Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Arrêté du 2 juillet 2018 portant approbation de l'instruction méthodologique d'analyse de risque d'un secteur d'activités d'importance vitale

NOR : *PRMD1818232A*

Le Premier ministre,

Vu le code de la défense, notamment ses articles L. 1111-1, L. 1131-1, L. 1332-1 et suivants, R.* 1132-3 et R. 1332-18 ;

Vu l'avis de la commission interministérielle de défense et de sécurité des secteurs d'activités d'importance vitale en date du 11 décembre 2015,

Arrête :

Art. 1er. – La méthode d'analyse et de gestion du risque et la méthode pour déterminer, par secteur d'activités d'importance vitale, les scénarios de menace et leur hiérarchisation selon le type ou le niveau de menace envisagé, prévues respectivement au 1° et au 2° de l'article R. 1332-18 du code de la défense, sont fixées dans l'instruction méthodologique d'analyse de risque d'un secteur d'activités d'importance vitale annexée au présent arrêté.

Art. 2. – L'arrêté du 12 mars 2007 pris pour l'application du 1° et du 2° de l'article 12 du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale est abrogé.

Art. 3. – Le présent arrêté est applicable sur l'ensemble du territoire de la République.

Art. 4. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait le 2 juillet 2018.

Pour le Premier ministre et par délégation :
La secrétaire générale de la défense et de la sécurité nationale,
C. LANDAIS

ANNEXE

Instruction méthodologique d'analyse de risque d'un secteur d'activités d'importance vitale

La méthode d'analyse de risque d'un secteur d'activités d'importance vitale vise, d'une part, à assurer une couverture complète des risques associés au secteur, d'autre part, à apprécier le niveau de ces risques afin de définir les objectifs de sécurité et d'optimiser les moyens à mettre en œuvre pour assurer la sécurité du secteur, en cohérence avec les plans gouvernementaux de défense et de sécurité. Reprenant les principes de méthodes connues, elle regroupe les deux méthodes prévues à l'article R. 1332-18 du code de la défense et est présentée ci-après en quatre étapes.

La méthode d'analyse et de gestion du risque, prévue au 1° de l'article R. 1332-18, est exposée aux étapes 1, 3 et 4 de la présente instruction portant respectivement sur le contexte et les spécificités du secteur, l'évaluation des risques et la détermination d'un dispositif de sécurité. La méthode pour déterminer, par secteur d'activités d'importance vitale, les scénarios de menace et leur hiérarchisation selon le type ou le niveau de menace envisagé, prévue au 2° de l'article R. 1332-18, correspond à l'étape 2.

Les directives nationales de sécurité fondées sur l'analyse de risque et prévues à l'article R. 1332-17 du code de la défense, ainsi que les plans de sécurité d'opérateur, les plans particuliers de protection et les plans de protection externe subséquents, sont protégés dans les conditions prévues par les articles R. 2311-1 à R. 2311-9 du code de la défense.

Les décisions portant approbation des directives nationales de sécurité sont notifiées à chaque opérateur d'importance vitale et à chaque autorité administrative ayant à en connaître.

Les directives nationales de sécurité et les plans précités sont révisés, s'il y a lieu, à la suite de modifications législatives ou réglementaires, d'audits internes et de contrôles qui devront être régulièrement effectués par les pouvoirs publics[1] ainsi que des enseignements apportés par les événements réels et exercices.

1 Première étape : étude du contexte et des spécificités du secteur

Cette étape a pour objectif d'identifier le périmètre du secteur d'activités d'importance vitale et de le situer dans son environnement avec ses enjeux pour déterminer précisément le champ de l'étude de risque. Elle conduit à renseigner les rubriques suivantes.

1.1 Cadre général

- **Contexte** : caractéristiques du secteur (libre ou réglementé, concurrentiel ou non, ouvert à l'international ou non), identification des opérateurs présents, substituabilité des activités, interactions avec d'autres secteurs d'activités d'importance vitale, complémentarités entre opérateurs du secteur, problématiques économiques et de sécurité, réglementation applicable, etc. Tous ces aspects peuvent avoir une incidence sur les interdépendances, sur les niveaux de contraintes acceptables par les opérateurs et sur la possibilité de remplacer un opérateur défaillant.
- **Enjeux** économiques, humains, environnementaux, politiques, scientifiques, sociaux, etc.
- Contraintes d'ordre stratégique, économique, structurel, fonctionnel, réglementaire, etc. pesant sur le secteur, et **contraintes induites par des activités d'importance vitale**

[1] Préfecture, commission interministérielle ou zonale de défense et de sécurité des secteurs d'activités d'importance vitale, autorité militaire compétente.

relevant d'autres secteurs, la proximité des secteurs et leurs interdépendances influant effectivement sur la continuité des activités de chaque secteur.

1.2 Spécificités du secteur

- **Terminologie**, en établissant les équivalences entre les termes utilisés dans le secteur et les termes définis dans le glossaire en appendice 1.
- **Spectre d'activités** regroupant les métiers caractéristiques du secteur étudié, permettant d'identifier les opérateurs d'importance vitale.
- **Décomposition de chacune des fonctions du secteur** en systèmes ou points essentiels et, à un niveau plus fin, en composants névralgiques[2]. Différentes approches peuvent être utilisées :
    - par **processus organisationnels** : organisation générale du secteur ; nombre et taille des opérateurs ; répartition géographique ; interdépendances entre acteurs et secteurs ; impossibilité de substitution ; liens avec les clients, les fournisseurs et les prestataires externes ; recours aux importations etc.
    - par **processus fonctionnels** : liens ou interdépendances (logiques, humains, etc.) ; systèmes d'information (cartographie, systèmes d'information traitant d'éléments vitaux) etc.
    - par **éléments opérationnels** : installations ; zones spécifiques de production ; locaux partagés ; systèmes mutualisés etc.
    - par **éléments humains** : acteurs majeurs et personnel du secteur ; population au voisinage d'une installation, éventuellement tributaire de l'activité concernée ; éléments sociaux et culturels etc.
    - par **éléments environnementaux** : situation géographique ; circulation et flux ; ressources utilisées par l'entreprise ; impact sur l'environnement etc.
    - par **facteurs de dangerosité**.

A l'issue du renseignement du cadre général et des spécificités du secteur, le champ de l'étude de risque est clairement délimité, les obligations et les contraintes sont recensées, et les sujets à traiter sont connus.

L'étape 1 se conclut par la priorisation des éléments essentiels à la sécurité et à la continuité de l'activité, qui constitue le « besoin de sécurité » du secteur.

2 Deuxième étape : scénarios de menace

La qualité de l'appréciation des menaces dépend de l'aptitude à correctement **évaluer l'intention** de l'acteur malveillant - notamment terroriste - et son **habileté** à mener une action délibérée.

Des scénarios de menace sont établis et hiérarchisés sur la base des actes susceptibles de présenter le plus d'intérêt ou le **meilleur rapport efficacité/coût** pour un acteur malveillantou terroriste. **L'efficacité** est mesurée au regard des résultats attendus (humains, économiques, médiatiques, psychologiques). **Le coût** représente la difficulté d'accéder à la cible sans être détecté et de conduire l'opération. Cette appréciation est formalisée selon les notions d'attractivité de la cible et de faisabilité de l'attaque le croisement des niveaux d'attractivité et de faisabilité permettant de hiérarchiser les menaces.

---

[2] Point ou composant névralgique : élément à la fois indispensable au fonctionnement d'un point d'importance vitale et vulnérable (voir glossaire).

2.1 Éléments pris en compte dans les scénarios de menace

a Cibles et niveau d'attractivité

L'ensemble des scénarios de menace, y compris ceux *a priori* peu vraisemblables, est examiné en partant de l'identification des cibles, distinguées selon leur nature, et de la détermination de leur niveau d'attractivité, fonction des effets espérés d'une attaque.

Les cibles peuvent être diverses :

- systèmes essentiels ou composants névralgiques pour le secteur dans son ensemble ;
- personnes physiques : personnel, clients ;
- installations et équipements pouvant être à l'origine de suraccidents (équipements dangereux), ou indispensables à la sécurité, ou nécessaires compte tenu d'interactions avec d'autres secteurs ;
- population, biens et structures situés au voisinage des installations ;
- environnement naturel : nappe phréatique, cours d'eau, air, etc.

Il convient ensuite de définir, du point de vue de l'agresseur, **le niveau d'attractivité des cibles**, variable selon les effets espérés de leur atteinte, en prenant en compte le fait que l'agresseur n'a pas nécessairement la connaissance exacte des sites les plus vitaux pour le secteur ou pour la nation.

b Types de menace

Il convient ensuite d'identifier les menaces et les vecteurs (ou modes d'attaque) utilisables pour atteindre ces cibles :

- attentat à l'explosif ;
- attentat nucléaire, radiologique, biologique ou chimique ; libération de substances dangereuses ;
- détérioration ou destruction par incendie ou par sabotage ;
- perturbations électromagnétiques ;
- introduction de codes malveillants dans un système informatique ou déni de service ;
- détournement, vol ou extorsion ;
- enlèvement, chantage, prise d'otages, etc.

Sont également recensés les facteurs aggravants tels que les risques de contamination du milieu, les attaques sur les systèmes électriques ou de télécommunications, la compromission interne, etc.

c Vulnérabilités

Pour chaque menace précisée par un vecteur ou un mode d'attaque, sont déterminées **les vulnérabilités** des systèmes supposées connues de l'agresseur et pouvant être exploitées.

2.2 Élaboration et classement des scénarios de menace

L'élaboration et le classement des scénarios de menace peuvent se dérouler en trois étapes :

- rédaction de **scénarios génériques** sous la forme : *un agresseur active une menace en exploitant une vulnérabilité portée par un système, pour obtenir des effets* ;
- estimation de la **faisabilité des scénarios** clé retenus : facilité d'acquisition des connaissances et des moyens nécessaires à l'attaque, accessibilité des cibles, vulnérabilités exploitables, capacité à ne pas être détecté ;

- **hiérarchisation des scénarios** retenus en fonction de leur vraisemblance, en combinant le degré d'attractivité d'une cible au degré de faisabilité d'une attaque.

Les résultats sont amendés ou complétés, selon le cas, en fonction de la connaissance, par les services compétents, de la menace et des attaques passées. Les opérateurs sont utilement consultés pour faire part de leur connaissance d'incidents ou de vulnérabilités exploitables.

Il en résulte un **classement des scénarios de menace par valeur décroissante de vraisemblance**, valeur correspondant au produit du niveau d'attractivité et du niveau de faisabilité.

L'élaboration des scénarios de menace est liée à l'appréciation des capacités d'action des agresseurs. Les scénarios et leur classement sont révisés chaque fois qu'il y a lieu de prendre en compte une évolution de ces capacités (nouveaux savoir-faire, etc.).

3 Troisième étape : évaluation des risques

L'évaluation des risques vise à appréhender les facteurs structurels de risque en combinant la vraisemblance de la réussite d'une attaque (attractivité, faisabilité, vulnérabilité) et son impact (gravité des conséquences). La terminologie est définie dans le glossaire en appendice 1.

3.1 Schéma d'évaluation des risques

a Éléments de l'évaluation

L'évaluation des risques combine trois éléments : les scénarios de menace retenus, l'analyse des vulnérabilités et l'appréciation des impacts (conséquences dommageables) en cas de succès d'une agression.

Les scénarios de menace (fonction de l'attractivité et de la faisabilité), classés par degré de vraisemblance, ont été répertoriés lors de l'étape 2.

L'analyse de vulnérabilités peut être effectuée à l'aide de différents outils tels que des questionnaires, analyses par scénarios, retours d'expérience, arbre des causes, analyses cindyniques, etc. Il est recommandé que l'ensemble des acteurs du secteur (pouvoirs publics et opérateurs) utilise les mêmes outils afin de faciliter la compréhension des problématiques et les échanges sur ces sujets.

La combinaison de ces deux éléments permet de déterminer **la vraisemblance d'une agression réussie** (« V »).

Les impacts (« I ») sont appréciés dans l'hypothèse du succès de l'agression, selon deux critères :

- l'atteinte aux activités du pays (dommages causés à l'ensemble du secteur ou au fonctionnement de la société ou de l'économie, impossibilité de substitution, délai de rétablissement, coût de reconstruction, etc.) ;
- le niveau de danger pour la population.

L'appréciation des **impacts**, combinée à la **vraisemblance d'une agression réussie** permet de mesurer **le risque encouru**.

b Résultats de l'évaluation

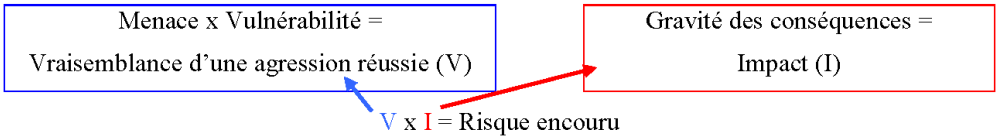
L'étape finale de l'évaluation vise à hiérarchiser les risques encourus. Elle peut se faire de la manière suivante, présentée à titre d'illustration.

La **vraisemblance** d'une agression réussie et son **impact** peuvent être **appréciés selon des échelles qualitatives**.

vraisemblance	niveau	description
forte	3	attaque très probable (devrait survenir à court terme)
moyenne	2	attaque plausible (pourrait arriver)
faible	1	attaque improbable

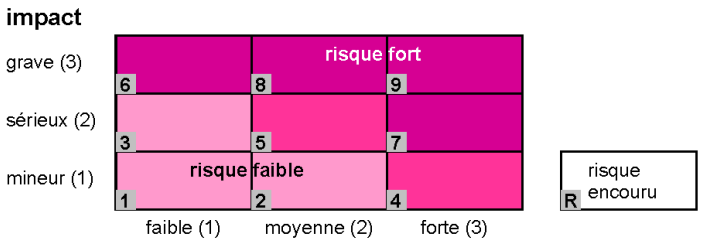
impact	niveau	description
grave	3	- dangerosité élevée pour la population - effet important sur l'activité du pays
sérieux	2	- dangerosité sérieuse pour la population - effet sensible sur l'activité du pays
mineur	1	- dangerosité faible pour la population - effet faible sur l'activité du pays

Résumé schématique :



Les résultats doivent être interprétés ; on peut par exemple qualifier de fort le risque afférent à une attaque ayant un impact grave, même si la vraisemblance de sa réussite est faible. On doit également tenir compte de l'intensité de la menace, qui est un facteur conjoncturel : accroissement du nombre d'acteurs malveillants, de leur agressivité, de leurs capacités.

L'évaluation structurelle des risques se conclut par une **« matrice des risques »**. Cet outil formalise l'évaluation de l'impact et de la vraisemblance d'une agression réussie, ce qui permet à tous d'utiliser des critères communs pour l'évaluation des risques.



4 Quatrième étape : détermination d'un dispositif de sécurité

4.1 Objectifs de sécurité du secteur

L'évaluation des risques permet de déterminer, **pour chaque secteur d'activités d'importance vitale**, les **objectifs de sécurité** définis comme buts à atteindre pour amener un risque identifié à un niveau acceptable en agissant sur l'attractivité, la faisabilité, la vulnérabilité et les impacts potentiels.

Les objectifs de sécurité les plus importants portent sur les risques encourus les plus élevés apparaissant dans la « matrice des risques » et pour lesquels il n'y a pas de solution de substitution. Pour autant les scénarios à faible risque encouru ne doivent pas être éludés : ils peuvent en particulier être les signes précurseurs d'une agression plus grave.

4.2 Exigences de sécurité

Ces objectifs de sécurité conduisent à formuler des **exigences de sécurité**, éléments requis pour atteindre les objectifs de sécurité en prenant en compte le contexte : enjeux, contraintes, réglementation, etc. Elles sont exprimées dans l'un ou plusieurs des cinq domaines suivants :

- **planification** : mise au point des mesures particulières de protection et mode de passage de la posture permanente de sécurité aux mesures graduées associées aux niveaux d'alerte ;
- **sensibilisation et formation** : recommandations adressées aux opérateurs, y compris à ceux qui ne sont pas désignés opérateurs d'importance vitale (fournisseurs, etc.) ;
- **organisation** : préparation de tous les moyens humains et matériels d'alerte et de gestion de situation d'urgence, solutions de secours palliant une impossibilité de substitution ;
- **prévention** : mécanismes ou procédures permettant de diminuer les vulnérabilités et/ou de dissuader de réaliser une attaque ; installation de systèmes de surveillance et de détection ;
- **protection** : mécanismes ou procédures permettant de limiter les effets d'une attaque, avant ou après l'agression (bouclier de protection, mécanismes d'intervention, de sauvegarde et de restauration, etc.).

Les exigences de sécurité d'un secteur peuvent concerner d'autres secteurs du fait des interdépendances. Elles sont alors communiquées aux ministres coordonnateurs de ces secteurs pour être prises en compte au titre des contraintes pesant sur ces secteurs.

Ces exigences de sécurité se traduisent, dans les plans de sécurité des opérateurs, par des **mesures** distinguées en deux types :

- des **mesures à effet dimensionnant**, qui doivent être prises en compte dès la mise en place du dispositif de sécurité ;
- des **mesures portant sur les procédures ou l'organisation**, en cohérence avec la logique de mesures graduées utilisée dans les plans gouvernementaux de défense et de sécurité.

Le type de mesure dépend de facteurs structurels tandis que la gradation de la mesure dépend de facteurs conjoncturels (intensité de la menace).

Si le secteur fait apparaître l'intérêt de sous-secteurs différenciés, dont chacun correspond à une logique opérationnelle ou fonctionnelle, la méthode d'analyse de risque est appliquée pour élaborer les directives nationales de sécurité de ces sous-secteurs.

Appendice 1 - Glossaire

Attractivité : attrait d'une cible pour un acte de malveillance ou de terrorisme, par suite des effets attendus sur les plans humain, économique, médiatique ou psychologique.

Composant névralgique : élément à la fois indispensable au fonctionnement d'un point d'importance vitale et vulnérable, de niveau plus fin que ce point (salle de contrôle ou de commande…).

Danger : toute situation, condition ou pratique qui comporte en elle-même une capacité à occasionner des dommages aux personnes, aux biens ou à l'environnement[3] (falaise, flacon d'acide sulfurique…).

Directive(s) nationale(s) de sécurité (DNS)[4] : fondées sur une analyse de risque du secteur concerné en tenant compte des scénarios de menaces élaborés par le ministre coordonnateur, la ou les directives nationales de sécurité d'un secteur d'activités d'importance vitale précisent les **objectifs et les politiques de sécurité du secteur ou d'une partie du secteur**.

Exigences de sécurité : éléments requis pour atteindre les objectifs de sécurité, exprimés dans un ou plusieurs des cinq domaines *planification*, *sensibilisation*, *organisation*, *prévention* et *protection*.

Faisabilité d'une action malveillante ou d'un acte de terrorisme : possibilité pour l'auteur de l'acte de conduire une telle action à partir de connaissances, de l'acquisition de moyens, de l'exploitation de vulnérabilités, de sa capacité à accéder à la cible sans être détecté dans un délai qui rendrait l'action impossible.

Impacts (ou conséquences dommageables) : effets prévisibles d'une agression réussie sur une cible, estimés en termes d'atteinte aux activités du pays ou de danger pour la population.

Menace : tout événement physique, phénomène ou activité humaine potentiellement préjudiciable, susceptible de provoquer des décès ou des lésions corporelles, des dégâts matériels ou immatériels, des perturbations sociales et économiques ou une détérioration de l'environnement. Pour la démarche de sécurité des secteurs d'activités d'importance vitale, les menaces sont réputées avoir un caractère malveillant ou être de nature terroriste.

Mesures de sécurité : systèmes ou procédures identifiés pour répondre aux exigences de sécurité.

Ministre coordonnateur[5] : le ministre coordonnateur d'un secteur d'activités d'importance vitale **désigne** les opérateurs d'importance vitale relevant du ou des secteurs d'activités dont il a la charge, **élabore** la ou les directives nationales de sécurité du ou de ces secteurs et **notifie** la liste des points d'importance vitale. Il est responsable de la coordination du secteur vis-à-vis des autres secteurs et, pour chaque secteur dont il est chargé, de la prise en compte des intérêts des autres ministères. Ce rôle ne lui donne toutefois aucune tutelle sur les opérateurs du secteur concerné par la directive nationale de sécurité qui relèvent d'autres ministères.

Objectif de sécurité : but à atteindre pour amener un risque identifié à un niveau acceptable, en agissant sur l'attractivité, la faisabilité, la vulnérabilité ou les impacts.

---

[3] Voir référentiel international de bonnes pratiques *Occupational Health and Safety Assessment Series* [18001].
[4] Article R. 1332-17 du code de la défense.
[5] Article R. 1332-2 du même code.

Opérateur d'importance vitale (OIV)[6] : entité (structure juridique : entreprise, établissement public :

- exerçant une activité comprise dans un secteur d'activités d'importance vitale ;
- gérant ou utilisant au titre de cette activité un ou plusieurs « points d'importance vitale » (voir *infra*) ;

Plan de sécurité d'opérateur (PSO) [7] : plan **définissant la politique générale de protection** de l'ensemble des activités de l'opérateur, notamment celles organisées en réseau, **comportant des mesures permanentes de protection et des mesures temporaires et graduées**. Il n'est requis que si l'opérateur gère plusieurs points d'importance vitale.

Plan particulier de protection (PPP) [8] : plan établi pour chaque point d'importance vitale à partir du plan de sécurité d'opérateur d'importance vitale, qui lui est annexé, et **comportant des mesures permanentes de protection et des mesures temporaires et graduées**.

Plan de protection externe (PPE)[9] : plan établi pour chaque point d'importance vitale par le préfet de département en liaison avec le délégué de l'opérateur pour la défense et la sécurité de ce point, **récapitulant les mesures planifiées de vigilance, de prévention, de protection et de réaction prévues par les pouvoirs publics**.

Point d'importance vitale (PIV)[10] : **tout établissement, installation ou ouvrage** dont le **dommage** ou l'**indisponibilité** ou la **destruction** par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :

- si son activité est difficilement substituable ou remplaçable, d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation,
- ou de mettre gravement en cause la santé ou la vie de la population.

Risque encouru : appréciation combinée de la vraisemblance d'une agression réussie (résultant des scénarios de menace et de l'analyse des vulnérabilités) et de ses impacts.

Secteur d'activités d'importance vitale (SAIV)[11] : secteur constitué d'activités concourant à un même objectif :

- qui ont trait à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, ou à l'exercice de l'autorité de l'État, ou au fonctionnement de l'économie, ou au maintien du potentiel de défense, ou à la sécurité de la nation, dès lors que ces activités sont difficilement substituables ou remplaçables ;
- ou qui peuvent présenter un danger grave pour la population.

Vulnérabilité : tendance d'un milieu, d'un bien ou d'une personne à subir des conséquences dommageables à la suite d'un événement. Elle ne produit pas nécessairement de dommage par elle-même.[12]

---

6 Article R. 1332-1 du code de la défense.
7 Article R. 1332-19 du même code.
8 Article R. 1332-23 du même code.
9 Article R. 1332-32 du même code.
10 Article R. 1332-4 du même code.
11 Article R. 1332-2 du même code.
12 Par exemple, par la porte d'un local contenant des matières dangereuses restant ouverte en permanence (vulnérabilité), des personnes mal intentionnées pourraient pénétrer pour commettre un vol (menace) ; un temps très long peut s'écouler avant que des personnes identifient la vulnérabilité et s'introduisent dans les locaux pour voler les matières en vue d'un usage malveillant.

Appendice 2 - Mesures à appliquer par l'opérateur et par l'État

Les mesures des plans gouvernementaux de défense et de sécurité sont déclinées dans la directive nationale de sécurité du secteur ou du sous-secteur concerné. Une grille de correspondance entre celle-ci et les mesures particulières est établie.

Ces mesures sont de portée générale et doivent viser tous les opérateurs du secteur, qu'ils soient désignés d'importance vitale ou non. Elles sont réparties en :

- **une posture permanente de sécurité**, correspondant à l'acquisition de moyens de protection ainsi qu'à des actions permanentes de vigilance, et préparant à la mise en œuvre de toutes les mesures graduées ;
- **des mesures graduées** techniques, organisationnelles ou comportementales, activées en fonction des consignes transmises en application des plans gouvernementaux.

1 Posture permanente de sécurité

L'objectif de la posture permanente de sécurité (PPS) est, d'une part, de mettre en place des « capteurs »[13] et des moyens de protection qui ne peuvent pas être installés dans l'urgence et, d'autre part, d'entretenir une organisation permanente contre la menace ou l'agression, sans pour autant perturber les activités administratives, économiques et sociales.

Cette posture peut être organisée en référence aux cinq domaines d'expression des exigences de sécurité : planification ; sensibilisation et formation ; organisation ; prévention ; protection.

Dans certains secteurs, la posture permanente de sécurité est spécifiée par des dispositions législatives ou réglementaires. Dans d'autres, elle est une attitude logique découlant des responsabilités des acteurs du secteur en matière de sécurité de ses personnels, de ses moyens de production et de ses clients, voire du voisinage de ses installations.

2 Mesures graduées associées aux niveaux d'alerte

Cette partie traite des actions à mener par les opérateurs du secteur pour faire face à une menace en fonction du niveau d'alerte. Avec une attention particulière portée à celles dont l'application relève conjointement des opérateurs et des pouvoirs publics, elles doivent couvrir l'ensemble des dispositions de défense et de sécurité suivantes, à mettre en œuvre en cas d'apparition d'incidents :

- gestion des signaux faibles,
- gestion de l'alerte,
- actions de prévention et de protection,
- liaisons avec les pouvoirs publics,
- fonctionnement en mode dégradé et application d'un plan de continuité d'activité,
- gestion de la crise (mise en place d'un centre de crise en liaison avec les centres opérationnels des pouvoirs publics),
- gestion de situations exceptionnelles.

---

[13] Le terme ne doit pas être limité à son acception courante d'élément technique : il peut aussi bien s'agir de recueillir de l'information humaine, donc d'en assurer la remontée.