



**Centre interarmées
de concepts,
de doctrines et
d'expérimentations**



**Protection des
installations
militaires**

**Doctrine interarmées
DIA-3.32.4_PIM(2012)**

N°016/DEF/CICDE/NP du 16 janvier 2012



Intitulée *Protection des installations militaires de défense*, la Doctrine interarmées (DIA) 3.32.4_PIM (2012) respecte la charte graphique définie dans la Publication interarmées (PIA) 7.24_RDRIA(2010), n° 161/DEF/CICDE/ NP en date du 18 juin 2010. Ladite charte graphique est elle-même conforme aux prescriptions de l'*Allied Administrative Publication (AAP) 47(A)* intitulée "*Allied Joint Doctrine Development*"). Elle applique également les conseils du *Lexique des règles typographiques en usage à l'Imprimerie nationale* (LRTUIN, ISBN¹ 978-2-7433-0482-9) dont l'essentiel est disponible sur le site Internet www.imprimerienationale.fr ainsi que les prescriptions de l'Académie française. La jaquette de ce document a été créée par le CICDE². L'impression a été réalisée par le Service parisien d'administration centrale (SPAC) / Pôle graphique de Paris (PGP). **Attention : la seule version de référence de ce document est la copie électronique mise en ligne sur les sites Intradef et Internet du Centre interarmées de concepts, de doctrines et d'expérimentations (<http://www.cicde.defense.gouv.fr>) dans la rubrique *Corpus conceptuel et doctrinal interarmées*.**

¹ *International Standard Book Number* / Numéro international normalisé du livre.

² Photos ministère de la Défense (MINDEF).



DIA-3.32.4_PIM(2012)

**PROTECTION DES
INSTALLATIONS MILITAIRES
(PIM)**

N°016/DEF/CICDE/NP du 16 janvier 2012

(PAGE VIERGE)

Lettre de promulgation



Paris, le 16 janvier 2012
N°016/DEF/CICDE/NP

Le général de corps d'armée Didier CASTRES
Sous-chef d'état-major Opérations
(SCEM-OPS)

1. La Défense occupe des installations militaires, dont certaines revêtent une valeur opérationnelle en raison des matériels ou des informations qu'elles renferment, et d'autres parce qu'elles contribuent directement à la mise en œuvre de l'appareil de défense. Aussi leur protection générale constitue-t-elle un impératif pour les militaires et le personnel civil de la Défense.
2. Dans la continuité du Concept interarmées (CIA-3.30_SG) traitant de la *Sauvegarde générale*, ce document décrit la responsabilité des nombreux acteurs de la Protection des installations militaires (PIM), tant dans le domaine de la préparation que dans celui de la réalisation de cette mission.
3. Après avoir décrit le cadre général de l'action, le document précise les volets défensif et réactif de la protection. Il tient compte d'aspects juridiques, contractuels et d'infrastructure rendant le sujet aujourd'hui encore plus complexe qu'autrefois.
4. Ce document est destiné, avant tout, aux responsables de terrain qui doivent être conscients de la portée opérationnelle de cette protection des installations militaires, en particulier pour les plus sensibles d'entre elles.

Le général de corps d'armée Didier Castres
sous-chef d'état-major « opérations »
de l'état-major des armées



(PAGE VIERGE)

Récapitulatif des amendements

1. Ce tableau constitue le recueil de tous les amendements proposés par les lecteurs, quels que soient leur origine et leur rang, transmis au Sous-directeur Synergie doctrinale (SD-SD) du Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE) en s'inspirant du tableau proposé en annexe A (voir page 41).
2. Les amendements validés par le CICDE sont inscrits **en rouge** dans le tableau ci-dessous dans leur ordre chronologique de prise en compte.
3. Les amendements pris en compte figurent **en violet** dans la nouvelle version.
4. Le numéro administratif figurant au bas de la première de couverture et de la fausse couverture est corrigé (**en caractères romains, gras, rouge**) par ajout de la mention : « **amendé(e) le jour / mois / année.** »
5. La version électronique du texte de référence interarmées amendé remplace la version antérieure dans toutes les bases de données informatiques.

N°	Amendement	Origine	Date de validité
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			

(PAGE VIERGE)

Références

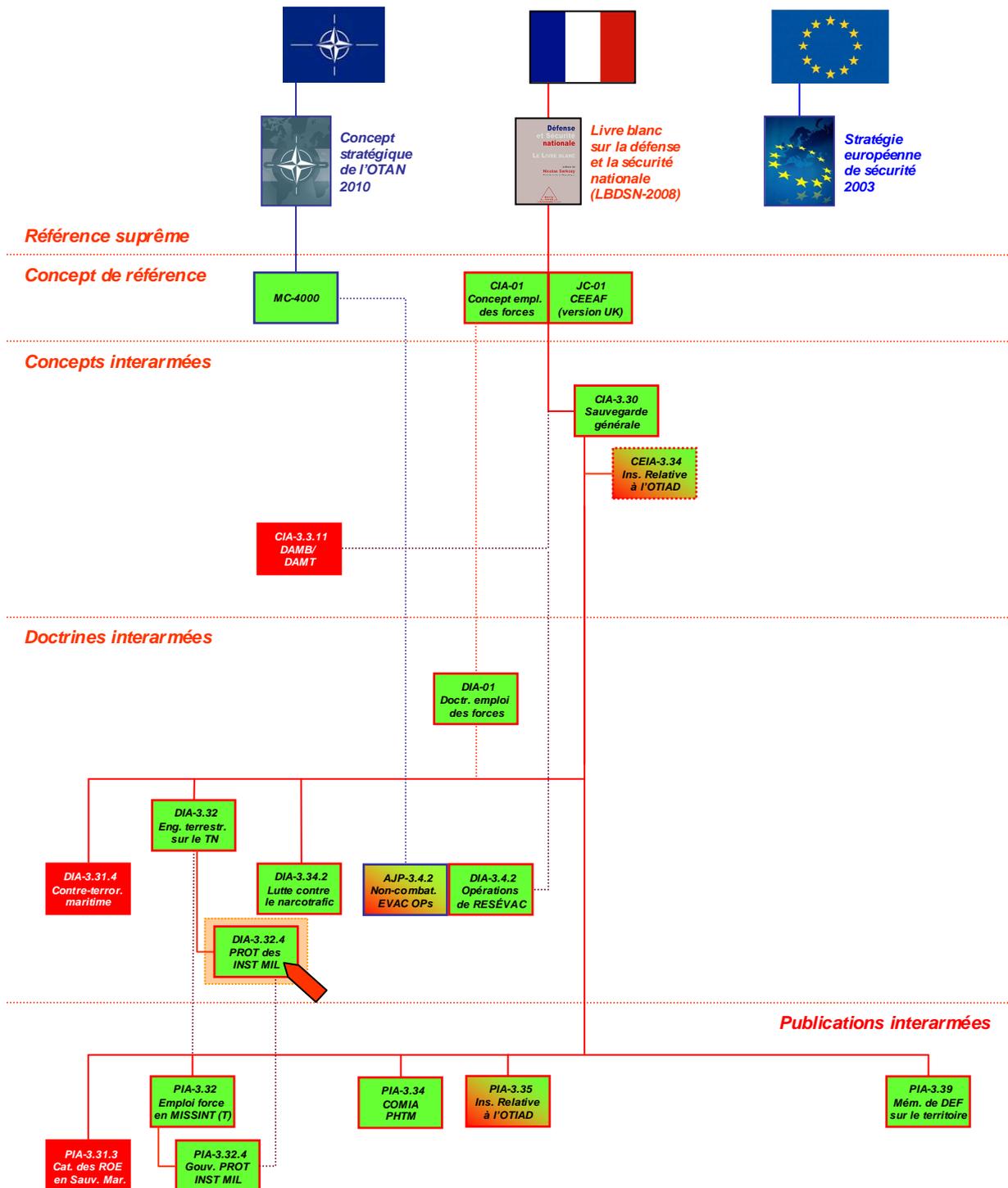
- a. Code pénal, code de procédure pénale et code de la défense.
- b. Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des Activités d'importance vitale (AME).
- c. Instruction générale interministérielle n°1300 du 23 juillet 2010 sur la protection du secret de la défense nationale.
- d. Arrêté portant Directive nationale de sécurité (DNS) « *Activité militaire de l'État* » (AME) du 7 mars 2001
- e. Décret n° 2009-869 du 15 juillet 2009 relatif aux attributions du ministre de la Défense, du chef d'état-major des armées et des chefs d'état-major de l'armée de terre, de la marine et de l'armée de l'air.
- f. Arrêté du 27 octobre 2009 fixant les attributions de l'Inspection des armées (IdA).
- g. Décret n° 2004-1102 du 15 octobre 2004 portant règlement du service de garnison.
- h. Arrêté du 24 décembre 2008 portant organisation des bases de défense et fixant les attributions des commandants des bases de défense expérimentales.
- i. Instruction n° 398/DEF/EMA/SC-SOUT relative à l'organisation et au fonctionnement des bases de défense du 17 décembre 2010.
- j. Instruction n° 900/DEF/CAB/DR du 18 juin 2007 relative à la protection du secret de la défense nationale au sein du ministère de la Défense.
- k. Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, article 10 relatif à la vidéosurveillance.
- l. Loi n° 83-629 du 12 juillet 1983 relative aux activités privées de sécurité, art.3-1 sur les attributions des agents.

Préface

1. La modernisation de l'appareil militaire de défense impose une rénovation des mesures de protection des installations de la Défense placées sous la responsabilité des armées. Par ailleurs, une plus grande harmonisation des méthodes et des procédures facilitera l'émergence d'une culture opérationnelle de sécurité au sein de l'ensemble des organismes.
2. La Protection des installations militaires (PIM), selon leur importance respective, concourt :
 - a. à l'exercice de l'autorité de l'État ;
 - b. au maintien du potentiel de défense de la nation ;
 - c. à la sécurité du territoire et des populations.

3. Afin d'améliorer les dispositifs de protection, de concentrer les efforts en la matière et de favoriser l'engagement des responsables militaires, l'organisation des mesures de sûreté vise à :
 - a. mettre en cohérence les mesures de protection des installations militaires avec la définition des risques et des menaces figurant dans les plans gouvernementaux ;
 - b. associer les acteurs de la sûreté militaire, permanents ou non, à l'effort de vigilance, de prévention et de protection ;
 - c. disposer de procédures juridiquement solides et de définitions claires et homogènes ;
 - d. sélectionner les points devant faire l'objet d'une protection efficace en fonction du niveau de la menace.
4. L'objectif de ce document est, d'une part, de définir une approche interarmées de la protection des installations militaires sur le Territoire national (TN) et, d'autre part, de valoriser le recours à de nouveaux modes d'action afin d'améliorer et d'entretenir la sûreté faisant appel, si cela s'avère utile, aux technologies modernes, voire à l'externalisation.
5. La protection s'entend ici comme un dispositif physique et humain. La protection électronique des informations, objet de la cyberdéfense, est exclue du champ de ce document.
6. Les principes préconisés dans le présent document devront être adaptés aux caractéristiques propres à chaque site.

Place de la DIA-3.32.4_PIM(2012) dans le CCDIA-FRA*



Légende

*Corpus conceptuel et doctrinal français

- Document OTAN
- Document français (ici, classifié)
- Document UE

- Document classifié (triangle en bas à droite)
- Texte en cours de validité
- Texte existant / Nouvelle édition proposée à la signature
- Texte existant / Nouvelle édition en cours / Révision

- Texte à la signature
- Texte en cours de développement / à l'étude
- Texte à supprimer après incorporation dans un texte du niveau supérieur ou après rempl. par un autre texte

(PAGE VIERGE)

	Page
Chapitre 1 – L’organisation de la protection	15
Section I Cadre de la protection des installations militaires de défense.....	15
Section II Responsabilités des acteurs du domaine de la protection	17
Section III Mode de fonctionnement de la protection	19
Chapitre 2 – Le volet défensif de la protection	23
Section I Le cadre général	23
Section II Équilibre entre les ressources et les moyens de protection	24
Section III Équilibre entre besoin d'accès et protection des sites.....	26
Section IV Contrôles, inspections et enquêtes	32
Chapitre 3 – Le volet réactif de la protection	35
Section I Le processus de réaction à la menace.....	35
Section II Les conditions d'application de l'emploi de la force dans l'intervention.....	36
Section III L'Élément d'intervention (EI) dans le volet réactif de l'intervention	38
Section IV Le contrôle <i>a posteriori</i> de la protection (RETEX PROT)	39
Annexe A – Demande d’incorporation des amendements	41
Annexe B – Lexique	43
Partie I Sigles, acronymes et abréviations.....	43
Partie II Termes et définitions.....	45
Résumé (quatrième de couverture)	46

(PAGE VIERGE)

Chapitre 1

L'organisation de la protection

Section I — Cadre de la protection des installations militaires de défense

101. La mission de Protection des installations militaires (PIM) n'est pas l'addition de mesures particulières de protection. Elle relève d'une coopération permanente de tous les acteurs responsables de la protection des installations et de ceux qui y sont associés.

Le contexte de mise en œuvre de la protection

102. Sur le TN, les armées ont pour mission³ de participer à la protection de leurs installations.
103. Cette mission constitue une partie du pilier militaire de la défense et de la sécurité nationale. Elle s'exerce en partenariat avec les autres acteurs institutionnels concourant à la résilience de la Nation et participant à la crédibilité de l'appareil de Défense. Aussi, la protection des installations militaires et les mesures à prendre dans ce domaine nécessitent-elles une coordination dépassant le strict périmètre des intérêts de défense.
104. De plus, la protection des installations ne correspond pas à une simple addition des protections particulières des installations, mais met en jeu une mobilisation fonctionnelle (cf. chapitre 2) permanente de tous les acteurs responsables de la protection des installations ou y contribuant. Cette mobilisation est réalisée par le pilotage d'un processus transverse de gestion de la « *protection des installations militaires de défense* ». Ce mode de gouvernance de la « *fonction protection* » relève d'un souci constant d'amélioration de son efficacité.

La fonction protection

105. S'appuyant sur des contrats opérationnels et sur le RETour d'EXpérience (RETEX), une fonction est comprise comme un ensemble cohérent englobant notamment les domaines suivants : documentation, organisation, commandement, personnel, équipements, soutien, cohésion et formation/entraînement.
106. La fonction **protection** engage l'ensemble des chaînes de commandement, du plus haut niveau des armées, des directions et des services jusqu'à l'ensemble des chefs de formation et d'établissement.
107. La notion de fonction permet de faire le lien entre l'organique et l'opérationnel, entre la gestion d'une capacité et la réalisation d'une mission opérationnelle, entre souteneurs et soutenus, entre ceux qui expriment des besoins et les détenteurs des leviers d'action.

La mission de protection

108. La protection des installations militaires est une mission opérationnelle où chaque décision de commandement se traduit en ordres engageant la responsabilité des autorités qui les prescrivent. En conséquence, il appartient à chaque autorité de mettre en œuvre, dans un premier temps, les mesures de protection nécessaires et réglementaires, d'en contrôler la bonne exécution et de s'assurer que le personnel placé sous ses ordres est instruit et sensibilisé en la matière. Dans un deuxième temps, face à une menace avérée, l'autorité doit organiser le renforcement des mesures, que ce soit au sein de sa chaîne fonctionnelle ou dans le cadre d'une réponse interarmées s'appuyant sur l'Organisation territoriale interarmées de défense (OTIAD).
109. Les contributions à la protection des installations doivent être traitées sous l'angle opérationnel. Une action ou une décision dans ce domaine doit être considérée comme un acte de commandement.

³ Dispositions générales du Code de la défense.

110. La mission de « *protection des installations militaires* » recouvre l'ensemble des voies et moyens (hors engagements des forces) permettant de prévenir tout événement⁴ et, le cas échéant, de faire cesser par une intervention appropriée l'exposition du personnel, des installations, du matériel et des informations⁵ détenues par la défense à toute forme de risques ou de menaces.

111. Elle procède de l'effet recherché sur le terrain et de l'exécution des mesures qui s'y rapportent. Elle s'exerce au niveau national et au niveau local, et constitue une responsabilité partagée et individualisée.

Définition de la protection des installations

112. Sur le TN, la mission de protection des installations sensibles est une mission militaire permanente consistant :
- a. à empêcher la pénétration par inadvertance ;
 - b. à détecter, si possible, toute intrusion ;
 - c. en cas d'intrusion, à faire cesser l'infraction et éventuellement, tout en continuant à assurer la protection de l'installation, à intercepter le délinquant⁶ (l'agresseur) en liaison avec les forces de sécurité.
113. L'emploi envisagé de la force, incluant l'usage éventuel des armes, rappelle qu'il s'agit d'une mission opérationnelle.
114. La protection couvre à la fois les notions de prévention et de réaction. La prévention permet d'anticiper les « *agressions* » et leurs effets. La réaction permet d'y faire face et, dans la mesure du possible et dans des cas bien précis, de les stopper. Dans tous les cas, il s'agit de mettre en œuvre des mesures conformes au droit.

Les principes associés

115. Compte tenu de la contribution essentielle des forces armées à la défense et à la sécurité nationale, et selon le principe de subsidiarité, le ministère de la Défense doit garantir la résilience de ses propres installations militaires sur le TN.

Résilience

116. La résilience⁷ est définie comme « *la volonté et la capacité d'un pays, de la société et des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeure, puis à rétablir rapidement leur capacité de fonctionner normalement* ». Elle est un objectif de la stratégie de défense et de sécurité nationale.
117. Toutes les formations administratives de la défense doivent faire l'objet de mesures de protection. Toutefois, elles ne représentent pas toutes le même intérêt pour la sûreté de l'État et au regard des enjeux de défense.

Discrimination

118. La loi distingue des Secteurs d'activité d'importance vitale (SAIV) et identifie, pour l'État, des sites associés appelés Points d'importance vitale (PIV). Si tous les sites militaires doivent être défendus, les PIV font logiquement l'objet d'un traitement prioritaire, notamment dans l'attribution des moyens consacrés à la protection.
119. Les armées doivent organiser la protection de leurs emprises pour assumer les responsabilités de la défense au titre des AME.

⁴ Le terme événement couvre les risques et les menaces.

⁵ La protection des informations s'entend notamment à travers des documents classifiés. Elle ne couvre pas leur protection électronique, objet de la cyberdéfense, exclue de ce document.

⁶ Le terme de délinquant, préféré ici au terme d'ennemi ou d'adversaire, est avant tout un terme juridique : il permet de souligner le cadre juridique national dans lequel se déploie la protection, c'est-à-dire un cadre avant tout pénal.

⁷ LBDSN-2008, chapitre 3 : *La stratégie de sécurité nationale*, p. 64.

- 120. Chaque site à protéger présente des caractéristiques propres : sensibilité, localisation, dimensions, nature des constructions, etc. Ces différents facteurs, confrontés à la menace à prendre en compte, confèrent au site une certaine vulnérabilité⁸ qu'il s'agit de réduire.
- 121. Le niveau de protection d'un site et les moyens qui y sont consacrés résultent d'un équilibre. Les choix arrêtés en la matière doivent, en effet, intégrer l'évaluation de la menace et l'efficacité requise du dispositif associé, les ressources humaines et financières disponibles, la sensibilité du site à protéger ainsi que les spécificités locales.
- 122. Ambitionner une protection absolue n'est pas réaliste sur le plan budgétaire. Le dispositif considéré doit être adapté à une crise ponctuelle, pouvoir atténuer ses effets, et permettre de disposer des outils qui maintiendront un niveau satisfaisant de résilience.
- 123. Ainsi, l'organisation de la protection hiérarchise les efforts à consentir dans ce domaine en fonction de ressources comptées et identifiées. Elle doit être harmonisée pour assurer une cohérence sur l'ensemble des installations similaires et faciliter les prises de décision en gestion (en temps normal) comme en conduite (en cas de crise).

Section II – Responsabilités des acteurs du domaine de la protection

- 124. La responsabilité se définit d'abord et principalement sur le plan pénal. La loi précise les responsabilités et organise les modalités génériques d'emploi de la force.
- 125. La protection des installations militaires incombe à la chaîne de commandement. Elle ne constitue pas une finalité en soi de l'organisation militaire ; elle est une fonction que doit assumer toute autorité militaire, responsable à titre individuel ou collectif, d'entreprises militaires.
- 126. Les Opérateurs d'importance vitale (OIV), désignés responsables dans leurs domaines respectifs par le ministre de la Défense, tiennent une place primordiale dans l'organisation de la protection.
- 127. La responsabilité se définit également au regard des charges administratives et des responsabilités de commandement pour les chefs des organismes qui apportent leur soutien à cette mission.

Le commandant de la formation administrative

- 128. Tout commandant de formation administrative est responsable de la protection et de la sauvegarde de son personnel, de ses informations et de ses biens mobiliers et immobiliers vis-à-vis de ses autorités⁹ hiérarchiques, organiques et opérationnelles.
- 129. Il doit exprimer le juste besoin de protection, puis s'assurer de la définition des mesures de protection adaptées et enfin veiller à leur mise en œuvre.

L'officier de sécurité

- 130. Sous l'autorité du commandant de formation, les officiers de sécurité, pénalement responsables :
 - a. fixent les règles et consignes de sécurité et contrôlent leur application, y compris en matière de protection du secret¹⁰ ;
 - b. gèrent les habilitations.

Les Opérateurs d'importance vitale (OIV)

- 131. Les acteurs primordiaux de la protection des installations militaires sont les OIV. Ils sont nommément désignés par un décret qui précise leur responsabilité pénale.

⁸ La « vulnérabilité » désigne la propension d'un milieu, d'un bien ou d'une personne à subir des conséquences dommageables à la suite d'un événement (cf. PIA-7.2.6, *Glossaire interarmées de terminologie opérationnelle* [GIAT-O]).

⁹ Au sens de la chaîne de responsabilité pénale.

¹⁰ Instruction ministérielle 1300 et Instruction ministérielle 900.

132. Placés sous leur responsabilité, les PIV constituent, au quotidien, les objectifs prioritaires de la mission de protection des installations militaires de défense.
133. Les chaînes de commandement, sur lesquelles s'appuient les OIV, leur permettent de développer leurs stratégies de sûreté à la hauteur des moyens dont ils disposent et qu'ils consentent. Selon leur culture managériale, les OIV articulent également leurs lignes d'efforts de protection avec leurs partenaires institutionnels respectifs, à tous les niveaux de décision.
134. La protection d'un PIV relève de la Directive nationale de sécurité (DNS). Le Délégué pour la défense et la sécurité¹¹ (DDS dit « Local » ou DDSL) d'un PIV applique les dispositions fixées par le Plan de sécurité opérateur (PSO). L'organisation de la protection du PIV nécessite la rédaction d'un Plan particulier de protection (PPP).
135. Pour chaque OIV, la gestion du dispositif de défense est un effort quotidien décrit et organisé dans le PPP. L'autorité militaire doit porter à la connaissance de l'autorité administrative les informations, extraites du PPP, strictement nécessaires à l'élaboration du PPE.
136. Partagée par toute la chaîne de commandement organique impliquée et par les organismes y concourant, cette mission se décline depuis les OIV jusqu'aux commandants de formation administrative. Ces différents niveaux constituent une chaîne de responsabilité pénale¹².
137. Il appartient à chaque autorité responsable de mettre en œuvre à cet effet les mesures réglementaires de protection, d'en contrôler la bonne exécution et de s'assurer que le personnel placé sous ses ordres est instruit et sensibilisé en la matière.
138. Prescrite par la loi, cette cohérence impose des coopérations constantes entre le responsable de site et ses interlocuteurs locaux, polices administrative et judiciaire notamment. Pour une meilleure intégration locale d'un site, son responsable veille à l'information des riverains par des moyens variés allant d'une signalétique codifiée et entretenue jusqu'à des manifestations de relations publiques.

La chaîne de soutien (OIAS¹³)

139. La protection des installations est une mission dynamique exigeant un entretien permanent et des adaptations constantes, réalisés par la fonction soutien. La gouvernance de la fonction « *protection* » repose ainsi en grande partie sur la contribution de la chaîne de soutien des armées¹⁴ et notamment de la chaîne de soutien par les Bases de Défense (BdD).
140. La gestion de la fonction protection intègre donc la distinction et la complémentarité entre les chaînes des forces d'une part et les chaînes de soutien commun/spécialisé d'autre part.
141. Plus spécifiquement, pour le soutien à la mission de protection sur le TN :
- a. toute décision prise dans le cadre du soutien à la fonction protection implique la responsabilité de celui qui est en charge de la mission de protection dans sa globalité ; dans ce cadre, ce dernier est en position de « *soutenu* ». De telles décisions font aussi endosser une responsabilité à celui dont la mission est de soutenir la fonction protection ; dans ce cadre, celui-ci est en position de « *soutenant* » ;
 - b. la protection d'une installation militaire lie soutenant et soutenu sur les emprises où ils cohabitent. Les enjeux en matière de protection sont ainsi partagés ; ils exigent une collaboration dans la mesure où toute décision de l'un affecte le domaine de responsabilité de l'autre (cas particulier du contrôle périphérique d'un site). Dans la quasi-totalité des cas, le soutenu constitue l'enjeu prioritaire du dispositif de protection ;
 - c. les formations administratives telles que les Groupements de soutien des Bases de Défense (GSBdD) relèvent d'un commandement identifié qui exerce par conséquent ses responsabilités dans le domaine de la protection. Elles doivent être organisées afin

¹¹ La sécurité considérée implique la sécurité nationale.

¹² La responsabilité des autorités chargées de la protection est administrative, mais aussi pénale : toute autorité relevant du ministère de la Défense et exerçant un commandement ou des fonctions de direction est, dans le cadre de ses attributions, responsable (au sens juridique) de la sécurité des personnes et des biens (informations, matériels et installations) qui lui sont confiés.

¹³ Organisation Interarmées de l'Administration et du Soutien.

¹⁴ Dont le Service Infrastructure de la Défense.

de satisfaire leurs besoins propres en matière de protection (secret, habilitation, infrastructure...).

142. Les COMBdD et COMGSBdD doivent définir des procédures formelles de travail avec les unités soutenues, le premier au titre de son rôle de coordination des soutiens et d'arbitrage, et le second en sa qualité de responsable de formation d'emploi. Le processus de soutien conduisant *in fine* à une décision du soutenant, une méthode de travail doit permettre d'établir un « *contrat de soutien* » qui fait apparaître le « *soutien à la mission de protection* ».
143. Avenant à chaque plan de sécurité, ce contrat permet :
 - a. d'agréger les besoins en matière de protection et de sécurité ;
 - b. d'arrêter la liste des priorités « *communes* » en permettant de confronter les priorités exprimées par les soutenus¹⁵ conformément à leurs responsabilités en la matière ;
 - c. d'avoir la connaissance du coût (humain, financier et/ou matériel), même approximatif, de chaque opération pour construire un plan d'action, lequel doit se traduire en plan de charge pour l'unité du soutien concernée.
144. Parfois, des opérations ou certains leviers d'action peuvent échapper à l'autorité et à la décision de l'échelon local. Ils sont alors traités à un niveau de responsabilité supérieur. Ce processus est l'objet de la gouvernance placée au niveau des OIV têtes de chaîne, sous l'autorité du Chef d'état-major des armées (CEMA).

Le niveau de l'administration centrale

145. La protection étant une fonction transverse, elle nécessite des mesures d'anticipation, de coordination et d'arbitrage y compris au plus haut niveau.
146. Les échanges de prestations entre les grands services du MINDEF seront pris en considération dans des réunions *ad hoc* de niveau ministériel dans lesquelles les différentes entités du ministère seront représentées.
147. En situation de crise majeure sur le TN, la conduite de la mission de protection et la coordination des moyens s'effectueront, pour la Défense, sous l'autorité du CEMA à partir du Centre de planification et de conduite des opérations (CPCO) grâce à la chaîne OTIAD. Pour la gestion de cette situation exceptionnelle qui correspond à l'activation de la Cellule interministérielle de crise (CIC), la coordination des moyens s'effectuera au sein du Comité de DÉFense (CODEF)

Section III - Mode de fonctionnement de la protection

148. La gouvernance de la fonction protection s'exerce sous la direction du CEMA. La charge de la mission de protection incombe au personnel et aux organismes concernés, qu'ils soient désignés par décret ou que leur action concoure à la protection effective des installations militaires.
149. L'entretien de la protection est un processus qui nécessite une évaluation et une adaptation permanentes ; il valorise les choix de commandement.

La gouvernance de la fonction protection

150. Le périmètre de la « *protection des installations* » doit être sans cesse actualisé par la mise à jour de l'appréciation des enjeux et des moyens pour les protéger. En conséquence, un processus de dialogue itératif doit être entretenu au niveau interministériel.
151. Au sein du ministère de la Défense, les acteurs du domaine (OIV) se trouvent dans des situations disparates. Pour autant, ils ont la même obligation en matière de protection vis-à-vis de leurs emprises, notamment une obligation de moyens. Pour chaque OIV, la protection des installations militaires mobilise des ressources (infrastructure, équipements, personnel,

¹⁵ Les unités du Soutien exprimant, à l'occasion de ce processus, pour certaines fonctions, leurs propres besoins.

finances) dont la gestion organique est transverse et interarmées, notamment depuis la refonte de l'organisation du soutien. Il est donc nécessaire de mettre en relation étroite ceux qui expriment des besoins et ceux qui doivent les satisfaire¹⁶, ceux qui constatent les dysfonctionnements sur le terrain et ceux qui doivent les traiter, dans une logique d'obligation de moyens¹⁷ rationnelle et performante. Pour fonctionner, la protection des installations militaires fait l'objet d'une gouvernance permanente¹⁸, pilotée par l'EMA pour le CEMA.

152. Ce processus vise à entretenir la connaissance partagée des dimensions humaines et matérielles de la protection des installations, à harmoniser les concepts de protection et à anticiper la mutualisation de moyens entre OIV, afin de garantir l'homogénéité du niveau de protection global des installations militaires.

Hors situation de crise

153. Hors situation de crise, les outils et les procédures de protection mis en place permettent de hiérarchiser les efforts et les actions à mener pour garantir le niveau nécessaire de protection de chaque installation militaire.
154. La gouvernance est alimentée par les comptes-rendus des inspections conduites notamment par les Officiers généraux de zones de défense et de sécurité (OGZDS) qui permettent de suivre l'évolution de la protection des installations militaires au niveau régional et national, et de déceler les points préoccupants.
155. Les OGZDS effectuent annuellement une synthèse des inspections des PIV dans leurs zones respectives de responsabilité. Ces synthèses sont transmises à l'Inspection des Armées (IdA) qui les compile au niveau national. Les travaux de gouvernance peuvent simplifier cette procédure.
156. La gouvernance de la protection des installations militaires permet à tous les inspecteurs relevant du CEMA (IdA, OGZDS) de se concerter pour élaborer des procédures et des outils communs d'inspection.
157. Le CEMA doit disposer de deux échelles de valeurs :
- a. celle de l'urgence sécuritaire, issue des synthèses annuelles des OGZDS et de l'IdA ;
 - b. celle des coûts d'infrastructure à fin de « *Protection défense* ».
158. Les objectifs généraux de la politique de la gouvernance de protection, pilotée par l'EMA, sont de deux ordres :
- a. assurer le suivi du niveau de protection requis en application de la DNS « *AME* » dans un cadre interarmées et l'entretenir dans la durée ;
 - b. optimiser, hiérarchiser et répartir / attribuer les ressources disponibles au sein des armées, directions et services pour améliorer le niveau de protection et le maintenir à un niveau adapté aux menaces et aux risques que présente la situation.
159. L'information de la gouvernance n'est pas exclusive. Elle est ouverte à tous les acteurs majeurs des inspections. Ainsi, par exemple la Direction de la protection et de la sécurité et de la Défense (DPSD) et le Service infrastructure de la Défense (SID) participent à cette gouvernance en apportant leurs compétences aux inspections relevant du CEMA. La participation du SID à cette démarche est primordiale, dans la mesure où cet organisme est le seul à pouvoir chiffrer les besoins en aménagements nécessaires au maintien des conditions minimales de protection des installations militaires.

En situation de crise

160. En cas de crise, le dispositif de protection peut bénéficier d'un renforcement.

¹⁶ La protection des PIV est une préoccupation majeure de l'effort collectif de protection.

¹⁷ À hauteur de la ressource consentie par l'autorité responsable.

¹⁸ Qui a pris la forme d'une *Task Force* interarmées (*TFA*).

161. Les décisions de commandement et d'orientation de la protection en cas de crise font basculer cette mission de l'organique à l'opérationnel. Ainsi, une disposition renforcée¹⁹ de protection implique un poids supplémentaire correspondant à des arbitrages pouvant dépasser le domaine de compétence des chaînes de commandement fonctionnel des OIV.
162. Les efforts consentis entraînent un surcoût budgétaire lié à la mobilisation de ressources humaines et matérielles supplémentaires. Une telle manœuvre appelle l'implication de la chaîne OTIAD, sous l'autorité du CEMA.
163. Les choix arrêtés doivent être :
- a. adaptés aux difficultés du moment et à l'analyse des risques et menaces à venir ;
 - b. justifiés par sa nécessité militaire.
164. Ils découlent de contrats opérationnels particuliers qui détaillent les capacités à mettre en œuvre en soutien de la protection des installations militaires.

La conduite de la mission de protection

165. Le dispositif de protection doit empêcher les intrusions, les attaques ou toute autre menace par la prévention, la sensibilisation et le renseignement ; il contribue à la résilience. La résilience d'une installation réside dans son aptitude à conserver en situation dégradée puis à retrouver un équilibre de fonctionnement propre à permettre la mise en œuvre opérationnelle des capacités militaires auxquelles cette installation est dédiée.
166. Le processus de protection s'attache à la préservation de l'intégrité du patrimoine militaire. Il débute par l'évaluation de la menace, puis la mise en œuvre d'un plan de continuité de l'activité, il se poursuit par la « *contre agression* » et se termine par le retour à son niveau préalable de protection. Il peut fournir des capacités à d'autres installations ou accueillir lui-même des capacités en renfort.
167. La conduite de la mission de protection ne consiste donc pas à mobiliser systématiquement le maximum de forces pour obtenir la sécurité maximale, mais à mobiliser des moyens avec discernement, en tenant compte de leur utilité tactique et dissuasive, et en fonction de l'évaluation de la menace. Au fait des conditions imposées par la loi et conseillé par les officiers de sécurité, le commandement opère ainsi des choix²⁰ dans plusieurs domaines :
- a. humain (personnel et statuts afférents) ;
 - b. infrastructure et matériel (nature et fonction) ;
 - c. spatial (périmètre considéré pour les ressources de protection) ;
 - d. temporel (durée de la mobilisation des ressources) ;
 - e. opérationnel (priorités entre sites ou entre secteurs d'activités).
168. La protection d'une emprise militaire combine une approche interne relevant de l'OIV et une approche externe relevant du préfet.
169. La manœuvre extérieure porte sur l'ensemble des voies et moyens mobilisés, d'une part, pour faire face à l'agression de quelque nature que ce soit²¹ et, d'autre part, pour coopérer autant que de besoin avec les acteurs chargés de l'ordre public, c'est-à-dire les forces dont la mission relève de la police administrative et de la police judiciaire ; toutes leurs démarches de prévention et de répression visant à renforcer la protection d'un site doivent être favorisées.

¹⁹ Déclenchement possible, dans le même temps, du contrat « *protection* » 10 000 hommes sur le TN. Cette disposition (réflexe) ne peut être tenue que pendant quelques semaines, car elle affecte, potentiellement lourdement, le fonctionnement de l'organisation au sens où elle mobilise des ressources humaines exceptionnelles, comparables pour les armées à un effort de guerre.

²⁰ Les choix veillent à satisfaire les dispositions de la loi. Ils veillent à ce que toute évolution de cette dernière n'entraîne pas des conséquences matérielles insoutenables dans son application.

²¹ Mais prévue dans les PSO et PPP, en particulier, pour les PIV, en cohérence avec la Directive Nationale de Sécurité Activités Militaires de l'État (DNS-AME).

170. La coordination de tous les moyens d'intervention est précisée dans les PPP et les PPE. Ces efforts respectueux des missions, des prérogatives et des moyens de chacun concourent aux mêmes objectifs de sécurité. Cette manœuvre à part entière pour les Installations prioritaires de défense (IPD) s'effectue pour les autres sites de la Défense dans le cadre des missions de sécurité générale.

Chapitre 2

Le volet défensif de la protection

201. La protection est une mission permanente donnant lieu à un processus de type préventif.
202. Elle dispose de ressources et de moyens.
203. Le commandement organise ces éléments en fonction des nécessités.

Section I – Le cadre général

204. Les critères d'évaluation des choix de commandement pour la conduite de la mission de protection ne sont pas équivalents pour tous les sites.
205. Ils varient selon l'importance des sites et évoluent selon les circonstances.

Les ressources et les moyens

206. Initiée dès les premières réflexions de la conception d'une installation militaire, la résilience d'un site est entretenue au moyen d'un processus permanent de coordination des ressources et de combinaison des moyens²² consacrés au titre de la protection. Les dispositions d'infrastructure sont définies en fonction des menaces prises en compte lors de la définition de l'installation, avec donc un caractère pérenne (murs, merlons, bunkers...).
207. Les ressources correspondent aux effectifs consacrés participant à la mission de protection. La coordination des ressources vise à optimiser leur emploi en fonction des contraintes imposées par leur nature (statut, régime, poste...).
208. Les moyens correspondent aux dispositifs déployés. Ils concourent à la réalisation effective de la protection. La combinaison des moyens a pour objet d'optimiser leur mise en œuvre en fonction de leurs aptitudes et de leurs caractéristiques (technologies diverses).
209. La protection des installations repose sur des dispositifs de plusieurs natures qui répondent à des obligations distinctes :
 - a. la protection statique passive : clôtures, merlons, durcissement, camouflage... ;
 - b. la protection statique active : elle peut être matérielle (senseurs, effecteurs, sas...) ou humaine (gardiens, surveillants, filtreurs...) ;
 - c. la protection dynamique interne : patrouilles, intervention... ;
 - d. la protection dynamique externe ; recherche du renseignement, patrouilles relevant des autorités civiles ou militaires, dans le cadre de leurs attributions.
210. Spécifiques à chaque site, ces dispositifs humains et matériels relèvent soit directement du MINDEF, soit lui sont rattachés par un contrat d'externalisation.

Le niveau de risque

211. Les dispositifs de protection doivent pouvoir répondre à des situations qui peuvent évoluer en intensité. Pour cela, leur architecture et leur composition procèdent d'une aptitude à « monter en puissance » en adoptant l'une des trois dispositions génériques retenues : normale, renforcée et réflexe.

²² Notamment le personnel dûment formé, matériels de protection (vidéo protection, barrières et portiques...).

212. Le passage d'une posture à la suivante correspond à un renforcement progressif en moyens humains et matériels, ainsi qu'à la mise en œuvre de procédures particulières afin de densifier le dispositif de protection de chaque site.
213. La disposition normale peut être tenue, à moindre coût, sans limites de temps, la disposition de protection renforcée peut être tenue dans la durée²³, et la disposition réflexe, de quelques jours à quelques semaines. Cette dernière peut remettre en cause la capacité des sites à réaliser leur mission ordinaire, notamment si celle-ci ne revêt pas de caractère opérationnel particulier pour le traitement de la crise en cours.
214. Les dispositions de prévention s'inscrivent dans le cadre des PPP pour chaque site, en fonction des prescriptions de chaque OIV. Elles correspondent au degré de sensibilité des installations militaires considérées. À l'échelle du TN, elles imposent une connaissance de la ressource nécessaire et des modalités de sa mise en place, certains OIV ne possédant pas en propre la ressource prévue.
215. Ainsi, le volet défensif de la protection repose sur des choix de commandement et d'opportunité qui correspondent à une économie basée sur la coordination des ressources et la combinaison des moyens. La définition de niveaux de risque et de niveaux de menace contribue à harmoniser et à réguler la réponse des armées sous la forme de postures de protection. Cette harmonisation participe de l'efficacité globale du dispositif.

Section II – Équilibre entre les ressources et les moyens de protection

216. La protection est une mission opérationnelle de la défense. Sa réalisation s'inscrit dans une logique d'efficacité et de rationalisation.

Ressources dédiées à la protection

217. Toutes les personnes du MINDEF servant au sein d'une emprise militaire participent à sa protection.
218. Le personnel affecté ou en poste sur une installation militaire est responsable de sa défense en fonction de ses aptitudes et de ses obligations.

Personnel associé à la mission de protection

219. Le personnel associé à la mission de protection recherche essentiellement la détection des dangers et des menaces, notamment des intrusions. Il réalise des missions de surveillance, depuis le poste central de protection et par l'exécution de rondes avec si possible des équipes cynotechniques, et assure l'intervention si nécessaire.
220. Il s'adosse au dispositif statique, en particulier pour les emprises vastes et/ou particulièrement sensibles. Il ne doit pas s'y substituer, sauf en solution palliative et de court terme.

Le personnel militaire dédié

221. Il s'agit du personnel des unités militaires spécialisées (gendarmeries spécialisées, commandos de l'air...) ainsi que du personnel militaire qui peut, temporairement avoir des missions de protection dans le cadre de son service (service de garde de formations militaires telles que les bases, les régiments, les écoles, etc.).

Le personnel militaire en renfort

222. La protection des installations militaires de défense ne repose pas au premier chef sur leurs propres agents. La possibilité existe toutefois de les faire intervenir en renfort du dispositif normal de protection. Ce choix doit répondre à des critères d'efficacité et d'opportunité. L'efficacité du renfort est à considérer à la mesure des missions spécifiques des armées. Son opportunité est appréciée en considérant la plus value de ces renforts au regard du besoin conjoncturel accru de protection.

²³ Avec la mise en œuvre des plans VIGIPIRATE (Rouge), cette posture de protection renforcée s'est inscrite dans la durée.

- 223. De manière générale, les renforts en militaires sont consentis avec parcimonie. Autant que faire se peut, les moyens technologiques et les infrastructures de protection seront développés afin de pouvoir réduire le nombre de plantons, sentinelles et filtreurs et diminuer la vulnérabilité aux actions à distance.
- 224. Les ressources humaines constituent à la fois un objectif défini dans les contrats opérationnels et un levier d'action dans la gestion de la protection.
- 225. La définition et la mise en œuvre des contrats opérationnels entretiennent une dynamique dans la gestion des ressources disponibles, notamment du personnel et du budget alloué. Il s'agit d'honorer les exigences des engagements militaires, d'abord dans les opérations de combat puis, et de manière significative, dans les contributions militaires aux politiques publiques. Enfin, dans le cas des crises majeures, les contrats opérationnels guident la possibilité d'adaptation et d'orientation des ressources, tant pour la gestion de la fonction protection que pour la conduite des opérations.
- 226. En cas de crise majeure, la conduite de la mission de protection est exercée au niveau des sites par chacun des commandements. La coordination territoriale est du ressort de la chaîne OTIAD sous l'autorité du CEMA. Les grands équilibres ministériels sont décidés en CODEF et sont déclinés par les acteurs de la protection.

Le personnel civil associé à la mission de protection

- 227. Parmi le personnel lié à la mission de protection figurent également les employés des entreprises de sécurité investis d'une mission de protection en vertu d'un marché contracté avec le MINDEF.
- 228. Si des missions liées à la protection des installations militaires de défense peuvent être confiées à des vigiles en temps « *normal* », sous la forme de contrats passés avec des sociétés de prestation de service, les capacités de montée en puissance et d'intervention doivent relever de contrats opérationnels tant pour la protection intérieure que pour le renforcement extérieur.
- 229. L'externalisation de l'accueil, du filtrage et de la surveillance (au sens du gardiennage) est possible pour certains types de zone où la mission ne nécessite pas d'être armé.
- 230. Le gardiennage d'emprises ne présentant pas de caractère opérationnel, il a pour but de faire face aux responsabilités civiles du propriétaire (y compris dans les emprises en voie d'aliénation). Il consiste à surveiller et à alerter. Les agents qui la remplissent ne devant pas être obligatoirement armés, ce travail peut être externalisé et confié en totalité à une société de gardiennage.
- 231. Inversement, l'accueil/filtrage au sein d'une IPD ne peut pas être externalisé. Il en est de même pour les Zones de défense hautement sensibles (ZDHS). L'autorité militaire doit en garder le contrôle permanent : toutes les fonctions (accueil, filtrage, etc.) doivent être laissées au seul personnel de la défense.

Le personnel lié à la mission de protection

- 232. La protection des installations (terrain, construction, engin ou appareil quelconque²⁴...) intéressant la défense ou relevant du ministre de la Défense concerne chaque personnel du ministère, militaires et civils, et pas uniquement ceux dont l'emploi est dédié à la protection. Le professionnalisme de tous est l'une des conditions de l'efficacité de la protection. Ainsi, la vigilance générale (autocontrôle²⁵) complète le dispositif spécifique de protection.
- 233. De même, le personnel du GSBdD contribue à la mission de protection dans le domaine du service général, filtrage /renfort filtrage, surveillance, levée de doute et, s'il a bénéficié de la formation appropriée, en intervention.
- 234. Il revient à chaque OIV de faire acquérir au personnel placé sous son autorité cette culture de la protection puis de l'entretenir.
- 235. Pour cela, le personnel de la défense doit être persuadé :

²⁴ Ex. : art. 413-5 du Code pénal.

²⁵ Le port apparent d'un laissez-passer.

- a. de la réalité de la menace, des enjeux et des vulnérabilités ;
 - b. de la valeur du potentiel à sauvegarder ;
 - c. de l'importance de la participation de chacun.
236. En dehors des rappels, notamment par des circulaires, ou des indicateurs visuels, la sensibilisation du personnel de la défense s'obtient par une instruction relative à la protection et à la sécurité des moyens dispensée lors de périodes :
- a. de formation initiale en école et en centre de formation ;
 - b. de formation et d'information continue dans les unités et les formations d'emploi ;
 - c. d'exercice et d'entraînement ;
 - d. de contrôles de sécurité, programmés ou inopinés, qui contribuent également à la sensibilisation du personnel.

La combinaison des moyens de protection

237. Les moyens passifs et technologiques sont intégrés autant que de besoin à tous les projets de protection des installations militaires.
238. Ils permettent de limiter le personnel dédié. Toutefois, au bilan, l'entretien et la maintenance de ces moyens peuvent parfois s'avérer plus coûteux que les gains en personnel.
239. La signalisation est harmonisée et favorise l'information pour la sécurité de tous.

La crédibilité des infrastructures et des équipements

240. La protection s'appuie sur des infrastructures adaptées aux exigences de sûreté. Elle est même un critère d'élaboration des infrastructures. L'architecture et la prévention fondent en effet la qualité de la protection d'un site militaire. Elles concernent également les équipements qui concourent à la mission de sécurité.
241. L'évolution des critères de sûreté ou de la menace estimée peut entraîner des modifications du dispositif global ou particulier de la sûreté d'un site. Les adaptations des dispositifs de sûreté peuvent inclure des moyens techniques nouveaux. Les services rendus par ces derniers doivent s'intégrer durablement dans la mission de protection sans en alourdir le coût.
242. Les moyens et les équipements comprennent notamment :
- a. Des moyens de dissuasion visant à signaler la nature de l'emprise, les risques encourus en cas d'intrusion ainsi qu'à souligner les difficultés pour réaliser une intrusion. Ces moyens permettront de plus d'affirmer l'identité militaire de l'emprise.
 - b. Des moyens de détection, de levée de doute et de surveillance (détecteurs, capteurs et effecteurs) pour la protection contre l'intrusion, qui assurent l'essentiel des fonctions de filtrage, de détection et d'alerte.
 - c. Des moyens de liaison sûrs et fiables (internes et externes différenciés).
 - d. Des moyens de freinage adaptés aux délais d'intervention (clôtures, fossés, murs, portes, baies, toitures, meubles, barreaux... – armoires fortes si la cible est le Secret de la défense nationale - la liste n'étant pas exhaustive), mais aussi de durcissement, de camouflage et de masquage aux vues.
 - e. Des moyens pour l'intervention (armement, munitions, optronique, véhicules...).
 - f. Un Poste central de protection (PCP), ensemble de locaux où sont centralisées toutes les informations intéressant la protection (détection, vidéo, contrôle d'accès, levée de

doute, état d'équipements particuliers, rondiers...) et d'où sont déclenchées l'alerte et les réactions aux incidents.

Section III – Équilibre entre besoin d'accès et protection des sites

La visibilité de la protection

243. Les installations militaires de défense sont implantées au milieu des populations. Les citoyens, riverains ou passagers sont en devoir de respecter les restrictions aux libertés de circulation que ces installations imposent conformément à la loi. Les riverains doivent même bénéficier d'une information spécifique et épurée, donc non classifiée.
244. Pour cela, toutes les voies et tous les moyens qui contribuent à l'information de la population doivent être mis en œuvre par l'échelon de commandement *ad hoc*. En outre, cet effort d'information et de communication fortifie le lien Armées/Nation.
245. L'information à dispenser concerne à la fois les infrastructures (démarcations, signalétiques et servitudes) et les activités générales. Elle intervient au travers de campagnes d'information et de contacts variés avec la population et les élus locaux, et à l'occasion de patrouilles sur le périmètre militaire.
- La délimitation exhaustive d'une emprise militaire (signalétique, barrières, clôtures...) et la mention explicite des restrictions aux libertés individuelles et collectives (panneaux d'information, panneaux d'avertissement...) qui s'y exercent sont un gage de la volonté d'informer qui permet, autant que de besoin, le rappel des dispositions de la loi. Pérenne et cohérente sur l'ensemble du TN, la visibilité de la protection résulte des efforts consentis au moment de la construction et à l'occasion de la maintenance et de l'entretien des installations.
 - De plus, la communication externe (portes ouvertes, réunions d'information...) à l'adresse des populations est un levier complémentaire de l'efficacité du dispositif d'une installation militaire. Elle repose sur l'initiative et l'engagement des échelons de commandement considérés.
246. Ainsi, la bonne intégration d'une installation militaire dans son environnement géographique et administratif concourt au renforcement de sa protection. Elle favorise l'intérêt qui lui est porté par la population.

L'accessibilité aux installations militaires

247. L'accès à un site militaire bénéficiant d'une protection dynamique repose sur trois éléments :
- le Poste d'accueil et de filtrage (PAF), et éventuellement les autres postes de filtrage ;
 - le Poste central de protection (PCP) ;
 - l'Élément d'intervention (EI).
248. Le PAF²⁶ délivrant les autorisations d'accès, sa sécurité doit être assurée et les informations transmises entre le PCP, l'EI et le PAF doivent être garanties par des liaisons sécurisées (fiables et redondantes).
249. Toutes les installations sont particulièrement vulnérables aux endroits où le contact avec l'extérieur est le plus direct, et aux moments où ceux-ci sont plus nombreux, lors de l'arrivée ou du départ du personnel notamment. Le filtrage consiste à contrôler et à limiter l'accès au site. Il est le premier obstacle à une agression éventuelle. En tant que point de contact entre le domaine militaire et le domaine civil, le PAF est un enjeu particulier. Il devra être cohérent avec la périmétrie (clôture, accès secondaire...).
250. L'autorité en charge de l'installation doit définir les mesures générales et particulières propres à assurer le contrôle d'accès le mieux adapté aux conditions locales.

²⁶ Le PAF est le premier lieu de détection d'une éventuelle personne suspecte.

251. Le poste d'accueil est destiné :
- a. à informer personnel et visiteurs des conditions d'accès ;
 - b. à permettre aux usagers de se mettre en conformité avec la réglementation en vigueur.
252. Le filtrage concerne à la fois les personnes et les véhicules, et doit suivre les recommandations suivantes :
- a. le système de contrôle d'accès doit être du type « *identification* » pour les accédants. En l'absence de personnel de filtrage, un système automatisé d'identification devra être couplé à une fonction d'unicité de passage. Pour certains sites particulièrement sensibles, une authentification du porteur sera requise (code pin, données bio...).
 - b. l'accès des véhicules sera limité aux seuls véhicules autorisés²⁷. Sur autorisation du commandement, les véhicules désignés, par exemple appartenant à des entreprises titulaires de marchés, pourront accéder au site considéré, après contrôle physique du conducteur et des passagers et, si nécessaire, en fonction du niveau d'alerte, examen visuel du véhicule (chargement, châssis, moteur, habitacle...) et plus approfondi le cas échéant ;
 - c. l'infrastructure du PAF est située, le plus souvent, à proximité de l'entrée principale (éventuellement d'entrées secondaires) pour faciliter le contrôle et le filtrage des accès. Il ne doit pas être commun avec le PCP. S'il est contigu, ce qui est à éviter, aucune ouverture ne doit permettre le passage de l'un à l'autre.
253. Il est recommandé que le poste de filtrage soit protégé contre les tirs directs. Il est utile qu'il dispose de vitrages opaques aux vues extérieures et de dispositifs permettant la mise en œuvre d'armes de défense (sabords ou opercules manœuvrables de l'intérieur).
254. Le poste de contrôle doit être équipé :
- a. de commandes d'ouverture et de fermeture des barrières et du portail ;
 - b. de liaisons phoniques permettant le dialogue avec le poste d'accueil et le PCP ;
 - c. d'un interphone relié à celui du portail ;
 - d. des commandes d'éclairage de la zone d'accès ;
 - e. d'une alarme « *coup de poing* » reliée au PCP.
255. L'accès au site doit être configuré de telle manière qu'il concilie trois impératifs :
- a. permettre d'améliorer la sécurité du personnel et de l'emprise lors des opérations de filtrage ;
 - b. ne pas entraver le bon fonctionnement du site quelles que soient les situations ;
 - c. permettre de s'adapter sans délai à un besoin soudain comme une urgence médicale.
256. Pour ce faire, il est nécessaire de disposer :
- a. d'une signalisation conforme au statut de la zone.
 - b. de panneaux d'accueil informant les usagers des modalités d'accès ;
 - c. d'un portail permettant d'assurer la continuité du dispositif de protection périmétrique ;
 - d. d'un dispositif d'arrêt permettant soit un libre passage des véhicules, soit un passage automatique après identification, soit une ouverture à la demande ;

²⁷ Tout véhicule conduit par une personne autorisée est réputé autorisé hormis, éventuellement, certains véhicules atypiques.

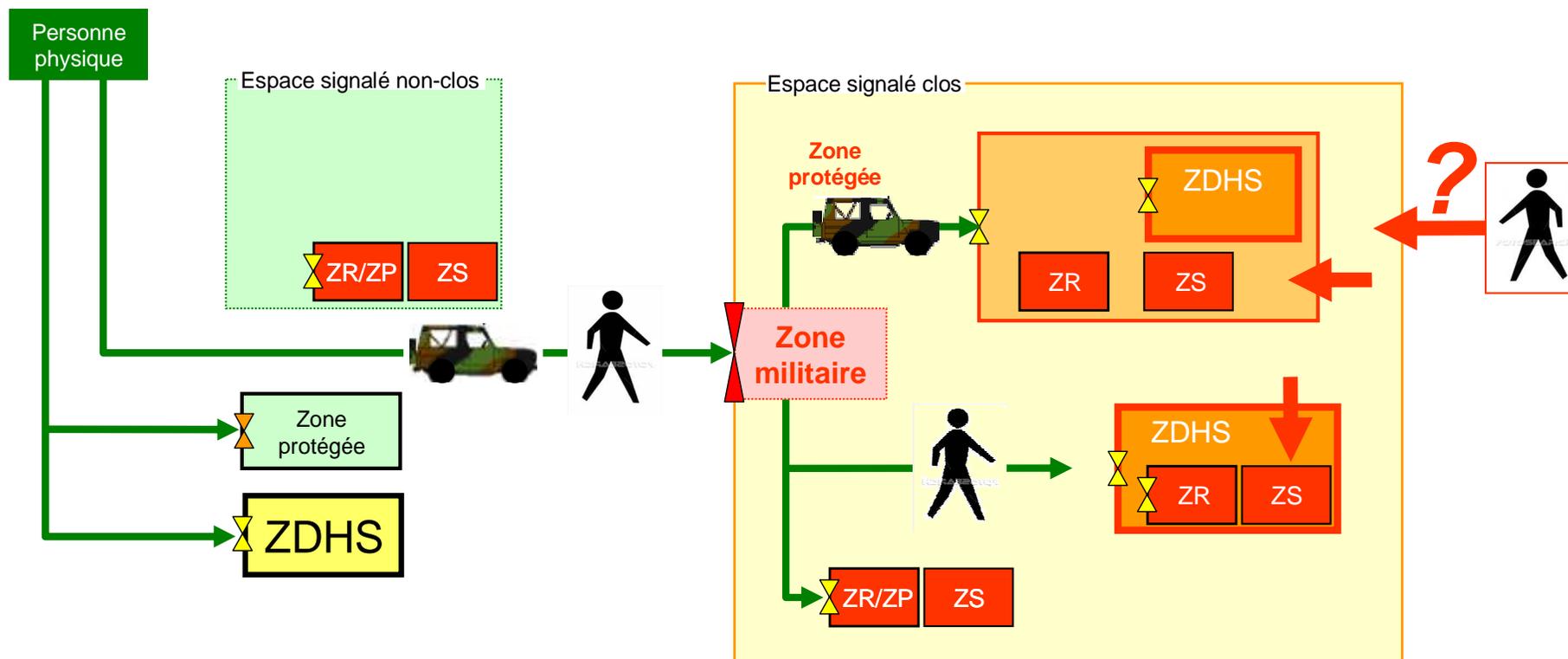
- e. d'une aire permettant le stationnement des véhicules ne disposant pas d'autorisation, de préférence située à l'extérieur de la zone protégée ;
 - f. d'une aire suffisamment large pour, d'une part, favoriser le contrôle des véhicules entrants (véhicule, cargaison) et, d'autre part, permettre le dégagement des véhicules ne présentant pas les garanties suffisantes à l'entrée (fin de validité des droits, cargaison non conforme...) ;
 - g. de dispositifs d'identification pour le personnel autorisé ;
 - h. de dispositifs antivéhicules, si possible à déploiement rapide, automatique ou manuel ;
 - i. d'un éclairage sur toute la zone ;
 - j. d'une visualisation de la zone d'accès et de ses abords.
257. La liste de ces mesures pérennes n'est pas exhaustive. Elle doit être appliquée avec discernement. Son application stricto sensu n'est nécessaire que pour les sites qui présentent une vulnérabilité et une sensibilité incontestables.

Le contrôle d'accès de protection

258. Le contrôle des personnes et des biens est une nécessité de la protection. La nécessité du contrôle permanent des accès aux sites protégés ne doit pas conduire à la congestion des flux concourant à leur fonctionnement normal, sauf pour les sites et les installations ayant une sensibilité le justifiant, dans le respect des contraintes liées à la sécurité des personnes.
- a. L'accès physique au site, notamment par le poste d'accueil et de filtrage, est un point particulier du dispositif général de la protection du site. Il combine des dispositifs techniques qui viennent s'ajouter à la présence d'un personnel qui requiert sa propre protection.
 - b. La protection des Informations et des supports classifiés (ISC) procède de l'ensemble des dispositions physiques prises sur le site et complétées par un processus d'habilitation et de l'application du principe du « *besoin d'en connaître* » traduit, sous la responsabilité du chef de site, par la tenue d'un catalogue des emplois (habilités **SECRET DÉFENSE** [SD] et, désormais, **CONFIDENTIEL DÉFENSE** [CD]) et la maîtrise de la gestion du courrier classifié.

Droit d'accès aux sites : le Laissez-passer (LP)

259. L'accès aux emprises et aux installations militaires correspond à une autorisation délivrée par l'autorité légitime.
260. Les commandants de formation définissent les règles d'accès à leur installation/site et en attribuent les droits, car ils en sont responsables pénalement. Un droit d'accès est nominatif. Il est délivré en principe par l'autorité du site qui détient le secret ou qui est responsable de l'installation, du matériel ou de l'activité à protéger. Son attribution est un acte de commandement.
261. Tout officier de sécurité doit, pour le commandant de formation dont il relève, se prémunir contre les atteintes à la sécurité qui pourraient venir des personnes qui demandent un accès au site. Dans ce cadre, il doit effectuer un contrôle élémentaire. En cas d'impossibilité, il doit mettre en place une procédure palliative pour permettre l'accès au site (dans le respect de la protection du secret) comme une escorte ou tout autre moyen approprié.
262. Une distinction claire doit être faite entre les permanents du site et les visiteurs (extérieurs, de passage...). Dans les zones protégées, le Laissez-passer (LP) est porté en permanence afin de permettre une identification visuelle aisée du porteur.



ZS / LS : Zone ou local sécurisé

ZR : Zone réservée

Contrôle d'accès : Poste d'accueil et de filtrage (PAF)

Contrôle d'accès : Poste AF ou de filtrage

Contrôle d'accès Poste F

Principes :

- le contrôle d'accès sur une installation militaire close est obligatoire
- une ZR doit être incluse dans une ZP
- de préférence, une ZDHS devrait être incluse dans une ZP (profondeur)
- ZP et ZDHS sont obligatoirement closes. Une ZP est ouvrable dans un environnement et selon des procédures à définir localement
- au classement en ZP ne correspond pas de mesure de protection physique
- l'entrée d'une ZR pour les personnes habilitées et ayant besoin d'en connaître
- le LP est principalement destiné à entrer dans une ZP

Figure 1 – Organisation du contrôle d'accès

263. Cas des Bases de Défense (BdD).
- a. Les commandants de formation demeurent responsables de la protection de leur installation même si tout ou partie des prestations liées à la protection a été externalisé. Ils doivent avoir une possibilité d'intervenir auprès des prestataires.
 - b. Une gestion complète des LP peut être recherchée au niveau des formations soutenues si elles en font la demande, à condition de disposer des ressources nécessaires.
 - c. Sous l'autorité du COM BdD, un catalogue du personnel d'intervention est élaboré et mis à jour périodiquement, au moins annuellement, et est diffusé aux officiers de sécurité des unités soutenues afin de faciliter l'accès à leurs installations.
 - d. La mise en place au plan national d'une carte d'identité militaire sécurisée doit orienter tous les sites de la Défense vers la création d'un LP unique, chaque site pouvant faire l'objet d'un visuel spécifique. Sur la plupart des sites militaires, le besoin d'un LP spécifique peut subsister, notamment en l'absence de dispositifs de filtrage automatisés et pour l'accès à des installations présentant une sensibilité supérieure aux exigences du contrôle périphérique du site d'accueil.
264. Cas des Groupements de soutien des Bases de Défense (GSBdD).
- a. Pour tous les contrats initiés par le GSBdD, mais aussi vis-à-vis des entreprises intervenant dans le cadre de contrats avec détention d'Informations et de supports classifiés (ISC) et contrats avec accès à des ISC²⁸, le bureau de protection du GSBdD peut centraliser et initier toutes les demandes de contrôle élémentaire du personnel des entreprises amené à travailler au sein des formations soutenues. Les conclusions doivent être systématiquement transmises aux commandants des formations soutenues afin qu'ils accordent temporairement le droit d'accès à leurs installations respectives.
 - b. Ce type de rationalisation est souhaitable. La présence d'un interlocuteur unique pour la DPSD minimise les difficultés en supprimant le risque de multiplication des demandes de Contrôle élémentaire (CE) pour une même entreprise sur le territoire de la BdD. L'initiateur du contrat (GSBdD) conserve la direction du dossier tout en permettant à un chef de corps soutenu de faire valoir ses prérogatives en termes d'accès à son emprise, car la décision finale lui revient. Cette procédure permet un dialogue entre soutenant et soutenu sur l'intervention des entreprises (échéances, prestations, ouverture et fermeture de chantier, etc.).

Le droit d'accès à l'information : l'habilitation

265. L'habilitation donne accès à de l'information classifiée en vertu du besoin d'en connaître qui est apprécié par le détenteur du secret. Le chef d'établissement gère les demandes de LP et les cartes d'accès aux locaux sensibles. Il lui appartient le cas échéant de procéder au retrait du LP en cas d'insatisfaction motivée.
266. L'habilitation ne constitue pas un droit d'accès à une installation. En revanche, elle constitue un prérequis pour l'établissement d'un droit d'accès à une installation classifiée.
267. Le bureau de protection est directement rattaché au commandant de formation. Il assure le traitement administratif des demandes d'habilitation et de renouvellement des habilitations pour tout le personnel soutenu. Il exprime les demandes de contrôle élémentaire vers la DPSD (antenne locale).
268. Le traitement des habilitations et la confection des LP peuvent opportunément être colocalisés au sein d'un même « local ». Ce local doit être sécurisé, en cohérence avec la confidentialité des dossiers d'habilitation et la confection et la manipulation des LP.

²⁸ L'arrêté du 23.07.2010 à préciser par la DGA.

Section IV – Contrôles, inspections et enquêtes

269. La mise à l'épreuve formelle des installations militaires correspond à la vérification du dispositif de protection. Elle relève de différents organismes. Les conclusions de leurs rapports visent à l'entretien et à l'amélioration du niveau de protection. Elles éclairent et orientent l'exercice de la responsabilité de protection.

Les structures visant à l'amélioration de la protection

270. Les différentes inspections compétentes en matière de protection défense se distinguent par le niveau des autorités au profit desquelles elles agissent et par leurs buts.
- a. L'Inspection des armements nucléaires (IAN) dépend directement du président de la République.
 - b. Le Contrôle général des armées (CGA) dépend du ministre de la Défense. Il l'assiste pour la direction de la gestion de son ministère. Il s'assure de l'adéquation des structures et des moyens aux missions des armées, de l'opportunité des décisions et de l'efficacité des résultats obtenus au regard des objectifs fixés et du bon emploi des financements publics. Il vérifie dans les armées et les services du ministère l'observation des lois, des règlements et des instructions ministérielles.
 - c. L'Inspection générale des armées (IGA) dépend également du ministre de la Défense.
 - d. La DPSD dépend elle aussi du ministre de la Défense. Ce service a une action essentiellement préventive. Il permet au ministre de la Défense d'assumer pleinement ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles. Lorsque la DPSD inspecte des installations de protection des emprises militaires, elle apporte son concours aux opérateurs d'importance vitale par :
 - (1) ses conseils techniques ;
 - (2) le contrôle des mesures prises en matière de protection et de sécurité globale ;
 - (3) la recherche du renseignement d'environnement ;
 - (4) sa participation au contrôle du personnel et sa sensibilisation en matière de sécurité.
 - e. L'IdA dépend directement du CEMA. Elle l'assiste pour ce qui concerne l'exercice de son pouvoir permanent d'inspection²⁹. Elle inspecte toutes les IPD et peut inspecter tous les PIV, lesquels relèvent normalement des attributions des OGZDS en métropole et des COMSUP dans les Départements et collectivités d'outre-mer (DOM-COM). Elle tient les OIV informés de ses observations. Elle propose au CEMA des mesures propres à améliorer la sécurité des installations.
 - f. Les inspections d'armées et de grands services, qui agissent au profit des OIV.
 - g. Les OGZDS, responsables au niveau zonal de l'inspection des PIV.
 - h. Dans les départements et collectivités d'outre-mer, les PIV sont inspectés par les COMSUP.
 - i. Le SID qui, comme indiqué à l'article 160, conseille, conçoit et vérifie les installations de protection tant dans les domaines du freinage que de la détection, du contrôle d'accès ou encore de la levée de doute et de l'exploitation.

²⁹ Article 1 de l'arrêté du 05 janvier 2004 fixant les attributions de l'inspecteur des forces en opérations et de la défense du territoire (IFODT), complété par l'arrêté du 27 octobre 2009 fixant les attributions de l'inspection des armées.

Les buts du contrôle

271. Le contrôle est une démarche qui s'inscrit naturellement dans les prérogatives du commandement.
272. Il permet à tout responsable de vérifier ou de faire vérifier la mise en application de ses ordres, en conformité avec les lois et les règlements.
273. Les inspections sont les entités identifiées pour effectuer officiellement le contrôle au nom de l'autorité responsable qu'elles représentent.
274. Elles permettent de mesurer la réalité des situations en matière de protection des installations militaires et de rendre compte directement aux décideurs des difficultés rencontrées. Elles sont donc un outil d'alerte pour les responsables de la protection des installations militaires.
275. Les inspections permettent ainsi de vérifier :
- a. La connaissance et la mise en application des textes légaux et réglementaires, du niveau central au plan local.
 - b. La traduction concrète de ces textes au plan local :
 - (1) Par la mise en place de procédures relatives à la protection des emprises militaires. Ces procédures doivent être rédigées dans le respect des textes légaux et réglementaires, et compléter ces derniers pour permettre leur mise en œuvre locale.
 - (2) Par la mise en œuvre de moyens de protection passifs. Ces moyens regroupent les infrastructures de protection au sens large, depuis les clôtures des enceintes jusqu'aux bâtiments, en incluant les moyens de détection et de surveillance.
 - (3) Par la mise en place du personnel dédié à la protection « active » et la sensibilisation du personnel non dédié, cependant responsable de la protection de son lieu de travail.
 - c. La cohérence d'ensemble de ces mesures à son niveau d'inspection, central, régional ou local, se traduisant par la vérification :
 - (1) De la complémentarité entre les moyens matériels et le personnel dédié à la protection.
 - (2) De la réalisation effective d'une défense en profondeur selon le principe d'« emboîtement » des différents périmètres le plus difficile d'accès devant être le plus sensible.
 - (3) De la capacité de résistance des infrastructures, proportionnelle aux délais d'intervention de l'élément dédié.
276. Elles visent donc à :
- a. examiner les dispositions prises au niveau contrôlé et à évaluer leur efficacité ;
 - b. vérifier la connaissance, la compréhension et l'application effective des consignes par le personnel concerné ;
 - c. évaluer les capacités de réaction du personnel chargé de la protection des installations ;
 - d. appréhender les lacunes du dispositif ou observer les écarts par rapport aux normes, et à recommander des actions pour y remédier.
277. Chaque mission d'inspection donne lieu à un compte-rendu écrit, destiné à l'autorité dont dépend le contrôleur. Ces documents doivent pouvoir distinguer ce qui relève de l'échelon local

ou de l'échelon central. Ils permettent de confirmer les bonnes pratiques au sein des unités inspectées et d'attirer l'attention des décideurs sur les dysfonctionnements constatés relevant de leur responsabilité.

278. Toute inspection, quel que soit son niveau, émet des recommandations. Ses conclusions sont proposées à l'autorité qui l'a mandatée.
279. Les modalités du contrôle dépendent de son niveau d'exercice.
280. Au plan national, les modalités des inspections et des contrôles des installations militaires en matière de protection sont fixées dans le cadre des attributions des organismes chargés de ces contrôles.
281. Les OIV qui assument des responsabilités directes sont engagés à exercer leur tutelle afin de vérifier la bonne application de la politique de protection qu'ils ont arrêtée. Le cas échéant, il leur appartient de prendre les mesures d'adaptation qui leur seraient suggérées par le contrôle ou le retour d'expérience.
282. Au plan local, le contrôle s'exerce de façon inopinée (visiteur mystère par exemple) ou sous la forme d'inspections programmées par l'autorité en charge de la protection.
283. La fréquence du contrôle doit être proportionnelle à la sensibilité des installations et matériels à protéger, et adaptée à la nécessité d'entretenir la connaissance de la situation.
284. Les contrôles internes sont portés sur un registre adéquat afin d'en garder une trace écrite.
285. Le contrôle s'exerce plus particulièrement :
 - a. aux niveaux central et intermédiaire, conformément aux attributions des organismes chargés des inspections et du contrôle des installations militaires dans le domaine de la protection ;
 - b. au plan national, où les organismes chargés du contrôle et des inspections établissent, généralement après consultation du responsable de chaque installation objet du contrôle, un calendrier prévisionnel annuel des contrôles qu'ils envisagent de mener.

Chapitre 3

Le volet réactif de la protection

- 301. La réaction consiste à maintenir le potentiel capacitaire des armées contre toute forme d'intrusion malveillante. Elle comprend la neutralisation de l'agression, mais également l'adaptation du dispositif pendant et après l'agression (effet de résilience).
- 302. Le volet réactif de la protection consiste en une intervention qui vise à reprendre le contrôle complet de la situation, tel qu'il existait avant l'intrusion, par une manœuvre planifiée et conduite jusqu'à son terme.
- 303. L'intervention signifie une décision de commandement de recourir à la force. Elle s'articule autour d'un EI ; l'autorité responsable de la protection veille à la bonne mise en œuvre de ses prérogatives en matière d'emploi de la force et, le cas échéant, d'usage des armes.

Section I - Le processus de réaction à la menace

- 304. Fondée sur la détection, c'est-à-dire encore en amont sur la vigilance, la réaction à la menace commence par la transformation d'une détection en alerte et repose ensuite sur sa bonne diffusion.
- 305. La réaction à la menace vise à rétablir le niveau d'intégrité d'une installation. Elle vise la préservation du potentiel militaire, participe à la réduction de la menace identifiée, comporte l'adaptation du dispositif de protection et, au besoin, débouche sur son amélioration en concertation avec les acteurs chargés de l'ordre public.

Intervenir

- 306. Dans la protection, la chaîne de commandement est confrontée à des situations variées et parfois inhabituelles qui exigent des réactions immédiates ou quasi immédiates, adaptées et proportionnées.
- 307. Le dispositif coercitif « *en place* », ou déployé, doit montrer clairement une maîtrise tactique de l'emploi de la force.
- 308. La neutralisation de l'intrusion ou de l'agression passe par une intervention puis se prolonge par une adaptation du dispositif. La priorité consiste à faire cesser la menace, si nécessaire par l'emploi de la force.
- 309. Dans le cadre d'une intervention, l'emploi de la force est limité au périmètre de la responsabilité juridique du déploiement de la force légitime (légitime défense). Elle vise à réduire ou neutraliser l'élément perturbateur.
- 310. Le coût de l'intervention comme le degré d'emploi de la force autorisé doivent être à la hauteur de l'enjeu opérationnel.

Concourir

- 311. Une intervention est menée en liaison avec les forces de l'ordre, avec comme objectif la protection immédiate de l'installation et la perspective de suites données dans le cadre de la police judiciaire. Le personnel et les capacités du MINDEF consacrés à la mission de protection agissent notamment dans la collecte des informations générales et la préservation des indices en cas d'intrusion. Cette action de concours s'exerce dans le cadre de la responsabilité juridique sur les alentours immédiats de l'installation.

Tirer les enseignements

312. La fin de l'intervention ne signifie pas le retour à l'état initial de protection du dispositif. L'expérience vécue motive la relance d'une réflexion autour de la cohérence du dispositif défini dans le plan de protection.
313. Ayant identifié l'autorité administrative (préfet) chargée de la coopération, le commandement agit en partenariat étroit avec les autres acteurs afin de favoriser l'efficacité des capacités engagées selon leurs domaines de compétence. Il sollicite le concours des forces de sécurité territorialement compétentes et informe les autorités chargées de l'ordre public autant que de besoin. Il entretient les contacts nécessaires avec l'autorité judiciaire compétente (procureur de la République).

Section II – Les conditions d'application de l'emploi de la force dans l'intervention

314. L'emploi de la force répond aux dispositions de la loi.

Des prérogatives de droit commun

315. L'emploi gradué de la contrainte s'exerce dans le cadre de la loi³⁰.
316. La contrainte comporte non seulement l'intervention elle-même, et donc l'usage de la force, mais aussi tous les dispositifs humains et techniques qui visent à ralentir ou empêcher une intrusion : murs d'enceintes, grillages, etc. Dispositif après dispositif, la contrainte se fait plus pressante : cette gradation correspond à différents régimes juridiques et à une responsabilité pénale de plus en plus forte pour la personne qui s'introduit et, à l'inverse, de moins en moins forte pour les personnes chargées de la protection.
317. Les militaires sont soumis au droit commun. Aux abords de l'installation, ils peuvent demander à une personne inconnue les raisons de sa présence et, ensuite, décider de la conduite à tenir en fonction de sa réaction.

Les applications selon les zones d'intervention

318. Les armées étant responsables de la protection à l'intérieur de leurs emprises, elles doivent être en mesure de faire cesser une intrusion, voire une agression. L'infraction étant constituée, il s'agit de permettre aux forces de l'ordre de diligenter la suite de la procédure judiciaire.
319. L'objectif commun pour la protection des installations, des activités et/ou des matériels n'est pas, pour la majorité des sites, d'arrêter l'intrus, mais de caractériser l'action qu'il entreprend et de la faire cesser.
320. Les règles « *d'emploi de la force* » correspondent aux « *mesures actives* » décidées pour conduire l'intervention qui peuvent consister à :
- Zone militaire (ZM)³¹ : reconduire l'intrus à la sortie ou, s'il n'obtempère pas et se place donc en situation de délit, l'immobiliser et le confier à un Officier de police judiciaire (OPJ) territorialement compétent à fin de poursuites judiciaires.
 - Zone protégée (ZP) : immobiliser l'intrus et le présenter à un OPJ territorialement compétent à fin de poursuites judiciaires.
321. ZDHS : même action que pour TM/ZP et, en cas extrême et sous certaines conditions, neutralisation. L'usage des armes à feu est possible en dehors du cadre de la légitime défense.
322. **Nota** : la ZDHS ne se situe pas sur le même plan qu'une ZM ou une ZP. La notion de ZDHS a été voulue par le législateur pour permettre l'usage des armes, y compris des armes à feu, en dehors de la légitime défense. Concrètement, une ZDHS est une aire géographique qui doit

³⁰ La loi française sur le TN.

³¹ Communément appelée « *Terrain militaire* ».

être identifiée et instaurée en ZP si la ZDHS n'est pas initialement incluse dans une ZP. Le fondement juridique de la ZDHS n'est pas celui des ZM/ZP.

Les applications selon les niveaux de menace

323. Les « règles d'engagement » sont couvertes par la notion de « mesures actives ». Si le niveau de menace augmente, la densité du dispositif de protection et, par conséquent, la présence sur zone de moyens humains seront renforcées. On parle de niveaux de protection (traduits en mesures adaptées dans les plans particuliers). Ils sont en général liés aux stades (et aux mesures prévues) de VIGIPIRATE (qui ne concerne que la menace terroriste). Les Règles opérationnelles d'engagement (ROE) demeureront les mêmes. Seuls les « états d'exception » pourraient permettre d'y déroger.

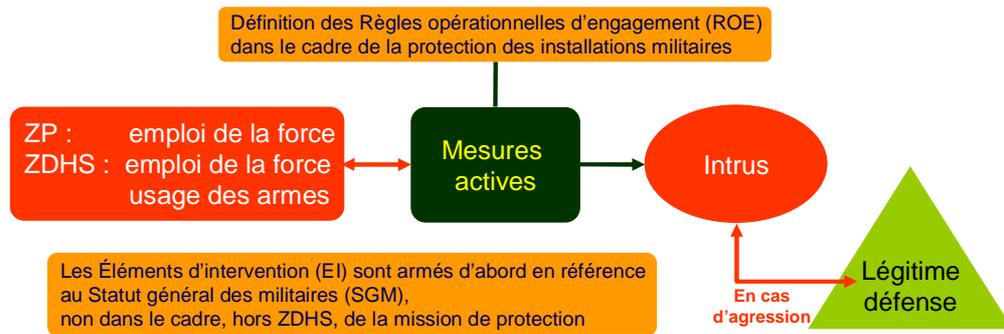


Figure 2 – Application

324. Au sens de la loi, l'intervention et les mesures actives impliquent l'emploi de la force ; dans une ZDHS, la mesure active peut consister en l'usage des armes.

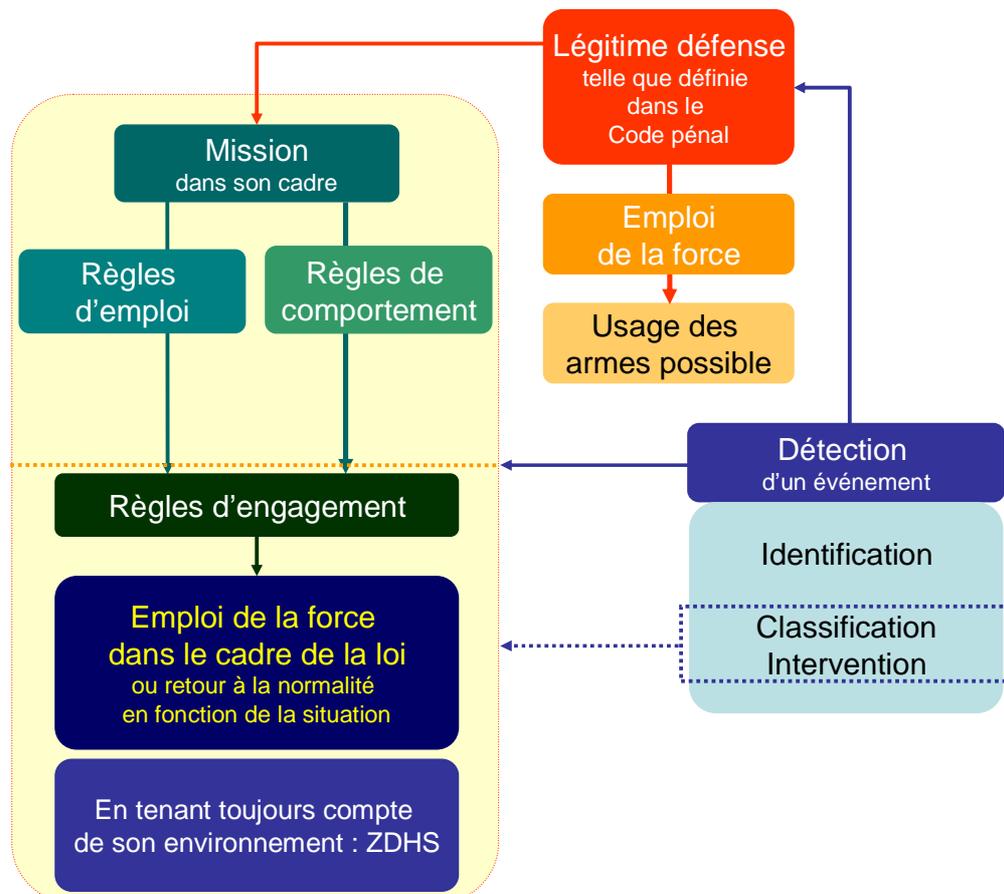


Figure 3 – Synoptique d'exécution des mesures de PIM

Section III - L'Élément d'intervention (EI) dans le volet réactif de l'intervention

325. Un élément d'intervention est un élément autonome et instruit, en mesure de réaliser une mission dynamique au profit exclusif de la mission de protection au sein d'un site militaire.

Missions de l'EI

326. En alerte permanente, l'élément d'intervention a pour missions principales :
- a. D'intervenir rapidement, dans un laps de temps court en intervention immédiate, sur les lieux d'une intrusion localisée ou en tout point du site, mais aussi à partir d'une installation ou d'un site voisin (PIV, mutualisation) pour, *a minima*, procéder au lever de doute.
 - b. De faire face à un agresseur malveillant ou à un intrus et, le cas échéant, de le maîtriser, en relation avec le PCP (ou les forces de l'ordre), pour l'empêcher d'atteindre les points névralgiques et les locaux sensibles du site.
327. Il peut participer aux rondes et patrouilles sans toutefois compromettre sa capacité à intervenir dans des délais acceptables en tout lieu de l'installation qu'il protège, ou de celles pour lesquelles la mutualisation est possible.
328. L'EI agit selon les ordres qui sont prescrits, en général, par le chef du PCP.
329. Le chef de l'EI, nommé désigné par l'autorité responsable de l'installation militaire, assure la sécurité de l'armement de son équipe dans le cadre de l'exécution de sa mission menée en dehors de la zone militaire (ou de l'intervention mutualisée au profit de sites isolés).
330. Chaque équipier de l'EI est responsable de l'application des consignes liées à l'emploi de la force.
331. L'instruction en matière de sécurité des installations est une responsabilité du commandant de formation ou d'établissement.
332. L'instruction du personnel, dédié ou non à la protection des installations, doit porter sur la connaissance des enjeux, des moyens et des limites pour assurer la mission de protection :
- a. connaissance approfondie de l'armement dont il est doté ;
 - b. habilitation à l'emploi des armes dont il est doté ;
 - c. formation à l'emploi de la force dans le cadre de cette mission particulière ;
 - d. connaissance approfondie du site, des systèmes de détection (type, localisation) et des procédures d'intervention.

Composition de l'EI

333. Seul l'élément d'intervention agissant au sein d'un PIV est exclusivement composé de personnel militaire.
334. L'EI est composé de personnels en nombre variable : il peut typiquement comprendre un sous-officier et quatre militaires du rang (format 0/1/4). Il ne doit pas descendre en dessous du binôme en situation normale, même pour des sites présentant une faible valeur opérationnelle quel que soit le niveau de menace.
335. Sa composition et son existence, in situ ou à distance, en réaction immédiate ou à temps, sont liées à la vulnérabilité du site et à la posture de protection. Il convient, dans ce domaine, de faire preuve de discernement pour éviter une inflation dans le coût humain de la protection.

- 336. Le personnel doit être instruit et recevoir des consignes précises sur sa mission, sur l'usage des armes, en particulier des armes à feu, puisque le régime d'emploi des armes et de la force en intervention change avec la nature juridique du terrain.
- 337. La technicité du personnel affecté à la protection est adaptée au niveau de sensibilité du site et aux enjeux liés à sa protection. Les consignes et les modes d'action en découlent.

Zones d'intervention de l'EI

- 338. La ZM n'impose aucun élément d'intervention. Si elle englobe une ZP, l'élément d'intervention pour la ZP peut être mutualisé, mais sans objectif opérationnel autre que la lutte contre la recherche de renseignements ou la prévention contre une intrusion.
- 339. La ZP n'impose pas la présence in situ de l'élément d'intervention qui peut donc être placé « à temps ». La ZP sert par ailleurs à donner de la profondeur à la ZDHS, à l'instar de toute installation que l'on veut protéger.
- 340. La ZDHS impose, par souci de cohérence :
 - a. La présence permanente sur le site de l'élément militaire d'intervention « *immédiate* ».
 - b. Le recours au seul personnel de la Défense.
- 341. L'intervention en ZP peut être déclenchée au moyen de systèmes de surveillance et/ou de détection. Ils permettent de faire l'économie du recours permanent à des moyens humains. En l'absence de ZDHS, l'économie des moyens humains doit être recherchée.
- 342. Si un élément d'intervention peut se trouver à « x » minutes du site à protéger (PIV), le même principe peut être appliqué à toute ZP.
- 343. L'action des forces de sécurité (gendarmerie nationale ou police nationale) revêt le caractère d'une opération ponctuelle visant à régler les incidents avérés dans leurs aspects administratifs et judiciaires. Selon les dispositions du PPE, cet élément externe est alerté par le PCP et sollicité par l'autorité responsable du site, ou son délégataire, lorsque le lever de doute est fait selon les modalités définies dans le PPP sur site.

Section IV - Le contrôle *a posteriori* de la protection (RETEX PROT)

- 344. Les plans de protection correspondent à des schémas d'analyse et d'anticipation qui doivent s'instruire des « *leçons apprises* » au gré des circonstances.

Définition

- 345. En cas de sollicitation et/ou de mise à l'épreuve du dispositif de protection, à l'occasion d'un événement et/ou en cas de contrôle, les enseignements tirés de ces événements participent à la bonne tenue de la mission de protection.
- 346. Les leçons établies permettent d'adapter le dispositif de protection de l'installation considérée, mais également d'autres qui présenteraient des similitudes avec celui que les circonstances ont conduit à mettre à l'épreuve. La démarche partagée de RETEX est indispensable ; elle correspond au projet de gouvernance qui préside à l'organisation de la fonction de « *protection* ».
- 347. Face à une menace insidieuse et latente, l'évaluation des vulnérabilités passe par une exploitation efficace du RETEX. Le cycle de l'information qui alimente la connaissance de l'état de la menace doit être maîtrisé. Grâce aux enseignements pertinents qui en sont tirés, ce cycle permet de déboucher sur des décisions efficaces.
- 348. Le RETEX sur la vulnérabilité de la protection recueilli en situation de crise ou lors de contrôles (missions de routine, enquêtes, inspections/audit de sécurité) doit servir à :
 - a. Identifier les enseignements en analysant les faits puis en les synthétisant ;

- b. exploiter les enseignements en formulant des recommandations puis, après validation, en les diffusant, et en assurant leur suivi et leur contrôle.
349. Ces leçons identifiées deviennent des leçons apprises à travers la phase d'exploitation qui alimente les instances chargées de la protection.

Principes

350. Les divers RETEX doivent être disponibles en temps réel, pour le personnel engagé dans cette mission et ayant donc besoin d'en connaître. La circulation de cette information favorisera l'adaptation de la protection des emprises.
351. Elle consiste notamment en une mise à jour régulière de la connaissance des nouvelles menaces.
352. La fluidité de la circulation de l'information suppose la désignation d'une entité, point d'entrée unique connecté aux différents niveaux de responsabilité, pouvant collecter, archiver, et redistribuer en temps réel les informations du domaine.
353. La mise en place de procédures ad hoc de demande, de partage et de fourniture d'informations aux unités concernées par la menace est indispensable à la fluidité de l'information.
354. Enfin, le décloisonnement de l'information et son exploitation dépendent également de la disponibilité des données, au profit des unités intéressées et bénéficiaires. Des marges de progrès importantes existent dans ce domaine.
355. La rationalisation du recueil de l'information du RETEX doit étayer le processus décisionnel lié au domaine. En cas d'urgence due à une lacune du dispositif sur une emprise, une autorité responsable de la sûreté est chargée d'étudier les mesures nécessaires :
- a. une « *boucle courte* » de traitement décentralisé du retour d'expérience permet à une autorité de décider à son niveau des mesures à prendre ;
 - b. une « *boucle longue* » de traitement centralisé du RETEX est activée lorsqu'un enseignement validé nécessite la prise de mesures correctives par l'OIV en lien, notamment, avec l'EMA (gouvernance de la fonction).

Annexe A

Demande d'incorporation des amendements

1. Le lecteur d'un Document de référence interarmées (DRIA) ayant relevé des erreurs, des coquilles, des fautes de français ou ayant des remarques ou des suggestions à formuler pour améliorer sa teneur, peut saisir le CICDE en les faisant parvenir (sur le modèle du tableau ci-dessous) au :

Sous-directeur Synergie doctrinale
CICDE
École militaire
21, Place JOFFRE
75700 PARIS SP 07

ou en téléphonant au **01 44 42 83 38** pour obtenir l'adresse électronique valide à cette époque

ou encore en ligne sur les sites Intradef ou Internet du centre à l'adresse <http://www.cicde.defense.gouv.fr>

N°	Origine	Paragraphe (n°)	Alinéa	Ligne	Commentaire
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					

2. Les amendements validés par le Directeur du CICDE seront répertoriés **en rouge** dans le tableau intitulé « *Récapitulatif des amendements* » figurant en **page 7 de la version électronique du document**.

(PAGE VIERGE)

Partie I – Sigles, acronymes et abréviations

Sigles

B01. Dans un sigle, chaque lettre se prononce distinctement comme si un point les séparait.

Acronymes

B02. Un acronyme se compose d'une ou de plusieurs syllabes pouvant se prononcer comme un mot à part entière.

Abrégements

B03. Ce lexique ne prend en compte que les abrégements conventionnels tels que définis dans le *Lexique des règles typographiques en usage à l'imprimerie nationale* (LRTUIN), pages 5 à 11.

Charte graphique du lexique

B04. À titre pédagogique, tous les caractères composant un sigle, un acronyme ou un abrégement sont écrits en lettres capitales afin que le lecteur puisse en mémoriser la signification.

B05. Les sigles, acronymes et abréviations d'origine française sont écrits en **Arial gras, taille 9, caractères romains, couleur rouge**. Les sigles, acronymes et abréviations d'origine étrangère ou antique sont écrits en **Arial gras, taille 9, caractères italiques, couleur bleu**.

Liste des sigles, acronymes et abréviations utilisés dans ce document

AAP	<i>Allied Administrative Publication</i>
AJP	<i>Allied Joint Publication</i>
AME	Activités militaires de l'État
BdD	Base de Défense
CD	CONFIDENTIEL DÉFENSE
CDAOA	Commandement de la défense aérienne et des opérations aériennes
CE	Contrôle Élémentaire
CEMA	Chef d'État-Major des Armées
cf.	<i>Confer</i> , voir, se référer à...
CGA	Contrôle Général des Armées
CIA	Concept InterArmées
CIC	Cellule Interministérielle de Crise
CICDE	Centre Interarmées de Concepts, de Doctrines et d'Expérimentations
CODEF	COMité de DÉFense
COMBdD	COMmandant de Base de Défense
COMGSBdD	COMmandant de Groupe de Soutien de Base de Défense
COMSUP	Officier Général Commandant Supérieur des Forces Armées
CPCO	Centre de Planification et de Conduite des Opérations
CZDS	Commission Zonale de Défense et de Sécurité
DEF	DÉFense
DIA	Doctrine InterArmées
DNS	Directive Nationale de Sécurité
DPSD	Direction de la Protection et de la Sécurité de la Défense
EI	Élément d'intervention
EMA	État-Major des Armées

EMIAZDS	État-Major Interarmées de Zone de Défense et de Sécurité
GSBdD	Groupeement de Soutien des Bases de Défense
HSCT	Hygiène, Sécurité, Conditions de Travail
IAN	Inspection des Armements Nucléaires
IGA	Inspection Générale des Armées
IPD	Installation Prioritaire de Défense
ISBN	<i>International Standard Book Number</i>
ISC	Information et Supports classifiés
LBDSN	Livre Blanc sur la Défense et la Sécurité Nationale
LP	Laissez-Passer !
n°	Numéro(s)
NP	NON PROTÉGÉ
OGZDS	Officier Général de Zone de Défense et de Sécurité
OIAS	Organisme Interarmées de l'Administration et du Soutien
OIV	Opérateur d'Importance Vitale
OPJ	Officier de Police Judiciaire
OTIAD	Organisation Territoriale Interarmées de Défense
IdA	Inspection <u>des</u> Armées
p.	Page(s)
PAF	Poste d'Accueil et de Filtrage
PCP	Poste Central de Protection
PIA	Publication InterArmées
PIM	Protection des Installations Militaires
PPE	Plan de Protection Externe
PPP	Plan Particulier de Protection
PSO	Plan de Sécurité d'Opérateur
PIV	Point d'Importance Vitale
PROT	PROtection
Réf.	Référence(s)
RETEX PROT	RETour d'EXpérience PROtection
ROE	Règles Opérationnelles d'Engagement
SAIV	Secteur d'Activités d'Importance Vitale
SD	SECRET DÉFENSE
SGM	Statut Général des Militaires
SID	Service Infrastructure des Armées
SSI	Sécurité des Systèmes d'Information
TF	<i>Task Force</i>
TFA	<i>Task Force</i> InterArmées
TN	Territoire National
ZDHS	Zone de Défense Hautement Sensible
ZIV	Zone d'Importance Vitale
ZM	Zone Militaire
ZP	Zone Protégée
ZR	Zone Réservée

Partie II – Termes et définitions

(Sans objet).

Résumé

DIA-3.32.4_PIM(2012)

1. La Défense occupe un certain nombre d'installations militaires revêtant toutes une valeur opérationnelle certaine, ne serait-ce que pour les informations ou les matériels qui y sont rassemblés, sans même parler des plus sensibles qui contribuent directement à la mise en œuvre de l'appareil de défense. Aussi, leur protection générale constitue-t-elle un impératif partagé par les militaires et le personnel civil de la défense.
2. Intitulée *Protection des installations militaires (PIM)*, la Doctrine interarmées (DIA) 3.32.4 s'inscrit dans le cadre de la Sauvegarde générale (SG) et, plus particulièrement, du Théâtre national (TN). Ce document ne traite pas de la sécurité électronique, mais couvre le champ de la sécurité des infrastructures, des personnes et des biens de la Défense. Ce document propose des solutions pour parer aux risques et aux menaces tout en précisant le cadre légal et réglementaire qui convient, mais également les responsabilités (opérationnelles, pénales, juridiques et budgétaires) des différents acteurs qui y prennent part, hors situation de crise ou en situation de crise.
3. Traitant de l'aspect défensif de cette protection le premier volet détermine les ressources à utiliser, qu'elles soient humaines (personnel militaire ou civil) ou matérielles (infrastructures et équipements), détaille l'équilibre à trouver entre le besoin d'accès aux sites et la nécessité de leur protection et définit les différentes modalités de contrôle, d'inspection et d'enquête vérifiant la solidité du dispositif, sa régularité et les mesures à adopter pour l'améliorer.
4. Le deuxième volet traite de l'aspect réactif de cette protection lorsqu'il y a intrusion.
5. Le processus de réaction à la menace est fondé sur la détection, puis sur l'alerte et, enfin, sur la diffusion de cette alerte pour conduire une réaction adaptée.
6. Les règles d'emploi de la force sont précisées à partir d'un droit commun, délaissé dans certaines circonstances liées à la qualité des lieux (zones militaires, zones protégées, zones de défense hautement sensible), et qui peut conduire à l'usage de la force.
7. Le rôle de l'Élément d'intervention (EI) est donc central, qu'il s'agisse de ses missions, de sa composition ou des zones de son intervention.
8. Enfin, comme toute activité opérationnelle, cette réaction fait l'objet d'un processus de RETour d'EXpérience (RETEX) permettant d'améliorer tant la protection de telle installation militaire que les principes d'organisation de cette protection au plan national.



Ce document est un produit réalisé par le Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE), Organisme interarmées (OIA) œuvrant au profit de l'État-major des armées (EMA). Point de contact :

CICDE, Sous-directeur Synergie doctrinale (SD-SD)
École militaire
1, place JOFFRE
75700 PARIS SP 07

Téléphone 01 44 42 83 38

Par principe, le CICDE ne gère aucune bibliothèque physique et ne diffuse aucun document sous forme papier. Il met à la disposition du public une bibliothèque virtuelle unique réactualisée en permanence. Les documents classifiés ne peuvent être téléchargés que sur des réseaux protégés.

La version électronique de ce document est en ligne sur les sites Intradef et Internet du CICDE à l'adresse <http://www.cicde.defense.gouv.fr> à la rubrique *Corpus conceptuel et doctrinal interarmées français (CCDIA-FRA)*.