi o componenti di ordigni) e dal livello di efficacia che si vuole ottenere in funzione dell’obiettivo di ricerca.

#### c. Capacità di *Explosive Ordnance Disposal*

La capacità EOD costituisce un fattore abilitante operativo che contribuisce sensibilmente alla libertà di movimento ed alla *Force Protection*. Nell’ambito del contesto capacitivo EOD si colloca anche la funzione IEDD<sup>14</sup> – definita quale la localizzazione, l’identificazione, la messa in sicurezza e lo smaltimento finale di ordigni esplosivi improvvisati – che richiede equipaggiamenti, mezzi, specializzazione ed addestramento specificamente dedicati: non tutti gli operatori EOD sono in grado di trattare ordigni di tipo IED e ancora meno son in grado di manipolare IED sofisticati. In ragione della delicatezza e della dimensione dei rischi connessi con lo svolgimento delle relative attività, il personale EOD/IEDD non deve mai essere messo sotto pressione e fatto operare oltre i limiti delle proprie abilità.

#### d. Capacità di *Electronic Warfare Support*

In ambienti operativi che includono, anche solo potenzialmente, la presenza di minaccia IED di tipo radiocontrollato<sup>15</sup> trova particolare utilità l’adozione di misure di supporto elettronico<sup>16</sup> e l’adozione di contromisure elettroniche<sup>17</sup> a fini C-IED, con particolare riferimento alle contromisure elettroniche di *Force Protection* ed alle contromisure elettroniche EOD.

Le prime forniscono protezione al personale, nei confronti di ordigni radiocontrollati, durante i movimenti lungo percorsi esterni alle basi protette, attraverso la generazione di “bolle elettromagnetiche” all’interno delle quali è di fatto inibito l’uso efficace di quelle specifiche porzioni dello spettro elettromagnetico normalmente impiegate per il radio

<sup>14</sup> IED Disposal.

<sup>15</sup> *Remote Controlled IED* – RC-IED.

<sup>16</sup> *Electronic Support Measures* – ESM.

<sup>17</sup> *Electronic Counter-Measures* – ECM.

controllo degli RC-IED. Le Forze dislocate in zona di operazioni devono avere dimestichezza con gli apparati, gli equipaggiamenti e le procedure relative alla implementazione delle contromisure elettroniche di *Force Protection* senza necessitare dell'intervento di personale specializzato durante ciascun movimento.

Le seconde, di contro, sono finalizzate alla protezione elettronica dei *team* EOD che, per la natura stessa della loro funzione, entrano deliberatamente in aree ove sono collocati ordigni esplosivi reali o sospetti. Ne derivano pertanto esigenze di protezione che massimizzino, con adeguata ridondanza, i livelli di sicurezza consentendo al contempo l'efficace sviluppo delle pertinenti attività. L'impiego delle contromisure elettroniche EOD richiede l'inserimento nei *team* EOD di personale appositamente qualificato.

**e. Capacità di *Technical Intelligence***

La capacità di investigazione scientifica e quella di analisi tecnico-biometrica dell'organizzazione C-IED nazionale deve poter permettere l'acquisizione delle informazioni tecniche e forensi necessarie ad implementare con successo la strategia di contrasto al Sistema IED. La conoscenza delle caratteristiche tecniche e di posizionamento sul terreno degli ordigni esplosivi improvvisati, unitamente a quelle biometriche derivanti dagli elementi di prova raccolti sui componenti degli IED, consente infatti di pervenire ad una comprensione più vasta del sistema IED e dei network che lo sostengono. In tal modo, si possono ricavare informazioni sulle TTP utilizzate dall'avversario, sulla catena logistica di approvvigionamento dei materiali e sul livello di conoscenze tecniche da essi posseduto.

I risultati dell'analisi forense, quando messi a sistema con gli altri pertinenti dati informativi, consentono di approfondire la conoscenza della componente umana del Sistema IED ed i suoi legami con altre organizzazioni eversive operanti dentro e fuori la zona di operazioni.

**f. Fattori abilitanti locali**

Il perseguimento degli obiettivi di Campagna di lungo termine, quali il rafforzamento del sistema di governo locale ed un più generale sviluppo del paese, richiede e promuove al tempo stesso la riduzione della minaccia IED in zona di operazioni. Le forze di sicurezza locali possono essere incaricate – qualora le condizioni di preparazione ed equipaggiamento, unitamente alla postura mentale, risultino sufficientemente attaggiate alla situazione in atto – di compiti che ben contribuiscono a contrastare con efficacia la minaccia IED.

D'altra parte, la svolta nello sforzo C-IED può aversi solo mediante il concorso della popolazione locale attraverso meccanismi sociali che rafforzino l'accettazione delle Forze in zona di operazioni ed incentivino la produzione di intelligence locale (ricompense, anonimità, amnistie, pulizia delle strade, ecc.). L'avvio di programmi in tal senso deve essere incoraggiato e sostenuto ogni qualvolta risulti opportuno, avendo cura di prestare comunque grande cautela nella scelta delle iniziative ed assicurando assolutamente rispetto degli schemi socio-culturali indigeni al fine di evitare qualsivoglia forma di conseguenze non intenzionali nell'ambito della sfera di influenza socio-culturale.



## LA PROTEZIONE SANITARIA DELLE FORZE

### 1. Introduzione

#### a. Generalità

Lo schieramento di forze di proiezione nazionali nel quadro di operazioni interforze e/o Alleate avviene nell'ambito di scenari complessi e di ambienti estremamente diversificati. La vulnerabilità delle forze schierate nei confronti di minacce e di rischi sanitari può diventare un fattore critico per il successo della missione. È pertanto di cruciale importanza che la componente sanitaria di *staff* assicuri elementi di cognizione circa la Protezione Sanitaria delle Forze<sup>1</sup> a supporto del processo decisionale del Comandante.

Scopo del presente documento, che tiene conto -con i dovuti temperamenti- della specifica dottrina di riferimento NATO<sup>2</sup>, è di delineare -in ambito nazionale- i principi ed i concetti generali ed indicare le linee guida strategiche concernenti gli aspetti sanitari della “Protezione delle Forze” cui dovranno conformarsi le subordinate pubblicazioni tecnico-sanitarie sull'argomento.

#### b. Definizione

La Protezione Sanitaria delle Forze (*Force Health Protection – FHP*) può essere definita come “*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*”. Come tale essa è parte integrante, costituendone un sottoinsieme, della più ampia Protezione delle Forze.

### 2. Processo di protezione sanitaria della forza

#### a. Generalità

La protezione sanitaria della forza, essendo uno degli aspetti della protezione della forza, deve integrarsi nell'ambito più generale del processo di protezione della forza.

Il processo FHP dovrà essere in linea con il modello generale di protezione della forza e partecipare a detto processo, mettendo in risalto gli aspetti sanitari connessi con la *Force Protection*.

L'intera fase di pianificazione sanitaria è effettuata a livello strategico ed è normalmente un'attività joint. Il primo aspetto da considerare è quello fornito dall'analisi di missione svolta dal Comando strategico che consentirà la successiva valutazione degli assetti/elementi critici per l'adeguata assistenza sanitaria nel corso della missione. La valutazione degli aspetti critici – basata su informazioni concernenti l'entità della forza schierata, l'area di eventuale schieramento, la presenza di strutture sanitarie nazionali, di altri contingenti o civili, le informazioni inerenti ai rischi sanitari/ambientali e le minacce – consente l'individuazione degli assetti di personale medico/infermieristico, strutture sanitarie da schierare.

L'attività di *intelligence* è fondamentale nella valutazione della minaccia, che in ambito sanitario è sostanzialmente riferita all'intensità e frequenza delle azioni ostili in atto e alla minaccia CBRN. Il processo di FHP è, pertanto, una metodologia procedurale che coinvolge

---

<sup>1</sup> “*Force Health Protection*” (FHP), secondo la terminologia NATO.

<sup>2</sup> “*Allied Joint Medical Force Health Protection Doctrine*” (AJMedP-4).

unità sanitarie collocate sia al livello strategico che operativo e tattico<sup>3</sup>. L'intelligence sanitaria (*Medical Intelligence - MEDINT*) e la *Medical Survey* rappresentano dei fattori facilitatori fondamentali per l'FHP. Le informazioni raccolte sono necessarie per individuare e valutare i rischi di carattere sanitario per il personale schierato: fattori climatici, fattori infrastrutturali, inquinamento del suolo, delle acque, dell'aria, rischi alimentari, rischi per la salute psichica, presenza di focolai endemici ed epidemici.

In relazione all'esito della valutazione del rischio vengono, quindi, pianificate le misure di protezione, prevenzione e profilassi sanitaria del contingente consistenti in:

- informazione sui rischi, possibilmente attraverso briefing illustrativi;
- individuazione di misure di protezione (ad esempio norme comportamentali, utilizzo di dispositivi di protezione individuale);
- misure di prevenzione sanitaria (accertamenti sanitari mirati al rischio);
- misure di profilassi sanitaria (vaccini chemiopprofilassi).

Le attività sopra menzionate condotte in fase di pianificazione sono, infine, sottoposte a periodica revisione nell'ambito della procedura di gestione del rischio.

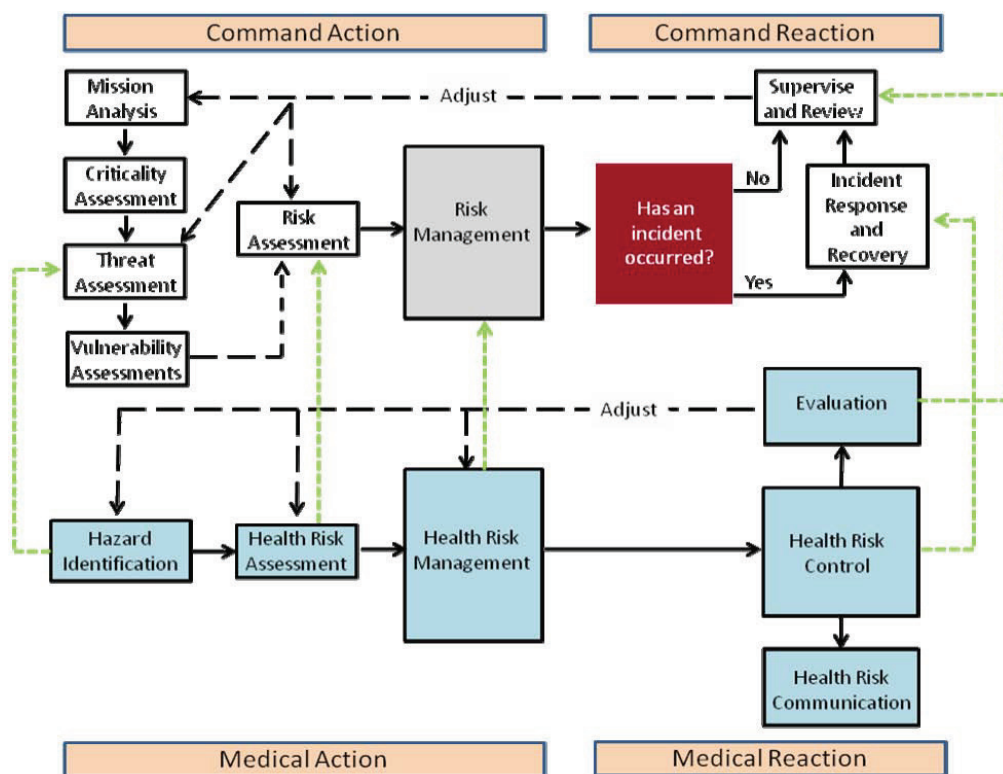


Figura 10 Integrazione del FHP nell'ambito del modello FP

**b. Fasi del processo di Protezione Sanitaria della Forza**

Il processo di FHP si sviluppa, sia in pianificazione che durante la condotta delle operazioni, nelle seguenti fasi:

- (1) Individuazione del rischio sanitario

<sup>3</sup> A seconda del livello e della complessità delle operazioni, a livello operativo e tattico le figure interessate possono essere il *Medical Advisor (MEDAD)*, il *JMED*, il Comandante Sanitario di Contingente, il Direttore Veterinario di Contingente, il *GMED* e i *DSS*.

La salute è minacciata da eventi infortunistici non dovuti al combattimento, lesioni da esposizioni a basse ed alte temperature, dall'esposizione ad agenti fisici, chimici, biologici, radiologici e nucleari e da rischi di tipo trasversale (fatica e stress operativo, alterazioni ritmo sonno – veglia, ecc.) dovuti a fattori operativi, occupazionali<sup>4</sup> o ambientali.

I dati raccolti in materia dovranno essere condivisi con tutte le unità responsabili della FHP ai vari livelli.

(2) Valutazione del rischio sanitario

Sebbene la valutazione generale del rischio consideri i seguenti tre elementi:

- la probabilità che un incidente causato da una minaccia o da un rischio si verificherà;
- la probabilità che una particolare vulnerabilità verrà sfruttata;
- l'impatto di un probabile incidente sul successo di una missione,

quella del rischio sanitario segue un approccio diverso e incorpora gli aspetti di seguito indicati:

- classificazione del rischio;
- valutazione della probabilità di rischio;
- valutazione della severità del rischio;
- caratterizzazione del rischio.

(3) Gestione del rischio sanitario

La gestione del rischio sanitario mira allo sviluppo di misure di controllo e di contromisure. Dette misure, sviluppate per eliminare o, almeno, per minimizzare i rischi sanitari individuati e valutati, costituiscono una parte essenziale del concetto di supporto sanitario e, su decisione del Comandante, diventano parte del piano di supporto sanitario. Lo sviluppo di controlli verte principalmente su attività di tipo informativo (divulgazione delle norme basilari di igiene personale, ecc.), preventivo (applicazione di protocolli vaccinali, ecc.) e comportamentale (utilizzo di dispositivi di protezione individuale, ecc.).

(4) Controllo del rischio sanitario

L'attivazione di misure di controllo del rischio sanitario è rinviata a documenti di livello operativo (OPLAN e D.O.N.) e deve essere specificata, a livello tattico, nelle *Standard Operating Procedures* (SOPs) e in altri ordini scritti o orali.

(5) Comunicazione del rischio sanitario

Informazioni accurate e tempestive sulle truppe schierate rappresentano un requisito di base per condurre con successo il controllo del rischio sanitario. Gli *staff* sanitari, pertanto, devono garantire che le informazioni siano opportunamente e, nel contempo, velocemente elaborate all'interno dei Comandi e lungo la linea di comando, procedendo secondo i previsti canali di comunicazione.

(6) Verifica

La verifica dell'efficacia delle misure adottate nel campo della protezione sanitaria è un processo continuo, sviluppato durante l'esecuzione dei programmi di protezione sanitaria della forza, che:

<sup>4</sup> Rischi legati alla professione svolta.

- fornisce allo *staff* sanitario informazioni sull'accuratezza dell'identificazione del rischio;
- consente la successiva valutazione del rischio sanitario;
- permette la definizione delle procedure di gestione del rischio sanitario;
- contribuisce al controllo e alla revisione del ciclo generale di protezione della forza.

Le osservazioni dovranno essere prese in considerazione per una successiva valutazione e sviluppo delle *lessons identified* e delle *lessons learned*.

In questo modo, i risultati della valutazione potranno essere presi in considerazione per la condotta di un processo FHP relativo ad altre operazioni.

### 3. Comando e Controllo

#### a. Responsabilità

I Comandanti, ai vari livelli, assicurano la protezione sanitaria della forza (FHP) ed assumono le decisioni nell'ambito delle proprie aree di responsabilità.

Lo Stato Maggiore della Difesa (SMD), in coordinamento con gli Stati Maggiori di Forza Armata e Comando Generale dell'Arma dei Carabinieri, elabora, per la successiva emanazione da parte del Capo di SMD, le indicazioni di *Policy* in materia di FHP.

#### b. Comandi schierati

L'Autorità Sanitaria di Teatro, al fine di monitorare al meglio gli aspetti sanitari della protezione della forza, di norma, in ambito NATO, può avvalersi di una *Force Health Protection Cell* (FHPC), cellula che garantisce che gli aspetti di FHP siano adeguatamente inglobati nel processo di pianificazione operativa (OPP) e nel processo decisionale del Comandante. In particolare dovrà:

- verificare la realizzazione di tutte le fasi del processo FHP (si veda il para. 2);
- fornire valutazioni sanitarie sull'ambiente;
- fornire consulenza in merito ai rischi sanitari aventi un impatto sull'operazione;
- fornire raccomandazioni sulle misure preventive di FHP e durante tutte le fasi dell'operazione, incluse il pre e post-schieramento;
- fornire consigli sulla prontezza sanitaria della forza;
- istituire e gestire un sistema campale di sorveglianza delle malattie e della salute;
- monitorare le misure di FHP attuate in teatro;
- fornire indicazioni FHP per il contributo sanitario da includere nell'OPP.

#### c. Sistemi di comunicazione e informazione

La comunicazione dei rischi sanitari e delle raccomandazioni individuate saranno di importanza cruciale per il raggiungimento di un efficace controllo del rischio sanitario.

Pertanto, la disponibilità di un sistema affidabile di comunicazione e informazione sanitaria<sup>5</sup> costituisce un requisito indispensabile per un efficace comando e controllo sanitario.

I dati sanitari provenienti da fonti diverse immessi nel sistema sopraccitato consentiranno di acquisire una *Situational Awareness*, permettendo all'Autorità Sanitaria, ai vari livelli, di

---

<sup>5</sup> Ad esempio il “Sistema Informativo Sanitario interforze dell'AD (SISAD)” che rappresenta un ottimo strumento informatico per la gestione dei dati sanitari del personale dell'AD.



disporre di un quadro generale in materia di rischi sanitari e, quindi, di intraprendere le azioni necessarie per il processo FHP che si concretizzerà in:

- valutazione della minaccia e del rischio, anche attraverso lo stretto collegamento con la componente G2 o J2 allo scopo di adottare tempestivamente le più adeguate misure di protezione, prevenzione e, se del caso, di profilassi sanitaria non preventivate in fase di pianificazione;
- risposta all'incidente, attraverso un efficace collegamento con le strutture sanitarie di livello superiore (Role 2 Role 3).

#### 4. **Aspetti specifici della protezione sanitaria della forza**

Gli aspetti da tenere in considerazione per l'elaborazione di un piano di FHP sono:

- a) i rischi sanitari di tipo operativo, occupazionale ed ambientale;
- b) la sorveglianza sanitaria ed epidemiologica;
- c) le misure di medicina preventiva;
- d) le misure di igiene campale, alimentare, idrica e di medicina veterinaria;
- e) le attività di promozione della salute;
- f) le minacce di carattere chimico, biologico, radiologico e nucleare (CBNR).

Benché le minacce CBRN ed i rischi sanitari occupazionali, ambientali ed industriali siano una componente dell'FHP, il presente documento non fornisce indicazioni specifiche in merito a tali aspetti sanitari. Indicazioni in tal senso possono invece essere rinvenute nello specifico “Annesso 6” alla presente Pubblicazione<sup>6</sup>.

##### a. **Sorveglianza Sanitaria ed epidemiologica**

L'Organizzazione Mondiale della Sanità (WHO) definisce la salute come “*uno stato generale di benessere fisico, psicologico e sociale, non semplicemente l'assenza di malattia o di infermità*”. È difficile misurare questo stato positivo, generalmente considerato come una “situazione di *default*”.

Il concetto di “*Iceberg delle malattie*” dimostra come le attività di sorveglianza sanitaria possano risultare ulteriormente difficoltose.

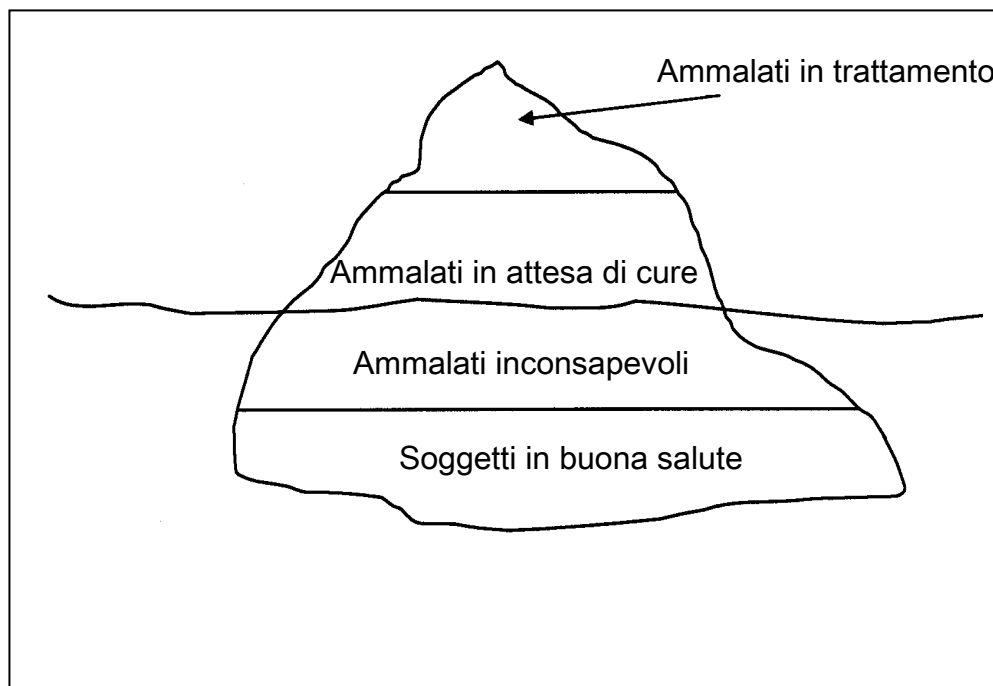
Dalla figura 19 risulta evidente che la maggioranza delle persone non sono in contatto con i *servizi* sanitari o perché sono in buona salute, oppure perché inconsapevoli di essere malati o perché non hanno ancora preso la decisione di chiedere aiuto.

Gli uomini giovani ricorrono ai servizi sanitari meno di altri settori della popolazione. Le forze *militari* sono costituite per la maggior parte da giovani uomini che, avendo superato una qualche forma di screening sanitario, possono essere ragionevolmente ritenuti idonei dal punto di vista sanitario. Tuttavia, l'interesse principale della catena di comando non è quello di valutare aprioristicamente lo stato di salute della popolazione militare, ma quello di avere la situazione continua della capacità e prontezza operativa di un'unità.

Ciò posto, è preferibile attuare un monitoraggio delle patologie (sorveglianza sanitaria ed epidemiologica) piuttosto che avere un dato generico sullo stato di salute della popolazione militare.

---

<sup>6</sup> “*La difesa CBRN*”.

Figura 11 *L'iceberg delle malattie*

## (1) Applicazioni

Nell'ambito della pianificazione e della condotta delle operazioni militari, la sorveglianza sanitaria ed epidemiologica ha diverse applicazioni, come ad esempio:

- un'indicazione relativa alla quantità ed alle tipologie di malattie che colpiscono la popolazione militare, dando ai Comandati un'idea delle dimensioni della forza schierabile;
- una valutazione delle esigenze sanitarie, che servirà di base per definire l'assistenza sanitaria in tempo di pace e la struttura del servizio sanitario proiettabili;
- il monitoraggio dell'incidenza delle malattie che, costituendo un sistema di allerta per il diffondersi di malattie trasmissibili, può avere un effetto positivo sulla loro prevenzione e, quindi, sulle stesse operazioni;
- il supporto all'individuazione di fughe di gas tossici industriali o di rischio CBRN;
- il controllo del servizio sanitario fornito alle Forze Armate in tempo di pace e di guerra;
- la raccolta dei dati di *intelligence* sanitaria.

## (2) Principi generali

La sorveglianza sanitaria ed epidemiologica è di enorme importanza, data la vastità degli aspetti sanitari da considerare. Le condizioni da controllare dovrebbero essere prontamente individuabili e comportano implicazioni di rilievo dal punto di vista sanitario e militare. Rientrano in questo quadro la sorveglianza delle malattie trasmissibili, i ricoveri ospedalieri, le lesioni riportate sul campo di battaglia, le ferite da traumi non da combattimento, le dimensioni e la natura della popolazione colpita.

È importante procedere ad una valutazione dell'incidenza delle malattie (numero di nuovi casi di malattia che si verificano in una popolazione in un determinato periodo di tempo) e della prevalenza delle stesse (numero di casi di malattia presenti nel periodo di

osservazione in una determinata popolazione), così come è importante valutare l'impatto delle malattie, elemento che, probabilmente, è misurato al meglio in termini di impossibilità a prendere parte alle operazioni.

I dati sull'incidenza e prevalenza delle malattie dovrebbero essere comunicati separatamente in quanto potrebbero fornire indicazioni sulle dimensioni della forza schierata. Inoltre è opportuno che i dati ricavati con la sorveglianza sanitaria ed epidemiologica siano analizzati, comunicati e pubblicati dai competenti organi, allo scopo di non inficiarne l'utilità ed evitare "fughe di notizie".

La raccolta di dati di sorveglianza sanitaria dovrebbe pesare quanto meno possibile sul personale medico preposto alla loro elaborazione. La crescente disponibilità di sistemi elettronici di memorizzazione dei dati sanitari dovrebbe rendere possibile questo risultato, in quanto i dati diagnostici potrebbero essere accuratamente codificati e, con i permessi adeguati, coloro che effettuano la sorveglianza sanitaria potrebbero interrogare i database esistenti piuttosto che fare affidamento sull'invio dei dati di analisi da parte del personale sanitario. L'analisi della crescente quantità di dati disponibili richiede risorse, in considerazione del fatto che l'informazione deve essere prodotta ed elaborata tempestivamente.

**b. Misure di medicina preventiva**

I Comandanti hanno l'esigenza di individuare le possibili minacce provenienti da malattie che potrebbero influire sulle operazioni e prendere in considerazione le necessarie contromisure di medicina preventiva per attutirne gli effetti.

(1) **Prioritizzazione dei rischi sanitari**

Le priorità assegnate ai rischi sanitari varieranno in relazione all'area di schieramento ed alla stagione, e potranno cambiare durante il corso dello schieramento operativo. I rischi connessi con la malattia possono, fino ad un certo punto, essere anticipati e dovrebbero esserlo durante la pianificazione sanitaria. Il rischio di una malattia dovrebbe essere classificato secondo la probabilità che personale non protetto si ammali e in base al potenziale impatto sulle operazioni. Ad esempio, le malattie infettive a trasmissione oro-fecale rappresenteranno la maggiore minaccia sanitaria per la maggior parte delle operazioni e dovranno figurare tra le priorità principali dei rischi sanitari da prendere in considerazione. Prima dell'inizio della missione e, in maniera continuativa, durante tutta l'operazione, sarà necessario raccogliere dati che consentiranno una accurata e continuativa valutazione del rischio.

(2) **Briefing pre-impiego sui rischi sanitari**

Prima dell'invio in missione, il personale militare dovrà essere adeguatamente istruito sulle minacce sanitarie presenti nelle aree di operazione, sulle principali misure di prevenzione esistenti e sulla loro applicazione sul campo.

(3) **Sorveglianza sanitaria pre-impiego e post impiego**

(4) **Vaccinazioni e chemioprofilassi**

Le misure di profilassi specifica (vaccino e chemioprofilassi) sono cruciali nella protezione sanitaria della forza militare. Le misure di profilassi immunitaria e di

chemioprolifassi da adottare nei confronti del personale militare sono definite da apposite disposizioni<sup>7</sup>.

(5) Misure individuali di protezione

Le malattie trasmesse da artropodi (come zanzare, pappataci, zecche, pidocchi, pulci) sono numerose e possono avere un impatto significativo sulla salute e sull'efficienza operativa delle forze militari, a meno che non vengano adottate delle misure protettive individuali. Le Forze Armate dovrebbero adottare un sistema di misure protettive individuali che, a titolo esemplificativo, dovrebbero includere:

- indicazioni sull'adeguato uso delle divise (come mezzo di difesa fisica contro gli insetti);
- divise trattate con insetticidi;
- zanzariere trattate con insetticidi;
- repellenti contro gli insetti.

La dottrina operativa dovrebbe prevedere l'adozione delle misure protettive individuali laddove il rischio di punture di artropodi è significativo, indipendentemente dall'eventualità o meno che siano anche disponibili vaccini o trattamenti chemioprolifattici volti a contrastare le malattie trasmesse da artropodi. La dottrina operativa dovrebbe anche contemplare attività di igiene e di controllo dell'area di operazioni, per ridurre l'impatto delle punture di insetti e le conseguenti malattie (ad esempio, ubicazione degli accampamenti in relazione agli habitat ed alle aree ove si sviluppano artropodi ed insetti nocivi, gestione delle acque stagnanti, ecc.).

(6) Controllo delle infezioni e della loro diffusione

Le caratteristiche stesse delle strutture sanitarie campali possono rendere difficile il controllo di un'infezione, sia dal punto di vista dell'asepsi chirurgica, sia da quello della trasmissione delle malattie. Inoltre, l'impiego di antibiotici ad ampio spettro per la cura dei feriti presso gli ospedali da campo può portare allo sviluppo di organismi resistenti agli antibiotici (ARO), fattore che mette il personale militare, già seriamente ferito, di fronte ad un ulteriore rischio e, nel contempo, aumenta la probabilità che un ARO si sviluppi all'interno di altre strutture sanitarie (sia militari sia civili). Tutte le strutture sanitarie ad ogni livello dovranno, comunque, adottare le migliori misure possibili per il controllo delle infezioni.

Le infezioni altamente contagiose, come ad esempio la diarrea o l'influenza, possono diffondersi rapidamente tra il personale dei contingenti schierati in operazioni ed inficiare notevolmente la capacità operativa di numerose componenti della forza militare. Una rapida individuazione delle informazioni epidemiologiche si rivela, pertanto, necessaria al fine di indirizzare il successivo intervento e le ulteriori indagini connesse con una diffusione. Pertanto, al fine di minimizzare l'impatto di una epidemia

---

<sup>7</sup> Attualmente le norme che disciplinano tale materia sono contenute nella Direttiva Tecnica, applicativa del D.M. 31 marzo 2003, recante “*Aggiornamento delle schedule vaccinali e delle altre misure di profilassi per il personale militare*”, emanata dalla Direzione Generale della Sanità Militare in data 14 febbraio 2008 (reperibile, nella versione modificata ed aggiornata, all'indirizzo: [https://archimede.difesa.it/Intranet/Direttive\\_regolamenti\\_circolari/Sanità+Militare/Direttiva\\_vaccini\\_2008/default.htm](https://archimede.difesa.it/Intranet/Direttive_regolamenti_circolari/Sanità+Militare/Direttiva_vaccini_2008/default.htm)).

infettiva sulle operazioni, si potrebbe sviluppare un'adeguata capacità campale di controllo epidemiologico all'interno degli assetti di medicina preventiva schierati.

(7) Malattie di origine animale

Oltre al rischio di danno fisico (ad esempio, trauma o avvelenamento da morso di serpenti), gli animali selvatici o addomesticati, nei quali ci si imbatte durante una missione, possono essere responsabili di zoonosi e trasmettere all'uomo una serie di malattie, anche gravi, come la rabbia, la febbre Q, la peste, ecc..

Durante la fase di pianificazione è quindi necessario tener conto del rischio che dette malattie possono rappresentare durante un'attività operativa, attuando misure di medicina preventiva volte a minimizzare il loro potenziale impatto sulle operazioni.

(8) Malattie non infettive

Le malattie non infettive o croniche, con l'esclusione di quelle psichiche, dovrebbero avere un impatto minimo sulle operazioni ove, prima dell'invio in teatro operativo, il personale sia stato sottoposto a procedure di controllo e di valutazione rigorose. Uno screening inadeguato del personale militare prima dell'impiego può esporlo ad inutili rischi e mettere a dura prova le risorse sanitarie disponibili.

(9) Malattie psichiche

Le situazioni che possono essere vissute negli ambienti operativi possono essere spesso responsabili di stress psicologico<sup>8</sup> (*operational* e *combat stress*). Sotto la pressione di forti tensioni operative, derivanti ad esempio da attività di guerra o di stabilizzazione, anche gli individui più resistenti possono “soccombere” e manifestare sintomi o comportamenti disadattativi. Si dovrebbero, pertanto, sviluppare ed applicare sul personale militare misure preventive di controllo dello stress sia prima, sia durante sia dopo il loro l'impiego in operazioni. Nell'ambito della prevenzione primaria dovrebbero essere incluse le strategie volte ad individuare, modificare e ridurre i fattori di stress prima che questi causino delle disfunzioni. L'obiettivo della prevenzione secondaria è la rapida identificazione di reazioni disfunzionali allo stress attraverso l'addestramento dei Comandanti ai vari livelli, dei cappellani e del personale militare; in tal modo i soggetti rimasti vittime dello stress operativo dovrebbero poter essere rapidamente individuati ed indirizzati presso le strutture sanitarie, facilitando il rapido ritorno in servizio e riducendo il rischio di cronicizzare i problemi di salute psichica, come ad esempio il Disturbo Post-Traumatico da Stress (DPTS)<sup>9</sup>.

(10) Salute orale e prevenzione delle malattie orali

I problemi odontoiatrici costituiscono una potenziale causa di morbilità per il personale in operazioni. Le malattie odontoiatriche tendono spesso, per loro natura, a cronicizzare.

---

<sup>8</sup> Al riguardo, vds lo STANAG 2565 MEDSTD “*A psychological guide for leaders across the deployment cycle*” che fornisce un ottimo riferimento per i leader militari in vista della preparazione alle attività operative (la pubblicazione è, sostanzialmente, mirata alla gestione dello stress al fine di ottimizzare l'efficacia delle attività).

<sup>9</sup> Definito, sostanzialmente (DSM-IV-TR), come una configurazione di sintomi tipici (quali la paura, l'impotenza, il continuo rivivere l'evento traumatico e lo sviamento dalle situazioni che potrebbero ricordarlo) che si manifestano a seguito dell'esposizione ad un “*fattore traumatico estremo*” (quali un'esperienza personale diretta di un evento che causa o può comportare la morte, lesioni gravi o altre minacce all'integrità fisica propria o altrui, oppure il venire a conoscenza della morte violenta ed inaspettata, di grave danno o lesioni sopportate da un membro della famiglia o da altra persona con cui si è in stretta relazione) e durano per più di un mese, condizionando in modo significativo importanti aspetti dell'esistenza, come la famiglia o il lavoro.

Inoltre, a causa della dieta non sempre ideale, dell'affaticamento e degli stress psicologici connessi con l'attività operativa, è molto probabile che la salute orale del personale tenderà a peggiorare nel corso della missione.

In merito, oltre ad una attenta valutazione pre-impiego, volta a ridurre l'insorgenza di emergenze odontoiatriche, dovranno essere sviluppati programmi sanitari di carattere preventivo, come ad esempio la somministrazione di fluoro sistemico, l'applicazione topica di fluoro, l'educazione al controllo della placca, alla lotta contro il tabagismo, consigli alimentari e l'educazione all'igiene orale, atti a minimizzare la possibile comparsa di tali malattie.

**c. Misure di igiene campale, alimentare, idrica e di medicina veterinaria**

(1) Igiene campale

L'igiene campale è una componente indispensabile della Protezione Sanitaria della Forza. Mantenere un ambiente campale igienico ridurrà significativamente il rischio sia di malattie infettive sia di malattie di origine alimentare o da inquinamento idrico sia di zoonosi. Conseguentemente, dovranno essere garantite le essenziali condizioni igieniche di vita attraverso:

- la promozione dell'igiene personale;
- l'approvvigionamento di derrate provenienti da filiere affidabili, certificate e controllate;
- la corretta conservazione, preparazione e distribuzione igienica degli alimenti;
- l'adeguato controllo e smaltimento dei rifiuti prodotti nella zona di operazioni;
- il controllo degli insetti e dei roditori.

(2) Igiene alimentare

Per ridurre l'incidenza di malattie di origine alimentare, è essenziale garantire una loro adeguata igiene e sicurezza sia in una situazione stanziale sia in ambienti operativi.

In assenza di un'adeguata prevenzione, le malattie causate dagli alimenti sono in grado coinvolgere intere comunità.

Lungo l'intero percorso che va dall'approvvigionamento del cibo, alla sua conservazione, distribuzione e preparazione, è necessario applicare i massimi standard di igiene e sicurezza. Le strutture devono essere ispezionate e controllate da personale adeguatamente formato ed esperto. Se perdura un livello di rischio inaccettabile dopo aver effettuato una valutazione del rischio e dopo aver attuato provvedimenti di gestione del rischio, si raccomanda di rivolgersi a fonti alimentari più sicure. In linea generale, in una situazione operativa gli alimenti che presentano un rischio maggiore sono quelli approvvigionati localmente, mentre le razioni da combattimento sono associate a un livello di rischio minimo.

(3) Igiene idrica

La disponibilità di acqua potabile in teatro costituisce una necessità operativa. La mancanza di adeguate quantità di acqua potabile può generare un numero significativo di perdite molto più velocemente di quanto non accada per la mancanza di cibo, di riposo o a causa di stress operativo o da combattimento. Fornire una quantità adeguata di acqua potabile alle forze schierate costituisce un elemento fondamentale per salvaguardare la salute e la prontezza operativa delle forze. In caso di inadeguata fornitura di acqua (sia

dal punto di vista qualitativo che quantitativo), sarà inevitabile l'aumento dei casi di malattia dovuti o alla scarsa qualità dell'acqua distribuita o alla disidratazione<sup>10</sup>. La disidratazione rappresenta, peraltro, una delle maggiori minacce all'efficienza operativa della forza. Particolare attenzione andrà riservata all'attività fisica, allo stress ambientale, all'abbigliamento ed all'equipaggiamento, tutti fattori che possono aumentare la perdita d'acqua da parte dell'individuo e condurlo alla disidratazione.

Sebbene risulti di fondamentale importanza fornire, al personale in missione, acqua potabile sulla base degli standard qualitativi adottati in Patria, è possibile che il Comandante, tenendo conto della situazione operativa, potrebbe essere costretto ad accettare una condizione di maggior rischio permettendo la distribuzione di acqua con parametri di qualità inferiori rispetto a quelli fissati a livello nazionale. Al fine di garantire comunque la potabilità dell'acqua dovranno essere stabiliti approcci standardizzati di potabilizzazione dell'acqua fornita alle truppe schierate in operazioni. Dovranno quindi essere definiti i requisiti minimi di potabilità per l'acqua che viene fornita in teatro alle truppe durante situazioni di emergenza e dovranno essere altresì definite le capacità minime di verifica della qualità dell'acqua.

#### (4) Medicina veterinaria

La presenza di servizi veterinari costituisce una componente fondamentale della Protezione Sanitaria della Forza. Esistono numerose malattie naturalmente trasmissibili da animali ad esseri umani; molte di queste possono avere un impatto significativamente sfavorevole sulle operazioni militari. L'individuazione, la prevenzione e il controllo di dette malattie risultano necessarie sia in situazioni stanziali sia in ambienti operativi. È pertanto di fondamentale importanza assicurare il monitoraggio delle condizioni degli animali che vivono a stretto contatto con il personale militare. Inoltre, poiché anche gli animali randagi che possono essere fonte di trasmissione di malattie agli esseri umani, è necessario esercitare uno stretto controllo su di essi mediante la loro cattura, sequestro od eliminazione. I servizi di medicina veterinaria dovranno peraltro assicurare la salute e il benessere degli animali di proprietà delle Forze Armate.

#### **d. Attività di promozione della salute**

La promozione della salute è parte integrante della Protezione Sanitaria della Forza. Il processo di promozione della salute deve garantire al personale militare gli strumenti e la formazione adeguata per consentire loro di effettuare delle scelte di salute informate in grado di migliorare la l'efficienza operativa delle Forze Armate. Senza un'adeguata attività di promozione della salute, i militari corrono il rischio di prendere decisioni in materia di salute che potrebbero impattare negativamente sulla loro prontezza operativa.

Un'importante ricerca ha dimostrato che le attività di promozione della salute, influenzando positivamente le scelte in materia di tabagismo, apporto calorico nutrizionale, efficienza fisica, gestione dello stress, hanno un impatto favorevole sulla capacità operativa del militare.

---

<sup>10</sup> Stato patologico, caratterizzato da sintomi quali bocca asciutta, ipotensione, vertigini, aumento della frequenza cardiaca, urine scure, che s'instaura quando la quantità di acqua persa con le urine, il sudore, ecc., è superiore alla quantità di acqua o assunta con le bevande o l'alimentazione.

Le attività di promozione della salute aumentano la prontezza operativa delle truppe. Essa si sviluppa attraverso l'implementazione di un modello sanitario olistico nel quale si integrano tra loro:

(1) Salute comportamentale

Consente al combattente di far fronte allo stress da impiego operativo. Aspetti fondamentali della salute comportamentale sono:

- i programmi di lotta al tabagismo;
- i comportamenti sessuali responsabili;
- la prevenzione dell'uso di droghe e dell'abuso di alcol;
- la gestione ed il controllo dello stress;
- la prevenzione e sorveglianza dei suicidi e dei comportamenti suicidiari.

(2) Salute fisica

Consente al militare di operare al massimo livello di forma fisica. I fattori in grado di influenzare la salute fisica sono:

- l'addestramento fisico;
- l'ergonomia;
- la prevenzione infortunistica;
- la salute orale;
- l'alimentazione (sotto tale aspetto, particolare importanza riveste la scelta della dieta più equilibrata, dal punto di vista plastico e calorico, per le diverse condizioni d'impiego ed in funzione delle attività svolte);
- il controllo del peso.

(3) Salute spirituale

Aspetto fondamentale dell'approccio olistico al benessere dei soldati. La salute spirituale riconosce che ciascuna persona ha esigenze spirituali individuali che necessitano di essere soddisfatte e prese in considerazione come uno degli aspetti del proprio stato di salute in generale e della propria efficienza. Esistono prove sufficienti a suffragio del fatto che la salute spirituale ha un impatto sul benessere dei combattenti e che, dando voce alle esigenze spirituali, i soldati sono maggiormente in grado di affrontare i fattori di stress che popolano la loro vita ed il loro ambiente. La salute spirituale è un aspetto importante per garantire che i soldati abbiano le conoscenze, le capacità, le abilità e il supporto di cui hanno bisogno per operare in un ambiente militare.

In tale contesto, appare evidente come il programma di promozione della salute sia un processo olistico che interviene su una popolazione agendo sui singoli individui. Traslando tale discorso in ambito militare, possiamo, pertanto, affermare che l'attuazione di un programma di promozione della salute a livello dei singoli militari si ripercuoterà positivamente sull'intera Forza, garantendo un elevato standard di efficienza operativa.

e. **Minacce di carattere chimico, biologico, radiologico e nucleare (CBNR)**

(Si veda l'Annesso 6 "La difesa CBRN").

f. **Rischi sanitari occupazionali, ambientali ed industriali**

(Si veda il successivo Annesso 4 "La Protezione dell'Ambiente").



## 5. Formazione e addestramento

L'obiettivo generale della formazione e dell'addestramento sanitario è quello di garantire, allo strumento militare in operazioni, un supporto sanitario quanto più simile possibile agli standard nazionali ed in linea con quelli delineati nei documenti nazionali e NATO.

Pur presentando delle peculiarità rispetto alla sanità civile, visto l'ambiente e le condizioni nelle quali la sanità militare è spesso chiamata ad operare, il personale militare che fornisce assistenza sanitaria riceve una formazione di base e specialistica identica a quella della compagine civile.

Tale approfondita formazione, associata con il successivo adeguato addestramento, consente al personale sanitario di poter esprimere, in operazioni, un supporto sanitario efficace. Inoltre, specifici programmi di formazione e di addestramento dovranno essere indirizzati a favorire le capacità e la volontà di mettere in atto tutte le misure di Protezione Sanitaria della Forza, inserendole nel più ampio processo di Protezione della Forza.

In tale contesto, i programmi formativi ed addestrativi da sviluppare nel campo della Protezione Sanitaria della Forza sono:

### a. Formazione e addestramento individuale

Volto a diffondere tra i militari la conoscenza della Protezione Sanitaria della Forza ed suo contributo al mantenimento/potenziamento dell'efficienza operativa delle Forze Armate.

### b. Formazione e addestramento del personale "chiave"

Finalizzata a sviluppare la capacità di elaborare una pianificazione di livello strategico/operativo che tenga conto anche degli aspetti di Protezione Sanitaria della Forza e consentire a tale personale ricoprire incarichi presso Alti Comandi in Patria o in operazioni.

### c. Formazione e addestramento di Staff

Diretta a sviluppare la capacità di attuare i programmi e coordinare le misure di Protezione Sanitaria della Forza.

### d. Formazione e addestramento collettivo

Rivolti a sviluppare la capacità di applicare le procedure sanitarie che, in linea con la dottrina nazionale e NATO, consentano di fornire alle truppe, in un *continuum* assistenziale, i migliori trattamenti sanitari e sgomberi tempestivi.

La formazione e l'addestramento non devono limitarsi ai soli periodi immediatamente precedenti all'espletamento delle missioni ma, piuttosto, dovranno essere previste, su base metodica, attività addestrative sulle procedure di Protezione della Forza e di Protezione Sanitaria della Forza. La periodicità ed il coordinamento di dette attività addestrative comporteranno un duplice vantaggio in quanto, generando una migliore comprensione degli elementi della Protezione Sanitaria della Forza, garantiranno una maggiore efficacia del più generale processo di Protezione della Forza.

Tuttavia, un programma formativo ed addestrativi, condotto in prossimità dell'inizio di una operazione, potrebbe risultare particolarmente utile ai fini del successo della missione. Il personale medico militare, come pure il personale di supporto, dovrebbe essere informato non solo riguardo agli aspetti generali della loro missione, ma anche sugli aspetti sanitari specifici.

In particolare, dovranno essere messi al corrente dei seguenti aspetti:

- situazione sanitaria della *Joint Operations Area* (JOA), incluse le popolazioni a rischio e

le possibili minacce;

- eventuale presenza di strutture sanitarie di cura nella JOA (ubicazione, capacità, standard sanitari, costi, ecc.);
- principali attori sanitari presenti nella JOA (Autorità locali, IOs e NGOs).

Inoltre, auspicando una formazione linguistica tecnica di base, a seconda delle esigenze della missione, il personale militare sanitario dovrà essere formato specificatamente sul:

- processo generale di Protezione della Forza relative alla JOA;
- programma di Protezione Sanitaria della Forza all'interno della JOA;
- Comando e controllo e canali di comunicazione dei rischi sanitari all'interno della JOA.

## LA PROTEZIONE DELL’AMBIENTE

### 1. Premessa

La tutela dell’ambiente, per gli effetti che essa può avere sulle forze militari, rientra nell’area della protezione delle forze.

In tale contesto, soprattutto nei casi di intervento in situazioni ambientali degradate e nelle immediate fasi post-belliche, è indispensabile adottare una serie di provvedimenti volti ad evitare che l’ambiente in cui si opera sia danneggiato e possa determinare, conseguentemente, una riduzione dell’efficienza operativa delle unità, ovvero effetti di carattere sanitario immediato o a lungo termine per il personale.

La Difesa ha posto in essere una serie di azioni volte ad affrontare il tema della tutela ambientale, con i riflessi che ciò comporta sulla tutela del singolo militare.

Il presente allegato, relativo al settore della “Protezione dell’Ambiente” (“*Environmental Protection*”), ha lo scopo di costituire un valido ausilio per i Comandanti ed i loro *staff*, nonché per tutto il personale militare, ad ogni livello, e rappresentare una guida nel delicato ambito della protezione dell’ambiente. Tale allegato, pertanto, descrive i principi e le attività che i Comandanti, gli *staff* ai vari livelli e i singoli individui, devono adottare, nel corso delle Operazioni militari svolte in patria e all’estero, al fine di preservare l’ambiente in cui operano e contenere, di conseguenza, i rischi dovuti ad un ambiente contaminato e nocivo, considerando tale fattore nell’ambito del proprio processo decisionale.

I riferimenti bibliografici utilizzati per la sua elaborazione sono:

- “Vademecum per i Comandanti dell’Esercito Italiano sulla protezione ambientale”, ed. 2002, di SME III RIF – Uf. DAR;
- “Vademecum sulle misure di protezione del personale contro rischi di natura ambientale e CBRN”, ed. 2009 di SME III RIF/COE – Uf. Operazioni Correnti;
- il documento “MC 0491/1 *NATO Principles and Policies for Environmental Protection (EP)*” Ed. 2011;
- lo STANAG 7141 EP (Edition 5) “*Joint NATO Doctrine for Environmental Protection during NATO Led Military Activities*”;
- la AJP 4(B) – “*Allied Joint Doctrine for Logistics*” laddove nell’Annesso “B” – *Roles and Responsibilities*. Viene puntualizzato che il *Joint Force Commander (JFC)* “*Provide infrastructure development plan including Force Protection and environmental protection requirements. Develop and execute environmental protection plans including the conduct of environmental baseline surveys for camps and major installations*”.
- la AJP 3.12 (A) – “*Joint Engineering*” che dedica un intero paragrafo (0308) all’*Environmental Protection*”.

In considerazione della complessità dell’argomento trattato e della specificità legata alla singola componente, il presente annesso è suddiviso in tre sezioni: Esercito Marina ed Aeronautica ciascuna con *focus* sugli argomenti di particolare impatto sulla singola FA. Tuttavia, considerato che alcune tematiche coinvolgono trasversalmente tutte le FFAA, è opportuno affrontare le problematiche relative alla protezione dell’ambiente considerando l’intero contenuto del presente annesso.

L'obiettivo ricercato è quello di fornire al Comandante e allo staff un utile strumento di consultazione, ma soprattutto di favorire in tutto il personale delle FF.AA. la crescita di una coscienza orientata alla tutela dell'ambiente e della salute pubblica.

## 2. Generalità

Nel passato, la principale minaccia per l'umanità era quella di un possibile conflitto nucleare. Oggi, con la caduta della contrapposizione est-ovest, l'ambiente e la sfida ecologica, ad esso connessa, rappresenta una delle maggiori preoccupazioni a cui si deve far fronte partendo dalla consapevolezza che la responsabilità di porre rimedio al degrado ambientale ricade su ogni essere umano, ancor prima che sulle istituzioni.

La protezione dell'ambiente, nell'ambito della NATO, viene definita come segue:

*“Environmental protection is the application and integration of all aspects of environmental considerations as they apply to military operations. Factors that are considered include pollution prevention, waste management, conservation heritage protection (natural and man-made) and protection of flora and fauna”*.

Nel corso delle operazioni, le forze militari, che sempre hanno avuto un forte legame con l'ambiente, devono, più che nel passato, prendere tutte le misure idonee a proteggere l'ambiente naturale in cui esse operano. Ciò significa evitare l'inquinamento, gestire correttamente i rifiuti, proteggere l'eredità ambientale (naturale e creata dall'uomo) e salvaguardare la flora e la fauna.

Occorre, inoltre, porsi di fronte a tale tematica in una duplice veste: sia come parte della collettività che svolge un importante ruolo nel proteggere l'ambiente, sia come Istituzione che svolge specifiche attività di natura militare, che possono incidere profondamente sull'ambiente che li circonda.

Per quanto attiene alle attività svolte dal personale militare (in operazioni, in addestramento o in guarnigione) è necessario porre in essere una serie di accorgimenti per rendere minimi, possibilmente nulli, i danni che potrebbero essere arrecati all'ambiente.

Peraltro, va evidenziato che l'eventuale alterazione degli ecosistemi può costituire fonte di instabilità internazionale e sfociare in situazioni di crisi che potrebbero richiedere un impegno militare vero e proprio, al fine di scongiurarle.

Dal punto di vista normativo, è da tener presente che, se fino al 1978 il rapporto tra le Forze Armate e l'ambiente era regolato dalla prassi e dalle consuetudini, con la legge n. 382 dell'11 luglio 1978 “Norme di principio sulla disciplina militare” e il successivo Decreto legislativo n. 66 del 15 marzo 2010 “Codice dell'Ordinamento Militare” tale rapporto è stato ufficialmente regolamentato. Infatti, l'art. 15 comma 2 del citato Decreto legislativo fissa, fra le missioni delle F.A., “il concorso alla salvaguardia delle libere istituzioni ed al bene della collettività nazionale nei casi di pubbliche calamità”, ove la salvaguardia ambientale deve essere considerata un bene della collettività. Ciò ha posto, di fatto, la difesa dell'ambiente tra i compiti istituzionali delle F.A.

Per quanto precede, tenuto conto che la tutela dell'ambiente si ottiene partendo dalla consapevolezza del singolo individuo, al fine di sensibilizzare il personale sulla problematica in

---

<sup>1</sup> Rif. pubblicazione NATO AJP-01(D) “Allied Joint Doctrine”, ed. dic. 2010, para. 0522.

esame, è stato elaborato un "Decalogo Ambientale del Militare" (Appendice "1") allo scopo di accrescere la coscienza ecologica individuale, ponendo l'accento sull'impatto ambientale che egli stesso può causare.

Tuttavia, l'ambiente è anche un fattore da cui è opportuno "difendersi" in quanto la natura per sua definizione ha una forza infinita che può portare devastazione e perdita di vite umane. Ciò richiede un attento studio dei fattori fisici che la costituiscono (orografia, idrografia, meteorologia, ecc.) e di quei fattori di tipo sanitario (esistenza di insetti portatori di malattie, serpenti e più in generale presenza di batteri o virus nelle acque e negli alimenti) che sono sviluppati più approfonditamente nell'Annesso 3 che tratta proprio degli aspetti di protezione sanitaria).

### **3. La politica ambientale**

#### **a. Precedenti storici**

La politica ambientale della Comunità Europea muove i suoi primi passi nella Conferenza di Stoccolma del 1972. Durante tale consesso, i Capi di Stato e di Governo dell'Unione Europea concordarono sul fatto che la questione ambientale era diventata un nodo cruciale nel contesto dello sviluppo civile dei popoli. In particolare, si maturò la consapevolezza che il degrado subito dall'ambiente fosse da imputarsi prevalentemente ai Paesi maggiormente industrializzati. Successivamente, durante il Consiglio dei Capi di Stato, tenutosi a Dublino nel 1990, i Paesi membri si impegnarono a garantire, quale comune obiettivo, il diritto dei cittadini ad un ambiente pulito e salubre. Nel Trattato di Maastricht del 1992 è stato riconosciuto che lo sviluppo delle attività economiche deve avvenire in maniera tale da rispettare l'ambiente. Infine, nel Trattato di Lisbona del 2007, che apporta ampie modifiche al Trattato sull'Unione europea e al Trattato che istituisce la Comunità Europea, si stabilisce che uno degli obiettivi dell'Unione è operare per uno sviluppo sostenibile dell'Europa sulla base, in particolare, di un elevato livello di tutela e del miglioramento della qualità dell'ambiente. Sebbene l'idea dello sviluppo sostenibile figurì anche negli attuali trattati, il trattato di Lisbona la rafforza e ne precisa la portata. Lo sviluppo sostenibile rientra anche tra gli obiettivi fondamentali dell'UE nelle sue relazioni con il resto del mondo.

L'ambiente, pertanto, rappresenta una delle sfere di competenza che l'Unione europea condivide con gli Stati membri, perseguendo obiettivi chiari: preservare, tutelare e migliorare la qualità dell'ambiente; proteggere la salute; incoraggiare un uso prudente e razionale delle risorse naturali; promuovere misure a livello internazionale per affrontare problemi ambientali di portata regionale o mondiale.

Con il trattato di Lisbona, la lotta a livello internazionale contro i cambiamenti climatici diventa un obiettivo specifico della politica ambientale dell'UE. In tal modo, viene riconosciuto chiaramente il ruolo di primo piano che l'UE può svolgere in questo campo sulla scena mondiale.

In ambito nazionale<sup>2</sup>, la presa di posizione decisiva, in materia di politica ambientale, è rappresentata dalla legge n. 349 del 1986 "Istituzione del Ministero dell'Ambiente e norme in

---

<sup>2</sup> La Corte Costituzionale, inoltre, ha sancito che "nel nostro ordinamento giuridico la protezione dell'ambiente è imposta da precetti costituzionali ed assurge a valore primario ed assoluto (artt. 9 e 32 della Costituzione della Repubblica Italiana)".

materia di danno ambientale"<sup>3</sup>.

**b. La politica ambientale nazionale**

In Italia, la politica intrapresa dal Ministero dell'Ambiente si basa su tre pilastri fondamentali:

- il risanamento del *deficit* ambientale del Paese, al fine di recuperare i ritardi rispetto a quanto chiesto dalla Comunità Europea;
- l'attuazione di programmi per lo "sviluppo sostenibile", nell'ambito dei quali gli indirizzi di tutela ambientale si integrano con le politiche tecnico-economiche nazionali, rispettando il modello ambientale di riferimento (sviluppo sostenibile);
- la promozione ed il sostegno di politiche ambientali innovative.

Nell'ambito militare, dal termine della guerra fredda ad oggi, l'Italia e la NATO hanno guardato in maniera crescente alle minacce non tradizionali e hanno riconosciuto che la sicurezza è influenzata da fattori politici, economici ed ambientali.

In ambito Alleanza, sono stati istituiti una serie di comitati e gruppi di lavoro che trattano le problematiche relative alla tutela ambientale. Ciò, in quanto non è più possibile scindere lo sviluppo di qualsivoglia tipologia di attività militare da considerazioni di carattere ambientale.

Oggi, la politica ambientale nazionale si fonda sulla consapevolezza che l'attenzione dell'opinione pubblica è sempre più focalizzata verso quelle problematiche, scaturite dallo sviluppo della società moderna, le quali suscitano una crescente preoccupazione in virtù delle eventuali loro ripercussioni sullo stato della salute pubblica e del territorio.

A tale preoccupazione non è estraneo il Ministero della Difesa che, da sempre, ha contribuito alla tutela ambientale del Paese.

L'Amministrazione Difesa allo scopo di contribuire alla sicurezza ambientale, fonda il proprio operato sulle seguenti "Linee Guida"<sup>4</sup>:

- considerare il parametro "tutela ambientale" nell'ambito dei processi decisionali e di pianificazione;
- allineare le norme e i regolamenti nazionali presenti in ambito alla Difesa, agli accordi internazionali a tutela dell'ambiente;
- creazione di una coscienza ecologica attraverso una serie di attività specifiche nei settori dell'istruzione, dell'addestramento e dell'informazione del proprio personale;
- integrazione nei processi d'approvvigionamento, di manutenzione, di riparazione e di dismissione di sistemi, di materiali, di equipaggiamenti e di infrastrutture di particolari specifiche tecniche volte alla tutela dell'ambiente;
- prevenzione dell'inquinamento e abbattimento dell'impatto ambientale nello sviluppo di ogni attività (in guarnigione e fuori sede);
- ricerca delle procedure standardizzate volte al rispetto dell'ambiente nel corso di ogni impiego (nazionale e internazionale);
- protezione, mantenimento e, quando necessario, ripristino e miglioramento della qualità dell'ambiente nelle installazioni militari;
- riduzione dei pericoli per la salute umana e per l'ambiente, tramite l'adozione di procedure

<sup>3</sup> Per un approfondimento: [www.minambiente.it](http://www.minambiente.it).

<sup>4</sup> Approvate dal Comitato dei Capi di Stato Maggiore del 09/12/1992.

valutative e di bonifica per possibili contaminazioni derivanti da pregresse attività della Difesa;

- partecipazione a studi e gruppi di lavoro specifici nazionali, internazionali e NATO;
- sostegno in ambito internazionale delle attività a favore dell’ambiente, in conformità con la politica di sicurezza nazionale;
- ricerca della collaborazione degli altri Ministeri nell’attuazione dei programmi di sicurezza ambientale;
- coordinamento preventivo delle iniziative e delle normative internazionali, comunitarie e nazionali che possono avere un impatto sull’ambiente;
- trasparenza in tutte le questioni ambientali che non inficiano la sicurezza e l’efficacia dello strumento militare.

### **c. Terminologia di riferimento**

Nell’accezione militare, il termine “ambiente” è spesso associato all’attributo operativo, significando l’insieme dei fattori di situazione che influiscono sulla condotta di un’attività militare. Tra tali fattori vi sono quelli così detti ambientali ed, in particolare, quelli relativi al terreno ed alle infrastrutture.

Nell’accezione più generale del termine<sup>5</sup>, l’ambiente è “il complesso delle condizioni esterne all’organismo ed in cui si svolge e si sviluppa la vita vegetale ed animale” ovvero “il complesso delle condizioni esterne materiali, sociali e culturali nell’ambito delle quali si sviluppa, vive ed opera un essere umano”. L’ambiente, quindi, deve essere considerato la risorsa per eccellenza, perché favorisce lo sviluppo della vita.

Negli ultimi anni, la consapevolezza secondo cui le attività dell’uomo comportano sempre conseguenze sull’ambiente e che tale risorsa, una volta depauperata, influenzerà negativamente la crescita e lo sviluppo delle generazioni future, è aumentata. Per tale ragione si è iniziato a parlare di impatto ambientale, inteso quale alterazione dell’ambiente conseguente ad un’azione, diretta o indiretta, dell’uomo.

Appare opportuno sottolineare che anche le attività militari producono, inevitabilmente, come tutte le altre attività umane, un impatto ambientale che deve essere attentamente valutato e, se negativo, minimizzato.

Pertanto, si rende necessario:

- valutare tale impatto e porre in essere tutti i possibili accorgimenti per ridurre al minimo le cause che possono produrre una ricaduta negativa sull’ambiente;
- determinare l’influenza che l’aspetto ecologico può avere sulle attività militari.

---

<sup>5</sup> Dizionario della lingua italiana “Zingarelli”.





**SEZIONE I – ESERCITO****1. La protezione dell'ambiente****a. Generalità**

Le condizioni in cui è possibile che avvengano delle alterazioni dell'ambiente naturale costituiscono le situazioni denominate **d'impatto ambientale** il cui esito negativo non può essere definito a priori, ma emerge a seguito di una attenta valutazione, tramite la compilazione di una serie di liste di controllo appositamente redatte da responsabili ben definiti in relazione all'attività di natura militare da svolgere ed in funzione:

- della natura dell'attività stessa;
- del luogo/località dove essa sarà svolta;
- della tipologia dei mezzi e dei materiali impiegati;
- della natura e dell'entità delle forze schierate sul terreno.

Le liste di controllo in argomento, inoltre, hanno lo scopo di:

- facilitare l'individuazione di possibili eventi negativi;
- evidenziare, con sufficiente approssimazione, l'impatto ambientale che potrebbe verificarsi;
- determinare gli eventuali fattori da analizzare nello sviluppo del processo decisionale allo scopo di escludere, rapidamente, gli effetti che si ritiene non si determineranno nel corso dell'attività<sup>1</sup>.

**b. La valutazione dell'impatto ambientale**

La valutazione dell'impatto ambientale ricade su ogni individuo e su ogni Comandante. Essi dovranno porre in essere tutte le misure volte a proteggere l'ambiente e, conseguentemente, dovranno prevedere l'impatto ambientale dell'attività militare da svolgere, effettuando una serie di valutazioni in tal senso. I Comandanti, in particolare, dovranno integrare i risultati di tale analisi nell'ambito del proprio processo decisionale, al fine di eliminare o ridurre il danno ambientale. Infatti, prevenire eventuali situazioni che possono mettere a rischio l'ambiente, è ben più remunerativo dell'intervenire successivamente.

Tale valutazione dovrà permettere la visualizzazione immediata della possibile situazione futura dell'ambiente in cui si andrà ad operare e, di conseguenza, dovrà consentire la ricerca di soluzioni adeguate, al fine di proteggere e preservare l'ambiente naturale. Le soluzioni in argomento scaturiscono dallo sviluppo logico-deduttivo del processo decisionale e dovranno essere integrate nell'ambito della pianificazione e dell'emanazione degli ordini, prevedendo lo sviluppo di un apposito allegato all'Ordine di Operazione denominato "Tutela ambientale" (Appendice "3").

---

<sup>1</sup> Le liste in argomento possono essere create ovvero modificate empiricamente sulla base delle esperienze maturate durante le attività già svolte. Inoltre, per la loro compilazione, può essere utile cooperare con gli organismi amministrativi territoriali preposti alla tutela ambientale. Cooperazione che può portare ad individuare, con maggior facilità e precisione, le possibili situazioni di impatto ambientale relative ad una determinata zona e quindi valutare gli eventuali effetti negativi che lo sviluppo delle attività potrebbe provocare. In Appendice "2", a titolo d'esempio, è stata elaborata una "lista di controllo per l'occupazione di una determinata area addestrativa".

L'esame, che conduce all'individuazione della situazione ambientale futura e alle relative soluzioni di protezione, scaturisce dalla correlazione di una serie di fattori, tra i quali si evidenziano:

- la normativa di riferimento;
- la tipologia dell'attività da svolgere (addestrativa, operativa, logistica);
- le condizioni ambientali di partenza;
- le possibili situazioni di impatto ambientale;
- le esigenze particolari di carattere puramente militare.

In merito a quest'ultimo fattore, da prendere in considerazione prevalentemente in operazioni, è necessario precisare che, sebbene le esigenze operative siano di primaria importanza, l'impatto ambientale in ogni caso deve essere valutato e, per quanto possibile, minimizzato. Detta valutazione, infine, dovrà essere verificata alla luce dei seguenti principi di riferimento:

- assicurare un'elevata protezione dell'ambiente, operando nel pieno rispetto delle norme vigenti;
- adottare tutte le possibili iniziative dirette a prevenire le situazioni negative di impatto ambientale;
- prevenire ogni comportamento che possa danneggiare la natura;
- sensibilizzare tutto il personale sull'importanza della tutela ambientale e sulle responsabilità del singolo individuo.

Per l'individuazione e la conseguente valutazione dell'impatto ambientale all'interno di un'infrastruttura militare è necessario far riferimento alla normativa esistente in materia ambientale<sup>2</sup>.

Per identificare ogni possibile evento negativo derivante dalle attività svolte, che possa arrecare nocimento all'ambiente, i Comandanti, a tutti i livelli, devono redigere uno specifico "Questionario ambientale"<sup>3</sup>, che costituisce un valido ausilio per individuare i necessari correttivi da apportare alla vita quotidiana. Poiché la protezione ambientale rappresenta una disciplina complessa, non solo in termini legislativi e di controllo, ma soprattutto in termini di eterogeneità e numero di materie coinvolte, il Comandante dovrà necessariamente avvalersi soprattutto del proprio organo logistico che, in materia di protezione ambientale, provvede a svolgere i seguenti compiti:

- consulenza in merito alle questioni ambientali in qualsiasi situazione operativa (stasi, addestramento ed operazioni). È responsabile della preparazione delle linee d'azione ovvero degli ordini in materia di protezione e tutela ambientale che dovranno essere approvati dal Comandante;
- controllo, nell'ambito dell'Unità, dell'Ente o del Comando, dell'applicazione e del rispetto delle leggi, delle normative, delle direttive e delle procedure in materia di ambiente;
- concorso nella formazione del personale, allo scopo di:

---

<sup>2</sup> Per un approfondimento in merito, consultare il sito del Ministero dell'Ambiente ([www.minambiente.it](http://www.minambiente.it)) nella sezione "NORMATIVA".

<sup>3</sup> Elaborato dal Sottogruppo di Lavoro Interforze per le Installazioni Militari (cfr. "Vademecum per i Comandanti dell'Esercito Italiano sulla protezione ambientale", ed. 2002).

- sensibilizzare sulle problematiche ambientali;
- prevenire eventuali situazioni di impatto ambientale negativo, mediante l'integrazione fra sensibilizzazione e ricerca della protezione dell'ambiente;
- fornire gli elementi concettuali indispensabili per agire in caso di impatto ambientale negativo.

Tale organo, inoltre, dovrà essere aggiornato sui dati pertinenti alla tutela ambientale relativamente a:

- poligoni ed aree addestrative;
- possibili aree d'operazione;
- legislazione nazionale, regionale ed europea.

## **2. La protezione dell'ambiente in guarnigione**

### **a. Generalità**

La guarnigione è il luogo dove le Unità sono normalmente dislocate. Essa comprende le infrastrutture utilizzate nel periodo di tempo durante il quale le unità si approntano per l'esecuzione di un Ordine di Operazione ovvero per un successivo impiego. Nelle infrastrutture militari si svolgono delle attività che possono dare vita a possibili fonti d'impatto ambientale<sup>4</sup>. Tali attività soggiacciono alla normativa nazionale vigente in materia, quindi, la responsabilità dei danni causati all'ambiente è direttamente connessa al rispetto delle leggi nazionali e risale al Comandante dell'unità o dell'infrastruttura. L'esecuzione delle attività in questione richiede una presa di coscienza dei potenziali rischi in esse insiti, anche per la possibile risonanza che le questioni ambientali esercitano, tramite i media, sulla società civile.

È necessario considerare, inoltre, che la sensibilità della pubblica opinione spinge il legislatore all'emanazione di norme sempre più specifiche e, talvolta, restrittive delle attività militari. La trasformazione in reato penale del reato contro l'ambiente comporta una maggior attenzione dell'Autorità giudiziaria e una maggiore esposizione personale dei Comandanti, a tutti i livelli. Pertanto, si rende necessaria una puntuale e precisa attuazione di tutti gli adempimenti di legge, nonché un'azione volta a minimizzare ogni tipologia di evento negativo tramite uno sforzo sia dal punto di vista concettuale, sia da quello organizzativo.

### **b. La protezione dell'ambiente in guarnigione**

Nel caso delle attività svolte in guarnigione, l'individuazione delle possibili situazioni d'impatto ambientale è semplificata dai seguenti fattori:

- esistenza di norme precise che regolano tutte le attività che possono recare danno all'ambiente;
- circoscrivibilità del campo di applicazione all'interno del comprensorio;
- facilità di prevenzione dovuta allo scarso numero delle cause d'impatto.

In tale contesto ogni Comandante dovrà porre in essere azioni sistematiche di controllo, volte a verificare il rispetto assoluto della normativa vigente e, per far ciò, si avvarrà del proprio organo logistico che sovrintende alla maggioranza di quelle attività che, per loro intrinseca

<sup>4</sup> Quali, ad esempio, quelle che si possono verificare presso le officine, le mense, i depositi di carburanti e lubrificanti, le aree di stoccaggio di materiali inquinanti.

natura, possono dar vita ad un possibile impatto ambientale negativo<sup>5</sup>. Infine, particolare attenzione deve essere posta alla produzione di rifiuti legata allo svolgimento di attività di natura logistica o infrastrutturale<sup>6</sup>.

I rifiuti, si suddividono in:

- urbani o speciali, secondo l'origine;
- pericolosi o non pericolosi, secondo le caratteristiche di nocività.

### **3. La protezione dell'ambiente in addestramento ed in esercitazione**

#### **a. Generalità**

Nell'esaminare le possibili situazioni di impatto ambientale causate da attività militari in campagna è necessario distinguere tra la condotta di operazioni e lo svolgimento del normale addestramento e/o di esercitazioni. Infatti, mentre nel primo caso valgono particolari considerazioni che verranno in seguito esaminate, nel secondo caso, l'impatto ambientale durante l'addestramento o le esercitazioni deve essere sempre analizzato con particolare cura e attenzione.

Infatti, il preventivo esame del possibile impatto ambientale, nonché la determinazione delle predisposizioni da adottare prima, durante e dopo l'attività addestrativa, sono da considerarsi tra i fattori che determinano la buona riuscita dell'attività stessa, in tema di sicurezza ambientale.

In generale, nelle attività di campagna è importante essere consapevoli dell'esigenza di adeguare il proprio operato all'ambiente circostante e non pretendere che accada il contrario.

È fondamentale comprendere che una esercitazione può essere organizzata, con apposite cautele e soluzioni alternative, in funzione delle esigenze di salvaguardia ambientale senza, peraltro, venir meno agli obiettivi addestrativi prefissati.

#### **b. Predisposizioni afferenti alla protezione dell'ambiente in addestramento ed in esercitazione**

Le misure da porre in essere per prevenire situazioni d'impatto ambientale connesse con l'attività addestrativa devono integrarsi con l'organizzazione posta in atto per la specifica attività. Esse sono semplificate dal fatto che l'addestramento:

- è condotto in zone per lo più conosciute (ovvero in poligoni o aree addestrative permanenti ove molte delle predisposizioni da attuare sono già previste dal regolamento d'utilizzo del poligono/area addestrativa);
- raramente dà luogo a situazioni di impatto ambientale non preventivabili (ovvero di grande portata);
- è di norma preceduto da attività di sensibilizzazione del personale sul rispetto delle più elementari norme per la salvaguardia della natura e dell'ambiente.

Dette predisposizioni sono riconducibili alle seguenti situazioni:

- allestimento dell'area di accampamento o bivacco;

---

<sup>5</sup> Ad esempio, le attività sanitarie, il mantenimento, le attività sulle infrastrutture.

<sup>6</sup> Il rifiuto è definito, a mente del Decreto Legislativo n. 22 del 5 febbraio 1997, come "qualsiasi sostanza od oggetto che rientra nelle categorie di seguito riportate e di cui il detentore abbia deciso o abbia l'obbligo di disfarsi"– Appendice "4".

- uso, manutenzione e riparazione di mezzi;
- svolgimento di attività a fuoco.

(1) L'allestimento della zona di accampamento

La sistemazione nella zona di accampamento costituisce una delle più frequenti situazioni di impatto ambientale che, ancorché limitata in termini di portata, è opportuno valutare preventivamente, anche in considerazione della ricaduta di “immagine” che ciò può comportare nei confronti delle comunità locali.

Normalmente, ogni unità utilizza delle aree addestrative nell'ambito delle quali sono stabilite le zone adibite ad accampamento. In tale situazione, sarà utile prendere visione della “Scheda Notizie” (Appendice “4”) relativa al poligono/area addestrativa da utilizzare, che costituisce un valido ausilio all'analisi della situazione e consente di organizzare l'area che si intende utilizzare. Inoltre, nel caso di aree o poligoni permanenti, occorre contattare la competente Direzione del poligono, per acquisire notizie in merito a particolari problematiche ambientali connesse con la zona che si andrà ad occupare. Tenuto conto che numerose aree sono sottoposte a vincoli (ad esempio di tipo paesaggistico, idrogeologico, panoramico), nel predisporre l'accampamento sarà necessario adottare una serie di possibili accorgimenti volti a:

- evitare di danneggiare la flora (ad es. le piante);
- preservare l'ecosistema della zona, evitando di disturbare la fauna;
- evitare di inquinare il suolo, le acque e l'aria;
- salvaguardare il paesaggio.

Nella realizzazione di un accampamento è, inoltre, necessario evitare:

- l'utilizzo di percorsi “alternativi” con veicoli ruotati e cingolati;
- l'attraversamento di aree coltivate;
- l'accensione di fuochi;
- l'abbattimento di alberi.

Al termine dell'esigenza, e a premessa dell'abbandono dell'accampamento o del bivacco, il terreno deve essere riportato alle condizioni ambientali iniziali, avendo cura di ricomporre il terreno eventualmente sollevato<sup>7</sup>.

(2) L'uso, la manutenzione e la riparazione dei mezzi

Nel corso di attività addestrative, particolare attenzione dovrà essere posta in merito all'utilizzo dei veicoli, nonché alle connesse attività di manutenzione e riparazione.

In tale ambito, un'accurata azione di prevenzione ed una capillare organizzazione logistica possono evitare situazioni d'impatto ambientale di una certa gravità.

Ad esempio, l'utilizzo di percorsi “alternativi” con veicoli ruotati e cingolati (fuoristrada) di veicoli in alcune Regioni Amministrative è limitato, per norma, a specifiche aree ed itinerari *ad hoc*.

Pertanto è opportuno:

- contattare la Commissione Liquidazione Danni, al fine di verificare gli itinerari da

---

<sup>7</sup> La citata Appendice “2” riporta, in merito, un esempio di lista di controllo per lo svolgimento di tali attività.

utilizzare nello svolgimento delle attività;

- individuare ulteriori itinerari, richiedendo l'autorizzazione alle competenti Autorità locali;
- utilizzare piste, percorsi ed itinerari preventivamente ricogniti ed autorizzati.

Per quanto riguarda la manutenzione e la riparazione dei veicoli in campagna, oltre al rispetto della normativa in vigore sul trattamento dei residui di lavorazione, è necessario:

- individuare una zona idonea dove ubicare il posto manutenzione, qualora non prevista dal regolamento di utilizzo dell'area;
- porre in atto tutti i possibili accorgimenti, per evitare un impatto ambientale negativo nei confronti del terreno, della flora, della fauna e dei corsi d'acqua;
- dotare l'officina o il posto manutenzione di appositi contenitori per lo stoccaggio temporaneo dei residui delle lavorazioni.

Per lo smaltimento dei rifiuti in campagna, è opportuno ricordare che:

- alcuni materiali vengono classificati come rifiuti particolari e, pertanto, lo smaltimento segue precise disposizioni legislative;
- le norme in vigore in merito ai danni ambientali arrecati in esercitazioni ne attribuiscono la responsabilità diretta al Comandante, ovvero al Direttore dell'esercitazione.

Infine, è da tenere in considerazione che il lavaggio e la rimozione del fango rientra nel contesto delle attività di mantenimento. Tale operazione deve essere condotta in maniera tale da incanalare e convogliare le acque reflue in apposite vasche per la raccolta e il successivo smaltimento.

L'approntamento della zona idonea alle attività in esame può essere facilitato considerando i contenuti degli Appendice "2", "5", "6" e "7", che rispettivamente riportano:

- una possibile lista di controllo per l'occupazione di un'area addestrativa;
- alcune norme pratiche per la realizzazione di un deposito carburanti e lubrificanti in campagna;
- una serie di norme elementari pratiche per la realizzazione di un deposito temporaneo di rifiuti in campagna;
- le attività da compiere per la raccolta degli oli e dei grassi animali ed esausti in campagna.

### (3) Le attività addestrative a fuoco

Le esercitazioni a fuoco possono essere considerate alla stessa stregua di tutte le altre attività addestrative.

In merito alla loro condotta, particolare attenzione dovrà essere posta circa la possibilità che l'utilizzo di munizionamento possa generare dei principi d'incendio e, quindi, recare danno alla flora esistente nell'area. Pertanto, a premessa dell'avvio dell'attività, sarà necessario effettuare un accurato studio del terreno in modo da poter individuare le zone a rischio (arbusti, erbe secche, ecc.) ed evitare, così, di batterle con il fuoco. Tale attività dovrà essere svolta con più attenzione nella stagione primaverile ed estiva. Inoltre, bisogna rammentare che il vento facilita l'insorgere di incendi e, associato al fuoco, trasforma quest'ultimo in un'arma di distruzione ambientale.

Per intervenire prontamente in caso di focolai di incendi, si dovrà sempre predisporre un'aliquota di personale per garantire un servizio antincendio di emergenza.

Ancorché, di norma, la composizione e le modalità di intervento di tale aliquota siano stabilite nel regolamento per l'utilizzo del poligono, è bene accertarsi che l'aliquota sia:

- composta da personale in numero adeguato all'attività da svolgere e preventivamente addestrato all'esigenza da affrontare;
- dotata di veicoli idonei al tempestivo intervento;
- in possesso di apparati radio per il collegamento;
- equipaggiata con materiali idonei all'entità dell'intervento da eseguire.

Al termine dell'attività a fuoco si dovrà provvedere ad una bonifica dell'area utilizzata per l'esercitazione, al fine di:

- accertarsi che non vi siano ordigni inesplosi (compilando, successivamente, apposito rapporto di bonifica);
- rastrellare il materiale impiegato (ad es. i bossoli) e gli eventuali imballaggi del munizionamento;
- asportare i rifiuti solidi e liquidi derivanti dallo stazionamento del reparto;
- verificare che i veicoli impiegati (ruotati e cingolati) non abbiano avuto fuoriuscite di carburanti e/o lubrificanti e, se del caso, provvedere alla bonifica;
- assicurarsi dell'inesistenza di focolai di incendio (redigendo, successivamente, apposito verbale).

#### **4. La protezione dell'ambiente in operazioni**

##### **a. Generalità**

La condotta di operazioni militari:

- dà luogo ad una variegata gamma di situazioni di impatto ambientale;
- può originare un impatto di non trascurabile entità;
- può indurre a sottovalutare ovvero a tralasciare del tutto la valutazione dell'impatto ambientale, in relazione alla prioritaria esigenza di assolvere il compito.

##### **b. La protezione ambientale in operazioni**

Nella condotta di operazioni, non è sempre possibile ricorrere, ai fini della salvaguardia dell'ambiente, all'ausilio di documenti come quelli presi in esame per l'utilizzo delle aree addestrative, ovvero ricorrere alla conoscenza, acquisita nel tempo, della zona per quanto concerne il rispetto della natura.

Le operazioni militari, inoltre, per la complessità ed il ritmo<sup>8</sup> che le contraddistinguono, producono un impatto ambientale sicuramente negativo. I Comandanti hanno l'obbligo, in ogni caso, di inserire l'analisi della valutazione di tale impatto nel contesto del proprio processo decisionale, al fine di minimizzarlo ovvero, qualora possibile, evitarlo.

Si tratta, in sostanza, di un obbligo etico che può essere considerato un vero e proprio dovere in base a quanto stabilito dai vigenti codici di Diritto Bellico e di Diritto Umanitario Internazionale, che definiscono l'ambiente "patrimonio dell'umanità".

---

<sup>8</sup> Ritmo: frequenza con la quale si sviluppano le attività nell'ambito di azioni tattiche, battaglie e operazioni maggiori.

Ai fini della tutela ambientale la classificazione prevista dalla NATO delle operazioni militari in operazioni di guerra art. 5 ed in quelle non art. 5<sup>9</sup> conserva la sua validità.

(1) Operazioni di guerra - art. 5

Nelle operazioni militari di guerra, stante la priorità degli obiettivi militari da raggiungere, può essere difficoltoso integrare gli elementi scaturiti dalla valutazione dell'impatto ambientale nell'ambito del processo decisionale.

Pur nella consapevolezza che la principale responsabilità di ogni Comandante consiste nel raggiungimento degli obiettivi militari, non possono non essere considerate valide le norme per il rispetto e la salvaguardia dell'ambiente: il rischio ambientale causato dalla condotta delle operazioni militari deve essere conciliato con gli obiettivi della missione ricevuta.

Un'operazione di guerra deve essere pianificata e condotta, nei limiti del possibile e senza inficiarne gli esiti della stessa, cercando comunque di minimizzare le ripercussioni negative sull'ambiente e sulla salute dell'uomo.

Peraltro, non può essere sottaciuta la possibilità che un considerevole danno ambientale, causato durante un'operazione militare di guerra, possa tramutarsi in vero e proprio crimine di guerra.

Infatti, negli "Usi e Convenzioni di Guerra" è classificato quale crimine di guerra "la distruzione senza motivo di abitati e le devastazioni non giustificate dalle necessità militari".

Alla stessa stregua, sono considerate le infrazioni gravi alle convenzioni internazionali ed ai protocolli aggiuntivi alle stesse quali "gli attacchi all'ambiente naturale ed alle installazioni che racchiudono forze pericolose".

Le citate norme, inoltre, vietano la rappresaglia posta in essere contro l'ambiente naturale.

Di seguito vengono riportati gli articoli del Protocollo aggiuntivo adottato a Ginevra l'8 giugno 1977<sup>10</sup> riguardanti l'ambiente e la sua protezione.

*Art. 35 - Regole fondamentali*

- 1. In ogni conflitto armato, il diritto delle Parti in conflitto di scegliere metodi e mezzi di guerra non è illimitato.**
- 2. È vietato l'impiego di armi, proiettili e sostanze nonché metodi di guerra capaci di causare mali superflui o sofferenze inutili.**
- 3. È vietato l'impiego di metodi e mezzi di guerra concepiti con lo scopo di provocare, o dai quali ci si può attendere che provochino, danni estesi, durevoli e gravi all'ambiente naturale.**

---

<sup>9</sup> Il riferimento NATO è dato dalla pubblicazione NATO AJP – 3.4(A) "Allied Joint Doctrine for Non Article 5 Crisis Response Operations".

<sup>10</sup> Protocollo aggiuntivo alle Convenzioni di Ginevra del 12/8/1949.



*Art. 55 - Protezione dell'ambiente naturale*

- 1. La guerra sarà condotta curando di proteggere l'ambiente naturale contro danni estesi, durevoli e gravi. Tale protezione comprende il divieto di impiegare metodi o mezzi di guerra concepiti per causare o dai quali ci si può attendere che causino danni del genere all'ambiente naturale, compromettendo, in tal modo, la salute o la sopravvivenza della popolazione.**
- 2. Sono vietati gli attacchi contro l'ambiente naturale a titolo di rappresaglia.**

Inoltre, occorre fare riferimento, quale supporto generale in materia di protezione ambientale, ai contenuti dello STANAG 7141 Ed. 5 "Dottrina Interforze della NATO per la protezione ambientale durante le esercitazioni e le operazioni a guida NATO"<sup>11</sup>.

(2) Operazioni "Non-Art. 5"

Le operazioni "non-art. 5" sono operazioni multifunzionali, poste in essere dalla Comunità Internazionale, e che comprendono iniziative politiche, militari e civili aventi lo scopo di prevenire i conflitti attraverso la risoluzione ovvero la gestione delle crisi internazionali e variano dall'assistenza umanitaria all'impiego coercitivo dello strumento militare.

Tale tipologia di operazioni comprende una vasta gamma di attività che interessano, in maniera diversa, l'impiego di forze militari ovvero la minaccia dell'impiego di tale strumento. Si tratta di operazioni di tipo multifunzionale che devono essere condotte in conformità ad una serie di principi<sup>12</sup> la cui osservanza è di fondamentale importanza non solo per l'assolvimento della missione, ma anche per la salvaguardia ambientale.

Facendo riferimento al principio del "rispetto reciproco", ad esempio, è facile intuire come la forza incaricata della missione di pace, dovendo dimostrare rispetto per le leggi, gli usi ed i costumi delle parti in conflitto, dovrà necessariamente rispettare anche le più elementari regole di tutela dell'ambiente e della natura.

Pertanto, la salvaguardia dell'ambiente contribuirà ad accrescere la credibilità e la legittimità delle attività svolte dalla forza di intervento.

Nella condotta di tale tipologia di operazione si dovrà sempre procedere alla valutazione dell'impatto ambientale di ogni singola attività ed all'inserimento dei risultati di tale valutazione nell'ambito del processo decisionale.

Inoltre, al pari del risultato dell'analisi condotta sui fattori di situazione, anche i risultati derivanti dalla valutazione dell'impatto ambientale dovranno subire una verifica di validità alla luce dei principi dianzi citati.

È opportuno sottolineare che nella condotta di una operazione "non-art. 5", la forza di pace normalmente opera sulla base di un mandato formulato da un'organizzazione internazionale, generalmente l'ONU. In tale ambito l'ONU, già dal dicembre del 1976, ha formalizzato, con la Risoluzione 31/72, una Convenzione relativa al "Divieto di utilizzare tecniche di modifica dell'ambiente naturale per scopi militari o per qualsiasi altro scopo

---

<sup>11</sup> STANAG 7141 Ed. 5 "Joint NATO doctrine for environmental protection during NATO led military activities" Ed. 2008

<sup>12</sup> Consenso - Imparzialità - Credibilità - Rispetto reciproco - Trasparenza - Libertà di movimento - Cooperazione civile-militare.

ostile". Tale Convenzione, che si affianca a quelle già citate in precedenza, ha valore anche durante la condotta di tale tipologia di operazioni.

Pertanto, nella condotta delle operazioni, che non prevedono uno stato di guerra e quindi l'applicabilità dei codici riguardanti i conflitti armati, si può fare riferimento a tale strumento normativo per la protezione e la salvaguardia dell'ambiente.

Anche in questo caso, un ruolo di particolare importanza deve essere attribuito all'organo logistico. Quest'ultimo, infatti, nello svolgimento delle proprie attribuzioni dovrà tener conto della legislazione, ovvero degli usi e delle consuetudini vigenti sul territorio ove il Contingente opera.

Egli dovrà agire in stretto coordinamento con:

- il Consigliere Legale<sup>13</sup> del Comandante (*Legal Advisor*), per quanto concerne la vigente legislatura e per le problematiche di natura giuridica connesse con la tutela dell'ambiente e della natura;
- con il personale operante nella branca CIMIC, per quanto attiene alle attività di precipua competenza di quest'ultima;
- eventuale personale specialistico<sup>14</sup> dello *staff*, esperto in materia ambientale.

## 5. La protezione dell'ambiente in attività logistiche

### a. Generalità

Alla stessa stregua delle operazioni, le attività logistiche condotte in campagna o, in ogni caso, fuori dalla sede stanziale possono:

- dar luogo ad una variegata gamma di situazioni di impatto ambientale;
- generare un impatto di consistente entità.

Ciò in quanto:

- assumono una connotazione differente da quella che le caratterizza all'interno di una infrastruttura;
- sono contraddistinte da una elevata dinamicità;
- risentono dell'indeterminatezza ovvero della precarietà connessa alla situazione contingente;
- possono dare luogo ad un impatto ambientale non del tutto trascurabile.

Le possibili situazioni d'impatto ambientale in simili condizioni non sono facilmente determinabili a priori<sup>15</sup>. In ogni caso, possiamo individuarne alcune (quelle più frequenti), che devono essere analizzate in sede di valutazione dell'impatto ambientale, quali:

- le emissioni di gas nell'atmosfera;
- la contaminazione di acque;
- il rilascio di sostanze e rifiuti (tossici e non);
- lo spargimento di carburanti e lubrificanti.

---

<sup>13</sup> Ufficiale o funzionario civile specializzato nelle problematiche di natura giuridica, affiancato al Comandante in operazioni per fornire adeguata consulenza in campo giuridico.

<sup>14</sup> SME: *Subject Matter Expert*.

<sup>15</sup> Basti pensare, ad esempio, ad un rifornimento urgente di carburante in zona d'esercitazione che determini, che a causa dei ritmi dell'azione, lo spargimento di liquido/sostanze inquinanti sul terreno.

**b. Emissione di gas nell’atmosfera**

Tale situazione si verifica, normalmente, durante i movimenti ed i trasporti.

Le misure principali da adottare, al fine di minimizzare i danni all’ambiente, consistono:

- nell’approvvigionamento di mezzi tecnologicamente avanzati nel campo delle emissioni dei gas di scarico;
- nel controllo costante del livello di emissione dei gas di scarico (competenza che ricade sui Comandanti).

Si possono verificare anche situazioni di emissione di gas nell’atmosfera non causate direttamente dallo sviluppo di un’attività logistica vera e propria.

A tal riguardo, si pensi alle emissioni dovute al malfunzionamento di automezzi ovvero a quelle prodotte a seguito di cause accidentali.

Tali situazioni devono essere tenute sotto controllo continuo, allorquando si verificano, ed è necessario porre in essere ogni azione per minimizzare l’impatto ambientale.

**c. Contaminazione di acque**

Si tratta di una tipologia di impatto ambientale che può essere causata dall’uso improprio di strumenti, mezzi e materiali impiegati nell’ambito delle attività logistiche.

A titolo d’esempio, nel caso di attività rivolte verso il personale, si possono menzionare i servizi di lavanderia e i bagni. In tal caso, al fine di prevenire la contaminazione dell’ambiente, sarà necessario:

- ricorrere a mezzi che permettano la totale canalizzazione dei citati servizi;
- incanalare o smaltire le acque reflue in apposite vasche di raccolta;
- prevedere, in alternativa, la raccolta delle acque reflue in appositi contenitori ovvero cisterne, per il successivo smaltimento autorizzato nella rete fognaria;
- evitare lo spargimento delle acque sul terreno per non inquinare le falde acquifere;
- fare ricorso, qualora possibile, ad unità o ditte specializzate nel settore.

Inoltre, nello svolgimento dell’attività di mantenimento, si può presentare analoga situazione, allorquando vengano effettuati il lavaggio e la rimozione del fango dai mezzi (ruotati e cingolati). Valgono, in tal caso, le precauzioni citate nel precedente paragrafo 3 “La protezione dell’ambiente in addestramento ed in esercitazione”.

**d. Rilascio di sostanze e rifiuti (tossici e non)**

Le attività logistiche in generale comportano la produzione di sostanze e rifiuti (tossici e non). Ciò può dar luogo, qualora tali elementi fossero rilasciati nell’ambiente, ad una situazione di impatto ambientale, che risulta essere in assoluto la più comune è che, sebbene di modesta entità, produce un effetto sicuramente duraturo nel tempo.

Tale possibile situazione può essere evitata attraverso la sensibilizzazione di tutto il personale al rispetto delle norme, da ricercarsi mediante la creazione di una coscienza ambientale che entri a far parte dell’addestramento di ogni singolo individuo al pari della coscienza che ogni militare ha sviluppato in merito ai problemi della sicurezza in addestramento e operazioni.

Alla normativa in vigore<sup>16</sup> che prevede ogni possibile situazione legata alla produzione di

---

<sup>16</sup> Per un approfondimento in merito, consultare il sito del Ministero dell’Ambiente ([www.minambiente.it](http://www.minambiente.it)) nella sezione “NORMATIVA”.

rifiuti, nonché al loro smaltimento, si affiancano le varie direttive in materia. Nella citata Appendice "4" sono riportate le norme per la realizzazione di un deposito di rifiuti in campagna, nonché le attività da svolgere in caso di pericolo concreto d'inquinamento.

**e. Spargimento di carburanti e lubrificanti**

La situazione d'impatto ambientale in esame può verificarsi nelle seguenti condizioni:

- durante le normali operazioni connesse con l'attività di rifornimento;
- accidentalmente, per ragioni non legate direttamente ai rifornimenti.

Nel primo caso, normalmente lo spargimento di carburante non è di notevole entità e lo si può prevenire utilizzando appositi contenitori in grado di raccogliere piccole fuoriuscite di liquidi. A tal fine possono essere utilizzati dei contenitori da posizionare al di sotto dei bocchettoni di alimentazione. Nonostante le precauzioni adottate, può comunque accadere che il liquido si riversi sul terreno. In tal caso si dovrà:

- interrompere il rifornimento;
- contenere il versamento di liquido;
- asportare la parte di terreno che ha assorbito il carburante, ovvero utilizzare della sabbia per assorbirlo;
- riportare il terreno alle condizioni ambientali iniziali e, ove necessario (ad esempio nel caso del manto stradale), ripulire accuratamente il luogo che è stato oggetto di impatto ambientale.

Nel secondo caso, l'impatto ambientale prodotto potrebbe essere di maggiore entità e richiedere provvedimenti differenti.

Qualora si verificasse una tale evenienza si dovrà:

- contenere, arginare o, se possibile, sospendere la fuoriuscita del liquido inquinante mediante gli appositi materiali in dotazione agli autorifornitori;
- creare una prima cornice di sicurezza della zona, segnalando l'area interessata all'accaduto;
- dare immediata comunicazione dell'evento al Comando d'appartenenza e, contestualmente, agli organi preposti al primo intervento e alla messa in sicurezza della zona<sup>17</sup>;
- tenere sotto controllo la zona interessata all'evento al fine di scongiurare ogni possibile fonte di rischio;
- procedere, qualora possibile, ad una prima azione sommaria di bonifica che impedisca o moderi l'assorbimento del carburante da parte del suolo.

**6. Aspetti connessi con la protezione dall'ambiente**

**a. Protezione da eventi naturali**

Nella condotta delle operazioni militari, ed in particolare nella valutazione di idoneità dei siti per la costituzione di basi militari, il Comandante ed il suo *staff* devono tenere in debita considerazione la minaccia costituita dall'ambiente naturale e dalle alterazioni prodotte al suo interno dall'uomo. Un adeguato Studio dell'Area di Interesse deve quindi analizzare l'ambiente circostante in relazione al verificarsi di fenomeni meteorologici violenti, alla predisposizione locale per i fenomeni alluvionali, franosi, alle valanghe, agli incendi

---

<sup>17</sup> Vigili del Fuoco, Polizia Stradale, Carabinieri, Organi locali per la protezione ambientale.

boschivi, alle eruzioni vulcaniche, ai terremoti, ai maremoti, all'inquinamento ambientale inteso quale rilascio nell'ambiente di sostanze tossiche, di natura chimica, biologica o radioattiva. L'intervento incontrollato dell'uomo sull'ambiente spesso modifica gli equilibri idrogeologici locali amplificando la potenza distruttiva dei fenomeni calamitosi naturali. A loro volta, i fenomeni calamitosi possono causare incidenti industriali, ovvero accentuarne il negativo impatto ambientale.

(1) Fenomeni metereologici

I fenomeni naturali più frequenti che possono scatenarsi sul territorio sono quelli meteorologici. In molti casi si riducono a semplici rovesci, all'aumento repentino della velocità del vento e per condizioni particolari della temperatura, a grandinate, anche di una certa entità. Quando più cause entrano in gioco, le conseguenze risultano catastrofiche. Si ha così la formazione di uragani, cicloni, tornado, trombe d'aria e nubifragi. Durante il decorso di un temporale o di fenomeni meteorologici di maggiore intensità il paesaggio si trasforma (le strade diventano impercorribili con le autovetture e con i mezzi di trasporto di ogni giorno), i punti di riferimento diventano deboli e difficili da individuare (riduzione della visibilità).

(2) Alluvioni

Come per altri fenomeni terrestri, le alluvioni si realizzano solo in seguito alla combinazione tra un evento prettamente naturale (precipitazioni copiose) ed uno status presente e costante sul territorio (argini poco profondi o presenza di detriti). In pratica la combinazione di queste due forze porta, in un caso, allo straripamento di notevoli masse d'acqua a seguito di un violento innalzamento dei livelli di scorrimento e nell'altro allo stesso risultato, ma a seguito di ostruzioni dovute a detriti od ostacoli più prettamente artificiali (rifiuti solidi urbani). Pertanto l'individuazione di irregolarità nello scorrere dei fiumi e dei torrenti è di fondamentale importanza; soltanto con un'efficace indagine preventiva si può realizzare un altrettanto efficace intervento protettivo. Le inondazioni sono fenomeni che si sviluppano con estrema rapidità: sono infatti le conseguenze di eventi meteorologici che si abbattono su una porzione di territorio, modificando le condizioni superficiali del terreno.

(3) Fenomeni franosi

I fenomeni franosi hanno inizio quando la forza di gravità che grava su una porzione di terreno vince la forza interna di coesione del materiale costituente la porzione medesima. Le cause quindi che possono portare al distacco di una certa quantità di terreno sono da ricercarsi tra quelle che riducono la coesione o che, interponendosi tra due strati di terreno di diverso aspetto, riducono le forze di attrito presenti sulla superficie di contatto.

Molto importante è l'indagine puntuale sullo stato idrogeologico del sito prescelto al fine di individuare le possibili superfici che potrebbero distaccare e le eventuali costruzioni e manufatti realizzati su tali siti. Le tipologie dei movimenti franosi sono molteplici: la più frequente è caratterizzata dallo scivolamento di due masse per mancanza o riduzione delle forze di attrito interno. Le cause scatenanti possono essere esterne (reazione all'aumento del peso su una porzione di terreno) oppure interne (imbibizione della porzione dello spazio compresa fra i due strati, a seguito di

precipitazioni o di eventi esterni, naturali od artificiali).

(4) Valanghe

Le valanghe sono fenomeni particolarmente diffusi in ambienti montagnosi che si instaurano generalmente nei periodi successivi a grosse precipitazioni nevose. Lo strato di neve depositandosi su uno strato omogeneo e compattato non instaura quelle forze di attrito necessarie al suo sostentamento. L'elemento scatenante della valanga è quasi sempre di portata limitata, infatti il rapporto di equilibrio tra gli strati di neve di diversa età è estremamente ridotto ed un piccolo spostamento delle forze componenti (aumento della temperatura) può scatenare una reazione a catena e coinvolgere interi versanti. La presenza di un solo sciatore su un pendio a rischio, l'onda sonora provocata da un'altra valanga o da un rumore artificiale, possono essere forze sufficienti a mettere in moto un fenomeno irreversibile e devastante. La valanga è un concentrato di neve, alberi, terreno e ghiaccio: la sua forza distruttiva e la sua velocità di propagazione sono estremamente elevate.

(5) Incendi boschivi

Gli incendi boschivi sono fenomeni che si ripetono con notevole frequenza durante tutto l'arco delle stagioni cosiddette secche. Le condizioni climatiche favoriscono l'aumento della velocità di propagazione delle fiamme, pertanto l'immediata segnalazione di un focolaio riveste un'importanza fondamentale.

(6) Eruzioni vulcaniche

Le eruzioni vulcaniche sono fenomeni naturali caratterizzati da un'emissione enorme di energia sotto forma di calore, di lancio di materiale combusto ed in combustione e dall'uscita di lava a temperature elevatissime. Le frequenze sono abbastanza basse, come anche le conseguenze immediate, mentre le conseguenze nel medio termine (in funzione della velocità della lava e della distanza dei centri abitati e degli insediamenti in generale) sono elevatissime. Lo studio del territorio e delle possibili situazioni incidentali è il primo importante passo per l'identificazione delle aree a maggior rischio di coinvolgimento. I piani di urbanizzazione, fino a pochi anni fa troppo permissivi o addirittura inesistenti, hanno dato un contributo non indifferente alla soluzione dei problemi che derivano dall'emissione di sostanze incandescenti dai vulcani. Gli abitanti di settori prossimi alle bocche dei vulcani oppure che dimorano su possibili canali di discesa della lava devono essere pronte in ogni istante, a lasciare le abitazioni ed a mettersi in salvo. La lava, in molti casi, sopraggiunge solo dopo l'emissione di lapilli e di sostanze incandescenti che permettono, a volte, alla popolazione colpita, di radunare poche cose e di raggiungere luoghi più sicuri.

(7) Terremoti

I terremoti sono fenomeni naturali caratterizzati da una liberazione di energia sotto due forme distinte: una a livello potenziale (onde d'urto causate dal movimento della crosta terrestre o degli strati profondi) ed una a livello cinetico (rottura di strati superficiali di crosta terrestre con magnitudo decrescente al crescere della distanza dall'epicentro). Le frequenze del fenomeno sono molto elevate; le conseguenze variabili da caso a caso. La distribuzione sul pianeta degli eventi sismici è piuttosto regolare: si può infatti parlare di aree a rischio minimo, aree a rischio medio ed aree a rischio elevato. Risulta quindi

molto importante lo studio del territorio, il monitoraggio delle zone più a rischio (faglie, rotture superficiali, superfici di scivolamento).

(8) Maremoti

I maremoti sono fenomeni naturali molto simili ai terremoti per quanto riguarda la formazione dell'evento. La trasformazione dell'energia potenziale in energia cinetica si manifesta con il coinvolgimento e la movimentazione di enormi masse d'acqua. Le conseguenze possono essere disastrose se non viene effettuato un attento controllo dei fondali marini, sempre tenendo conto delle condizioni terrestri prossime alla superficie marina.

(9) Rilascio di sostanze inquinanti

L'inquinamento è una forza dotata di un potere distruttivo lento ma, talvolta, inesorabile, strettamente collegata alle attività produttive dell'uomo. Le sue manifestazioni più classiche, come ad esempio la riduzione della fascia di ozono, l'aumento del gradiente di temperatura terra-aria, l'aumento della percentuale di CO nell'atmosfera, sono divenute ormai parte integrante dell'ambiente. Altre, quali i rilasci di sostanze tossiche, risultanti da una scarsa manutenzione degli impianti di produzione, dalla non osservanza di precise norme di sicurezza nella costruzione, nell'impiego degli stessi e nelle connesse attività di trasporto, possono avere effetti più gravi, ovvero catastrofici come nel caso degli incidenti con dispersione di considerevoli quantità di sostanze radioattive. Le sostanze "pericolose" possono essere di origine naturale o di origine antropica. Quelle d'origine naturale sono essenzialmente legate alla natura del terreno e alla concentrazione di minerali e di metalli pesanti in esso presenti. Le sostanze d'origine antropica, invece, sono frequentemente associate ai "rifiuti". I rifiuti, a loro volta, sono classificati secondo l'origine, in rifiuti urbani o rifiuti speciali, e secondo le caratteristiche di pericolosità, in rifiuti pericolosi o non pericolosi. Alcune tipologie di rifiuti sono classificate come pericolose o non pericolose in base all'origine, mentre per altre la pericolosità dipende dalla concentrazione di sostanze pericolose e/o metalli pesanti presenti nel rifiuto.

(10) Valutazione dello stato di inquinamento

La valutazione dello stato d'inquinamento naturale del terreno è possibile solo a seguito d'indagini di tipo geologico e/o di analisi strumentali di laboratorio.

È più semplice, invece, valutare la presenza di fonti inquinanti se le cause sono di tipo antropico, infatti, la presenza d'impianti industriali, ospedali, discariche, miniere, poligoni ecc., sono un chiaro indice di possibili fonti di inquinamento, ancor più pericolosi se i siti appena descritti sono in un evidente stato di abbandono e fatiscenza. All'interno di queste aree possono essere rinvenute sostanze chimiche altamente tossiche, come ad esempio pesticidi, amianto (molto diffuso nei vecchi siti industriali e nelle discariche, soprattutto sotto forma di "eternit"), materiale radioattivo, miscele di gas infiammabili/esplosivi, acque superficiali e sotterranee inquinate (dovute agli scarichi di impianti industriali o per il dilavamento di terreni contaminati).

(11) Rumore

Il rumore può causare dei danni anche permanenti all'apparato uditivo se la frequenza e l'ampiezza dell'onda sonora che lo hanno generato superano determinati parametri.

Infatti, ambienti ad elevata rumorosità ed esposizioni prolungate nel tempo, comportano possibili disturbi neurovegetativi e psicosensoriali con effetti sulle performance dei militari.

(12) Sorgenti di radiazioni non ionizzanti

L'uso crescente delle nuove tecnologie ha implicato l'aumento esponenziale nella presenza sul territorio delle sorgenti di campo elettrico, magnetico ed elettromagnetico ed ha reso di estrema attualità la problematica delle conseguenze correlate all'esposizione dell'uomo a tali radiazioni. Impianti che possono emettere radiazioni elettromagnetiche di entità tale da costituire un pericolo per la salute sono:

- impianti per la produzione, il trasporto e la distribuzione di energia elettrica;
- ponti radio;
- impianti di trasmissione radiotelevisiva;
- talune apparecchiature industriali o di ricerca;
- radar;
- sistemi radio-disturbatori (*jammer*).

Tra le sorgenti emettitrici di radiazioni ottiche pericolose, sono da menzionare, invece, i LASER.

(13) Impianti/Infrastrutture

Sono da considerare potenzialmente pericolosi tutti gli impianti/apparati di uso industriale, medico o di ricerca. Tra gli esempi si possono citare:

- macchinari in genere, in particolare quelli di vecchia concezione, privi di dispositivi di protezione attualmente obbligatori per legge;
- impianti e recipienti in pressione, a rischio esplosione;
- impianti chimici.

Gli impianti chimici, in particolare, rappresentano la fonte di rischio più significativa nel comparto industriale. Tra gli impianti considerati a rischio di incidente rilevante, sono da menzionare:

- impianti per la produzione, la trasformazione o il trattamento di sostanze chimiche organiche o inorganiche in cui vengono utilizzati particolari processi chimici;
- impianti per la distillazione o raffinazione, ovvero altre successive trasformazioni del petrolio o dei prodotti petroliferi;
- impianti per la produzione, la trasformazione o il trattamento di gas energetici, per esempio gas di petrolio liquefatto, gas naturale liquefatto e gas naturale di sintesi.

Altri impianti potenzialmente a rischio di incidente sono gli impianti nucleari, gli impianti a combustibile per la produzione di energia elettrica, e tutti gli impianti per lo smaltimento e il recupero di rifiuti, in particolare di rifiuti pericolosi. Ai fini della sicurezza del personale è fondamentale il controllo ed in alcuni casi l'esclusione, di questi "punti caldi" o "zone sospette a rischio".

I centri di ricerca e i siti industriali possono essere identificati da strutture come capannoni, palazzine uffici, coperture a *shed* (modulari), silos, serbatoi in pressione e tramogge, macchine uso industriale, tubazioni, logiche d'impianto (parti idrauliche, elettriche, elettroniche connesse tra loro).

I siti di stoccaggio rifiuti, prevedono tre tipologie differenti:



- discarica per rifiuti inerti;
- discarica per rifiuti non pericolosi (tra i quali gli RSU, Rifiuti Solidi Urbani);
- discarica per rifiuti pericolosi (tra cui ceneri e scarti degli inceneritori).

Possono essere identificati da accumulo di rifiuti e/o da camini di esalazione e recupero di gas. Anche all'interno di queste aree è facile trovare sostanze pericolose in grado di provocare un incendio/esplosione ovvero creare un elevato sviluppo di calore.

(14) Misure preventive e cautelative

Qualora si operi in uno scenario in cui si configura un rischio TIM (*Toxic Industrial Materiel*), deve essere sviluppato e diffuso, fino ai minori livelli un piano di contingenza per fronteggiare i pericoli derivanti dal rilascio di sostanze tossiche di origine industriale TIH (*Toxical Industrial Hazard*), tenendo in considerazione, in particolare per il rischio chimico industriale, quanto previsto dallo STANAG 2521 ATP-3.8.1 Vol. I. A premessa dello schieramento di un'unità sul terreno è, pertanto, necessario valutare i suddetti elementi inquinanti, inizialmente, mediante opportune attività di ricognizione ed analisi degli elementi raccolti ad opera di specifico personale appartenente alla componente NBC e medica del contingente. Successivamente, con l'intervento di personale altamente specializzato e dotato di attrezzature adeguate in grado di effettuare accurati controlli (Ce.TLI NBC, CISAM).

(15) Protezione da eventi di natura sanitaria

La protezione da eventi di natura sanitaria è trattata esaustivamente nell'Annesso 3 al quale si rimanda per la consultazione.



## DECALOGO AMBIENTALE DEL MILITARE

- I. *L'ambiente non appartiene solo a te.*
- II. *La difesa della natura è compito d'ogni soldato.*
- III. *Salvaguarda l'ambiente, migliorerai la qualità della tua vita.*
- IV. *Un buon combattente non lascia "tracce" del suo passaggio.*
- V. *L'uomo, come le altre specie animali, è ospite del pianeta Terra.*
- VI. *Ricorda, in operazioni la natura ti protegge.*
- VII. *Rispetta l'ambiente, rispetterai te stesso. Le future generazioni erediteranno ciò che tu gli lascerai.*
- VIII. *L'ambiente non fa parte dei tuoi avversari.*
- IX. *Meno danni alla natura, meno danni alla tua salute.*
- X. *Sii ambasciatore della coscienza ambientale.*



**LISTA DI CONTROLLO PER L'OCCUPAZIONE DI UN'AREA  
ADDESTRATIVA**

<b>PRIMA DI OCCUPARE L'AREA ADDESTRATIVA</b>			
<b>ATTIVITÀ</b>	<b>SI</b>	<b>NO</b>	<b>NOTE</b>
Nominare un responsabile per l'applicazione della lista di controllo.			
Attenersi scrupolosamente al regolamento di utilizzazione del poligono.			
Consultare la scheda notizie che il Comando/Ente gestore del poligono ha elaborato.			
Effettuare una ricognizione preventiva volta ad accertare l'esistenza di siti inquinati o potenzialmente a rischio inquinamento.			
Effettuare, presso ciascun reparto, sotto il diretto controllo del Comandante e di concerto con l'Ufficio Logistico, il censimento delle varie tipologie di rifiuti e prevedere per ciascun tipo lo smaltimento mediante ditta specializzata.			
Controllare che gli impianti dotati di motori a combustione interna ed i veicoli a motore, siano stati sottoposti, nei limiti di tempo previsti dalle norme di manutenzione, ai controlli di efficienza.			
Predisporre una adeguata squadra antincendio.			
<b>DURANTE IL PERIODO DI PERMANENZA NELL'AREA ADDESTRATIVA</b>			
Ridurre al minimo i danni alla flora e alla fauna.			
Evitare di utilizzare la vegetazione per eseguire operazioni di mascheramento od occultamento di mezzi e/o sistemi d'arma.			
Seguire quanto riportato in Appendice "5" per la realizzazione di depositi di carburanti e lubrificanti.			
Seguire quanto riportato in Appendice "6" per la raccolta ed il trattamento degli oli e dei grassi vegetali ed animali esausti.			
Non scavare buche di circostanza al fine di smaltire in proprio i rifiuti, anche se non pericolosi.			
Non immettere rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali o sotterranee.			
Non immettere nel normale circuito di raccolta dei rifiuti urbani imballaggi terziari di qualsiasi natura.			
Non immettere nel normale circuito di raccolta dei rifiuti urbani quelli derivanti da attività sanitarie.			
Servirsi di un centro di raccolta autorizzato, nel caso in cui si debba procedere allo smaltimento di rifiuti costituiti da parti di veicoli a motore.			
Servirsi unicamente di ditte autorizzate per lo smaltimento delle batterie.			
Servirsi di ditte specializzate per lo smaltimento dei rifiuti pericolosi e, in assenza di ditte specializzate, raccogliere i rifiuti pericolosi in contenitori idonei e trasportarli nei punti di raccolta stabiliti.			
Etichettare chiaramente in modo permanente i contenitori per garantire la corretta identificazione del relativo contenuto.			
Seguire quanto riportato in Allegato "G" per la realizzazione di depositi temporanei di rifiuti.			
Eliminare, non appena possibile, attraverso un sistema di smaltimento autorizzato, i rifiuti pericolosi adeguatamente etichettati ed impacchettati.			
Smaltire le acque reflue, in presenza di rete fognaria, operando di concerto con gli Enti locali che la gestiscono, per conoscere e valutare i livelli e i tipi di inquinanti che è possibile immettere negli scarichi.			
In assenza di rete fognaria o dell'autorizzazione al suo utilizzo, le acque reflue dovranno essere raccolte in apposite cisterne e smaltite a mezzo ditta specializzata.			
Limitare l'utilizzazione di caldaie, gruppi elettrogeni, inceneritori, veicoli a motore allo stretto indispensabile per ridurre al minimo le emissioni e mantenerle comunque entro i limiti fissati dalla legge.			
Utilizzare i mezzi (cingolati e ruotati) su piste, percorsi e aree preventivamente riconosciute.			
<b>PRIMA DI ABBANDONARE L'AREA DI ADDESTRATIVA</b>			
Ripristinare, documentandole possibilmente con materiale fotografico, le condizioni ambientali originarie nei settori maggiormente a rischio, e cioè: - deposito carburanti e lubrificanti; - deposito munizioni ed esplosivi; - aree di parcheggio, manutenzione e riparazione dei veicoli; - deposito temporaneo di rifiuti; - deposito di materiali pericolosi; - fognature a cielo aperto, latrine, ecc..			
Effettuare il rastrellamento della zona impiegata.			
Attuare una scrupolosa bonifica del poligono.			
Redigere il "Rapporto di Bonifica" del poligono.			
Redigere il "Verbale di inesistenza di focolai d'incendio".			
Lasciare la proprietà o il poligono nelle stesse, o addirittura migliori, condizioni ambientali rispetto a quelle esistenti al momento dell'occupazione.			



## SCHEMA PER LA STESURA DELL'ALLEGATO "TUTELA AMBIENTALE" ALL'ORDINE DI OPERAZIONE

### GENERALITÀ

Il presente allegato fornisce le direttive del Comandante ai Comandanti delle unità dipendenti in merito alla tutela ed alla protezione dell'ambiente.

L'allegato "Tutela Ambientale" costituisce base per la stesura di analoghi documenti ai livelli inferiori.

Il format di seguito fornisce una guida e costituisce una lista di controllo.

Il contenuto dettagliato dei sottoparagrafi sarà inserito in base alle necessità.

### CLASSIFICA DI SEGRETEZZA

Copia N. \_\_\_\_ di \_\_\_\_ copie.

Comando originatore.

Località di diramazione (eventualmente in codice).

Gruppo data-orario della firma.

Numero di protocollo \_\_\_\_\_

### ALLEGATO "TUTELA AMBIENTALE" ALL'ORDINE DI OPERAZIONE N. \_\_\_\_\_

#### Riferimenti:

- carte geografiche, topografiche (Vds. Parte I dell'Ordine di Operazione);
- legislazione e normativa internazionale (viginti codici di Diritto Bellico e di Diritto Umanitario Internazionale);
- legislazione e normativa locale.

#### Fuso Orario utilizzato nell'Ordine di Operazione:

Vds. Parte I dell'Ordine di Operazione.

**1. SITUAZIONE** Riportare in questo paragrafo tutte le informazioni sulle attività militari che possono influenzare l'ambiente, con riferimento alle singole unità.

**2. MISSIONE** Enunciare la missione delle unità relativamente alla protezione ambientale (priorità alle situazioni di impatto ambientale da evitare).

#### **3. ESECUZIONE**

##### **a. Caratteristiche ambientali**

- (1) Condizione ambientale generale dell'area di operazione.
- (2) Clima.
- (3) Qualità dell'acqua e dell'aria.
- (4) Risorse naturali, flora e fauna.
- (5) Presenza di specie in pericolo di estinzione ed habitat particolari.
- (6) Diversità biologiche.

##### **b. Quadro complessivo del rischio ambientale**

- (1) Inquinamento dell'acqua e dell'aria.
- (2) Contaminazione da agenti chimici, da scorie pericolose e rifiuti solidi, medici ed infetti.
- (3) Perdite di prodotti carbolubrificanti.
- (4) Altro.

##### **c. Misure preventive dell'inquinamento e conservazione delle risorse**

- (1) Riduzione delle fonti di inquinamento derivanti dall'uso di sostanze pericolose e delle relative scorie residue.
- (2) Trattamento - trasformazione delle scorie.
- (3) Trattamento - trasformazione dei residui pericolosi in sostanze non pericolose.

##### **d. Misure correttive**

- (1) Operazioni di pulizia.
- (2) Operazioni di riparazione.
- (3) Operazioni di bonifica.

##### **e. Tutela del paesaggio e del patrimonio artistico (naturale e prodotto dall'uomo)**

**4. ORGANIZZAZIONE LOGISTICA - SERVIZI** Distribuzione delle risorse essenziali.

### CLASSIFICA DI SEGRETEZZA





**SCHEMA NOTIZIE POLIGONO/AREA ADDESTRATIVA**

<b>Poligono/Area addestrativa di:</b> .....		
1. Tipo di poligono/area add.: (occasionale / semipermanente / permanente)		
2. Comune e Provincia:		
3. Regione Amministrativa:		
4. Regione Militare:		
5. Ente/Comando responsabile:		
6. Distanza dall'Ente/Comando responsabile: km		
7. Ente/Comando responsabile dell'organizzazione logistica:		
8. Capacità ricettiva della Base Logistica (eventuale):		
Ufficiali:	Sottufficiali:	Truppa:
9. Scalo marittimo:		distante km
10. Scalo Ferroviario:		" "
11. Scalo Aereo:		" "
12. Città più vicina:		" "
13. Stazione CC competente per territorio:		
14. Corpo Forestale dello Stato competente:		
15. Riferimenti Cartografici: .....		
16. Coordinate UTM dei principali osservatori:		
17. Area Totale: _____ ettari, dei quali:		
- demaniali (specificare il tipo di demanio <sup>1</sup> ): _____ ettari		
- privati (specificare se di Enti e/o cittadini): _____ ettari		
18. Livello massimo di esercitazione a fuoco consentito:		
19. Giornate Poligono/Anno (rese disponibili dal Comitato Misto Paritetico):		
20. Giornate Poligono/Anno (effettivamente utilizzate):		
21. Costo Medio (di una giornata di sgombero): .....		
22. Periodi Annuali, sottoposti a limitazioni d'impiego:		
da _____ a _____		
23. Sistemi d'arma / armi / munizionamento / esplosivi / artifici utilizzabili:		
- _____		
24. Limitazioni all'impiego di sistemi d'arma / armi / munizionamento / esplosivi / artifici:		
- _____ da _____ a _____		
25. Dati riferiti allo sgombero:		
a. Personale:		
- _____		n. _____
b. Mezzi:		
- _____		n. _____
c. Materiali:		
- _____		n. _____
26. Situazione Ambientale:		
a. Descrizione:		
.....		
b. Riferimenti Carte Tematiche:		
.....		
c. Esigenze di carattere ambientale:		
.....		
27. Varie		
a. Principali itinerari di afflusso:		
b. Itinerari di prevalente interesse logistico:		
c. Coordinate aree di possibile attendamento:		
d. Ulteriori dati di interesse:		

<sup>1</sup> Tipi di demanio:  
 - demanio dello Stato: E.I./M.M./A.M./Corpo Forestale dello Stato;  
 - altri demani: Regionali / Provinciali / Comunali.



**NORME PRATICHE PER LA REALIZZAZIONE DI UN  
DEPOSITO CARBURANTI E LUBRIFICANTI IN CAMPAGNA**

Il deposito carburanti e lubrificanti deve essere realizzato in un'area tale da non costituire pericolo per la flora e la fauna circostante.

Esso deve essere ubicato:

- lontano da sorgenti o corsi d'acqua;
- lontano da zone ad elevato rischio d'incendio (ad esempio zone con vegetazione secca);
- in posizione facilmente raggiungibile per i rifornimenti, in modo da ridurre i rischi legati al trasporto.

Per il deposito, inoltre, deve essere previsto un adeguato sistema antincendio che, oltre a rispettare la normativa vigente in materia, deve essere munito di materiali adatti alla situazione generale dei luoghi in cui si opera, con particolare riferimento:

- al tipo di terreno e vegetazione;
- alle temperature ed alle condizioni meteorologiche medie;
- ai venti e ad altri ulteriori fattori ambientali;
- alla viabilità.

Devono essere adottate tutte le precauzioni affinché non si verifichino perdite significative di sostanze nocive all'ambiente circostante prevedendo, ad esempio, l'uso di opportuni teli impermeabili; evitando che rigagnoli di carbolubrificanti possano confluire e disperdersi in corrispondenza di corsi o di sorgenti d'acqua provvedendo, eventualmente, alla realizzazione di argini di contenimento.

Qualora durante l'utilizzo o lo stoccaggio si verifichino delle perdite, di entità tale da costituire un rischio ambientale per il terreno o per le falde acquifere, è opportuno seguire le seguenti indicazioni:

- arrestare con immediatezza la perdita;
- arginare lo spargimento di materiale inquinante;
- informare la catena di comando, dando una descrizione dell'incidente ed indicare l'azione intrapresa, e successivamente:
  - fare in modo che il materiale versatosi non penetri nel suolo e non raggiunga le acque superficiali (buoni risultati si possono ottenere utilizzando sacchetti di sabbia o terra);
  - tenere sotto controllo la zona al fine di scongiurare incendi e/o pericoli all'incolumità rappresentati dai vapori o dal prodotto libero.
  - effettuare una prima sommaria azione di bonifica del suolo e delle acque;
  - se possibile, cominciare la rimozione del prodotto libero.

Tutti i rifiuti provenienti dalla gestione dei carbolubrificanti, compresi i materiali (solidi e liquidi) utilizzati per la pulizia dei serbatoi e dei fusti di stoccaggio devono essere trattati come rifiuti pericolosi.



## **NORME PER LA REALIZZAZIONE DI UN DEPOSITO TEMPORANEO DI RIFIUTI IN CAMPAGNA**

Un deposito temporaneo di rifiuti è realizzato, prima della raccolta vera e propria, nel luogo in cui i rifiuti sono prodotti. Trattandosi di sostanze che potrebbero produrre un impatto ambientale considerevole, nel predisporre il deposito è necessario tener conto dei seguenti aspetti:

- i rifiuti depositati non devono contenere sostanze pericolose in quantità superiore ai limiti previsti dal Decreto Legislativo n. 22 del 5/2/1997;
- il quantitativo di rifiuti pericolosi depositato non deve superare i 10 metri cubi, ovvero i rifiuti stessi devono essere raccolti con frequenza bimestrale;
- il quantitativo di rifiuti non pericolosi non deve superare i 20 metri cubi, ovvero i rifiuti stessi devono essere raccolti con frequenza trimestrale;
- il deposito temporaneo deve essere realizzato per tipologia omogenea e nel rispetto delle norme, nonché, per i rifiuti pericolosi, nel rispetto delle leggi che disciplinano il deposito delle sostanze pericolose in essi contenute;
- devono essere rispettate le norme che disciplinano l'imballaggio e l'etichettatura dei rifiuti pericolosi;
- deve essere data comunicazione alla Provincia amministrativa dell'eventuale realizzazione del deposito temporaneo di rifiuti pericolosi;
- in caso di pericolo concreto d'inquinamento, si deve procedere alla messa in sicurezza, alla bonifica ed al ripristino ambientale delle aree inquinate. A tal fine:
  - . deve essere data immediata notifica al Comando gerarchicamente superiore, al Comune, alla Provincia ed alla Regione territorialmente competenti, nonché agli organi di controllo sanitario e ambientale, della situazione di inquinamento ovvero del pericolo concreto di inquinamento del sito;
  - . entro le quarantotto ore successive la citata comunicazione, devono essere notificati al Comune, alla Provincia ed alla Regione territorialmente competenti, gli interventi di messa in sicurezza adottati per non aggravare la situazione di inquinamento o di pericolo di inquinamento, contenere gli effetti e ridurre il rischio sanitario ed ambientale;
  - . entro trenta giorni dall'evento che ha determinato l'inquinamento ovvero dalla individuazione della situazione di pericolo, deve essere presentato al Comune ed alla Regione il progetto di bonifica delle aree inquinate.



**NORME PER LA RACCOLTA E TRATTAMENTO DEGLI OLI E DEI  
GRASSI VEGETALI ED ANIMALI ESAUSTI IN CAMPAGNA**

La raccolta ed il trattamento degli oli e dei grassi vegetali e animali esausti in campagna avviene, obbligatoriamente, attraverso lo stoccaggio del materiale in appositi contenitori a tenuta posti sotto tettoia.

Parimenti, anche lo stoccaggio dei filtri dell'olio usati deve essere effettuato in appositi contenitori a tenuta anch'essi posti sotto tettoia.

Peraltro, oltre a tali procedure previste dalla vigente normativa in materia, è in ogni modo buona norma attenersi alle seguenti indicazioni:

- stoccare il materiale in zone ove non sussiste il pericolo d'incendio;
- assicurarsi che i previsti contenitori dei predetti materiali siano:
  - . in buone condizioni, privi di ruggine, sporgenze o altri difetti strutturali;
  - . costruiti con materiali compatibili con quelli custoditi e tali da permettere il carico e lo scarico dei materiali stessi in condizioni di massima sicurezza;
  - . tenuti sempre chiusi, tranne quando si debba aggiungere o rimuovere del materiale;
  - . maneggiati in modo da evitare rotture dei contenitori ed evitare perdite del contenuto;
  - . controllati periodicamente, per accertare che non vi siano perdite o rotture;
- controllare periodicamente l'area dove sono stoccati i contenitori, per evitare l'insorgere di eventuali situazioni di impatto ambientale;
- non riutilizzare tali contenitori per altre esigenze, in particolare, per custodire generi alimentari o materiali di equipaggiamento individuale del personale.





**SEZIONE II – MARINA****1. Generalità**

L'ambiente marino rappresenta una risorsa naturale ed economica imprescindibile per il benessere dell'essere umano.

In particolar modo, il trasporto via mare è un settore fondamentale e pulsante dello sviluppo economico mondiale che, negli ultimi 20 anni, ha visto l'incremento esponenziale delle quantità e dei volumi di beni primari, di prodotti lavorati e di risorse energetiche, soprattutto sulle rotte europee e mediterranee. Ciò comporta inevitabilmente la crescita dei fattori di rischio per il mare e, più in generale, per l'ambiente. Conseguentemente la comunità internazionale ha maturato una maggiore sensibilità nei confronti del bene ambientale marino ed ha altresì garantito la realizzazione di un variegato quadro normativo in grado di prevenire, preservare e valorizzare l'impiego dello spazio marittimo.

Alla luce di quanto detto, di seguito sarà analizzato il principale quadro normativo di riferimento internazionale, comunitario e nazionale diretto alla tutela dell'ambiente marino in senso generale.

A causa delle specificità del “mezzo navale militare”, dei diversi ambienti operativi di riferimento e delle tipologie di missione da realizzare, il citato quadro normativo sarà adottato, tenendo conto dei limiti di applicabilità espressamente riportati nella citata normativa.

**2. Quadro giuridico: “Normativa antinquinamento”**

Il *corpus* normativo di tutela ambientale, concernente i vari settori dell'economia del mare, è oggi assai vasto e complesso.

Il primo pilone della normativa internazionale è stata la convenzione di Londra del 1954 (Oilpol), successivamente è stato stipulato il trattato di Mosca del 1963 (divieto di esperimento di armi nucleari subacquee) e le due convenzioni di Bruxelles di cui la prima nel 1969, riguardante l'intervento in alto mare in caso di incidente e di contenimento dei rischi da inquinamento da idrocarburi, la seconda sulla responsabilità civile per danni da oli minerali (CLC69). Fasi importanti sono state segnate anche dalle convenzioni di Londra del 1972 (LC72), sulla prevenzione dell'inquinamento marino derivante dallo scarico di rifiuti e di altre sostanze, e dalla convenzione Marpol 73/78.

Inoltre, per quanto riguarda la tutela di specifiche regioni, è da citare l'accordo di Bonn del 1969 (inquinamento di idrocarburi nel Mar del Nord), l'accordo di Belgrado del 1974 sulla collaborazione per la salvaguardia degli inquinamenti costieri tra ex Jugoslavia ed Italia e la convenzione di Barcellona del 1976 sulla protezione del Mediterraneo.

Successivamente, importanti novità di approccio al problema vennero alla luce per mezzo della convenzione di Montego Bay del 1982, in cui si definisce inquinamento marino “*qualunque introduzione diretta od indiretta, da parte dell'uomo, di sostanze o di energia nell'ambiente marino, ivi compresi gli estuari, quando questa ha o può avere effetti nocivi quali: danni alle risorse biologiche, alla fauna ed alla flora marine, rischi per la salute umana, intralci alle attività marittime comprese la pesca e gli altri usi legittimi del mare, alterazione della qualità di mare dal punto di vista della sua utilizzazione e del degrado dei valori di gradevolezza*”.

Per quanto concerne le attività del trasporto marittimo, la Convenzione Marpol 73\78 è il punto

di riferimento per le misure atte a prevenire e ridurre non solo l'inquinamento accidentale da sostanze pericolose/idrocarburi, ma anche quello operativo. La convenzione è stata inizialmente concepita per dare risposta all'inquinamento accidentale; successivamente il protocollo del 78 ha esteso il requisito costruttivo delle cisterne di zavorra segregate (importante ai fini del contenimento degli sversamenti, che inizialmente era stato imposto solo alle petroliere con portata lorda superiore a 70.000 t) alle petroliere adibite al trasporto di greggio maggiori di 20.000 t ed a quelle adibite al trasporto di prodotti petroliferi maggiori di 30.000 t. Inoltre, ha introdotto il requisito della protezione delle cisterne del carico con spazi perimetrali vuoti o adibiti a zavorra ("*protective location*") in maniera tale da ridurre i rischi in caso di incaglio o collisione: primo passo verso l'obbligo dell'adozione del doppio scafo.

Finalmente nel 1992 è stato introdotto l'obbligo del doppio scafo per tutte le unità con portata lorda superiore a 5.000 t.

In seguito, a causa di altri nefasti eventi quali l'affondamento della M/T Erika e della M/T Prestige, l'"*International Maritime Organization*" (IMO) è intervenuta accentuando il processo di "*phase out*" delle navi petroliere monoscafo, tramite il pacchetto normativo ERIKA I (relativo a: standards minimi da parte dello Stato di bandiera e delle organizzazioni per l'espletamento dell'ispezione della nave, adempimenti del *Port State Control* (PSC) con specifici requisiti per le *tanker*, ecc.). Il pacchetto ERIKA II ha comportato una serie di misure ancora più restrittive, corroborando il processo di "*phase out*" delle cisterne monoscafo ed emanando una direttiva per un sistema di monitoraggio, controllo ed informazione europeo sul traffico marittimo e la direttiva 2002/84/CE, modificativa delle previsioni di implementazione della sicurezza marittima e degli inquinamenti provenienti da navi.

Inoltre l'annesso I Marpol, al fine di prevenire eventuali inquinamenti causati dallo sversamento di idrocarburi in mare, ha introdotto ulteriori criteri costruttivi ed operativi divisi nei sotto elencati annessi:

- **Annesso I:** Regole per la prevenzione dell'inquinamento da idrocarburi (emendamenti, cogenti dal 2007, riferiti alla regola 20 e 21 circa l'implementazione completa delle cisterna doppio scafo e le caratteristiche costruttive delle nuove costruzioni);
- **Annesso II:** Regole per la prevenzione dell'inquinamento da sostanze liquide nocive alla rinfusa (emendamenti cogenti dal 2007, con il nuovo sistema di caratterizzazione delle sostanze nocive X,Y,Z ed altre sostanze);
- **Annesso III:** Regole per la prevenzione dell'inquinamento da sostanze nocive in colli;
- **Annesso IV:** Regole per la prevenzione dell'inquinamento dalle acque grigie e reflue;
- **Annesso V:** Regole per la prevenzione dell'inquinamento da rifiuti prodotti da nave;
- **Annesso VI:** Regole per la prevenzione dell'inquinamento dell'aria da emissioni prodotte da nave (cogente dal 01 maggio 2005).

Tale convenzione non si applica alle navi da guerra, o ausiliarie e alle navi possedute o gestite dallo Stato, solo se impiegate per servizi governativi e non commerciali.

Nel settore del trasporto marittimo, la Comunità Europea continua a porre un forte accento sugli sversamenti accidentali di idrocarburi e sui temi della sicurezza. In particolare, per quanto concerne gli inquinamenti marini, grande rilievo è stato dato dalla direttiva 2000/59/CE che impone agli stati membri di dotarsi di impianti di *Port Reception facilities* idonei allo scarico dei rifiuti suddivisi per categoria e tipologia, senza causare ritardo alcuno alla nave. Occorre, inoltre,

evidenziare che questa normativa ha ricompreso nella nozione di rifiuto anche i residui associati al carico ovvero le risultanze ottenute dal lavaggio di cisterne del carico (decreto legislativo 182/03). In base a tale direttiva i porti italiani e comunitari hanno dovuto e devono istituire (laddove non presenti) sistemi di recupero che incentivino la consegna a terra dei rifiuti e disincentivino la discarica in mare.

Altre importanti iniziative strettamente connesse con il pacchetto ERIKA II sono:

- il divieto di ingresso ai porti comunitari ed alle stazioni *off shore* di navi monoscafo di qualunque bandiera di portata pari o superiore a 5000 *gross tonnage*;
- rafforzamento del potere ispettivo dello stato di approdo, introducendo misure rinforzate nei confronti delle navi manifestamente sotto gli *standard* previsti;
- rafforzamento del controllo dello stato di bandiera sui registri nazionali e sulle società di classifica (RINA);
- miglioramento delle attività di monitoraggio del trasporto marittimo di merci pericolose e della definizione di porti rifugio;
- istituzione dell'Agencia Europea per la Sicurezza Marittima;
- istituzione del COPE, fondo europeo di compensazione per danno ambientale (fino a 200 milioni di euro).

Ancora, è fondamentale rammentare la direttiva 2004/35/CE in materia di inquinamento provocato da navi, ad opera della quale è stato istituito un quadro per la responsabilità ambientale, basato sul principio "chi inquina paga" (al riguardo, cfr. anche il Decreto Legislativo 6 novembre 2007, n. 202 "Attuazione della direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni" pubblicato nella *Gazzetta Ufficiale* n. 261 del 9 novembre 2007 - Supplemento ordinario n. 228).

Infine, in ambito nazionale, è necessario fare riferimento alla disciplina generale prevista dal D.Lgs. 152/2006 T.U. Ambientale, successivamente integrato e modificato dal D.lgs 4/2008 del 16 gennaio ed alla legge 979/82 "Disposizioni per la difesa del mare".

La Legge sulla difesa del mare, prevede un sistema *ad hoc* posto a tutela dell'ambiente marino; in particolar modo gli articoli da 15 a 23, impongono divieti ed obblighi per evitare l'immissione di idrocarburi e di altre sostanze inquinanti in mare, riconnettendo alle diverse fattispecie sanzioni amministrative e penali.

È fatto divieto assoluto a tutte le imbarcazioni, senza discriminazione di nazionalità, di sversare nelle acque territoriali e in quelle marittime interne, idrocarburi o miscele di idrocarburi, nonché altre sostanze nocive. Maggior rigore è poi contemplato per le navi battenti bandiera italiana, per cui i Comandanti, proprietari ed armatori sono imputabili penalmente, anche se l'inosservanza del divieto in esame sia avvenuta al di fuori delle acque territoriali.

### **3. La Marina Militare a difesa dell'ambiente marino – L'attività delle Capitanerie di Porto**

Ferme restando le competenze specifiche attribuite all'Autorità Marittima dalla legge 31.12.1982, n. 979 e dal Codice della Navigazione, la legge 24.12.1993, n. 537 ed il successivo decreto interministeriale 28.04.1994, nel trasferire al Ministero dell'Ambiente e della Tutela del Territorio le funzioni del soppresso Ministero della Marina Mercantile in materia di tutela e difesa del mare, affidano al Corpo delle Capitanerie di Porto della Marina Militare Italiana l'espletamento di tutte le attività operative nel settore, ivi compresa la sorveglianza delle Aree Marine Protette.

Il Corpo delle Capitanerie di Porto esercita, tramite la propria Centrale Operativa, i Comandi Periferici ed i mezzi navali ed aerei, i servizi di istituto relativi all'azione contro l'inquinamento marino. Il legislatore ha disposto infatti che il Ministero della marina mercantile (ora Ministero delle Infrastrutture e dei Trasporti) si adoperi per il potenziamento dell'attività di vigilanza in mare, attraverso il Corpo delle Capitanerie di porto – Guardia Costiera, con il coinvolgimento dello Stato Maggiore della Marina per l'utilizzo delle unità navali M.M. specializzate nella bonifica degli inquinamenti marini.

La normativa in esame prevede l'elaborazione di una pianificazione operativa per gli interventi di antinquinamento, strutturata su due livelli: uno locale ed uno nazionale. In particolare, si dispone che, in presenza di un inquinamento di piccola rilevanza, siano competenti ad intervenire le Autorità marittime locali, le quali devono comunicare al Ministero dell'ambiente le azioni intraprese.

Nell'ipotesi di eventi di particolare gravità, il Capo del Compartimento marittimo, dichiara lo stato di “emergenza locale”, dandone immediata notizia al Ministero dell'ambiente, coinvolgendo le rappresentanze del governo a livello locale. L'attività di coordinamento e di direzione operativa degli interventi è assunta, allora, dalla locale Autorità Marittima. A tal fine ogni Capitaneria di Porto adotta un “Piano locale di pronto intervento antinquinamento” e può disporre di mezzi e dotazioni antinquinamento in convenzione con il Ministero dell'Ambiente.

Qualora, poi, l'emergenza non sia fronteggiabile con le risorse disponibili, il Ministro dell'ambiente deciderà in merito alla dichiarazione di stato di “emergenza nazionale” interessando il Dipartimento per la Protezione Civile presso la Presidenza del Consiglio dei Ministri. Le procedure da seguire dopo tale dichiarazione sono regolamentate nel “Piano di pronto intervento nazionale per la difesa da inquinamento di idrocarburi o di altre sostanze nocive causate da incidenti marini”, approvato nel 2010.

In ogni caso il Capo del Compartimento Marittimo interessato mantiene la direzione ed il coordinamento operativo, a livello locale, di tutte le operazioni in mare.

#### **4. La Marina Militare a difesa dell'ambiente marino – La gestione dei rifiuti sulle navi militari**

La scelta della Marina Militare di rispettare le norme della MARPOL 73/78 è un impegno da intendere su base assolutamente volontaria. Infatti, sebbene le leggi internazionali e nazionali non vincolino le Unità militari al rispetto della norma in questione, la Marina Militare, consapevole che le tematiche correlate alla salvaguardia dell'ambiente, compreso quello marino, stanno assumendo sempre maggiore importanza e valenza, ha preso l'impegno di adeguarsi a tale normativa.

A tal proposito si cita testualmente l'articolo 3 della Legge di ratifica della MARPOL (n° 662 del 29/09/1980):

*“La presente Convenzione non si applica né alle navi da guerra o alle navi da guerra ausiliarie né alle altre navi appartenenti ad uno Stato o gestite da tale Stato fintantoché quest'ultimo le utilizzi esclusivamente per servizi governativi o non commerciali. Tuttavia, ciascuna Parte deve accertarsi, nell'adottare delle misure adeguate che non compromettano le operazioni o la capacità operativa delle navi di questo tipo che le appartengono o che siano da essa gestite, che*

*queste agiscano in modo che sia compatibile con la presente Convenzione, per quanto ciò sia ragionevole e praticabile”.*

Tale regime è confermato sia dall'articolo 236 della Convenzione delle N.U. sul Diritto del mare del 1982 (ratificata con L. 02/12/19, n. 689) sia dall'art. 18 della L. 31/12/1982, n. 979 sulla Difesa del Mare.

Per quanto detto, il Naviglio Militare, deve astenersi, “in tutti i casi ove ciò sia possibile e ragionevolmente attuabile” dal provocare inquinamento di qualsiasi genere dell'ambiente. In particolare, ogni Unità della Marina Militare deve differenziare i rifiuti sistemandoli secondo le procedure antinquinamento che saranno oggetto d'analisi nei paragrafi successivi.

Preme, comunque, sottolineare che all'interno delle acque territoriali (ed a maggior ragione quelle portuali) di qualsiasi nazione, l'evento inquinamento prevede sanzioni amministrative e, ove ricorra il caso, anche penali da parte dell'Autorità giudiziaria inquirente, previa contestazione di negligenza, imperizia e mancanza di adozione di misure preventive. Per tale motivo, sebbene le direttive contenute nel presente documento siano più che altro orientate al rispetto della MARPOL ed all'ottenimento della relativa certificazione (per alcune Classi d'UU.NN.), tutte le Unità della Marina Militare dovranno seguire le procedure di seguito descritte per la gestione dei rifiuti.

Qualora le Unità si trovino all'interno delle acque territoriali di una Nazione, essendo in tali condizioni soggette a norme locali assolutamente vincolanti e in genere più restrittive della MARPOL, dovranno essere adottate le misure atte al rispetto di tali norme.

#### **a. Certificazione MARPOL**

La Marina Militare, per alcune Classi d'Unità Navali, richiede e mantiene nel tempo una notazione di classe in tema di tutela ambientale (mediante certificazione da parte di un ente riconosciuto) che attesti il rispetto delle norme della MARPOL 73/78 nella gestione dei rifiuti di bordo (certificazione MARPOL). Sulla base di tale processo di certificazione, le Unità Navali vengono suddivise in navi “dotate di certificazione” e navi “prive di certificazione”. A prescindere dall'appartenenza al primo o al secondo gruppo, i Comandi di bordo dovranno comunque adoperarsi per rispettare le direttive del presente documento. Ovviamente, per le Unità prive di sistemi di trattamento dei rifiuti (che presumibilmente apparterranno al gruppo delle “non certificate”) non potranno applicarsi alcune delle procedure di trattamento descritte nel documento.

#### **b. La tipologia dei rifiuti**

I rifiuti prodotti dalle Unità M.M.I. possono essere suddivisi in tre classi:

- Residui oleosi
- Liquami
- Rifiuti solidi

##### **(1) Residui oleosi**

Con il termine residui oleosi s'intendono i residui oleosi (morchie) propriamente detti e le acque oleose di sentina.

Per **residui oleosi** o **morchie** s'intendono:

- le morchie provenienti dal processo di depurazione del combustibile/olio lubrificante,

e dal filtraggio/separazione delle acque oleose di sentina;

- le acque di lavaggio derivanti dalla pulizia delle casse adibite al trasporto d'olio lubrificante, combustibile e residui oleosi;
- gli oli esausti comprendenti oli lubrificanti, oli idraulici, e qualunque altro liquido a base d'idrocarburi non più riutilizzabile a causa del suo deterioramento e/o contaminazione.

Per **acque oleose di sentina** s'intendono:

- l'acqua di sentina accumulata nei locali macchine;
- i drenaggi e le perdite provenienti da motrici principali o da macchinari ausiliari situati in locale macchina;
- tutte le emulsioni d'olio in acqua, anche in piccole concentrazioni.

(a) Trattamento e scarico

In qualsiasi area marina, speciale e non, (Aree speciali: Mar Baltico, Mar Nero, Mar Rosso, Zona dei Golfi, Golfo d'Aden, Antartide, Mari Europei Nord Occidentali, Mar Mediterraneo), è vietata la discarica in mare d'olio minerale o di miscele oleose da parte delle Unità Navali della Marina Militare ad eccezione dei seguenti casi:

- la concentrazione d'idrocarburi contenuti nell'effluente abbia una concentrazione inferiore alle 15 ppm;
- la nave stia navigando "in rotta"<sup>1</sup>;
- la nave abbia in funzionamento un sistema di filtraggio e monitoraggio della miscela scaricata, con relativo allarme, che fermi automaticamente lo scarico se questa supera le 15 ppm. (Tale sistema deve essere approvato e certificato secondo quanto previsto dalla Reg. 16(5) Annesso I e quindi conforme alle Res. IMO-MEPC 60(33), 107(49) ed A 393(X)).

Le prescrizioni indicate ai punti precedenti si possono non applicare nei seguenti casi particolari (regola 1 dell'annesso I):

- quando la discarica dei residui oleosi dalla nave è indispensabile per garantire la sicurezza della nave e del suo equipaggio e per la sicurezza della vita umana in mare;
- quando la discarica dei residui oleosi è causata da un'avaria alla nave o al suo equipaggiamento e se tutte le ragionevoli precauzioni sono state prese prima e dopo il guasto con lo scopo di prevenire e minimizzare la discarica in mare.

Le navi dotate di "Certificazione MARPOL" saranno sottoposte a visita iniziale e, a buon esito, sarà rilasciato un Certificato Internazionale di Prevenzione dall'Inquinamento da Idrocarburi e Oli minerali (*International Oil Pollution Prevention Certificate* – IOPP Certificate), valido 5 anni (con visite obbligatorie di convalida annuali ed intermedie del certificato).

Annualmente dovrà essere prelevato un campione d'effluente da ciascun impianto di separazione delle acque oleose di sentina presente a bordo ed inviato ad analisi. Il

---

<sup>1</sup> Navigare in rotta da "en route", cioè sta navigando tenendo una rotta lineare e non a zig-zag per esempio.

campione dovrà essere prelevato con impianto di separazione in funzione impedendone però la scarica a mare.

(b) Registro degli idrocarburi e degli oli minerali "*Oil Record Book*"

Il registro degli idrocarburi è formato da un elenco d'operazioni relative ai locali macchine, che, quando applicabili, devono essere registrate nel Registro in accordo alla regola 20 dell'Annesso I della MARPOL 73/78. Le voci sono state raggruppate in sezioni operative, ciascuna delle quali è contraddistinta da una lettera di codice.

Quando si registra qualche operazione nel Registro Idrocarburi, dovranno essere annotate nelle colonne appropriate la data, la lettera di codice, il numero della voce per l'operazione in atto e le annotazioni richieste, che dovranno essere registrate cronologicamente negli appositi spazi. Ciascuna pagina completata dovrà essere firmata dal Comandante dell'Unità.

Il Registro degli Idrocarburi contiene molti riferimenti alle quantità d'idrocarburi, tuttavia la limitata precisione dei dispositivi per la misurazione dei depositi e casse e le variazioni di temperatura influenzano l'accuratezza delle letture. Le registrazioni nel Registro degli Idrocarburi, quindi, saranno valutate in conformità.

(c) Piano d'emergenza di bordo contro l'inquinamento da oli minerali

Il Piano è redatto in conformità con la Regola 26 dell'Allegato I della Convenzione Internazionale per l'inquinamento da Navi 1973, come modificato dal relativo Protocollo del 1978. Lo scopo del piano è quello di fornire al Comandante e agli Ufficiali a bordo della nave una guida in relazione alle misure da prendere nel caso in cui sia avvenuto o sia probabile che avvenga un incidente con inquinamento.

Il Piano contiene tutte le informazioni ed istruzioni operative richieste dalla Guida emessa dalla International Maritime Organization (IMO). Le Appendici contengono i nomi, nonché i numeri di telefono, telefax e telex di tutti gli uffici con cui mettersi in contatto, citati nel piano, come pure altro materiale di riferimento.

Il Piano risulta così articolato:

- I) lista dell'autorità o persone con cui mettersi in contatto nel caso di un incidente con inquinamento da olio minerale;
- II) procedure da seguire da parte dei responsabili della nave nel redigere il rapporto su un incidente con inquinamento da olio minerale;
- III) descrizione particolareggiata delle misure da prendere immediatamente da parte delle persone a bordo dopo che sia avvenuto un versamento;
- IV) procedure e punto di contatto sulla nave per coordinare le attività di bordo con le autorità nazionali e locali nel combattere l'inquinamento.

(2) Liquami

L'Annesso IV della MARPOL detta le norme per la prevenzione dall'inquinamento marino da liquami provenienti da navi. Per liquami s'intende:

- drenaggi ed altri rifiuti provenienti da qualunque tipo di gabinetti, orinatoi e scarichi di W.C.;
- drenaggi provenienti da lavabi, lavandini, docce, tinozze e condotte di scarico situate nei locali riservati a cure mediche (infermeria, ambulatorio ecc.);

- altre acque di scolo quando miscelate con i drenaggi sopra definiti.

(a) Trattamento e scarico

Di norma lo scarico a mare è vietato, salvo che non siano rispettate le seguenti condizioni (Regola 8, Annesso IV):

- la nave scarichi liquami triturati e disinfettati usando un sistema approvato, ad una distanza maggiore di 3 miglia dalla costa, oppure liquami non sminuzzati e disinfettati a più di 12 miglia dalla costa; in ogni caso i liquami raccolti in una apposita cisterna non devono essere scaricati tutti in una volta ma con un rateo moderato e mentre la nave mantiene rotta costante e velocità di almeno 4 nodi;
- la nave sia dotata di un impianto di trattamento dei liquami approvato in base agli standard e metodi di prova della risoluzione IMO MEPC. 2(VI) "Raccomandazioni sugli standard internazionali dell'effluente e guida per l'esecuzione delle prove per gli impianti di trattamento dei liquami";
- i risultati delle prove dell'impianto siano riportati sul Certificato Internazionale di Prevenzione dall'Inquinamento da liquami (ISPP Certificate);
- l'effluente non lasci tracce visibili, solide o liquide, nella scia della nave;
- quando i liquami sono mescolati con rifiuti o acqua reflua aventi prescrizioni di scarica differenti, devono essere applicate le prescrizioni più severe.

Le navi dotate di "Certificazione MARPOL" saranno sottoposte a visita iniziale e, a buon esito, sarà rilasciato un Certificato Internazionale di Prevenzione dall'Inquinamento da Liquami (*International Sewage Pollution Prevention Certificate* – ISPP Certificate), valido 5 anni (con visite obbligatorie di convalida annuali ed intermedie del certificato). Le prescrizioni indicate ai punti precedenti si possono non applicare nei seguenti casi particolari (regola 9 dell'annesso IV):

- la scarica dei liquami dalla nave è necessaria per garantire la sicurezza della nave e del suo equipaggio e per la sicurezza della vita in mare;
- la scarica dei liquami è dovuta ad una avaria alla nave o al suo equipaggiamento, se tutte le ragionevoli precauzioni sono state prese prima e dopo il guasto, con lo scopo di prevenire e minimizzare la scarica in mare.

Annualmente dovrà essere prelevato un campione d'effluente da ciascun impianto di trattamento dei liquami presente a bordo ed inviato ad analisi. Il campione dovrà essere prelevato con impianto di trattamento in funzione impedendone però la scarica a mare.

(3) Rifiuti solidi

L'Annesso V della MARPOL detta le norme per la prevenzione dall'inquinamento marino dai rifiuti solidi delle navi.

Per rifiuti solidi s'intende qualunque specie di viveri, di rifiuti domestici ed operativi che si formano durante il normale esercizio di una nave e che possono essere scaricati in modo continuo o periodico.

Ai fini dell'Annesso V sono state individuate le seguenti aree che, a causa delle particolari condizioni oceanografiche, ecologiche e per la peculiarità del traffico che vi



si svolge, sono state dichiarate aree speciali: Mar Baltico, Mar Mediterraneo, Mar Nero, Mar Rosso, Zona dei Golfi, Mare del Nord, Antartide, Mar dei Caraibi.

(a) Norme comportamentali a carattere generale

A cura dei Comandi di Bordo devono essere effettuate periodicamente e frequentemente a tutto l'equipaggio delle conferenze sulla salvaguardia dell'ambiente marino, semplici nei contenuti e chiare negli obiettivi, mirando innanzitutto alla riduzione dei rifiuti solidi prodotti. Dovranno essere illustrati, i principi e le modalità della raccolta differenziata la suddivisione dei vari tipi di rifiuti, con particolare riferimento ai tossici e nocivi e, soprattutto, le sanzioni previste nei confronti di coloro i quali non rispetteranno le disposizioni in materia di educazione ambientale e gestione dei rifiuti di bordo.. Le elementari norme di comportamento a carattere generale dovranno essere richiamate nei locali di vita mediante cartelli, tabelle e disegni di libera ideazione e reperimento.

(b) Raccolta differenziata dei rifiuti

I rifiuti prodotti dalle Unità Navali, in accordo con il D.P.R. 912/82 e la L. 979 del 31/12/1982, possono essere suddivisi in:

- rifiuti alimentari;
- rifiuti speciali biodegradabili (carta, legno, lattine, vetro);
- rifiuti speciali non biodegradabili (plastiche, gomma, caucciù, scarti di pelle, espansi, lana di vetro e affini);
- rifiuti tossici e nocivi;
- rifiuti medico/sanitari.

(c) Trattamento e scarico

Entro le Aree Speciali è vietato scaricare in mare:

- qualsiasi materiale plastico;
- materiali galleggianti d'avvolgimento, legatura ed imballaggio;
- carta, stracci, vetro, bottiglie, metalli, utensili da cucina e simili anche se triturati o frantumati.

È consentita la discarica di rifiuti alimentari, anche se non triturati, ma ad una distanza dalla costa superiore a 12 NM.

Fuori dalle Aree Speciali, rimane il divieto di scaricare in mare qualsiasi materiale plastico, inclusi cavi sintetici, reti da pesca e sacchetti per rifiuti, ceneri dovute all'incenerimento di prodotti plastici che possono contenere residui tossici di metalli pesanti.

Viene consentita la discarica di:

- materiali galleggianti di avvolgimento, legatura ed imballaggio, di rivestimento interno, tappezzerie, purché a distanza superiore a 25 NM dalla costa;
- carta, stracci, vetro, bottiglie, metalli, terraglie e scarti simili, purché a distanza superiore a 12 NM dalla costa;
- gli stessi di cui sopra, ma frantumati o triturati, purché a distanza superiore a 3 miglia dalla costa e con dimensioni massime dei frammenti inferiori a 25 mm;

- rifiuti alimentari non triturati, purché a distanza superiore a 12 NM dalla costa;
- rifiuti alimentari triturati, purché a distanza superiore a 3 NM dalla costa.

Le prescrizioni indicate ai punti precedenti si possono non applicare nei seguenti casi particolari (regola 6 dell’annesso V):

- la scarica dei rifiuti solidi dalla nave è necessaria per garantire la sicurezza della nave e del suo equipaggio e per la sicurezza della vita in mare;
- la scarica dei rifiuti solidi è dovuta ad una avaria alla nave o al suo equipaggiamento, se tutte le ragionevoli precauzioni sono state prese prima e dopo il guasto, con lo scopo di prevenire e minimizzare la scarica in mare.

Le navi dotate di “Certificazione MARPOL” saranno sottoposte a visita iniziale e, a buon esito, sarà rilasciata una Dichiarazione Internazionale di Conformità alle norme sulla Prevenzione dall’Inquinamento da Rifiuti Solidi (*International Garbage Pollution Prevention Bill – ISPP Bill*), valida 5 anni (con visite di convalida annuali ed intermedie del certificato)<sup>2</sup>.

Ogni Unità Navale della marina Militare deve essere dotata del “Piano di gestione dei rifiuti” e del “Registro di scarico dei rifiuti”.

- (d) Linee guida per la compilazione del piano di gestione dei rifiuti (in accordo con MEPC. 70(38))

Il Piano deve contenere le procedure scritte per la raccolta, lo stoccaggio, il processo e la scarica dei rifiuti, compreso l’utilizzo d’impianti/attrezzature di bordo (tritarifiuti, compattatori ecc.) e l’indicazione dei soggetti responsabili del controllo, della compilazione del Piano e dell’attuazione delle direttive in esso contenute.

Una volta approvato dalle superiori Autorità, se l’Unità in questione dovrà essere certificata come rispondente alla MARPOL, il Piano verrà inviato ad un Istituto di Classifica per l’approvazione formale e quindi restituito all’Unità originatrice, divenendo così un documento ufficiale di bordo. Nel caso in cui l’Unità non debba essere certificata nel breve periodo, il Piano, con la sola approvazione in ambito Forza Armata, diverrà comunque un documento ufficiale di bordo.

- (e) Registro di scarico dei rifiuti

Il Registro di scarico dei rifiuti deve contenere una registrazione (con data e ora, posizione della nave, categoria dei rifiuti trattati, quantitativo stimato della scarica per ogni categoria in metri cubi e/o chilogrammi, firma dell’Ufficiale che esegue l’operazione) da effettuare in ciascuna delle seguenti occasioni:

- quando i rifiuti sono scaricati in mare;
- quando i rifiuti sono sbarcati a terra presso depositi autorizzati o su altre navi;
- quando i rifiuti sono inceneriti;
- quando vengono effettuate scariche accidentali od eccezionali.

---

<sup>2</sup> Allo stato attuale, non è previsto il rilascio di un certificato internazionale per la prevenzione dell’inquinamento dei rifiuti solidi; tuttavia l’Istituto di Classifica rilascerà un’attestazione che dichiara la conformità delle procedure di bordo nella raccolta, trattamento, stoccaggio e scarica a mare dei rifiuti prodotti a bordo e l’efficacia del trattamento da parte dei sistemi appositi (compattatori, triturator, *crusher* del vetro, ecc.). Per lo stesso motivo, si valuterà l’opportunità dell’effettuazione delle convalide annuali e dei rinnovi quinquennali.

Per gli scopi di questo registro, i rifiuti sono stati raggruppati nelle seguenti categorie:

- plastica;
- materiali galleggianti derivanti da imballaggi;
- materiali cartacei, stracci, vetro, metalli, bottiglie, triturati e ridotti in frammenti inferiori a 25 mm di diametro;
- materiali come sopra, non triturati;
- rifiuti alimentari;
- ceneri da inceneritori.

**c. Lo scarico dei rifiuti all'interno delle acque territoriali e nelle acque portuali**

Lo scarico dei rifiuti all'interno delle acque territoriali è regolamentato principalmente da leggi nazionali, pertanto, in generale, nessuna esenzione è prevista per il Naviglio militare. Inoltre, le norme nazionali (che in qualche caso possono essere regionali) sono solitamente più severe e dettagliate di quelle della MARPOL.

Fornire un elenco esaustivo della normativa riguardante la tutela ambientale delle Nazioni ove gravitano più frequentemente le Unità della Squadra, oltre a non essere tema del presente documento, sarebbe un lavoro di notevole complessità. Infatti, sebbene esistano, ad esempio a livello europeo, delle direttive comunitarie in materia, ogni Nazione ha le proprie norme, che a volte variano anche a seconda delle diverse regioni, e spesso subiscono frequenti aggiornamenti, con la crescente sensibilità nei confronti della tutela ambientale. Sarà cura del Comando di bordo verificare ed acquisire, in occasione di visite e soste in porti stranieri, la normativa vigente in materia di gestione dei rifiuti.

Per quanto riguarda specificatamente la situazione nazionale, vengono di seguito sommariamente analizzati i principali riferimenti normativi.

(1) Acque oleose

Nel panorama normativo italiano in materia, il ruolo di primo piano viene assunto dalla legge 31 dicembre 1982, n. 979, recante "Disposizioni per la difesa del mare". Per informazione si riporta che al titolo IV, art. 16 della citata legge, viene espressamente proibito al naviglio mercantile, nell'ambito delle acque territoriali e delle acque marittime interne compresi i porti, a tutte le navi senza alcuna distinzione di nazionalità, di versare in mare o di causare il versamento di idrocarburi o di miscele di idrocarburi, nonché delle sostanze nocive all'ambiente marino.

Ritornando al titolo IV art. 16 della legge 31 dicembre 1982 n. 979, è fatto divieto alle navi italiane mercantili di scaricare le sostanze nocive (elencate) anche al di fuori del limite esterno del mare territoriale italiano. Questo concetto è stato ulteriormente rafforzato dalla Legge 28 febbraio 1992, n. 220 – "Interventi per la difesa del mare" – che, all'art. 3, comma 1, ha esteso la portata del divieto assoluto di scarico di cui al citato art. 16 della legge 979/82 ed il conseguente trattamento sanzionatorio ex art. 200 in caso di sua violazione, introducendo il divieto di trasferimento delle morchie e delle acque di zavorra e lavaggio a bordo di navi non specializzate e non costruite ed attrezzate ai sensi del presente comma, effettuato nelle acque territoriali dal naviglio battente bandiera nazionale.

## (2) Liquami

Nelle acque territoriali nazionali, in vigore della vecchia normativa di tutela delle acque (319/76, c.d. "Legge Merli" abrogata) era previsto, dall'art. 11, una procedura particolare per lo smaltimento delle acque nere prodotte a bordo, culminante in un'autorizzazione ministeriale per lo scarico di materiale nelle acque marine. Dopo l'emanazione del Dlgs. 05.02.1997, n. 22 (c.d. "Decreto Ronchi"), si è assistito ad un cambio d'orientamento da parte del Ministero dell'Ambiente, che considera "rifiuti" le acque nere delle navi e, pertanto, a norma di legge devono essere smaltite a terra. Recentemente, per citare delle fattispecie concrete afferenti alla contestazione di scarichi in mare, la Corte di Cassazione – Sezione III Penale - con sentenza del 16.06.1998 ha stabilito che "l'autorizzazione per gli scarichi diretti in mare provenienti da navi è necessaria anche nel caso di scarichi dai servizi igienici di bordo; tuttavia, ai sensi della legge 172/95 (Legge Galli), tali scarichi senza autorizzazione costituiscono illecito amministrativo e non sono più previsti come reati".

Tra l'altro, il Dlgs. 152/99, c.d. "Testo unico per la tutela delle acque", stabilendo all'art. 45, comma 1, che "...tutti gli scarichi devono essere preventivamente autorizzati..." ha implicitamente ricompreso quelli effettuati in acque marine.

## (3) Rifiuti solidi

La vecchia disciplina che traeva origine dall'Ordinanza del Ministero della Sanità del 10 maggio 1973 e che prevedeva, tra l'altro, l'obbligo della termo-distruzione dei rifiuti alimentari mediante impianti collocati all'interno delle aree portuali o aeroportuali o, in alternativa, la sterilizzazione dei rifiuti medesimi tramite autoclavaggio, è stata sostituita dal Decreto Ministeriale – Ministero della Sanità di concerto con il Ministero dell'Ambiente – emanato il 22 maggio 2001.

Con il Decreto Interministeriale in questione, realizzato allo scopo di semplificare e rendere più omogenea la disciplina afferente il trattamento dei rifiuti alimentari provenienti dalle navi e dagli aeromobili che fanno scalo nei porti ed aeroporti nazionali, senza nulla togliere alla sicurezza ambientale in termini di prevenzione da possibili rischi sanitari, sono stati introdotti i seguenti punti innovativi:

smaltimento presso impianti di termo-distruzione ubicati nell'ambito delle regioni di provenienza dei rifiuti (non più, quindi, in impianti realizzati appositamente nelle aree portuali, oltretutto inesistenti nella quasi totalità dei porti italiani);

alternativa allo smaltimento in discarica per rifiuti solidi urbani, previo autolavaggio (ciò per non danneggiare i gestori dei pochi impianti portuali oggi esistenti);

maggiore incisività nei controlli (affidati agli Uffici di Sanità Marittima ed Aerea);

rilascio di autorizzazione ai sensi del Dlgs. 5 febbraio 1997, n. 22, per coloro che esercitano attività di gestione dei rifiuti di che trattasi.

**SEZIONE III – AERONAUTICA****1. Generalità**

La capacità operativa aeronautica (che coinvolge il mezzo aereo, lo spazio aereo, i servizi di supporto e gli aeroporti) è condizionata da problematiche ambientali che possono, in tempo di pace, influenzare lo sviluppo delle attività operative/addestrative.

È indubbio che i velivoli ed i sistemi aeroportuali condizionano sia l'ambiente nel suo complesso, sia la qualità della vita delle popolazioni che vivono nelle loro immediate vicinanze. Pertanto, pur considerando che l'ambiente operativo in cui si opera e la tipologia di intervento da effettuare<sup>1</sup> rappresenta una discriminante di riferimento per l'applicazione delle normative di riferimento, è sempre necessario svolgere un ruolo pro-attivo per coniugare, in modo bilanciato, gli interessi dello strumento aereo e della missione assegnata con le esigenze ambientali della collettività.

In tal senso una sana e corretta politica ambientale deve prevedere:

- l'applicazione coerente e costante del quadro normativo nazionale, nonché del relativo ed indispensabile monitoraggio;
- lo sviluppo di iniziative rivolte a produrre benefici ambientali;
- la promozione di interventi per la sensibilizzazione degli operatori aeronautici sul tema specifico;
- l'informazione nei confronti della collettività in merito alle azioni e all'impegno sviluppato per la tutela del territorio e della salute dei cittadini.

Pur riconoscendo che la tematica della tutela ambientale, dal punto di vista "aeronautico", è ampia e complessa, per motivi di opportunità saranno trattati solo alcuni argomenti ritenuti di maggiore impatto sull'ambiente e sulla salute pubblica. Quanto sopra con l'obiettivo di:

- assicurare ai Comandanti e agli "operatori" del settore di avere un utile strumento di riferimento per l'applicazione della normativa nazionale ed internazionale esistente in materia;
- sensibilizzare tutto il personale sulla necessità di garantire, in senso lato, l'adozione delle idonee misure ed accorgimenti orientati al pieno rispetto e alla tutela dell'ambiente e della popolazione civile.

**2. Idrocarburi alogenati e HALONS****a. Generalità**

I clorofluorocarburi (CFC o freon) sono degli "idrocarburi" in cui gli atomi di idrogeno vengono sostituiti da composti alogenati come cloro, fluoro e bromo.

Dalla loro introduzione, i CFC sono stati usati come:

- refrigeranti nei frigoriferi e negli impianti di condizionamento dell'aria;
- propellenti negli spray;
- agenti schiumogeni nella produzione degli imballaggi;

---

<sup>1</sup> In virtù dei compiti assegnati allo strumento militare, l'intera gamma delle operazioni militari può essere ricondotta a tre tipologie di intervento raggruppate, in funzione dell'intensità di applicazione della Forza Militare, in: attività militari in tempo di pace, gestione delle crisi e operazioni limitate contingenti, campagne e operazioni militari (cfr. "La Dottrina Militare Italiana" PID/S-1).

- detergenti usati nell'industria elettronica;
- prodotti chimici per estinguere incendi.

Essendo molecole molto stabili, i CFC hanno una lunga vita in atmosfera per cui riescono a raggiungere gli alti strati ove sembra esplicano la loro capacità distruttiva nei confronti dell'ozono<sup>2</sup>.

L'alternativa all'uso dei CFC è costituita dagli idroclorofluorocarburi (HCFC) nel rispetto, comunque, dei valori massimi dei parametri ambientali quali GWP (*Global Warming Potential* - potenziale di surriscaldamento totale, meglio noto come "effetto serra"), ALT (tempo di vita nell'atmosfera), ODP (*Ozone Depletion Potential* - potenziale di distruzione dell'ozono).

Gli HCFC, in cui sono assenti gli atomi di cloro e di bromo più aggressivi per l'ozono, sembrerebbero avere altri effetti, come ad esempio un potenziale di effetto serra e quindi essere tra i responsabili, seppure in modo minore, del riscaldamento dell'ambiente.

Tra gli idrocarburi alogenati, con elevato impatto sull'ozono, si segnalano anche gli *halons* che in ambito aeronautico sono particolarmente utilizzati sui velivoli in quanto garantiscono un elevato potere estinguente in un ridotto volume impiegato.

Con tali presupposti le norme europee, pur prevedendo la possibilità di impiego per dette sostanze, presuppongono l'esistenza di specifiche e rigide norme di controllo.

#### **b. Principali riferimenti normativi**

Il protocollo di Montreal del 1987, si pone all'origine della strategia necessaria per risolvere il problema ambientale della protezione dell'ozonosfera dall'azione distruttiva dei CFC, degli *halons* e di altre sostanze lesive.

Il documento, implementato dall'Italia nel 1997, mira a controllare la produzione e il consumo delle sostanze lesive, per mezzo di un calendario che prevede la loro totale dismissione<sup>3</sup>.

Anche la Comunità Europea ha elaborato una serie di regolamenti che hanno seguito l'evoluzione del Protocollo di Montreal, tra cui il n. 2037/2000, poi abrogato dal 1005/2009 nonché l'ultimo aggiornamento contenuto nel Regolamento 744/2010 con cui vengono stabilite la data ultima e la data limite di impiego dell'*halon* per usi critici (anche per le FF.AA.) in funzione delle differenti tipologie di *halons* e del loro diverso impiego. La data limite di utilizzo, per le sostanze lesive dell'ozono già in uso per gli ultimi impieghi previsti, è fissata al 2040.

#### **c. Adempimenti e obblighi**

Annualmente gli Enti/Reparti di FA sono obbligati ad inviare agli SS.MM. di FA, tramite catena gerarchica, il consuntivo delle quantità di *halons*/CFC per usi critici stoccate, disperse nell'ambiente e acquisite. Gli SS.MM. devono inoltrare, tramite SMD, tali dati al Ministero dell'Ambiente e della Tutela del Territorio e del Mare.

Le apparecchiature e gli impianti contenenti più di 3 Kg di sostanze controllate (riportate

---

<sup>2</sup> 100 grammi di CFC (contenuto tipico per una lattina di spray o per un frigorifero domestico) possono distruggere più di 3 tonnellate di ozono.

<sup>3</sup> Per i riferimenti normativi nazionali in materia cfr. Legge 28 dicembre 1993, n. 549 "Misure a tutela dell'ozono stratosferico e dell'ambiente" e Legge 16 giugno 1997, n. 179 "Modifiche alla legge 28 dicembre 1993, n. 549, recante misure a tutela dell'ozono stratosferico".

nell'allegato I del Regolamento 1005/2009), devono essere sottoposte frequentemente a controllo della presenza di fughe che, qualora riscontrate, devono essere riparate obbligatoriamente entro 14 giorni. Tali controlli devono essere registrati nel libretto di impianto.

Gli enti che gestiscono le apparecchiature contenenti idroclorofluorocarburi, in quantità pari o superiore a 3 kg, sono tenuti a registrare in apposito documento la quantità e il tipo di sostanza recuperata e/o aggiunta, nonché la società o il tecnico che ha effettuato l'eventuale manutenzione o assistenza.

Gli enti che utilizzano idroclorofluorocarburi rigenerati o riciclati per manutenzione o assistenza, gestiscono un registro nel quale riportano le imprese che hanno fornito gli idroclorofluorocarburi rigenerati e la provenienza degli idroclorofluorocarburi riciclati.

### 3. Rumore

#### a. Generalità

Il rumore è l'effetto di vibrazioni emesse da una sorgente sonora e da questa trasmessa ad un mezzo solido, liquido o gassoso che ne permette la propagazione sotto forma di variazioni di pressione (onde sonore)<sup>4</sup>. La sorgente sonora, come chiaramente è il mezzo aereo, emana una potenza che si trasforma in pressione-sonora. Una pressione sonora troppo elevata può causare danni all'udito ed è pertanto la grandezza da misurare.

#### b. Valori Limite (Zonizzazione)

A livello nazionale, ai fini della determinazione dei valori limite, il D.P.C.M. 01/03/91 (art. 2 comma 1) istituisce il criterio della zonizzazione: ogni Comune deve dividere il proprio territorio in sei fasce, ognuna soggetta ad un diverso limite di rumorosità<sup>5</sup>.

	<b>CLASSI DI TERRITORIO</b>	<b>Diurno (ore 6-22)</b>	<b>Notturmo (ore 22-6)</b>
1	<b>Aree particolarmente protette</b> (ospedali, scuole, parchi, aree di riposo).	50	40
2	<b>Aree prevalentemente residenziali</b> (aree urbane con basso traffico, bassa densità di popolazione, bassa presenza di attività commerciali, assenza di attività industriali).	55	45
3	<b>Aree di tipo misto</b> (aree urbane con normale traffico, media densità di popolazione, media presenza di attività commerciali, assenza di attività industriali).	60	50
4	<b>Aree di intensa attività umana</b> (aree urbane con intenso traffico, alta densità di popolazione, elevata presenza di attività commerciali, presenza di piccole industrie).	65	55
5	<b>Aree prevalentemente industriali</b> (aree interessate da insediamenti industriali e scarse abitazioni).	70	60
6	<b>Aree esclusivamente industriali</b> (aree esclusivamente industriali).	70	70

**Tabella 1-** Limiti massimi di rumorosità alla Zonizzazione Definitiva del territorio comunale (in dBA)

Fino a quando i Comuni non delibereranno in merito, valgono i limiti provvisori riportati nella tabella seguente.

<sup>4</sup> Il numero delle variazioni di pressione che avvengono in un secondo è definito Frequenza del Rumore e viene misurata in Hertz (Hz).

<sup>5</sup> Non tutti i Comuni hanno ancora adottato la zonizzazione acustica definitiva.

ZONA	Diurno (ore 6-22)	Notturmo (ore 22-6)
Tutto il territorio nazionale	70	60
Zona A (agglomerati urbani che rivestono carattere storico, artistico o di particolare pregio ambientale).	65	55
Zona B (le parti del territorio totalmente o parzialmente edificate, diverse delle zone A).	60	50
Zona esclusivamente industriale	70	70

**Tabella 2 - Zonizzazione provvisoria (in dBA)**

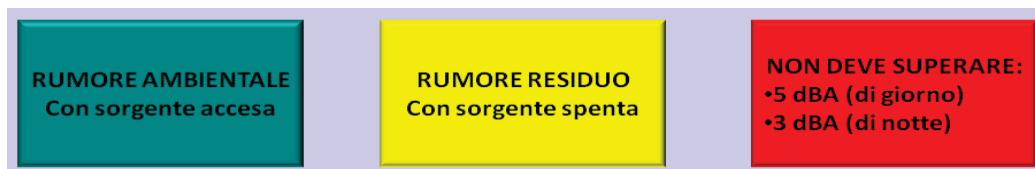
Un'applicazione pratica dei limiti di zonizzazione consiste nel verificare con opportune misure, lungo il perimetro esterno di una base militare, se il rumore prodotto dalle sorgenti varie (banco prove motori, officine, o macchine utensili, ecc.) rientri nei suddetti limiti, in modo da non arrecare disturbo o danno a:

- abitazioni limitrofe;
- luoghi di svago (parchi, centri creativi);
- ospedali, case di cura, scuole, ecc..

### c. Criterio differenziale

Il D.P.C.M. 01/03/91 (art. 2 comma 2), il D.P.C.M. 14/11/97 (art. 4) ed il D.M. 11/12/96 introducono ulteriori criteri per la tutela dell'uomo dall'inquinamento acustico.

La differenza tra il rumore ambientale (rumore rilevato con la sorgente rumorosa accesa) ed il rumore residuo (rumore rilevato escludendo la sorgente disturbante); non può essere superiore a 5 dBA in diurno o 3 dBA in notturno.



**Tabella 3 - Criterio differenziale tra il rumore ambientale ed il rumore residuo**

La verifica del livello di inquinamento acustico, secondo il criterio differenziale, si effettua nel luogo di ricezione del rumore (all'interno delle abitazioni con le finestre aperte) come previsto dall'art. 3 comma 1 del D.M. 11/12/96 e art. 2 comma 2 e punto 3.2 allegato B del D.P.C.M. del 01/03/91.

Nel settore del trasporto aereo, la Direttiva 92/14/CEE, in vigore dal 1995, ha introdotto la limitazione delle emissioni sonore degli aeromobili. Tale direttiva fa riferimento alle norme ICAO (Organizzazione Aviazione Civile Internazionale), le quali prevedono che dal 2002 in tutto il territorio dell'Unione Europea possono operare solo gli aerei più moderni e silenziosi. Anche se, ormai, gli effetti benefici della eliminazione degli aerei più rumorosi viene compensata, ai fini dell'emissione rumorosa, dall'aumento notevole del traffico aereo sulle città.

Nell'ambito della regolamentazione del rumore prodotto da attività aeroportuali il Decreto del Presidente della Repubblica n. 496 del 11/12/97 emanato in attuazione dell'art. 11 comma 1 della citata legge quadro 447/95, riguarda solo gli aeroporti civili, o gli aeroporti militari aperti al traffico civile, limitatamente al traffico civile. Per quanto concerne, invece, il traffico militare e gli aeroporti esclusivamente militari, il previsto Decreto attuativo collegato alla legge 447/95 non è stato ancora emanato.



**d. Principali adempimenti ed obblighi**

Di seguito viene riportata una sintesi degli adempimenti cui è soggetto il Comandante in funzione del tipo di sorgente di rumore.

Tipo di sorgente	Applicazione	Esclusione	Limiti di legge	Criterio differenziale
Attività volativa E tutto ciò che è connesso con la preparazione al volo.	Quando un centro abitato viene infastidito dal rumore prodotto dall'attività volativa dei velivoli militari.	Anche se la legge rimanda l'applicazione della 447/95 per i velivoli militari ad un Decreto attuativo specifico, si consiglia, comunque, di adottare procedure antirumore meno impattivi sulle popolazioni limitrofe.	I limiti dovrebbero essere inseriti all'interno del Decreto attuativo specifico per gli aeroporti militari. In mancanza applicare i limiti della zonizzazione.	Non si applica
Attività di manutenzione, dei centri di manutenzione, delle officine varie, le prove motori, ecc.	Quando l'attività delle officine varie, dei Centri Manutenzione, ecc., producendo rumore, arreca fastidio ai centri abitati limitrofi.	Si esclude la protezione dei lavoratori delle officine che è regolamentata dal D.Lgs. 81/01	Limiti da zonizzazione definitiva o provvisoria (la verifica può essere effettuata lungo il perimetro esterno della base.	<b>SI</b> (5 dBA di giorno, 3 dBA di notte) <b>NO</b> (se zona esclusivamente industriale)
Attività dei depositi, delle stazioni di pompaggio degli oleodotti, ecc..	Quando l'attività dei depositi, delle stazioni di pompaggio, ecc., producendo rumore, arreca fastidio ai centri abitati limitrofi.	Si esclude la protezione dei lavoratori delle officine che è regolamentata dal D.Lgs. 81/01	Limiti da zonizzazione definitiva o provvisoria (la verifica può essere effettuata all'interno delle abitazioni esposte.	<b>SI</b> (5 dBA di giorno, 3 dBA di notte) <b>NO</b> (se zona esclusivamente industriale)

**Tabella 4 - Adempimenti cui è soggetto il Comandante in funzione del tipo di sorgente di rumore**

In ogni caso, il Comandante deve porre in essere tutte le azioni per ridurre la generazione e/o propagazione del rumore, mediante accorgimenti tecnici organizzativi e procedurali. La riduzione della propagazione del rumore, ad esempio, è realizzabile mediante fonoisolamento e rivestimento dei locali con pannelli fonoassorbenti.

Relativamente ai sistemi di contenimento dei livelli sonori in aree vaste come le zone aperte di un interno aeroportuale, è necessario procedere, *in primis*, ad un monitoraggio dei livelli di rumore esistenti e successivamente, attraverso un'approfondita analisi degli elementi al contorno, progettare, caso per caso, opportuni sistemi di assorbimento o barriere acustiche. Gli interventi correttivi che si possono effettuare per limitare l'impatto acustico prodotto dagli aeromobili sono relativi all'adozione di procedure antirumore, modifica dei profili di decollo ed atterraggio fino ad arrivare alla limitazione del traffico relativo alle attività di volo addestrativo di un Ente.

**4. Gestione materiali pericolosi, agenti chimici, serbatoi e cisterne interrato****a. Agenti pericolosi e agenti chimici**

Lo sviluppo della chimica ha determinato un continuo proliferare di sostanze e preparati che possono rilevarsi pericolosi per l'uomo e per l'ambiente in generale. Le attività logistiche,

con particolare riferimento alle attività manutentive, prevedono l'impiego di materiali e sostanze che vanno sempre gestite in maniera corretta; in caso contrario si corre il rischio di procurare danni non solo per l'uomo ma anche per l'ambiente in cui si opera.

Ai fini della classificazione, le sostanze e i preparati pericolosi vengono distinti in esplosivi, comburenti, estremamente infiammabili, facilmente infiammabili, infiammabili, molto tossici, tossici, nocivi, corrosivi, irritanti, sensibilizzanti, cancerogeni, mutageni, tossici per il ciclo produttivo e pericolosi per l'ambiente (stessa classificazione si può di massima utilizzare per la gestione dei rifiuti). Questi ultimi riguardano sostanze e preparati che, qualora si diffondessero nell'ambiente, presentano o possono presentare rischi immediati o differiti per una o più componenti ambientali.

Per una migliore comprensione della problematica, si ritiene opportuno riportare alcune definizioni riportate nella norma che riguarda gli agenti chimici (D.Lgs 2 febbraio 2002, n. 25<sup>6</sup>, recepito dal 81/2008<sup>7</sup>, al "Titolo VII bis – Protezione da agenti chimici"). Per agenti chimici pericolosi si intendono: "le sostanze e i preparati che, ai sensi del D.Lgs 52/97 (sostanze) e del D.Lgs 65/2003<sup>8</sup> (preparati), sono classificati pericolosi".

Il riconoscimento della presenza di tali materiali in un ambiente lavorativo può essere effettuato attraverso:

- la semplice osservazione della presenza, obbligatoria per legge, di simboli ed etichette di pericolo sui contenitori di sostanze e preparati (miscela) pericolosi;
- la conoscenza dei processi lavorativi che possono originare sostanze pericolose per la salute quali: fumi di saldatura, polveri, metalli aerodispersi, gas di scarico di mezzi a combustione interna, saturazione di ambienti con gas inerti, gestione rifiuti pericolosi, ecc.

Quanto sopra riportato mette in evidenza che occorre, al di fuori di ogni dubbio, effettuare un'accurata informazione e formazione del personale che opera con detti materiali.

#### **b. Serbatoi e cisterne interrati**

I serbatoi interrati normalmente vengono destinati allo stoccaggio di prodotti petroliferi (carburanti ed oli) e di sostanze chimiche. Gli eventuali inquinamenti prodotti da inconvenienti nei sistemi di stoccaggio interrato sono particolarmente pericolosi per la difficoltà di immediata verifica delle dispersioni (anche per l'assenza di sistemi adeguati di monitoraggio), ma i cui effetti possono produrre danni gravissimi e spesso irreversibili sull'ambiente quali incendi ed inquinamenti di suolo e falde acquifere.

La gestione dei carbolubrificanti avio è normata per tutte le FA dalla **CLA-NL-4130-0001-00B00** in cui vengono dettagliati compiti e responsabilità del personale coinvolto, nonché le procedure di gestione dei depositi, a partire dalla ricezione del prodotto, all'immagazzinamento, alla distribuzione mediante autorifornitori o rete. Vengono inoltre specificati i controlli e le verifiche da mettere in atto sui prodotti e sui mezzi destinati al

---

<sup>6</sup> "Attuazione della direttiva 98/24/CE sulla protezione della salute e della sicurezza dei lavoratori contro i rischi derivanti da agenti chimici durante il lavoro". (Supplemento n. 40/L alla G. U. n. 57 dell'8 marzo 2002).

<sup>7</sup> Decreto Legislativo 9 aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro" (Testo unico in materia di salute e sicurezza nei luoghi di lavoro - TUSL).

<sup>8</sup> Il D.Lgs 65/2003 ha abrogato il D.Lgs 16 luglio 1998, n. 285.

Servizio carburanti lubrificanti.

**c. Procedure in caso di incidente/inconveniente**

I carburanti lubrificanti avio sono ricompresi tra i materiali di armamento secondo le vigenti norme in materia e pertanto, in caso di inquinamento dell'ambiente o anche solo di sospetto inquinamento, vanno applicate le procedure previste dal DM 22 ottobre 2009<sup>9</sup>.

Nella **Figura 12** a pag. 142 si riporta la flow-chart illustrativa delle azioni da mettere in atto in tale eventualità. Nel caso ciò avvenga in contesti internazionali, dovranno essere seguite le leggi locali, ma qualora esse risultino meno restrittive della norma nazionale, dovrà essere seguita quest'ultima.

---

<sup>9</sup> Procedure per la gestione dei materiali e dei rifiuti e la bonifica dei siti e delle infrastrutture direttamente destinati alla difesa militare e alla sicurezza nazionale (Gu 15 aprile 2010 n. 87)

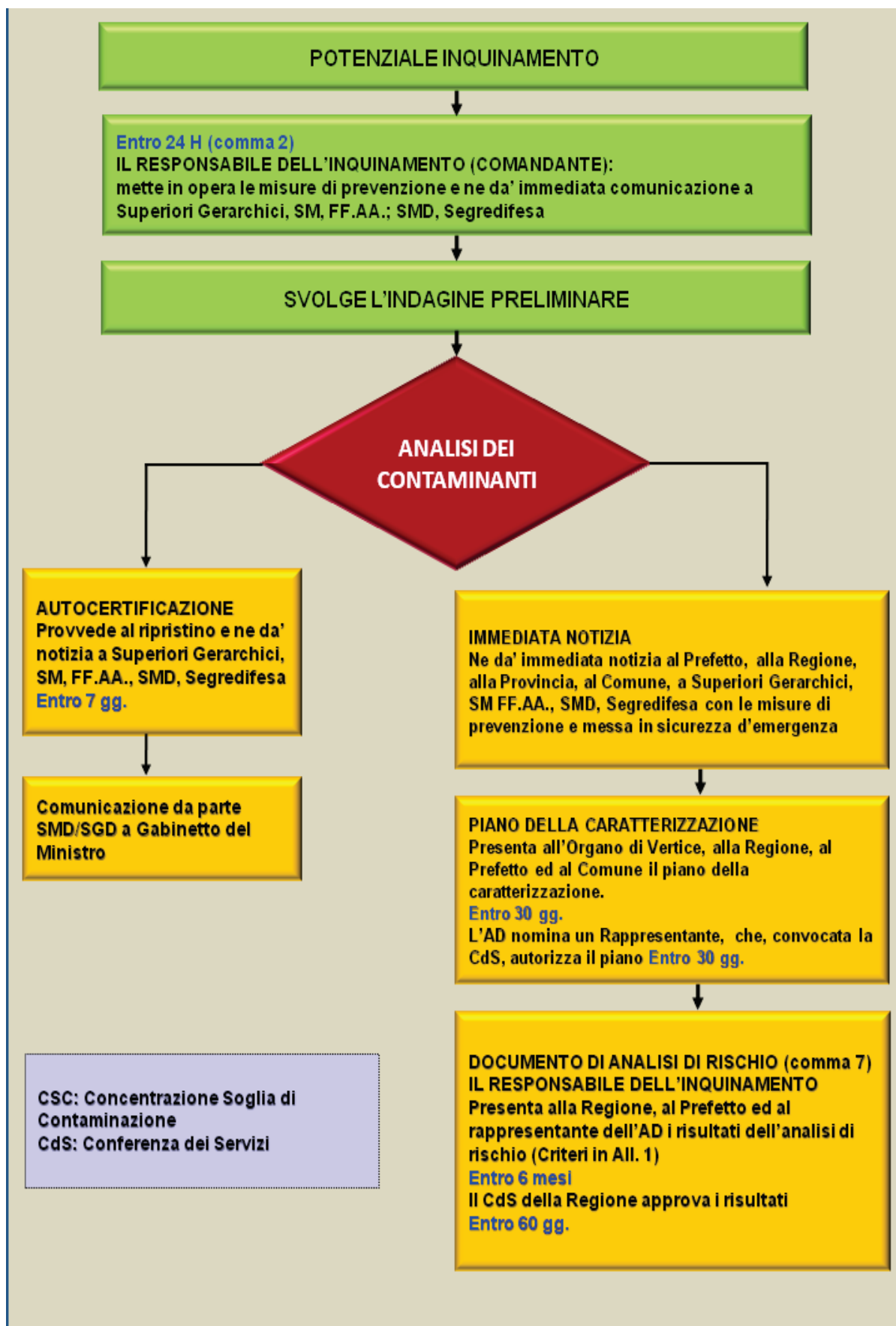


Figura 12 Azioni in caso di incidente con carbolubrificanti

## LA GESTIONE DELLE EMERGENZE (*CONSEQUENCE MANAGEMENT*)

### 1. Premessa

Nell'ambito della Protezione delle Forze, lo studio e la realizzazione di efficaci misure di gestione delle emergenze (*Consequence Management* - CM) assume una notevole importanza.

Il *Consequence Management* può essere definito come 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 (ad esempio attentati terroristici)<sup>1</sup>.

È opportuno precisare che un corretto approccio al CM implica l'attuazione dell'*Incident Management*<sup>2</sup> e del *Risk Management*<sup>3</sup>, ovvero di un unico sistema organizzato, coordinato ed organico che, attraverso una mirata attività di studio, analisi e programmazione, punti ad assicurare l'assolvimento/prosieguo dell'attività operativa, la tutela del personale e la salvaguardia dei servizi essenziali.

In tale prospettiva, a seguito dell'effettivo verificarsi di un incidente, diventa di vitale importanza minimizzarne gli effetti, ponendo immediatamente in essere un'adeguata struttura gestionale che consenta di coordinare gli interventi di risposta all'evento dannoso.

Un efficace CM permetterà di:

- limitare gli effetti di un incidente;
- contenere il numero delle vittime, anche fra la popolazione civile eventualmente coinvolta;
- ridurre il potenziale impatto ambientale;
- preservare le infrastrutture militari e civili, anche quelle appartenenti alla *Host Nation* (HN);
- garantire un ritorno altamente positivo in termini di consenso ed immagine.

### 2. Generalità

Il CM rientra nel campo della gestione delle emergenze e quindi, in particolari casi, dell'imprevedibile. Pertanto solo un'adeguata opera di pianificazione e previsione, unita alla disponibilità di prodotti un'*intelligence* aggiornati sulle potenzialità delle forze ostili, permetterà di gestire al meglio gli effetti di un evento disastroso e di contenere quanto più possibile le conseguenze:

- "dirette", sul personale e sulle infrastrutture;
- "indirette", sul morale delle forze amiche.

---

<sup>1</sup> Secondo quanto riportato nel documento "*ACO Force Standards Volume I – General*" in riferimento agli aspetti di *Force Protection* il "*Consequence Management comprising of contingency planning, emergency response, recovery, civil-military response and public information*".

<sup>2</sup> Attività di prevenzione, preparazione e risposta agli attacchi terroristici, catastrofi e altre emergenze che si sviluppa attraverso un approccio di tipo omnicomprensivo nazionale. L'*Incident Management* comprende le misure e le attività svolte al livello locale e nazionale per fronteggiare il possibile "incidente" e considera sia la gestione delle crisi (*Crisis Management*) che la gestione delle conseguenze dell'evento dannoso (*Consequence Management*).

<sup>3</sup> Processo di individuazione e valutazione (*risk assessment*), di controllo dei rischi derivanti da fattori operativi e determinazione delle discendenti decisioni che tengano conto del giusto equilibrio tra costi e benefici per l'assolvimento della missione.

In particolare un efficace sistema di CM dovrà contemplare specifiche misure orientate a:

- assicurare efficaci interventi di primo soccorso alle vittime, evacuando rapidamente eventuali feriti;
- ripristinare le capacità operative essenziali, in modo da garantire il prosieguo delle operazioni in modo più o meno regolare;
- isolare le zone di pericolo.

Con riferimento a tali importanti presupposti, il CM implica il coordinamento sistematico di un complesso di attività, quali:

- pianificazione;
- *intelligence*;
- comunicazioni;
- sicurezza;
- antincendio;
- neutralizzazione di ordigni inesplosi (UXO)<sup>4</sup> e sostanze esplosive;
- smaltimento materiali CBRN/pericolosi;
- prevenzione e assistenza sanitaria;
- supporto alla popolazione (incluso la fornitura di alloggi di prima accoglienza, acqua potabile, generi di prima necessità);
- sostegno logistico.

In tale quadro, risulta fondamentale definire a priori una struttura di collegamento che consenta di "mettere in sistema" le attività svolte dalle Forze Armate con quelle degli altri attori presenti (*Host Nation*, eventuali agenzie governative, organizzazioni non governative e/o internazionali, società private, specifiche agenzie, ecc.) nelle aree di rispettivo interesse:

- ingegneria civile;
- pubblica sicurezza;
- salute pubblica;
- antincendio;
- ricerca e primo soccorso;
- decontaminazione;
- trasporto.

In un settore così complesso, inoltre, particolare attenzione dovrà essere indirizzata all'istituzione di un idoneo servizio di diffusione delle informazioni, finalizzato alla gestione delle stesse (*Public Affair*) per meglio supportare la missione da adempiere.

### **3. Il piano di emergenza CM**

Le attività di pianificazione sopra descritte devono condurre alla definizione di un "Piano di emergenza" dedicato che contenga tutte le procedure da mettere in atto nel caso in cui si verifichi un evento dannoso.

---

<sup>4</sup> *Unexploded Explosive Ordnance (UXO)*.

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.

Il *piano* da considerare è perciò a carattere generale, e presenta differenti livelli di approfondimento a seconda della disponibilità di informazioni relative all'ambiente e al contesto operativo di riferimento. Ciò nonostante, dovendo fronteggiare tutti i possibili rischi dello scenario considerato, tale piano deve contenere specifiche sessioni tecniche, che potranno essere integrate in relazione al progressivo aggiornamento delle informazioni disponibili e al completamento del censimento degli elementi effettivamente esposti al rischio. Le conoscenze di dettaglio, che si andranno così a delineare, favoriranno, in un secondo momento, la redazione di *piani di emergenza* strutturati secondo allegati funzionali.

Nella stesura del *piano di emergenza*, dovranno essere considerate possibili implicazioni – soprattutto di natura legale – connesse alle attività di intervento. Durante le fasi di risposta ad incidenti, infatti, sarà necessario adottare metodi e procedure operative che garantiscano la possibilità di sfruttare l'ambiente (così come le persone coinvolte, materiali e documenti) a fini investigativi, evitando di compromettere eventuali fonti di prova. La stessa attenzione sarà necessaria per poter garantire il raggiungimento di positivi risultati nel settore dell'*intelligence*.

Al riguardo, nell'approntamento del relativo *piano di emergenza*, dovrà essere individuato l'assetto dell'Arma dei Carabinieri – nella sua funzione di Polizia Militare, sia in territorio nazionale che all'estero – che dovrà intervenire nella competenza.

Per essere efficace, il *piano di emergenza* deve, inoltre, definire le esigenze e la disponibilità di personale, mezzi ed attrezzature nonché stabilire a priori i compiti di ciascun Ente che, in funzione delle diverse ipotesi di rischio (scenari di evento attesi), potrebbe essere coinvolto.

In estrema sintesi i *piani di emergenza*, oltre a comprendere gli *scenari di evento attesi* e i relativi *modelli d'intervento*, rappresentano i documenti finalizzati alla salvaguardia delle infrastrutture e del personale, in quanto:

- delineano le specifiche responsabilità per l'esecuzione di particolari azioni;
- definiscono la catena di Comando e Controllo e le modalità di attuazione del coordinamento;
- individuano le risorse umane e materiali necessarie per fronteggiare e superare la situazione di emergenza.

**a. Scenari degli eventi attesi**

Gli *scenari degli eventi attesi* costituiscono il supporto fondamentale ed imprescindibile per la predisposizione dei modelli di intervento e comprendono:

- la “descrizione sintetica dell'evento considerato e della sua possibile dinamica” (nei documenti stralcio dovrà essere predisposta una opportuna scheda descrittiva);
- la “perimetrazione”<sup>5</sup>, anche approssimativa, dell'area che potrebbe essere interessata dall'evento (carta dello scenario ad opportuna scala da selezionare in funzione del rischio);
- la “valutazione preventiva del probabile danno” a persone e cose che si determina al verificarsi dell'evento atteso.

---

<sup>5</sup> La perimetrazione è finalizzata a definire le aree che dovranno essere oggetto delle successive fasi di lavoro ai fini della stesura del piano di emergenza.

La base fondamentale per la descrizione dell'evento e della sua possibile dinamica è rappresentata dall'analisi della criticità e dalla valutazione della pericolosità del sito considerato. Il tutto però, deve essere correlato in modo costante e continuo con gli altri elementi *intelligence* disponibili.

Per quanto riguarda la perimetrazione dell'area è importante precisare che non sempre è definibile a priori, ovvero l'evento può manifestarsi in un'area diversa o non coincidente con quella ipotizzata. In questo caso si procederà alla perimetrazione dell'area minacciata o interessata dall'evento imminente o avvenuto e, contestualmente, si provvederà al rilevamento del danno atteso o verificatosi.

Per la valutazione preventiva del probabile danno, è necessario, invece, procedere al censimento di tutti gli elementi esposti al rischio ubicati nelle aree considerate (i danni saranno classificati in : prevedibili quantitativamente - prevedibili qualitativamente - non prevedibili).

#### **b. Modello di intervento**

I *modelli di intervento* devono essere delineati sulla base degli scenari di evento e articolati per tipologia di rischio e definiti in riferimento alla valutazione del rischio. Tuttavia si devono tenere in considerazione le difficoltà intrinseche di detta valutazione. Infatti i danni causati dai fenomeni naturali o meteorologici, in relazione alla loro prevedibilità, estensione ed intensità, possono essere descritti con livelli di approssimazione molto diversi rispetto a quelli connessi alle attività svolte dall'avversario.

Per *modello di intervento* si deve intendere la definizione dei protocolli operativi da attivare in caso di situazioni di emergenza relativa ad un evento imminente o già verificatosi. Tali protocolli, finalizzati alla gestione dell'emergenza, individuano le fasi nelle quali si articola l'intervento, nonché le componenti e le strutture operative che devono essere gradualmente attivate, sia nei centri decisionali permanenti sia nell'area interessata dall'evento, stabilendone composizione, responsabilità e compiti.

In sintesi, il *modello di intervento* definisce:

- il complesso delle procedure da attuare;
- le fasi nelle quali si articola l'intervento;
- le componenti istituzionali e le strutture operative che devono essere attivate.

#### **4. Gestione del rischio**

La gestione del rischio si materializza in un processo di identificazione, valutazione, selezione e attuazione dei controlli e delle misure idonee a ridurre la minaccia/rischio identificato. Tale attività deve, in particolare, tenere conto, in rapporto alla necessità di conseguire il successo dell'operazione nei tempi stabiliti, delle:

- valutazioni delle criticità, delle minacce e delle vulnerabilità;
- considerazioni relative al costo (in termini di risorse, interferenza con la manovra, ecc.) che l'adozione dei controlli e delle misure di Protezione delle Forze comportano.

Una volta individuati sia le possibili sorgenti di pericolo che gli eventuali punti deboli del nostro sistema di protezione, considerato che è impossibile eliminare tutti i possibili rischi, diventa importante individuare le migliori opzioni che consentano sia di ridurre le probabilità di concretizzazione della minaccia sia, al contempo, di minimizzare il numero di perdite e



l'impatto sulla capacità operativa della forza nel caso di concretizzazione di una minaccia. La decisione sul livello di rischio e sulle conseguenze ritenute accettabili è propria del Comandante. Una volta che lo *staff* abbia accertato quali elementi critici del dispositivo amico possano essere soggetti a minacce/rischi, è necessario verificare che il *gap*, determinatosi dal confronto esigenze/possibilità, non superi i limiti fissati dal Comandante nella sua direttiva per la pianificazione. La fase della pianificazione termina con l'individuazione dei controlli e delle misure di protezione delle forze, nonché dei piani di emergenza da attuare in caso di incidente, che dovranno essere implementate dai vari Comandanti, a ogni livello ordinativo. Nella fase condotta della gestione del rischio, i controlli e le misure di protezione delle forze sono attuati, ad ogni livello.

## **5. Realizzazione del piano di emergenza CM**

La realizzazione di un adeguato *Piano di Emergenza CM* si sviluppa attraverso un processo suddiviso in tre fasi, indipendentemente dal fatto che si stia pianificando la gestione delle conseguenze causate da un disastro naturale, meteorologico, accidentale o da un deliberato attacco di terroristi e/o insorgenti.

Le fasi di sviluppo del *Piano di Emergenza CM* dovranno considerare gli elementi descritti nel precedente paragrafo 3 con particolare riferimento agli scenari degli eventi attesi e ai modelli di intervento, ponendo una particolare cura nel definire i sotto notati aspetti:

- impatto e conseguenze;
- risorse richieste;
- addestramento ed esercitazioni.

### **a. Impatto e conseguenze**

La prima fase del *Piano di Emergenza* deve valutare l'impatto e le possibili conseguenze associate ad un particolare tipo di incidente, avendo cura di focalizzare l'attenzione sullo scenario peggiore per una data unità o installazione. Per esempio, nel riferirsi ad una palazzina comando sviluppata su più piani, si può prevedere un possibile attacco perpetrato mediante auto bomba, e considerare, quale scenario peggiore, il collasso della struttura con conseguenti vittime intrappolate tra le macerie.

Per ogni scenario individuato dovrà, inoltre, essere identificata sia la catena di Comando e Controllo principale, che quella di riserva, entrambe comunque in grado di essere immediatamente attivate consentendo una corretta e costante interconnessione fra gli Enti responsabili della sicurezza, della sanità e antincendio con i servizi pubblici essenziali.

### **b. Risorse richieste**

La seconda fase prevede l'individuazione delle risorse necessarie per fronteggiare le conseguenze individuate nella prima fase, al fine di minimizzare quanto più possibile eventuali danni materiali o, nella peggiore delle ipotesi, la perdita di vite umane.

Si tratta quindi di disporre di personale medico, ambulanze e posti letto in ospedale, nonché di prevedere anche le misure necessarie per l'identificazione e la conservazione delle salme nonché delle misure da intraprendere per il loro rientro in Patria.

Le risorse ritenute necessarie devono quindi essere confrontate con gli assetti effettivamente a disposizione. Se la richiesta è superiore alle capacità del Comando, dovranno essere identificate le risorse disponibili sul luogo (a tale scopo potranno essere stabiliti degli

accordi di mutuo supporto), ovvero dovranno essere già individuate le eventuali ulteriori risorse da richiedere in supporto.

Durante la pianificazione deve tuttavia essere tenuto in considerazione che il sopraggiungere sul luogo interessato dall'evento di ulteriori assetti, richiede un'ulteriore coordinamento per il corretto impiego degli stessi.

**c. Addestramento ed esercitazioni**

In seguito allo sviluppo del *Piano di Emergenza*, il personale interessato dovrà essere adeguatamente addestrato, anche ricorrendo a specifiche esercitazioni.

L'iter addestrativo dovrà essere continuamente revisionato ed aggiornato, per garantire un'adeguata risposta alle conseguenze di un evento dannoso, anche in considerazione che la confusione, l'incertezza, lo *shock* e i limitati tempi di reazione richiesti al personale, possono influire negativamente sulla gestione della situazione verificatasi. Affinché l'addestramento sia condotto in maniera efficace, non deve limitarsi a coinvolgere solo il comparto Difesa, ma deve essere esteso anche alle eventuali organizzazioni civili previste nel Piano stesso.

**6. Gestione degli effetti di un evento disastroso (risposta all'incidente)**

La gestione degli effetti di un evento disastroso 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. Un'efficace risposta all'incidente richiede la coordinazione di molteplici attività, tra cui *intelligence*, contro-sorveglianza, sicurezza, polizia, carattere sanitario, antincendio, del genio (*C-IED* e *Field Engineering*), ricerca e recupero, comunicazioni, pubblica informazione e affari legali.

Al verificarsi di un incidente, di origine naturale, accidentale o a seguito di attività terroristica, si succedono tre fasi così suddivise:

- valutazione della situazione ed attività preliminari (valutazione e preparazione);
- intervento immediato (assistenza immediata);
- supporto successivo (operazioni di CM a lungo effetto).

Ognuna di queste fasi prevede delle attività specifiche.

**a. Fase 1 – Valutazione e preparazione**

Nell'ambito di questa fase dovranno essere intraprese le seguenti azioni:

- determinare il tipo di incidente;
- effettuare un'analisi della situazione, attivare una struttura di C2 e gli eventuali assetti CM disponibili per garantire una risposta efficace ed immediata;
- verificare gli assetti militari disponibili;
- determinare lo stato e la disponibilità di eventuali assetti forniti dalla HN, dalle Organizzazioni Internazionali, governative e/o non governative, nonché dalle altre Agenzie presenti sul luogo;
- determinare l'esistenza e l'adeguatezza di eventuali piani della HN per la gestione di incidenti, inclusi quelli causati dall'impiego di Armi di Distruzione di Massa (*Weapons of Mass Destruction - WMD*);
- determinare lo stato e la disponibilità degli assetti di trasporto e delle linee di comunicazione;

- effettuare una valutazione del possibile impatto ambientale causato dall'incidente, comprese le eventuali implicazioni per la salute delle truppe schierate e della popolazione civile;
- sviluppare e coordinare con i Media un piano per la gestione delle informazioni e definire le note di linguaggio.

**b. Fase 2 – Assistenza immediata**

La fase di intervento immediato prevede lo svolgimento delle seguenti azioni:

- creare una centrale operativa che coordini le operazioni;
- predisporre l'eventuale neutralizzazione di ordigni inesplosi (UXO);
- smaltimento di sostanze pericolose;
- assistere le forze della HN a delimitare l'area interessata;
- raccogliere ed analizzare campioni per valutare l'eventuale presenza di sostanze radioattive, chimiche o tossiche residue;
- assistere la HN nell'evacuare la popolazione civile dall'area interessata all'incidente, allo scopo di facilitare lo svolgimento delle attività;
- fornire la cornice di sicurezza per il personale e le strutture di soccorso interessate all'operazione di primo intervento;
- fornire assistenza per le attività di primo soccorso medico;
- fornire assistenza e supporto medico per il monitoraggio delle minacce alla salute della popolazione civile (prevenzione di epidemie) oltre alla valutazione dell'eventuale impatto ambientale;
- fornire assistenza per le operazioni di ricerca e soccorso;
- fornire assistenza nella condotta delle operazioni antincendio;
- assistere la HN nelle eventuali operazioni di decontaminazione del personale, dei materiali e delle infrastrutture;
- avviare una campagna di informazione "mirata" alla popolazione locale, ai Media presenti nella regione interessata e a quelli internazionali.

**c. Fase 3 – Operazioni di CM a lungo effetto**

Le attività di medio-lungo periodo comprendono:

- continuare nell'isolamento dell'area;
- assistere la HN alle operazioni di soccorso, nonché alla creazione di centri predisposti per la fornitura di posti letto e generi di prima necessità;
- rimuovere e smaltire eventuali detriti contaminati;
- riparare/ricostruire le infrastrutture danneggiate;
- assistere la HN nella fasi di ricostruzione.

**7. Revisione dei controlli e delle misure**

La revisione dei controlli e delle misure, prende spunto dall'esame comparato dell'incidente occorso e delle relative capacità di reazione messe in atto (*After Action Review*) ovvero dall'aggiornamento degli elementi di conoscenza sulla minaccia. Questo processo prevede un

continuo aggiornamento dell'esame delle vulnerabilità, nonché dei controlli e delle misure da implementare per la Protezione delle Forze, attraverso:

- l'*update* della situazione e della minaccia che deriva dallo sviluppo, senza soluzione di continuità, dei cicli *Intelligence*, sviluppo cognitivo, controinformazione e OPSEC;
- l'attività di raccolta dei dati e delle informazioni condotta nello *step* "Risposta all'incidente" a seguito di un evento;
- l'esecuzione di "*crash test live*" o simulati.

Per la corretta gestione delle attività di *Consequence Management*, deve essere costantemente enfatizzato il ricorso all'analisi delle Lezioni Apprese.

La sicurezza implica, indirettamente, la creazione di un patrimonio individuale di condivisione, consapevolezza e conoscenza del problema, che si può instaurare solo attraverso un addestramento mirato e continuo. Quest'ultimo deve essere svolto soprattutto per prepararsi e ottimizzare i tempi di risposta, considerato che gli eventi dannosi normalmente accadono con poco preavviso, generando, di conseguenza, condizioni di profonda indeterminatezza.

## 8. Il Comando e Controllo

L'individuazione di una struttura di Comando e Controllo ben definita è essenziale per assicurare un'efficace *Consequence Management*. La definizione delle responsabilità, delle priorità e delle procedure da attuare dovrà essere riferita, secondo una schema temporale, alle fasi precedenti, contestuali e successive all'incidente.

Le principali responsabilità si riferiscono alle capacità di gestione degli incidenti, all'esecuzione tempestiva di interventi di primo soccorso, all'esecuzione di risposte efficaci a danni correlati ad attività terroristiche, all'impiego di materiali pericolosi e/o di armi di distruzione di massa (WMD).

Per gli aspetti riguardanti la difesa CBRN, dovrà essere considerata l'intera gamma dei possibili interventi, comprendendo quelli relativi a situazioni di emergenza su piccola scala, fino a quelli più rilevanti. Per tali aspetti la pianificazione dovrà considerare l'analisi delle minacce, la valutazione delle vulnerabilità, la determinazione del rischio preliminare, l'individuazione e la segnalazione della contaminazione, il controllo della stessa e la sua decontaminazione.

La delicatezza della materia impone la necessità di predisporre un collegamento privilegiato con il COI, che si occuperà di fornire l'opportuna assistenza verificando, altresì, la possibilità di soddisfare ulteriori esigenze o supporti richiesti per affrontare casi specifici.

La HN, in funzione dei *Memorandum of Understanding* o dei *Technical Agreements* precedentemente concordati, può mantenere la piena responsabilità della gestione dell'evento verificatosi all'interno del proprio territorio. Tuttavia i contingenti presenti in Teatro, che rimangono responsabili degli aspetti afferenti la sicurezza, incluso il CM, all'interno dei *compound*, possono intervenire a sostegno della HN qualora previsto. In questo caso, normalmente, i Comandanti delle *Task Force* coinvolte sono identificati quali punti di contatto per coordinare le operazioni.

## LA DIFESA CBRN

### 1. Introduzione

I principi della *Force Protection* sono utilizzati come linee guida per le operazioni di difesa CBRN<sup>1</sup>, intesa come 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.

In questo documento, gli aspetti legati alle misure da adottare in caso di atti terroristici di tipo CBRN saranno trattati come parte integrante delle misure di difesa CBRN in generale.

La pianificazione e condotta di attività di difesa CBRN impongono un adeguato coordinamento tra tutti gli elementi interessati nella protezione delle forze, con particolare riferimento alle componenti EOR<sup>2</sup>/EOD<sup>3</sup>/IEDD<sup>4</sup> e Logistico/Sanitaria.

Le misure precauzionali per la protezione delle forze dai rischi CBRN sono necessarie per ridurre al minimo le possibilità di essere l'obiettivo di attacchi con armi CBRN e minimizzare gli effetti di tali armi nel caso vengano impiegate.

Pertanto, è di fondamentale importanza tenere in considerazione i principi di protezione delle forze di seguito specificati.

- a. **Valutazione della minaccia**, basata su una accurata e tempestiva raccolta di informazioni, da condurre con continuità, in modo tale da consentire di attivare le capacità di difesa CBRN più adeguate e adottare le misure appropriate.
- b. **Gestione del rischio**, allo scopo di limitare le perdite umane e i danni materiali, sarà necessario che i Comandanti definiscano e gestiscano il compromesso tra i costi in termini di vite umane e gli imperativi di tipo operativo.
- c. **Ottimizzazione delle risorse nelle operazioni interforze e multinazionali (Joint and Multinational Operation)**, la difesa CBRN deve considerare tutte le componenti delle Forze operanti nell'area di operazioni (JOA) e tenere conto di tutti gli aspetti della minaccia. Ogni sforzo deve essere profuso per ottimizzare gli assetti della difesa CBRN nel suo complesso, attraverso l'armonizzazione delle capacità con le quali le varie Nazioni contribuiscono, sia a livello operativo che tattico.
- d. **Attribuzione di priorità**, poiché è improbabile che le capacità esistenti consentano di proteggere tutti gli assetti con lo stesso grado di efficacia, la priorità più elevata dovrà essere assegnata a infrastrutture "critiche", ad alcuni particolari elementi della forza e ad assetti logistici.
- e. **Flessibilità**, allo scopo di rispondere con tempestività a una minaccia e un ambiente operativo in rapido mutamento.

La protezione delle forze è un'attività di gestione del rischio, basata sulla stima della minaccia, i

---

<sup>1</sup> *Chemical, biological, radiological and nuclear* (CBRN).

<sup>2</sup> *Explosive Ordnance Reconnaissance* (EOR).

<sup>3</sup> *Explosive Ordnance Disposal* (EOD).

<sup>4</sup> *Improvised Explosive Device Disposal* (IEDD).

cui risultati consentono di individuare le misure:

- di protezione collettiva;
- di sicurezza contro possibili minacce simmetriche/asimmetriche (es. azioni terroristiche);
- sanitarie.

Tuttavia, adottare misure eccessive di protezione, allo scopo di fronteggiare un’improbabile minaccia, può causare una dispersione delle limitate capacità e impedire l’esecuzione della missione.

Inoltre, la protezione delle forze in una coalizione multinazionale potrebbe risultare difficoltosa. Infatti, alcune Nazioni potrebbero imporre misure di protezione di livello più elevato e, in aggiunta, queste misure potrebbero cambiare in particolari situazioni.

## 2. **Componenti della Difesa CBRN**

La difesa CBRN garantisce la capacità necessaria ad assicurare la sopravvivenza in ambiente contaminato e, pertanto, è parte integrante della più ampia protezione delle forze. Allo scopo di garantire un elevato livello di sopravvivenza, la difesa CBRN deve essere flessibile, mobile, rapidamente schierabile e sostenibile.

Le cinque componenti della difesa CBRN, di seguito elencate, debbono essere concepite e implementate a premessa dell’operazione stessa mediante lo sviluppo di un’adeguata politica di base, di una specifica dottrina d’impiego, di equipaggiamenti efficienti, di tecniche tattiche e procedure (TTP<sup>5</sup>) aggiornate e di un addestramento alla difesa CBRN rigoroso e attagliato alla realtà operativa.

### a. **Individuazione, identificazione e monitoraggio (*Detection, Identification and Monitoring - DIM*)**

Le capacità DIM comprendono la rivelazione, caratterizzazione e misura di sostanze CBRN, l’identificazione dei pericoli associati e il controllo dei cambiamenti nel tempo.

### b. **Preavviso e segnalazione CBRN (*CBRN Warning & Reporting*)**

Il CBRN W&R consente la rapida raccolta, valutazione e diffusione dei dati che caratterizzano gli eventi di tipo CBRN, insieme alla previsione delle aree di pericolo che ne derivano, secondo quanto previsto dall’ATP-45(D)<sup>6</sup>. La diffusione dei dati e la previsione delle aree di pericolo sono consentite dai Sistemi di Comunicazione e Informazione (*Communication and Information System - CIS*).

### c. **Protezione fisica (*Physical Protection*)**

La protezione individuale e collettiva (*Collective Protection - COLPRO*) permette al personale di sopravvivere agli incidenti CBRN e di continuare a operare in ambiente CBRN. Comprende le misure per proteggere strutture ed equipaggiamenti, ad esempio anche mediante un particolare “*design*” (*CBRN hardening*).

### d. **Gestione del Pericolo (*Hazard Management*)**

Le misure di Gestione del Pericolo riducono l’impatto degli incidenti CBRN sulle operazioni. Tale attività è basata sui principi della “prevenzione” ovvero le precauzioni da

<sup>5</sup> *Tactics, Techniques and Procedures (TTP)*.

<sup>6</sup> STANAG 2103 “*Reporting nuclear detonations, biological and chemical attacks, and predicting and warning of associated hazards and hazard areas (operators manual) – ATP-45(D)*”

adottare prima che il pericolo si manifesti e del "controllo del pericolo", mediante l'adozione di misure volte a evitare il pericolo, a tenere sotto controllo la sua diffusione, a controllare l'esposizione del personale e a procedere alla eventuale decontaminazione.

e. **Sostegno sanitario e contromisure di natura sanitaria (*Medical Countermeasures and Support*)**

Contromisure di natura sanitaria (*Medical countermeasures* - MedCM) saranno adottate sia per ridurre la sensibilità del personale ai pericoli CBRN sia per trattare ed evacuare i colpiti. Anche il trattamento e l'evacuazione dei colpiti convenzionali in ambiente CBRN dovranno essere affrontati dalle suddette misure.

Sulla base delle diverse situazioni, tutte le componenti della difesa CBRN sopra elencate dovranno essere prese in considerazione. Tuttavia, sebbene le diverse tipologie di capacità possono essere in garantite, ad un certo livello, da tutte le unità, è necessario tenere presente che, allo scopo di garantire un più elevato livello di protezione delle forze, alcune capacità possono essere offerte solo dalle unità specialistiche. Il coinvolgimento di assetti specialistici di difesa CBRN, sin dalle prime fasi dello schieramento, costituirà un significativo elemento "moltiplicatore" della protezione delle forze.

### 3. **Rischio CBRN**

Il rischio CBRN è il risultato della combinazione delle probabilità di utilizzo di armi CBRN, da parte di forze avversarie e della magnitudo delle conseguenze di quest'utilizzo sulle persone e sull'ambiente nel quale potrebbe avvenire il rilascio.

Nel settore della sicurezza si preferisce l'utilizzo di una formula di derivazione militare più complessa, dove la Probabilità dell'evento (P) è scissa in due componenti: Minaccia (M) e Vulnerabilità (V), a loro volta misurate in termini di probabilità.

$$\text{Rischio CBRN (R)} = [\text{Minaccia (M)} \times \text{Vulnerabilità (V)}] \times \text{Conseguenze (C)}$$

In questa nuova formula:

- **Rischio (R):** è un numero, risultato della combinazione della probabilità di un intervento CBRN e della magnitudo delle conseguenze (unità di misura: basso, moderato, alto, estremo);
- **Minaccia (M):** è la misura della probabilità che uno specifico tipo di attacco sia portato contro uno specifico obiettivo;
- **Vulnerabilità (V):** è la misura della probabilità che vengano meno i dispositivi di sicurezza e sorveglianza predisposti per contrastare l'attacco;
- **Conseguenze (C):** rappresentano la misura della magnitudo degli effetti negativi, qualora un attacco abbia successo.

Per **armi CBRN** si intendono quei dispositivi che prevedono la dispersione di aggressivi chimici, agenti biologici, isotopi radioattivi o l'esplosione nucleare di materiale fissile allo scopo di produrre effetti mortali, inabilitanti per un significativo periodo di tempo o comunque dannosi su uomini e animali o interdire l'utilizzo di aree, strutture e materiali.

**a. Armi chimiche**

Sono costituite dall'insieme di un aggressivo chimico (sostanza chimica con effetti tossici ad azione rapida, lenta o ritardata) e di un opportuno dispositivo di rilascio correlato alla natura chimica della sostanza.

Per aggressivo chimico si intende una sostanza solida, liquida o gassosa in grado di produrre un elevato numero di perdite o di inabilitati nel personale, a seguito di inalazione di sostanze allo stato aeriforme, di assorbimento cutaneo e di ingestione di liquidi e di cibo contaminati.

Gli effetti di un attacco condotto con armi chimiche possono variare in funzione di alcuni fattori quali durata e quantità dell'aggressivo rilasciato, tipo di aggressivo, mezzo di rilascio, luogo del rilascio e condizioni meteorologiche se disperso all'aperto.

(1) Dal punto di vista fisico, in particolare, tali aggressivi si possono categorizzare in:

- persistenti (presenza superiore alle 24 h): nervini persistenti, vescicanti, incapacitanti;
- non persistenti (presenza inferiore alle 24 h): nervini non persistenti, soffocanti, tossici sistemici, irritanti, agenti anti-pianta.

(2) Dal punto di vista fisiologico, invece, si possono distinguere in:

- letali: nervini, tossici sistemici, vescicanti;
- non letali: soffocanti, irritanti, incapacitanti, agenti anti-pianta.

(3) In merito ai sistemi di dispersione utilizzati, che variano in relazione alla natura fisica dell'aggressivo e dell'agente, si possono menzionare:

- i generatori a pressione di aerosol liquido o solido;
- i dispersori a caduta di aerosol liquido o solido;
- i sublimatori;
- le granate di artiglieria, testate missilistiche, mine, bombe d'aereo, ecc..

**b. Armi biologiche**

Sono costituite da uno o più agenti biologici e da un opportuno mezzo di diffusione. Per agente biologico si intende un organismo (batterio, virus, rickettsia, fungo) o un prodotto del metabolismo di questi organismi (tossina) in grado di indurre una malattia, allo scopo di procurare un elevato numero di perdite o di inabilitati tra il personale, a seguito di inalazione, di contatto cutaneo o di ingestione di liquidi e di cibo contaminati.

Gli agenti biologici sono in grado di provocare malattie trasmissibili, ma solo alcune di queste possono definirsi contagiose, cioè trasmissibili direttamente da organismo malato a sano.

Caratteristica principale degli agenti biologici è il periodo di incubazione (periodo di latenza per le tossine), che rappresenta il periodo durante il quale non compaiono i sintomi della malattia, ma durante il quale risulterà maggiore il pericolo di contagio.

Tra i sistemi di dispersione utilizzati per gli agenti biologici si possono annoverare:

- l'aerosolizzazione (aerosol liquido o solido);
- i vettori animali (insetti: zanzare, mosche, pidocchi, ecc.);
- gli atti di sabotaggio (derrate e catena alimentare, impianti di distribuzione idrica);
- i vettori umani (impiego di aspiranti suicidi contaminati da infiltrare in luoghi affollati).



**c. Armi radiologiche**

Si identificano con sorgenti radioattive o materiali radiologicamente contaminati che, privi di sistemi di protezione o associati ad un dispositivo esplodente, comportano esposizioni a radiazioni ionizzanti di "basso livello" in grado di provocare un danno biologico di tipo "stocastico", rilevabile solo nel tempo e con valutazioni a carattere epidemiologico su un campione statisticamente significativo del personale esposto. I radioisotopi a breve, media e lungo periodo di dimezzamento, tutti emettitori " $\alpha$ ", " $\beta$ ", " $\gamma$ ", sono la causa di contaminazione di aria, acqua, terreno e polveri. Particolare attenzione deve essere posta nei confronti di quelli con tempi di dimezzamento superiori alle 24 ore.

**d. Armi nucleari**

Si definiscono come il complesso dell'ordigno (ogiva di missile, mina, bomba) dell'esplosivo nucleare e del relativo mezzo di lancio.

Gli ordigni possono essere a:

- fissione di nuclei atomici pesanti, come l'Uranio o il Plutonio;
- fusione (termonucleare) di nuclei leggeri, quali gli isotopi leggeri dell'Idrogeno;
- prevalente azione radiologica.

Gli effetti prodotti da una esplosione nucleare possono essere classificati in:

(1) effetti iniziali, che si verificano entro il primo minuto dall'esplosione:

- lambo di luce, in grado di provocare cecità nel personale presente;
- radiazione termica, che può determinare l'incendio o la carbonizzazione del materiale investito (in relazione alla natura del medesimo materiale e alla distanza dal punto di impatto);
- onda d'urto, che causa direttamente (sovrappressione dell'onda d'urto) la maggior parte dei danni materiali o indirettamente (caduta di fabbricati, proiezione di materiali) la maggior parte dei danni alle persone;
- radiazione nucleare iniziale, costituita, per lo più, da radiazioni gamma ( $\gamma$ ) e neutroni;
- impulso elettromagnetico (EMP)<sup>7</sup>, colpisce le apparecchiature elettriche, elettroniche, equipaggianti e impianti;

(2) effetti residui, i cui effetti si esauriscono in un tempo di gran lunga superiore:

- ricaduta radioattiva o "fall-out", ricaduta sulla superficie terrestre di particelle della nube generata dalla esplosione contaminate da materiale radioattivo;
- radiazione nucleare residua, rappresentata da particelle alfa ( $\alpha$ ) particelle beta ( $\beta$ ) e radiazioni gamma ( $\gamma$ ).

La radioattività non può essere eliminata, ma decade con il tempo. Il decadimento non può essere né accelerato né ritardato.

**e. Sostanze tossiche di origine industriale**

Alla minaccia militare conosciuta si è aggiunto un nuovo rischio, definito "**tecnologico-industriale**". Questo è associato al verificarsi di eventi, di origine dolosa o accidentale,

---

<sup>7</sup> Electromagnetic Pulse (EMP).

presso strutture prevalentemente civili (quali impianti produttivi, di stoccaggio e di ricerca che in qualsiasi fase del processo abbiano a che fare con sostanze pericolose) ove avvenga una dispersione di contaminante chimico, biologico o radiologico, risultante da cause diverse da attacchi con armi NBC. Analogamente a quanto avviene nel settore CBRN, sorge la necessità di adottare efficaci misure di prevenzione e protezione per la tutela dell'incolumità del personale e la prosecuzione delle attività. Per comprendere al meglio e valutare i possibili scenari connessi con il rischio tecnologico-industriale, bisogna tener conto dell'incremento e della diffusione di siti industriali produttivi e di laboratori di ricerca, e della conseguente creazione di un complesso sistema di trasporti di materie prime, prodotti intermedi e prodotti finiti, che costituiscono tutti delle potenziali fonti di contaminazione riconducibili al pericolo CBRN.

(1) Sostanze tossiche chimiche

In base alla quantità di sostanza chimica rilasciata nell'ambiente possiamo distinguere:

- rilascio di modeste quantità di prodotti chimici durante il trasporto o nei siti di stoccaggio;
- rilascio di grandi quantità (oltre 1500 kg) di prodotti chimici da raffinerie, industrie di sintesi, depositi di idrocarburi, ecc.. Premesso che in detti impianti sono presenti apparecchiature che operano in condizioni di pressione e temperatura diverse da quelle ambientali, le conseguenze del rilascio dipenderanno da tossicità, infiammabilità, potere esplosivo della sostanza coinvolta, oltre che dalle condizioni di pressione e temperatura di esercizio, nonché dalla quantità dispersa e dalle condizioni meteorologiche.

Gli eventi incidentali tipici ai quali, di norma, si fa riferimento sono i seguenti:

(a) incendio (irraggiamento) di:

- liquidi infiammabili contenuti in serbatoi a pressione atmosferica (*TANK-FIRE*);
- pozze di liquido al suolo derivanti da perdite da tubazioni e da recipienti (*POOL-FIRE*);
- gas/vapori effluenti ad alta velocità da un recipiente o da una tubazione (*JET-FIRE*);
- gas/vapori effluenti a bassa velocità (*FLASH-FIRE*);
- vapori in espansione a seguito del collasso di un recipiente contenente gas compressi in equilibrio con la fase liquida (*FIREBALL*);

(b) esplosione (onda d'urto) di:

- una nube in ambiente non confinato (*Unconfined Vapour Cloud Explosion - UVCE*);
- una nube di vapori infiammabili in ambiente confinato (*Confined Vapour Cloud Explosion - CVCE*);

(c) rilascio di sostanze tossiche/inquinanti (esposizione a sostanze tossiche):

- a bassa velocità, di gas con densità prossima a quella dell'aria (*PLUME, PUFF*);
- a bassa velocità, di gas con densità superiore a quella dell'aria (*DENSE GAS*);
- ad alta velocità, di gas tossici e/o infiammabili (*JET*);

(d) esplosione di gas liquidi (*irraggiamento - onda d'urto*): particolare tipo di evento che si verifica quando una sostanza, normalmente allo stato aeriforme, è conservata in un recipiente in pressione sotto forma di liquido in equilibrio con il suo vapore. Se il recipiente si rompe per una qualsiasi causa, il liquido tende a vaporizzare, aumentando istantaneamente il proprio volume, generando di conseguenza un'onda di pressione analoga a quella che si avrebbe in un'esplosione di tipo classico (*Boiling Liquid Expanding Vapour Explosion - BLEVE*). Se la sostanza è infiammabile, in caso di innesco, si ha la formazione di una palla di fuoco (*FIREBALL*).

(2) Sostanze pericolose di origine biologica

Può verificarsi una dispersione di sostanze pericolose di natura biologica da istituti di ricerca, industrie farmaceutiche, stabilimenti di produzione di vaccini ad uso commerciale, industrie nel settore alimentare, di trasformazione dei sottoprodotti di origine animale e della trasformazione dei rifiuti di origine animale.

(3) Sostanze radiologiche industriali

Sin dal 1997 in Italia il "Piano nazionale delle misure protettive contro le emergenze radiologiche" individuava la tipologia di emergenza radiologica o nucleare proveniente da:

- centrali elettronucleari italiane in fase di disattivazione;
- centrali elettronucleari oltre frontiera comportanti ricadute radioattive sul suolo nazionale;
- natanti a propulsione nucleare, inclusi i sommergibili, che incrociano in prossimità delle coste italiane;
- centri di ricerca, stabilimenti nucleari, o luoghi in cui comunque si detengono o si impiegano sostanze radioattive, ovvero nel corso del trasporto di dette sostanze;
- satelliti precipitati al suolo con sistemi nucleari a bordo;
- eventi incidentali derivanti da attività non conosciute a priori.
- In particolare, le possibili fonti di approvvigionamento del materiale radioattivo di origine industriale sono molteplici:
  - sorgenti in uso in campo medico-sanitario (Co60, Cs137, Sr90);
  - sorgenti in uso nel settore industriale per misurazioni di livello, densità, spessore (Ir192, Cs137, Co60);
  - parafulmini (Am241, Ra226);
  - apparati per gammagrafie, sterilizzatori di farmaci ed alimenti, rilevatori di fumo);
  - sorgenti "orfane";
  - impianti nucleari dimessi;
  - depositi di rifiuti radioattivi.

#### 4. **Principi di Force Protection e componenti della difesa CBRN**

##### a. **Principi di Force Protection applicati alla difesa CBRN**

Le misure di difesa CBRN, da implementare in relazione alla situazione contingente, si basano sull'adozione dei **principi** di seguito descritti.

(1) Acquisizione delle informazioni

Un accurato ed efficiente servizio di *Intelligence* risulta essere imprescindibile e alla base di tutte le ulteriori contromisure. Tale servizio dovrà essere in grado di fornire ogni aggiornamento riguardante la capacità CBRN delle forze avversarie e la situazione relativa a potenziali siti di rilascio di sostanze tossiche di origine industriale (TIM) presenti nell'area di operazione e zone limitrofe.

(2) Preparazione delle Forze

Le Forze devono essere messe in condizione di conoscere i termini della minaccia CBRN e di avere ricevuto, prima dell'immissione in Teatro, adeguato addestramento finalizzato alla conoscenza dell'organizzazione della difesa CBRN nonché all'utilizzo delle corrette procedure, degli equipaggiamenti e degli strumenti idonei alla difesa CBRN.

(3) Analisi e prevenzione

La miglior risposta consiste nell'anticipare qualsivoglia rischio e di conseguenza pianificare, riconoscere e gestire la situazione per garantire libertà di azione all'interno del Teatro.

(4) Flessibilità, integrazione e coordinamento

La massima flessibilità garantisce la miglior risposta a una minaccia CBRN che si presenta estremamente diversificata. A garanzia del miglior risultato, sarà da ricercare la stretta cooperazione e coordinamento tra tutte le componenti presenti in Teatro, comprese le Agenzie non governative e i Governi locali.

(5) Sostenibilità

Particolare attenzione, in fase di pianificazione, deve riguardare la protezione della catena logistica, particolarmente gravata dalle accresciute richieste e da malfunzionamenti dovuti ad attacchi.

##### b. **Componenti della difesa CBRN**

Le **componenti della difesa CBRN** descritte nel presente documento, preannunciate al para. 2., sono le medesime riconosciute in ambito NATO (vds. Pubblicazione Alleata AJP 3.8<sup>8</sup>).

La corretta applicazione di tali componenti permette alle Forze operanti in ambiente contaminato CBRN di portare a termine la propria missione, limitando gli effetti e le conseguenze dell'offesa CBRN.

(1) Individuazione, identificazione e monitoraggio

Hanno lo scopo di accertare la presenza di contaminazione CBRN, di identificare l'agente (o l'aggressivo) e di monitorare l'evolvere della situazione.

L'individuazione permette di accertare al più presto la presenza di un pericolo CBRN, per consentire l'adozione in tempo utile delle appropriate misure di difesa. Tale attività

---

<sup>8</sup> STANAG 2451 "Allied Joint Doctrine for NBC Defence – AJP-3.8".

viene espletata tramite tecniche di ricognizione e sorveglianza, condotte con strumentazione in grado di segnalare la presenza del contaminante sia sul luogo dell'evento (*Point detection*) sia a distanza dallo strumento (*Stand-off detection*).

L'identificazione è la determinazione del tipo di agente (o di aggressivo) CBRN. Essa viene acquisita attraverso 3 livelli di indagine di differente affidabilità:

- presunta (*provisional*), che garantisce un primo ed immediato avviso;
- confermata (*confirmed*), che fornisce certezza;
- inequivocabile (*unambiguous*), che assicura una certezza oltre ogni dubbio.

Alla base di questa componente c'è il campionamento, inteso come la raccolta di materiale condotta da personale specializzato NBC, opportunamente addestrato per garantire uniformità, facilità, sicurezza ed affidabilità delle procedure.

L'applicazione delle corrette norme di campionamento di materiali contaminati e l'analisi condotta con tecniche standardizzate in idonei laboratori campali o di riferimento, consente l'identificazione dell'agente CBRN disperso.

Il monitoraggio è il processo con cui si segue l'andamento nel tempo della presenza di un agente CBRN e serve per adeguare le misure di protezione del personale.

L'attività di monitoraggio, consistente in attività di controllo continuo o periodico dell'area di interesse, deve essere condotta con idonea strumentazione, soprattutto *Stand-off*, per consentire di mantenere un livello di protezione adeguato alla minaccia effettivamente accertata. In funzione dei livelli di minaccia, particolare attenzione deve essere posta nella dislocazione di sentinelle e di idonea strumentazione in grado di segnalare immediatamente la presenza di pericoli CBRN, consentendo la diffusione dei relativi allarmi locali e generali.

## (2) Preavviso e Segnalazione CBRN

Processo attraverso il quale l'allarme e le ulteriori informazioni vengono diramate nei due sensi lungo la catena di comando.

A seguito di attacco CBRN, le procedure prevedono la diffusione di allarmi locali e l'invio, la valutazione e la validazione di tutte le informazioni relative ad eventi CBRN, compresa l'elaborazione di previsioni e carte aggiornate delle aree di pericolo, utilizzando le procedure standardizzate NATO fornite dall'ATP-45(D).

L'allarme vero e proprio può essere preceduto, ove possibile, da un preavviso o un preallarme, che comportano l'adozione delle opportune misure preventive.

Per quanto riguarda i tipi di allarme, questi possono appartenere a due diverse tipologie di seguito illustrate.

- (a) Allarme locale, che interessa singolarmente ciascuna minore unità, in quanto destinato a garantire la sicurezza immediata del proprio personale.

Ciascun reparto provvede mediante i segnali acustici e visivi previsti dallo STANAG 2047<sup>9</sup>, che debbono essere conosciuti da tutto il personale. Particolarmente addestrati ad usare e riconoscere tali segnali debbono essere: sentinelle, vedette, personale specializzato o abilitato NBC e addetto alle trasmissioni;

<sup>9</sup> STANAG 2047 "Emergency alarms of hazard or attack (NBC and air attack only)".

(b) Allarme generale, che deve essere rapidamente inoltrato, mediante i sistemi di comunicazione ed informazione, utilizzando le procedure previste dalla citata Pubblicazione Alleata ATP-45(D).

(3) Protezione fisica

Seppure con decremento della prestazione operativa, permette all'individuo di continuare ad operare in ambiente contaminato CBRN.

La protezione fisica delle Forze può essere conseguita sia individualmente, indossando gli indumenti di protezione, sia collettivamente attraverso l'utilizzo di ricoveri adeguatamente equipaggiati (*Collective Protection* - COLPRO).

L'utilizzazione degli equipaggiamenti di protezione individuali comporta una riduzione della capacità operativa del personale (minore abilità, affaticamento, stress psico-fisico), che comporta una revisione sia dei carichi di lavoro e sia del numero del personale necessario all'assolvimento del compito assegnato.

Per contenere tale riduzione e garantire flessibilità alla manovra, sono stati individuati livelli di indossamento da adottare, a discrezione del Comandante dell'unità, in funzione della minaccia presente nella propria Area di Responsabilità.

Per operare in zone contaminate da sostanze tossiche di origine industriale (TIM), stante la inidoneità dell'equipaggiamento militare in dotazione contro tali sostanze, il personale deve indossare appositi dispositivi di protezione individuale (*Individual Protective Equipment* - IPE).

Le strutture di protezione collettiva (COLPRO), fisse, mobili o trasportabili possono consentire da un lato di ospitare in sicurezza funzioni particolarmente sensibili come C2, trasmissioni, sanitarie e dall'altro di costituire luogo di ristoro e di riposo per il personale operante in ambiente contaminato.

(4) Gestione del rischio

Attività complessa che consiste nell'evitare e/o minimizzare i pericoli conseguenti ad una contaminazione CBRN.

La gestione del rischio prevede una serie di misure precauzionali atte ad evitare il contatto con agenti contaminanti e, qualora inevitabile, una serie di procedure che ne limitino la diffusione e gli effetti.

Tali provvedimenti hanno lo scopo di diminuire il grado di vulnerabilità dei reparti, senza ricorrere all'impiego di mezzi protettivi specifici e comprenderanno misure quali diradamento, manovra a ritmi serrati e su ampi spazi, autonomia operativa fino ai minori livelli, sfruttamento del terreno e delle condizioni meteorologiche, occultamento, mascheramento e inganno.

Inoltre, devono risultare oggetto di attenta valutazione la scelta di vie tattiche e di itinerari, così come le circostanze e i tempi di abbandono di posizioni contaminate e delle protezioni, anche di fortuna, disponibili. Analogamente, in fase di pianificazione, è opportuno esaminare la necessità di perseguire la ridondanza di materiali, strumentazione ed equipaggiamenti e di implementare accorgimenti preventivi particolari come, ad esempio, il prelavaggio per le unità navali.

Qualora le misure preventive non abbiano sortito alcun risultato e sia rilevata la presenza di contaminazione, devono essere messe in opera procedure che permettano di

limitarne la diffusione. Tra queste:

- evitare il pericolo ovvero la segnalazione standardizzata delle zone contaminate, la sorveglianza dei movimenti in/da zone pericolose, la pianificazione di percorsi e zone di rischiarimento alternativi e la scelta di percorsi obbligati per personale contaminato;
- sorveglianza della diffusione attraverso la limitazione dei movimenti intorno alle aree di pericolo, il contenimento fisico della contaminazione, la creazione di zone di quarantena in caso di malattie trasmissibili e la gestione di materiali contaminati o residui provenienti da operazioni di bonifica;
- gestione del personale esposto evitando o riducendo il più possibile, limitando a compiti critici (salvataggio di vite umane), l'esposizione ad agenti CBRN e TIM, raccogliendo, ai fini sanitari, i dati del personale a rischio e stabilendo turni di rotazione degli assetti;
- decontaminazione ovvero la riduzione, il contenimento a livelli accettabili o la completa e assoluta eliminazione di un agente CBRN da personale, materiali o aree.

I principi guida della decontaminazione di personale, materiali e mezzi delle unità contaminate da agenti CBR e/o TIM sono:

- ***decontaminare il più presto possibile*** per ripristinare quanto prima la capacità operativa dell'unità;
- ***decontaminare solo quello che serve*** per non sprecare decontaminante e impiegare in maniera vantaggiosa e opportuna personale, mezzi e tempo;
- ***decontaminare il più avanti possibile*** per limitare la diffusione della contaminazione rispetto alle proprie posizioni;
- ***decontaminare secondo delle priorità*** per gestire al meglio equipaggiamenti e assetti chiave (aerei, elicotteri, equipaggi volo, ecc.), decontaminandone prima le parti essenziali.

La decontaminazione può essere condotta a tre diversi livelli:

- ***immediata***, eseguita subito dopo la contaminazione a livello individuale, allo scopo di salvare la vita dei colpiti e limitare la diffusione ulteriore della contaminazione. Consiste nel decontaminare la pelle e l'equipaggiamento individuale (*Individual Protective Equipment* - IPE). Viene eseguita da tutto il personale;
- ***operativa***, effettuata allo scopo di ridurre il pericolo da contatto, limitare la diffusione della contaminazione e consentire il prosieguo della missione. Questo tipo di decontaminazione è condotta su parti specifiche di materiali, equipaggiamenti, mezzi e aree di lavoro essenziali ai fini dell'operatività. È di norma eseguita dal personale dei nuclei di bonifica delle unità;
- ***approfondita***, eseguita per eliminare completamente il contaminante e quindi evitare o limitare la necessità di indossare l'IPE. In particolare, consiste nel lavaggio degli individui, degli equipaggiamenti e dei veicoli. Può essere effettuata solo dalle unità specialistiche (plotone bonifica della compagnia difesa NBC), presso la stazione campale di decontaminazione.

In aggiunta a questi tre livelli di decontaminazione, effettuati dalle unità militari, può esserne preso in considerazione un quarto, per la decontaminazione definita **certificata** (**CLEARANCE**). Si tratta di un livello di decontaminazione che può dover essere condotta nel caso di temporaneo o definitivo disimpegno di materiali e mezzi dal Teatro di Operazioni. L'attività risulta molto dispendiosa in termini di risorse e tempi di esecuzione, in quanto deve consentire il rilascio di una "certificazione" che garantisca il raggiungimento dei previsti standard internazionali, al fine di ottenere il permesso per varcare i confini tra i diversi Stati. Materiali e mezzi così decontaminati potranno essere re-impiegati senza restrizioni. Per la sua complessità, non è di norma svolta da unità militari, ma ci si avvale di organizzazioni civili specializzate in possesso di elevata competenza tecnica, con l'eventuale concorso di personale degli Enti Tecnici della Difesa e delle unità specialistiche NBC.

(5) Sostegno sanitario e contromisure di natura sanitaria

Il sostegno sanitario è di fatto implicato in tutte le componenti di difesa CBRN.

I sistemi di sorveglianza medica, così come la diagnostica, sono da considerarsi una componente del DIM e la conoscenza completa della reale situazione sanitaria (da parte dello Staff sanitario) può contribuire all'analisi dei dati forniti dall'*Intelligence* per le ulteriori decisioni in merito alle attività di preavviso e segnalazione. Inoltre, le unità mediche, dotate di sistemi di protezione collettiva, concorrono alla sopravvivenza delle unità che operano in ambiente CBRN, fornendo protezione fisica a personale sanitario e personale colpito. Inoltre, lo stesso personale medico può fornire qualificato supporto nella gestione del pericolo.

Lo *staff* sanitario, di concerto con il personale addetto alla difesa CBRN e all'*Intelligence*, concorre alla valutazione della minaccia CBRN, stimando le vulnerabilità e le capacità necessarie a ridurre il numero di personale colpito quando esposto ad eventi CBRN durante operazioni militari. Al fine di realizzare l'analisi delle vulnerabilità, devono essere presi in considerazione diversi aspetti, quali:

- dati epidemiologici;
- dati sanitari pre-dispiegamento;
- principi di protezione sanitaria delle Forze;
- *Intelligence* medica.

I principi del sostegno sanitario in ambiente CBRN vengono sviluppati nello STANAG 2873<sup>10</sup>.

Le contromisure di natura sanitaria riducono gli effetti sul personale esposto o potenzialmente esposto a sostanze CBRN. Queste comprendono non solo il trattamento medico di personale colpito da agenti CBRN, ma anche tutte quelle misure preventive mediche quali le misure di pre-trattamento, post-trattamento, la gestione di personale colpito in ambiente CBRN e la loro evacuazione, nonché l'adozione di severe misure igienico-profilattiche di sorveglianza e di limitazione alla circolazione per il personale

---

<sup>10</sup>STANAG 2873 "Concept of operations of medical support in chemical, biological, radiological and nuclear environments - AMedP-07".



potenzialmente esposto.

Inoltre, lo *staff* medico dovrà:

- predisporre una raccolta individuale e accurata dei dati clinici del personale in operazioni, per la creazione di una banca dati idonea ad assicurare nel lungo termine il monitoraggio relativo allo stato di salute del personale potenzialmente esposto;
- approntare un successivo programma di assistenza per il personale già esposto.

## 5. **Livelli di difesa CBRN (individuale/unità/unità specialistiche)**

La difesa CBRN ha lo scopo di evitare o quantomeno ridurre il più possibile le perdite e i danni conseguenti ad attacchi CBRN, in modo da consentire ai singoli individui ed ai reparti di continuare a svolgere il proprio compito nelle migliori condizioni di efficienza possibile, anche in ambiente contaminato.

La complessità tecnica acquisita nel tempo dall'attività CBRN ha determinato la necessità di disporre, in aggiunta alle capacità esistenti presso i reparti operativi, anche di realtà altamente specializzate in grado di sviluppare al massimo livello tutte le attività di difesa CBRN. Pertanto, possono essere presi in considerazione tre livelli di difesa NBC:

- individuale;
- unità operativa;
- unità specialistica NBC.

In particolare, l'organizzazione della difesa CBRN in ambito Esercito si fonda sui seguenti criteri:

- attribuire la responsabilità della difesa CBRN ai Comandanti a tutti i livelli, i quali si avvalgono di quadri addetti alla specifica branca;
- conferire:
  - a tutto il personale, la capacità di sopravvivere agli attacchi CBRN e di concorrere alla difesa CBRN di reparto;
  - alle unità operative, la capacità di svolgere tutte le attività di difesa CBRN, sebbene non al massimo livello;
  - alle unità specialistiche NBC, la possibilità di svolgere tutte le attività di difesa CBRN ad integrazione e/o concorso di quelle svolte dalle unità non-specialistiche.

Pertanto, risulta di fondamentale importanza, per il Comandante ed il proprio *staff*, l'essere in possesso di un quadro chiaro delle potenziali capacità ai vari livelli operativi. In particolare, debbono essere note le capacità di difesa NBC, ai livelli di seguito indicati.

### a. **Individuale**

Per quel che riguarda la difesa CBRN a livello individuale si rimanda alla Pubblicazione N. 6620 "Manuale di difesa NBC" (Ed. 2011).

### b. **Unità operativa**

L'organizzazione della difesa CBRN nelle unità operative dell'E.I., al fine di consentire l'attuazione dei provvedimenti di ordine tecnico, prevede tre diversi livelli ordinativi (equivalenti per M.M. e A.M.): compagnia, reggimento/battaglione, Grande Unità con

compiti e capacità descritte nelle pubblicazioni di singola F.A. che fanno riferimento allo STANAG 2521 ATP-3.8.1 Vol. I.

**c. Unità specialistica NBC**

Per quel che riguarda la difesa NBC a livello di unità specialistica NBC si rimanda a:

- Pub. N. 6588 "Impiego del reggimento di difesa NBC in Operazioni" (Ed. 2011);
- STANAG 2522<sup>11</sup>.

**6. Aspetti legati all'ambiente navale ed aereo**

**a. Ambiente Navale**

Per il personale destinato ad Enti a terra o truppe anfibie che si trovino ad operare in zona di operazioni vale quanto descritto per l'Esercito. Considerando, invece, l'ambiente navale, la minaccia CBRN nei confronti di unità navali e di sottomarini che operano in mare aperto differisce sostanzialmente da quella cui sono esposte unità operanti in prossimità della costa o stazionanti in porto.

Navi e sottomarini che operano in mare aperto sono meno vulnerabili ad attacchi condotti con armi biologiche o chimiche, mentre risultano comunque estremamente vulnerabili ad attacchi con armi nucleari. Inoltre non è da sottovalutare l'eventualità di contaminazione dovuta a velivoli imbarcati su una unità navale che, trovandosi ad attraversare una zona contaminata, necessitano di tornare a bordo dell'unità stessa.

In porto o sottocosta, invece, navi e sottomarini sono particolarmente vulnerabili a:

- attacchi terroristici condotti con armi CBR/TIM o con azioni di sabotaggio su riserve di acqua potabile o di aria all'interno delle unità navali;
- attacchi CBRN dal litorale, in prossimità di stretti o da riva di fiumi, condotti da piccole imbarcazioni, con unità in navigazione in acque ristrette;
- rilasci di TIM da petroliere o navi mercantili;
- attacchi o rilasci nel corso dello svolgimento di operazioni anfibie;
- dispersione o rilascio di agenti CBR, da terra o da piccole imbarcazioni in mare, con unità ferma in porto.

In generale la minaccia asimmetrica a navi e sottomarini, legata all'uso di agenti CBRN, è maggiormente probabile in porti/sottocosta piuttosto che in mare aperto. In entrambi i casi la difesa CBRN rappresenta un requisito fondamentale per la sicurezza della nave stessa.

La contaminazione a bordo rappresenta una seria minaccia. Al riguardo, specifici piani e procedure devono essere pianificati e adottati per mantenere l'efficienza dell'unità e per facilitarne il contenimento e l'eliminazione.

Il controllo della contaminazione consiste nell'adozione delle procedure necessarie ad evitare, ridurre, rimuovere o rendere innocue, temporaneamente o permanentemente, contaminazioni CBR, allo scopo di sostenere o aumentare le capacità di condotta delle operazioni da parte delle unità navali.

Dal punto di vista tecnico, il controllo della contaminazione è supportato dalla presenza di:

<sup>11</sup> STANAG 2522 "Specialist NBC defence capabilities – ATP-3.8.1 Volume II".

- **apparati automatici per l'individuazione e l'allarme di agenti (o aggressivi) CBRN:** consentono, sulle unità che ne sono dotate, l'individuazione degli agenti e/o degli aggressivi utilizzati dall'avversario;
- **impianto di prelavaggio:** ha lo scopo di proteggere la nave, mediante un film sottile di acqua nebulizzata, dal pulviscolo radioattivo, dagli aggressivi chimici e dagli agenti biologici;
- **stazione di decontaminazione:** consente l'attuazione delle procedure di decontaminazione del personale che ha operato all'esterno, per poter accedere in sicurezza all'interno dell'unità;
- **sistemi di filtro pressurizzazione:** creano una pressione di aria, in particolari zone e locali all'interno dell'unità navale, superiore a quella esterna, al fine di non permettere l'ingresso di sostanze contaminanti all'interno della cittadella;
- **cittadella:** è l'insieme dei compartimenti interconnessi e contenuti in una struttura a tenuta stagna ove l'aria viene filtrata e messa in ricircolo. L'integrità è garantita dalla sovrappressione interna dell'aria che impedisce, qualora sia compromessa la tenuta stagna dei compartimenti che ne fanno parte, rientranze di aria contaminata dall'esterno.

Le unità navali prive degli impianti fissi di protezione collettiva possono, comunque, venire a trovarsi nelle condizioni di operare in aree a rischio CBRN. Al riguardo, una efficace barriera alla contaminazione CBRN potrà essere garantita dalla predisposizione di sistemazioni di "fortuna" (oculato ed appropriato uso della portelleria stagna, delle serrande di estrazione e ventilazione, ecc.).

Il "Comando e Controllo" nella Difesa NBC è inserito nel contesto delle azioni per il Controllo del Danno della Difesa Passiva; per la descrizione delle figure chiave ed i relativi incarichi previsti per la Difesa NBC si rimanda alla pubblicazione "CAAMM 255 – Manuale applicativo per il controllo del danno e la difesa passiva" del Centro di Addestramento Aeronavale della Marina Militare (Ed. 2006).

Sotto il profilo strettamente operativo, l'impatto di operazioni condotte in ambiente CBRN è legato alla tipologia di operazione in corso. In particolare, devono essere osservate le seguenti predisposizioni:

- diramazione dell'allarme e previsione della contaminazione: avvalersi delle procedure riportate nella pubblicazione alleata ATP-45(D);
- operazioni di interdizione marittima (*Maritime Interdiction Operations* - MIO): qualora si sospetti una possibile contaminazione, far intervenire personale specialista e predisporre piani per la decontaminazione o condurre la nave verso un porto distante da aree popolate;
- soste in porto: in caso di incidente CBRN, le navi devono bloccare i sistemi di ventilazione ed eseguire controlli sanitari e di qualità riguardo ogni fonte di approvvigionamento di acqua potabile. In assenza di COLPRO (cittadella), attivare una stazione temporanea di decontaminazione;
- operazioni anfibe: eseguire la pianificazione e l'individuazione, a priori, delle unità addette alla raccolta dei colpiti (soccorso sanitario), dello stoccaggio dei materiali contaminati ed evitare che personale e materiali contaminati siano imbarcati;

- problemi derivati da velivoli imbarcati: occorre prevedere una gestione separata dei velivoli contaminati da quelli puliti, tenendo in considerazione la possibilità di contaminazione per gli addetti al supporto logistico, limitandone i movimenti (esterno/interno hangar) prima di una parziale decontaminazione.

Occorre inoltre tenere in considerazione gli aspetti logistici legati allo stoccaggio degli IPE a bordo delle unità navali, sia prima dell'utilizzo che una volta contaminati, nonché degli indumenti di immersione per gli operatori OSSALC<sup>12</sup> che siano intervenuti in acqua contaminata.

**b. Ambiente Aereo**

Le basi aeronautiche, sia per la loro nota dislocazione sia per le ampie dimensioni, offrono un facile obiettivo ad armi CBRN, rappresentando un appetibile obiettivo in particolare quando i velivoli sono a terra. Pertanto, la difesa CBRN nell'aeronautica si articola su misure basate sul rafforzamento delle strutture, sull'ampio ricorso a sistemi di protezione collettiva (COLPRO) e, quando possibile, sull'utilizzo di strutture alternative, qualora la base principale dovesse essere contaminata.

Attacchi con armi e dispositivi CBRN possono essere portati con l'ausilio di aerei e missili da crociera (della tipologia *cruise*) o anche da terra da parte di forze speciali, terroristi/insorgenti e sabotatori.

La ricaduta sull'operatività a seguito di attacco CBRN incide, in particolare, sull'utilizzo delle infrastrutture, in quanto è opportuno valutare il rapporto costo/efficacia nello sforzo necessario alla decontaminazione dei siti.

In particolare, si deve tener conto che un lavaggio integrale delle installazioni appare vantaggioso solo se è possibile gestirne i residui; in caso contrario ne consegue di lavarne solo una piccola porzione nella quale concentrare più funzioni.

Per quel che riguarda la decontaminazione di velivoli sia ad ala fissa sia ad ala rotante sono da tenere in considerazione:

- il completamento delle operazioni di decontaminazione di superfici porose o permeabili entro un'ora dalla contaminazione;
- l'assorbimento dell'aggressivo chimico entro 10 minuti da parte di superfici porose, verniciate o di gomma. Tale assorbimento, pur diminuendo il rischio da contatto, prolunga il tempo di rilascio di vapori pericolosi e la decontaminazione non sarà in grado di rimuovere l'agente una volta che questo viene assorbito dalle superfici;
- le superfici lisce sono relativamente semplici da decontaminare, ma gli agenti chimici si posizionano su fessure, rivetti, giunture;
- le soluzioni a base di cloro rappresentano la scelta migliore tra le sostanze decontaminanti, ma, su superfici verticali, non garantiscono un tempo di aderenza efficace;
- il miglior metodo di decontaminazione della superficie esterna di un velivolo è il volo a bassa quota per un periodo non inferiore a 60 minuti a velocità inferiori a quella del suono;

---

<sup>12</sup> Operatori del Servizio Sicurezza abilitati al lavoro in carena (OSSALC).

- un metodo alternativo è rappresentato dalla decontaminazione con aria calda forzata (nel caso di aggressivi chimici non persistenti);
- per la decontaminazione dell'interno dei velivoli non sono disponibili metodi sicuri. Pertanto è preferibile, in ragione delle esigenze d'impiego, condurre una decontaminazione di tipo operativo, che consiste nel rivestire con protezioni le parti contaminate e decontaminare la strumentazione con i mezzi più idonei disponibili, pur tuttavia contrassegnandola come contaminata, per i successivi interventi;
- la riduzione delle prestazioni del personale di terra che indossa l'IPE può variare dal 20 al 60%, soprattutto in relazione alle condizioni climatiche.

## 7. Elementi di particolare interesse per la condotta di operazioni in ambiente CBRN

### a. Livelli di minaccia

Affinché i Comandanti a tutti i livelli possano adottare le misure di difesa CBRN più idonee, è necessario che dispongano di situazioni accurate e aggiornate sulla minaccia e il rischio CBRN e informazioni su incidenti CBRN e sui pericoli a essi associati.

La **valutazione della minaccia** è basata su informazioni aggiornate e provenienti da varie fonti e deve essere continuamente condotta e rivista, in modo tale che le capacità e le misure di difesa CBRN possano essere individuate e variate a seconda della specifica esigenza e dei livelli di minaccia stabiliti.

La valutazione della minaccia CBRN consente al Comandante di determinare i "**livelli di minaccia**" CBRN e, in funzione di questi livelli, sarà possibile stabilire l'entità della protezione CBRN individuale e collettiva che dovrà essere adottata dalle unità.

I Comandanti, a tutti i livelli, debbono conservare una sufficiente flessibilità, allo scopo di poter bilanciare l'incremento delle misure di protezione con la riduzione di prestazioni che da esso deriva.

I livelli di minaccia per i rischi dovuti ad armi CBRN e TIM sono descritti, rispettivamente, nello STANAG 2521<sup>13</sup>.

Pertanto, nello stabilire le specifiche misure di protezione individuale e collettiva, i Comandanti "locali" dovranno tener conto dei seguenti elementi:

- **missione**. Maggiore è l'importanza del compito assegnato, maggiore sarà il rischio che dovrà essere accettato, per evitare che una protezione eccessiva comprometta l'assolvimento della missione nei tempi previsti;
- **posizione del personale**. La protezione fisica da garantire al personale influenzerà la vulnerabilità del singolo individuo. Ad esempio, il personale deputato ad agire sotto copertura potrebbe non aver bisogno di guanti e sopraccalzari, come il personale all'interno di sistemi di protezione collettiva normalmente non avrà bisogno di indossare l'equipaggiamento di protezione individuale;
- **condizioni meteorologiche**. La temperatura e l'umidità rappresentano fattori che influenzano il livello di stress da calore che si genera indossando l'equipaggiamento individuale di protezione CBRN;

---

<sup>13</sup> ATP-3.8.1 Vol I. "CBRN Defence on Operations".

- **sforzo fisico dell'attività.** Lo sforzo fisico, associato ad un determinato compito, ha un effetto diretto sulla riduzione della prestazione, soprattutto ove si renda necessario indossare l'equipaggiamento di protezione. Se uno sforzo fisico intenso è associato a un'elevata temperatura, il rischio di perdite da "colpo di calore" sarà particolarmente elevato. Si deve, pertanto, tenere conto di opportuni cicli di lavoro/riposo ed adeguato reintegro dei liquidi come indicato nello STANAG 2499<sup>14</sup>.

Allo scopo di garantire l'efficacia del sistema, per ciascuna operazione dovranno essere chiaramente individuate le responsabilità per fissare i "livelli di minaccia" e per innalzarli o ridurli, nonché le procedure per diramare tale informazione.

**b. Attivazione della rete di segnalazione e preavviso**

In operazioni, sia di tipo "Article 5" che di tipo "Non- Article 5" (CROs), dovrà essere garantito il rapido flusso della messaggistica prevista dalla Pubblicazione Alleata ATP-45(C) sulla base della direttiva di AJFC Naples n. 80-12<sup>15</sup>.

In funzione della particolare situazione, dovranno essere individuati i vari livelli di responsabilità, prevedendo la costituzione di Centri e Sottocentri di raccolta e di Posti di Osservazione che consentano di segnalare tempestivamente eventi riguardanti punti di particolare interesse operativo e strategico.

**c. Sorveglianza CBRN**

Tutte le unità militari, in funzione del "livello di minaccia CBRN/TIM" previsto nell'Area di Operazioni, dovranno prevedere la predisposizione e l'attuazione di misure di sorveglianza CBRN, mediante l'impiego di personale specificamente addestrato e di strumentazione per l'individuazione (anche a distanza) di sostanze pericolose. Quanto precede, sia nelle situazioni "statiche" (nelle aree di sosta o nelle zone di raccolta), sia in quelle "dinamiche" (movimenti e trasferimenti vari), allo scopo di garantire la tempestività nell'individuazione di pericoli di tipo CBRN e l'adozione delle più adeguate misure di protezione individuale e collettiva.

**d. Gestione dell'esposizione ai pericoli CBRN**

L'esposizione delle forze ai pericoli di tipo CBRN può avere un effetto immediato o a lungo termine sul personale. Ogni cura dovrà essere posta, da parte dei Comandanti a tutti i livelli, per evitare esposizioni non necessarie del personale ai pericoli CBRN. Quando a causa delle priorità di tipo operativo non sarà possibile evitare completamente il pericolo, l'esposizione dovrà essere la più limitata possibile, applicando il principio "ALARA" (*As Low As Reasonably Achievable*). Eventuali esposizioni del personale a pericoli CBRN dovranno essere registrate, per consentire l'oculato impiego del personale nel breve e lungo termine.

(1) Contaminazione radiologica - Linee guida per l'esposizione alle radiazioni

I Comandanti hanno la responsabilità per la protezione del proprio personale. Tale incombenza richiede equipaggiamenti e procedure adeguate per l'individuazione, il controllo e la gestione del rischio di esposizione alle radiazioni ionizzanti. I vari livelli di esposizione alle radiazioni (*Radiation Exposure States - RES*), previsti dagli

<sup>14</sup> ATP 65 "The effect of wearing CBRN individual protection equipment on individual and unit performance during military Operations."

<sup>15</sup> Southern Region Directive (SRD) 80-12 "NBC reporting organization and reporting system in the Southern Region".

STANAGs 2083<sup>16</sup> e 2473<sup>17</sup>, forniscono l'indicazione delle misure da prendere al crescere delle dosi di radiazioni assorbite dal personale.

Quando risulta impossibile evitare l'esposizione, a causa delle situazioni operative, questa deve essere la più bassa possibile. Nel caso di operazioni con contingenti multinazionali, è possibile che si debbano applicare regole diverse per le unità delle varie Nazioni, per quanto riguarda l'esposizione alle radiazioni ionizzanti. In caso di operazioni che prevedano una potenziale minaccia di tipo radiologico, dovranno essere fornite delle direttive specifiche, che indichino chiaramente il limite massimo di esposizione accettabile per tutto il personale interessato. La SOP del reparto dovrà fornire indicazioni su questo limite massimo di dose.

I Comandanti dovranno assicurarsi che:

- le esposizioni a radiazioni vengano registrate mediante dosimetri dati in distribuzione al personale;
- l'esposizione delle unità alle radiazioni vengano controllate attraverso lo Stato di Esposizione alle Radiazioni (RES), in modo tale che le radiazioni assorbite vengano distribuite tra i vari reparti. Regole diverse si applicano nel caso di operazioni di tipo "War" e in quello di "Non Article V Crisis Response Operations" (CROs);
- misure di controllo dell'esposizione alle radiazioni devono riflettere il bisogno di bilanciare la cura degli individui (tenendo conto sia degli effetti immediati che di quelli nel lungo termine) con il compimento della missione;
- il rischio totale è dovuto alla somma di tutti i rischi: convenzionale, ambientale, radioattivo e legato al combattimento. Tuttavia, il principio essenziale che dovrà essere applicato all'esposizione alle radiazioni è quello di mantenere tali esposizioni le più basse possibile (ALARA).

Le operazioni militari possono richiedere il **superamento** dei limiti di dose previsti dalla **normativa nazionale** del tempo di pace. Questo può accadere nel caso di azioni umanitarie, **per salvare vite** o in situazioni di **emergenza**. In questi casi, è comunque previsto che il personale chiamato ad operare lo faccia su **base volontaria** e dopo essere stato **informato** delle possibili **conseguenze** dell'attività.

Deve essere mantenuta un'accurata registrazione degli eventi CBRN e di ogni esposizione del personale a pericoli di tipo CBRN. Questo servirà per meglio pianificare le attività post-conflitto e per la gestione delle situazioni sanitarie nel lungo termine. In particolare, dovranno essere registrati i nominativi degli individui, la durata della permanenza nell'area contaminata, località, tipo di agente.

La rotazione degli assetti attraverso l'area CBRN deve essere presa in considerazione e pianificata. Vi è una necessità particolare di ruotare il personale in aree contaminate radiologicamente, giacché la dose radioattiva, che può essere monitorata, si accumulerà nel tempo. Tale rotazione richiederà un notevole sforzo di pianificazione da parte dello *staff*. Inoltre, grande attenzione dovrà essere posta per evitare la diffusione della contaminazione, a seguito dei movimenti dei reparti contaminati.

---

<sup>16</sup> STANAG 2083 "Commander's guide on nuclear radiation exposure of groups during war".

<sup>17</sup> STANAG 2473 "Commander's guide to radiation exposures in Non-article 5 Crisis Response Operations".

Il monitoraggio del cibo e dell'acqua è una specifica responsabilità medica.

(2) Operazioni in area di pericolo TIM – Materiali Tossici Industriali (TIC-TIB-TIR)

In Teatro, il personale militare potrebbe essere chiamato a fronteggiare i pericoli conseguenti ad un rilascio nell'ambiente, accidentale o premeditato, di grandi quantità di TIC presenti in impianti di produzione, stoccaggio, distribuzione e trasporto dislocati nelle zone di operazione.

Per questo, prima di schierarsi in Area di Operazioni, l'*Intelligence* (con il contributo degli assetti medici) deve fornire indicazioni a tutti i livelli di comando in merito alle aree in cui si conosce o si presume la presenza di TIM. Sulla base di tali informazioni, il personale addetto alla difesa CBRN, di concerto con il personale medico e CIMIC, deve acquisire, in collaborazione con le autorità civili locali, informazioni su ulteriori procedure di emergenza e su eventuali risorse utilizzabili in caso di incidente.

Per ciascuna tipologia di materiale tossico, in sede di valutazione della minaccia, dovranno essere considerate le caratteristiche legate a quantità, volatilità, tossicità, infiammabilità, corrosività, reattività e causticità.

Inoltre, nel medesimo contesto (valutazione della minaccia), sarà necessario considerare che il rischio non è rappresentato solo dalla presenza del singolo TIM, ma anche da esplosioni, incendi e derivati tossici che si possono liberare.

È importante quindi che i Comandanti a qualsiasi livello comprendano l'importanza di essere preparati e di possedere la cognizione del pericolo, assicurando, sulla base della normativa NATO (STANAG 2521<sup>18</sup>), che le misure preventive appropriate (distanze minime di rispetto, immediata evacuazione, dispositivi di protezione individuali idonei diversi da quelli in dotazione) siano predisposte e messe in atto, se necessario.

**e. Sostegno logistico**

Elevati consumi di decontaminanti, materiali di consumo, acqua, materiali per la protezione individuale e vaccini, unitamente alle contromisure mediche, rappresentano una caratteristica fondamentale delle operazioni di difesa CBRN. È necessario raggiungere il giusto equilibrio tra la fornitura di *stock* adeguati di materiali (per la difesa CBRN) e le esigenze logistiche generali della missione.

È difficile ipotizzare l'entità della richiesta futura per gli equipaggiamenti di difesa CBRN, in particolare, se sussistesse anche la necessità di fornire tale materiale a personale non nazionale del contingente e a quello di altre organizzazioni nel corso di Operazioni di Risposta alle Crisi (CRO). Infatti, sebbene sia previsto che le varie componenti del contingente appartenenti a varie Nazioni si schierino con la propria organizzazione logistica, potrebbe rendersi necessario fornire un'integrazione al sostegno, in particolare nel caso di forti disparità nelle capacità di difesa CBRN. Ne deriva che le risorse dovranno essere impiegate efficacemente e razionalmente, facendo anche il miglior uso possibile di ogni forma di sostegno che la *Host Nation* dovesse mettere a disposizione.

In un ambiente CBRN, il sistema logistico deve essere estremamente versatile e capace di reagire rapidamente a circostanze impreviste. I pericoli e i danni potenziali derivanti dalla presenza di agenti (o di aggressivi) CBRN e TIM possono rendere necessaria la

---

<sup>18</sup> ATP-3.8.1 Vol I "CBRN Defence on Operations".



ridislocazione delle basi logistiche, l'individuazione di nuovi itinerari per il flusso dei materiali, la redistribuzione dei sistemi di trasporto.

Anche la tempistica delle attività potrebbe dover essere rivista in caso di condizionamenti delle operazioni logistiche dovuti alla presenza di contaminazione CBRN. Inoltre, è necessaria una pianificazione dettagliata per la rapida fornitura di equipaggiamenti/materiali connessi con la difesa CBRN, verso zone nelle quali è anticipato il possibile impiego di armi CBRN o il rilascio di TIM.

Aspetti logistici particolarmente significativi sono:

- la protezione dei rifornimenti e degli assetti logistici dai pericoli di contaminazione a seguito di evento CBRN;
- i movimenti lungo gli itinerari logistici (*Main Supply Routes* - MSRs) per alimentare i punti di rifornimento e le basi logistiche, evitando, al contempo i pericoli CBRN. Questo può richiedere l'individuazione di siti e itinerari alternativi;
- il controllo dei movimenti di personale, equipaggiamenti e rifornimenti attraverso aree contaminate;
- il rifornimento e la sostituzione di equipaggiamenti individuali di protezione, di decontaminanti e di materiale sanitario;
- le esigenze, le priorità e le procedure per la decontaminazione ed evacuazione di materiali e rifornimenti contaminati;
- il bisogno di eventuale supporto di risorse locali, da individuare tramite il coordinamento tra il J4 e J5, J8 e J9 CIMIC;
- la priorità nell'evacuazione, decontaminazione, trattamento e isolamento del personale colpito da agenti CBRN o dei feriti da armi convenzionali che sono stati contaminati e l'integrazione delle capacità sanitarie della *Host Nation*;
- la decontaminazione di acqua e cibo per il consumo umano;
- le procedure per la gestione di un numero elevato di colpiti in ambiente contaminato;
- la disponibilità di docce o bagni e un cambio di vestiti almeno una volta a settimana per tutto il personale, allo scopo di mantenere un elevato standard di igiene;
- la gestione dei resti umani contaminati provvedendo alla sepoltura di emergenza in Teatro, secondo quanto previsto dallo STANAG 2070<sup>19</sup>.

---

<sup>19</sup> STANAG 2070 "*Emergency war burial procedures*".



## LA PROTEZIONE DELL’AMBIENTE CIBERNETICO

### 1. Introduzione

“L’ambiente cibernetico è un dominio creato dall’uomo caratterizzato da comunicazioni e sistemi informativi interconnessi. Tutti i sistemi di comunicazione e informativi dipendono da entità che risiedono o sono riconducibili a specifiche giurisdizioni legali”<sup>1</sup>.

Lo sviluppo delle reti e dei sistemi basati su tecnologie dell’informazione e della comunicazione ha generato un’infrastruttura interconnessa, dinamica e globale su cui si sviluppano e vengono svolte una notevolissima quantità di attività che crea moltissime opportunità di crescita, ma genera una serie di fragilità molto critiche nell’intero sistema che rimane esposto a minacce cibernetiche potenzialmente assai pericolose, in continua rapida evoluzione ed espansione e difficilmente identificabili compiutamente in via preventiva.

Oltre a possibili guasti di natura accidentale, le minacce variano dallo spionaggio agli attacchi veri e propri con finalità di inibire, alterare, o addirittura distruggere dati, hardware, reti o eventuali servizi/sistemi da essi dipendenti. I protagonisti di tali minacce possono essere attori statuali oppure gruppi di terroristi, organizzazioni criminali, attivisti o *hacker* malevoli che utilizzano tecnologie e capacità facilmente reperibili.

Lo spazio cibernetico è parte integrante degli ambienti ove condurre operazioni militari, ha implicazioni sia nel dominio fisico sia in quello informativo, ed è “trasversale” ai tradizionali ambienti operativi (terrestre, marittimo, aereo e spaziale). Come tale, il dominio cibernetico influenza direttamente la pianificazione generale, la pianificazione operativa e la condotta delle operazioni.

### 2. Elementi dello spazio cibernetico

Allo scopo di uniformare la terminologia utilizzata nello specifico settore, si riportano di seguito alcune definizioni<sup>2</sup> la cui conoscenza è fondamentale per inquadrare ed affrontare il tema dell’ambiente cibernetico e della sua protezione.

- a. **Information Assurance (IA)**: definita come il complesso di misure che proteggono e difendono le informazioni e i sistemi informativi attraverso la salvaguardia della loro disponibilità, integrità, autenticità, riservatezza e non ripudiabilità. Ciò include il ripristino dei sistemi informatizzati attraverso funzionalità incorporate di protezione, rilevazione e reazione.

L’IA si basa, con riferimento all’informazione, sui principi di riservatezza, integrità, disponibilità, autenticazione, autenticità, certezza dello scambio informativo, usabilità.

- b. **Cyber Defence (CD)**: il complesso di predisposizioni, misure, procedure e attività volte a proteggere i sistemi informativi e le infostrutture CIS<sup>3</sup> della Difesa dalle azioni cibernetiche ostili nella massima accezione possibile.

---

<sup>1</sup> Per ulteriori approfondimenti sull’argomento si rimanda ai contenuti delle pubblicazioni: “*Computer Network Operations JIC 011*” Ed. 2009 e “*Direttiva Interforze di policy sull’ambiente cibernetico*” SMD–G-032 Ed. 2012.

<sup>2</sup> Tali definizioni sono tratte dalla “*Direttiva Interforze di policy sull’ambiente cibernetico*” SMD–G-032 Ed. 2012

<sup>3</sup> *Communication Information Systems*.

È un concetto vasto che, nell’ambito dello *spazio cibernetico*, va oltre l’*Information Assurance* (IA) e implica i concetti di prevenzione, protezione, reazione, deterrenza e resilienza da un attacco cibernetico persistente. Pertanto ingloba anche le capacità di identificare, analizzare, allertare, proteggere, rispondere, riparare, descrivere, formare, addestrare. Il concetto di *Cyber Defence*<sup>4</sup> non va confuso con quello di *Computer Network Defence* (CND), di seguito riportato, poiché quest’ultimo concerne unicamente il dominio di una particolare operazione militare.

c. **Computer Network Operations (CNO)**: capacità di condurre operazioni deliberate nel settore informatico, telematico e cibernetico, aventi finalità offensive, difensive e/o di analisi e sfruttamento di dati, informazioni e servizi, realizzabili - in difesa dello Stato, sia sul territorio nazionale sia all’estero – attraverso l’integrazione delle capacità militari interforze. Le CNO costituiscono un moltiplicatore di forza e possono essere effettuate anche in concomitanza con le operazioni militari classiche. In particolare le CNO si basano su tre pilastri: *Computer Network Defence* (CND), *Computer Network Exploitation* (CNE) e *Computer Network Attack* (CNA):

(1) **Computer Network Defence (CND)**: “azioni volte a difendere, includendo anche la risposta attiva, le info-strutture CIS, gli assetti della Difesa e le informazioni ivi contenute da attività cibernetiche ostili.” Lo scopo della CND è quindi quello di proteggere le info-strutture militari da operazioni di CNE e CNA avversarie. L’attività di CND si sostanzia nelle seguenti azioni:

- attuazione di azioni di contrasto e risposta volte a impedire che un attacco cibernetico sia portato a termine, ovvero limitare gli effetti di tale attacco e arrestarlo il prima possibile;
- raccolta di ogni elemento utile all’analisi tecnico-forense dell’attività cibernetica ostile rilevata;
- concorso al ripristino rapido delle funzionalità dell’info-struttura qualora compromessa.

(2) **Computer Network Exploitation (CNE)**: “azioni tese ad acquisire e analizzare dati ed informazioni contenute su computer e *network* di interesse, al fine di ottenere un ragionevole vantaggio”.

Le CNE possono essere condotte per acquisire informazioni operative, catalogarne la presenza nello spazio cibernetico, misurare le capacità di potenziali oppositori di condurre operazioni cibernetiche e, infine, valutare la minaccia cibernetica dell’avversario. Ad eccezione del primo campo d’azione, che sottende ad attività intelligence tradizionali condotte nel dominio dello *spazio cibernetico* (pertanto, in ambito Difesa, di preminente competenza dello SMD-RIS), le CNE sono rilevanti e propedeutiche alla pianificazione e condotta delle CNO sia di natura difensiva che offensiva. Inoltre, si riconosce una funzionalità delle CNE nell’irrobustimento delle misure di protezione proprie della *Cyber Defence*;

---

<sup>4</sup> Con il termine *cyber defence* si deve indicare quella macro area entro cui si svolgono tutte quelle attività relative allo spazio cibernetico e che afferiscono alla *policy*, alle misure di protezione, alla *governance*, alla formazione/addestramento, al sistema di *early warning* ecc..

(3) *Computer Network Attack (CNA)*: “azioni volte a smembrare, rendere inaccessibili, degradare o distruggere informazioni contenute in un computer, in una rete o nel computer e/o la rete di computer di uno o più avversari”.

**d. Sicurezza cibernetica (cyber security)**. Usare indistintamente il termine comporta un possibile fraintendimento tra il “dominio sicurezza”<sup>5</sup> in generale e le “misure di sicurezza”, in senso specifico. Si raccomanda, pertanto, di affiancare sempre la parola “misure di sicurezza” (*security measures*)<sup>6</sup> quando si intende *sicurezza cibernetica*, significando che questa accezione rientra nell’ambito delle IA.

### 3. **Gestione operativa**

La “Direttiva Interforze di *Policy* sull’ambiente cibernetico” (SMD-G-032) prevede la costituzione di un **Centro Operativo Cibernetico Interforze (COCI)** e di **Cellule Operative Cibernetiche (COC)** per ciascuna Componente deputate alla condotta di operazioni cibernetiche difensive e offensive.

#### **a. Centro Operativo Cibernetico Interforze (COCI)**

Il ruolo di Centro Operativo Cibernetico Interforze è assunto nel transitorio dal Comando C4 Difesa. Il COCI seguirà le evoluzioni tecnico-funzionali e procedurali del NATO *Computer Incident Response Capability* (NCIRC) e il suo impiego dovrà essere previsto nell’elaborazione dell’OPLAN (*operations plan*). Tale struttura può interagire con omologhi organismi in ambito nazionale ed internazionale/multinazionale. Il COCI sviluppa una capacità cibernetica operativa con il compito di:

- monitorare gli sviluppi di attività nello *spazio cibernetico* (fornendo anche una *situational awareness/cyber picture* a tutta la comunità militare);
- svolgere analisi delle tendenze ed *Early Warning* (da condividersi con tutte le infrastrutture interdicasteriali e non, in piena sinergia con gli obiettivi fissati dal NISP attraverso il CIAC);
- fornire un *Vulnerabilities assessment* in conformità alla *policy* di sicurezza in vigore;
- fornire un *Risk Assessment* in conformità alle *policy* di sicurezza in vigore;
- gestire tutte le attività relative agli incidenti, anche di carattere operativo (CNO), ed in particolare quelli riguardanti l’*INFOSEC Management Capability, Information Assurance Services, Computer Incident Response Capability e Cyber C2 capabilities*;
- raccogliere, nel corso delle proprie operazioni cibernetiche e di quelle condotte dalle cellule operative (COC), i dati tecnici riferiti alla minaccia rendendoli disponibili all’assetto intelligence tecnico-militare.

#### **b. Cellule Operative Cibernetiche (COC)**

Il COCI interagisce con le Cellule Operative Cibernetiche (COC), che assumendo nuove funzioni inglobano i CERT<sup>7</sup> di FA, e sono impiegate normalmente per la difesa del proprio

<sup>5</sup> Spesso viene affiancato al dominio “difesa” oppure difesa e sicurezza.

<sup>6</sup> Ad esempio per analogia la Computer security è definita come l’applicazione di misure di sicurezza hardware, *firmware* e software a un sistema informatico per proteggere o prevenire, dalla divulgazione non autorizzata, dalla manipolazione, dalla modifica o cancellazione delle informazioni o da *denial of service* (NATO AAP-31A).

<sup>7</sup> *Computer Emergency Response Team*.

dominio dalle rispettive Forze Armate. Il COCI, attraverso collegamenti funzionali, espleta nel contempo direzione, coordinamento e controllo delle COC nell'ambito delle operazioni cibernetiche.

Le COC (che possono essere anche distaccate/*deployed* in operazioni *joint*) supportano le attività di *situational awareness*, *assessment* delle vulnerabilità e la gestione degli incidenti (CND). Inoltre, nelle operazioni fuori dai confini nazionali e/o in situazioni di crisi<sup>8</sup> potranno condurre, nei casi previsti, sotto OPCON del Contingente nazionale, con il supporto operativo del COCI e, qualora il quadro dei provvedimenti legislativi lo consenta, le operazioni di *Computer Network Attack* (CNA).

Tali articolazioni forniscono su canali dedicati, sia al COCI sia alla branca *intelligence*, ogni elemento tecnico raccolto dai propri sensori sulla minaccia valorizzato e utile alla condotta efficace delle CNO.

---

<sup>8</sup> Possono essere costituite diverse COC secondo la situazione contingente.







