Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale
Direction de la protection et de la sécurité de l'Etat

SÉCURITÉ DES ACTIVITÉS D'IMPORTANCE VITALE

RECUEIL DES TEXTES DE RÉFÉRENCE

Edition mars 2019

SGDSN

Présentation

Ce recueil regroupe l'ensemble des textes juridiques, nationaux et européens, nécessaires à la mise en œuvre du dispositif de sécurité des activités d'importance vitale (SAIV).

L'instruction générale interministérielle n°6600 du 7 janvier 2014 précise, par ailleurs, les modalités d'application de ce corpus.

Ce dispositif est principalement inséré dans le code de la défense, notamment ses articles R. 1332-1 à 1332-42, pris sur le fondement des articles L. 1332-1 à 1332-7. Ce cadre législatif et réglementaire permet d'associer les opérateurs d'importance vitale (OIV), publics ou privés, à leur protection contre toute menace, notamment à caractère terroriste, d'analyser les risques et d'appliquer les mesures de leur niveau, en cohérence avec les décisions des pouvoirs publics.

Les arrêtés du Premier ministre précisent la méthode permettant de répondre aux exigences de planification dans un dialogue permanent entre l'Etat et les opérateurs.

Ce régime de protection s'inscrit plus largement dans une démarche globale visant à adapter les conditions dans lesquelles le pays se prémunit contre toute menace, en améliorant l'articulation des dispositions que mettent en œuvre pouvoirs publics et opérateurs, en particulier dans le cadre du plan VIGIPIRATE.

Il s'articule avec d'autres dispositifs concourant à la politique de sécurité et de résilience de la Nation ; sécurité des installations prioritaires de défense, mise en œuvre des plans de continuité et de rétablissement d'activité, enquêtes administratives de sécurité préalablement à l'accès aux points d'importance vitale, sécurité des systèmes d'information, procédure d'autorisation préalable des investissements étrangers en France.

Enfin, ce dispositif trouve un prolongement dans le Programme européen de protection des infrastructures critiques (EPCIP).

La secrétaire générale de la défense
et de la sécurité nationale

Claire Landais

SOMMAIRE DU RECUEIL DES TEXTES DE RÉFÉRENCE

SOMMAIRE DU RECUEIL DES TEXTES DE REFERENCE

DISPOSITIONS PROPRES A LA SAIV

- Articles L. 1332-1 à L. 1332-7 du code de la défense.
- Articles R. 1332-1 à R. 1332-42 du code de la défense.
- Arrêté du Premier ministre du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs.
- Arrêté du 3 juillet 2008 portant modification de l'arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs.
- Arrêté du 31 mars 2017 relatif au secteur d'activité d'importance vitale dont le ministre de la défense est ministre coordonnateur.
- Arrêté du 2 juillet 2018 portant approbation de l'instruction méthodologique d'analyse de risque d'un secteur d'activités d'importance vitale.
- Arrêté du 2 juillet 2018 portant approbation du plan type des plans de sécurité d'opérateurs d'importance vitale.
- Guide pour l'élaboration du plan de sécurité d'opérateur, édition de juillet 2018.
- Arrêté du 2 juillet 2018 portant approbation du plan type des plans particuliers de protection des points d'importance vitale.
- Guide d'aide à l'élaboration et l'examen d'un plan particulier de protection, édition du 2 juillet 2018.
- Arrêté du 2 juillet 2018 portant approbation du plan type des plans de protection externe des points d'importance vitale.
- Guide d'aide à l'élaboration du plan de protection externe, édition du 2 juillet 2018.

DISPOSITIONS CONNEXES A LA SAIV

Installations prioritaires de défense

- Article L. 1321-2 du code de la défense.
- Articles R. 1311-39 à R. 1311-43 du code de la défense.

Service de sécurité nationale

- Article L. 2151-1 à L. 2151-5 du code de la défense.
- Articles R. 2151-1 à R. 2151-7 du code de la défense.

Enquêtes administratives

- Article L. 114-1, articles R. 114-1, R. 114-4 et R. 114-6 du code de la sécurité intérieure.
- Décret n° 2017-668 du 27 avril 2017 portant création d'un service à compétence nationale dénommé «service national des enquêtes administratives de sécurité».
- Décret n° 2017-588 du 20 avril 2017 portant création d'un service à compétence nationale dénommé «Commandement spécialisé pour la sécurité nucléaire».

Sécurité des systèmes d'information

- Articles L. 2321-2-1 à L. 2321-5 du code de la défense.
- Articles R. 2321-1-1 à R. 2321-1-5 du code de la défense.

Investissements étrangers

- Article L. 151-3 du code monétaire et financier.
- Articles R. 153-1 à R. 153-5 du code monétaire et financier.

Règlementation européenne

- Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

DISPOSITIONS PROPRES A LA SAIV

Protection des installations d’importance vitale

CODE DE LA DEFENSE

(partie législative)

DISPOSITIONS PROPRES A LA SAIV

Chapitre 2 : Protection des installations d'importance vitale

Section 1 : Dispositions générales

Article L1332-1

(Loi nº 2005-1550 du 12 décembre 2005 art. 3, art. 4 I Journal Officiel du 13 décembre 2005 en vigueur le 24 février 2006)

Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenues de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.

NOTA : Loi 2005-1550 du 12 décembre 2005 art. 3 : Les dispositions du présent article produisent effet à compter de l'entrée en vigueur des dispositions réglementaires désignant l'autorité administrative compétente. Cette autorité administrative a été désignée par le décret nº 2006-212 du 23 février 2006 publié au JORF du 24 février 2006.

Article L1332-2

(Loi nº 2005-1550 du 12 décembre 2005 art. 3 Journal Officiel du 13 décembre 2005 en vigueur le 24 février 2006)

(Loi nº 2006-686 du 13 juin 2006 art. 59 Journal Officiel du 14 juin 2006)

Les obligations prescrites par le présent chapitre peuvent être étendues à des établissements mentionnés à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire de base visée à l'article L. 593-1 du code de l'environnement quand la destruction ou l'avarie de certaines installations de ces établissements peut présenter un danger grave pour la population. Ces établissements sont désignés par l'autorité administrative.

Article L1332-2-1

L'accès à tout ou partie des établissements, installations et ouvrages désignés en application du présent chapitre est autorisé par l'opérateur qui peut demander l'avis de l'autorité administrative compétente dans les conditions et selon les modalités définies par décret en Conseil d'Etat.

L'avis est rendu à la suite d'une enquête administrative qui peut donner lieu à la consultation du bulletin n° 2 du casier judiciaire et de traitements automatisés de données à caractère personnel relevant de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'exception des fichiers d'identification.

La personne concernée est informée de l'enquête administrative dont elle fait l'objet.

Article L1332-3

(Loi nº 2005-1550 du 12 décembre 2005 art. 3, art. 4 I Journal Officiel du 13 décembre 2005 en vigueur le 24 février 2006)

Les opérateurs dont un ou plusieurs établissements, installations et ouvrages sont désignés en application du présent chapitre réalisent pour chacun d'eux les mesures de protection prévues à un plan particulier de protection dressé par l'opérateur et approuvé par l'autorité administrative.

Ces mesures comportent notamment des dispositions efficaces de surveillance, d'alarme et de protection matérielle. En cas de non-approbation du plan et de désaccord persistant, la décision est prise par l'autorité administrative.

NOTA : Loi 2005-1550 du 12 décembre 2005 art. 3 : Les dispositions du présent article produisent effet à compter de l'entrée en vigueur des dispositions réglementaires désignant l'autorité administrative compétente. Cette autorité administrative a été désignée par le décret nº 2006-212 du 23 février 2006 publié au JORF du 24 février 2006.

Article L1332-4

(Loi nº 2005-1550 du 12 décembre 2005 art. 3, art. 4 I Journal Officiel du 13 décembre 2005)

En cas de refus des opérateurs de préparer leur plan particulier de protection, l'autorité administrative met, par arrêtés, les chefs d'établissements ou d'entreprises assujettis en demeure de l'établir dans le délai qu'elle fixe.

NOTA : Loi 2005-1550 du 12 décembre 2005 art. 3 : Les dispositions du présent article produisent effet à compter de l'entrée en vigueur des dispositions réglementaires désignant l'autorité administrative compétente. Cette autorité a été désignée par le décret nº 2006-212 du 23 février 2006 publié au JORF du 24 février 2006.

Article L1332-5

(Loi nº 2005-1550 du 12 décembre 2005 art. 3 Journal Officiel du 13 décembre 2005 en vigueur le 24 février 2006)

Le plan de protection établi dans les conditions prévues à l'article L. 1332-4, l'autorité administrative met, par arrêtés, les chefs d'établissements ou d'entreprises en demeure de le réaliser dans le délai qu'elle fixe.

NOTA : Loi 2005-1550 du 12 décembre 2005 art. 3 : Les dispositions du présent article produisent effet à compter de l'entrée en vigueur des dispositions réglementaires désignant l'autorité administrative compétente. Cette autorité a été désignée par le décret nº 2006-212 du 23 février 2006 publié au JORF du 24 février 2006.

Article L1332-6

(Loi nº 2005-1550 du 12 décembre 2005 art. 3, art. 4 I Journal Officiel du 13 décembre 2005)

Les arrêtés de mise en demeure prévus aux articles L. 1332-4 et L. 1332-5 fixent un délai qui ne peut être inférieur à un mois, et qui est déterminé en tenant compte des conditions de fonctionnement de l'opérateur et des travaux à exécuter.

Les arrêtés concernant les entreprises nationales ou faisant appel au concours financier de l'Etat sont transmis au ministre de tutelle et au ministre de l'économie et des finances, qui sont immédiatement informés des difficultés susceptibles de se produire dans l'application de l'arrêté.

NOTA : Loi 2005-1550 du 12 décembre 2005 art. 3 : Les dispositions du présent article produisent effet à compter de l'entrée en vigueur des dispositions réglementaires désignant l'autorité administrative compétente. Cette autorité a été désignée par le décret nº 2006-212 du 23 février 2006 publié au JORF du 24 février 2006.

Section 2 : Dispositions spécifiques à la sécurité des systèmes d'information

Article L1332-6-1

(Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22)

Le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et des opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, ou pourrait présenter un danger grave pour la population. Ces opérateurs sont tenus d'appliquer ces règles à leurs frais.

Les règles mentionnées au premier alinéa peuvent notamment prescrire que les opérateurs mettent en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information. Ces systèmes de détection sont exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'autorité nationale de sécurité des systèmes d'information ou par d'autres services de l'Etat désignés par le Premier ministre.

Les qualifications des systèmes de détection et des prestataires de service exploitant ces systèmes sont délivrées par le Premier ministre.

Article L1332-6-2

(Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22)

Les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 informent sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité des systèmes d'information mentionnés au premier alinéa de l'article L. 1332-6-1.

Article L1332-6-3

(Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22)

A la demande du Premier ministre, les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 soumettent leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité prévues à l'article L. 1332-6-1. Les contrôles sont effectués par l'autorité nationale de sécurité des systèmes d'information ou par des services de l'Etat désignés par le Premier ministre ou par des prestataires de service qualifiés par ce dernier. Le coût des contrôles est à la charge de l'opérateur.

Article L1332-6-4

(Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22)

Pour répondre aux crises majeures menaçant ou affectant la sécurité des systèmes d'information, le Premier ministre peut décider des mesures que les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 doivent mettre en œuvre.

Article L1332-6-5

(Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22)

L'Etat préserve la confidentialité des informations qu'il recueille auprès des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 dans le cadre de l'application de la présente section.

Article L1332-6-6

(Créé par LOI n°2013-1168 du 18 décembre 2013 - art. 22)

Un décret en Conseil d'Etat précise les conditions et limites dans lesquelles s'appliquent les dispositions de la présente section.

Section 3 : Dispositions pénales

Article L1332-7

(Modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 22)

Est puni d'une amende de 150 000 euros le fait, pour les dirigeants des opérateurs mentionnés à l'article L. 1332-4 et à l'expiration du délai défini par l'arrêté de mise en demeure, d'omettre d'établir un plan de protection ou de réaliser les travaux prévus.

Est puni d'une amende de 150 000 euros le fait, pour les mêmes personnes, d'omettre, après une mise en demeure, d'entretenir en bon état les dispositifs de protection antérieurement établis.

Est puni d'une amende de 150 000 € le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations prévues aux articles L. 1332-6-1 à L. 1332-6-4. Hormis le cas d'un manquement à l'article L. 1332-6-2, cette sanction est précédée d'une mise en demeure.

Les personnes morales déclarées responsables, dans les conditions prévues à l'article 121-2 du code pénal, des infractions prévues à la présente section encourent une amende suivant les modalités prévues à l'article 131-38 du même code.

CODE DE LA DEFENSE

(partie réglementaire)

DISPOSITIONS PROPRES A LA SAIV

Chapitre 2

Protection des installations d'importance vitale

Section 1

Dispositions générales

(Art. 1er du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.)

Article R1332-1

I - Les opérateurs d'importance vitale sont désignés parmi :

1º Les opérateurs publics ou privés mentionnés à l'article L. 1332-1 ;

2º Les gestionnaires d'établissements mentionnés à l'article L. 1332-2.

II - Un opérateur d'importance vitale :

1º Exerce des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale ;

2º Gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations 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 :

a) D'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;

b) Ou de mettre gravement en cause la santé ou la vie de la population.

Article R1332-2

Un secteur d'activités d'importance vitale, mentionné au 1º du II de l'article R. 1332-1, est constitué d'activités concourant à un même objectif, qui :

1º Ont trait à la production et la distribution de biens ou de services indispensables :

a) A la satisfaction des besoins essentiels pour la vie des populations ;

b) Ou à l'exercice de l'autorité de l'Etat ;

c) Ou au fonctionnement de l'économie ;

d) Ou au maintien du potentiel de défense ;

e) Ou à la sécurité de la Nation,

dès lors que ces activités sont difficilement substituables ou remplaçables ;

2º Ou peuvent présenter un danger grave pour la population.

Le Premier ministre fixe, par arrêté pris après avis de la commission mentionnée à l'article R. 1332-10, les secteurs d'activités d'importance vitale. Cet arrêté désigne pour chaque secteur d'activités d'importance vitale un ministre coordonnateur, qui veille à l'application des directives du gouvernement dans ce secteur, le cas échéant en liaison avec le ou les ministres dont le domaine de compétence recouvre les activités qui y sont exercées.

Le ministre de la défense est le ministre coordonnateur des secteurs d'activités d'importance vitale constitués d'activités qui participent de façon directe à la satisfaction des besoins des armées et des formations rattachées.

Section 2

Désignation des opérateurs d'importance vitale, des délégués pour la défense et la sécurité et des points d'importance vitale

Article R1332-3

Les opérateurs d'importance vitale sont désignés pour chaque secteur d'activités d'importance vitale par arrêté du ministre coordonnateur. Cet arrêté est pris en concertation avec le ou les ministres intéressés, après avis de la commission mentionnée à l'article R. 1332-10.

Toutefois, les opérateurs d'importance vitale qui gèrent exclusivement un établissement mentionné à l'article L. 1332-2 sont désignés par arrêté du préfet du département dans le ressort duquel se trouve cet établissement, après avis de la commission mentionnée à l'article R. 1332-13.

Le ministre coordonnateur ou le préfet de département, selon le cas, notifie à l'opérateur son intention de le désigner comme opérateur d'importance vitale. L'opérateur dispose, pour présenter ses observations, d'un délai de deux mois à compter de la notification.

Les arrêtés mentionnés au présent article ne sont pas publiés. Ils sont notifiés aux opérateurs d'importance vitale intéressés ainsi qu'à toutes les autorités administratives qui ont à en connaître. En application des articles L. 311-5 et suivants du code des relations entre le public et l'administration, ils ne sont pas communicables.

(Art. 4 du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.)

Article R1332-4

Tout établissement, installation ou ouvrage répondant à la définition du 2º du II de l'article R. 1332-1 est qualifié de point d'importance vitale.

Chaque opérateur d'importance vitale propose en annexe à son plan de sécurité d'opérateur d'importance vitale une liste de points d'importance vitale. L'autorité administrative désigne les points d'importance vitale dans les conditions prévues à l'article R. 1332-22.

Article R1332-5

L'opérateur d'importance vitale communique au ministre coordonnateur de son secteur d'activités d'importance vitale le nom de la personne chargée d'exercer la fonction de délégué pour la défense et la sécurité. Cette personne doit être habilitée dans les conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale.

Le délégué pour la défense et la sécurité représente l'opérateur d'importance vitale auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de sécurité.

Article D1332-5-1

(Créé par Décret n°2010-225 du 4 mars 2010 - art. 9)

L'opérateur d'importance vitale communique au préfet de zone de défense et de sécurité dans le ressort de laquelle se trouve un ou plusieurs points d'importance vitale qu'il gère, ou à l'officier général de zone de défense et de sécurité pour les points dépendant d'opérateurs d'importance vitale relevant du ministère de la défense, le nom de la personne chargée de la fonction de délégué pour la défense et la sécurité. Cette personne doit être qualifiée pour connaître des informations classifiées dans les conditions prévues à l'article R. 2311-7.

Ce délégué exerce au niveau zonal les fonctions prévues au deuxième alinéa de l'article R. 1332-5.

Article R1332-6

(Modifié par Décret n°2017-282 du 2 mars 2017 - art. 2)

Pour chaque point d'importance vitale, l'opérateur d'importance vitale, après réception de l'avis mentionné à l'article R. 1332-21, communique au préfet du département dans le ressort duquel se trouve chacun de ces points, ou au ministre de la défense pour les points dépendant d'opérateurs d'importance vitale relevant de sa responsabilité, le nom de la personne chargée d'exercer la fonction de délégué pour la défense et la sécurité. Cette personne doit être habilitée dans les conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale.

Ce délégué exerce au niveau local les fonctions prévues au deuxième alinéa de l'article R. 1332-5.

Section 3

Organismes consultatifs

Sous-section 2

Commission interministérielle de défense et de sécurité

des secteurs d'activité d'importance vitale

(Al. 1 à 9 et alinéa 11 de l'article 8 du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.)

Article R1332-10

La commission interministérielle de défense et de sécurité des secteurs d'activités d'importance vitale est présidée par le secrétaire général de la défense nationale ou son représentant.

Cette commission comprend :

1º Le haut fonctionnaire de défense auprès du ministre de l'intérieur ou son représentant ;

2º Le directeur général de la police nationale ou son représentant ;

3° Le haut fonctionnaire de défense et de sécurité auprès du ministre de la défense ou son représentant ;

4º Le chef d'état-major des armées ou son représentant ;

5º Le directeur général de la gendarmerie nationale ou son représentant ;

6º Le haut fonctionnaire de défense et de sécurité auprès du ministre chargé de l'économie ou son représentant ;

7° Le directeur général de l'Agence nationale de la sécurité des systèmes d'information ou son représentant ;

8º En fonction des questions traitées et sur convocation du président, les hauts fonctionnaires mentionnés à l'article R. 1143-1 et les directeurs d'administration centrale intéressés, ou leurs représentants, ainsi que les présidents des commissions mentionnées à l'article R. 1332-13.

Sur décision de son président, la commission peut entendre toute personnalité qualifiée.

Article R1332-11

La commission se réunit sur convocation de son président, qui détermine l'ordre du jour de la réunion. Son secrétariat est assuré par le secrétariat général de la défense nationale.

Article R1332-12

I. La commission émet un avis sur :

1º La désignation des opérateurs d'importance vitale mentionnés au premier alinéa de l'article R. 1332-3 ;

2º La détermination des secteurs d'activités d'importance vitale ;

3º Les arrêtés mentionnés à l'article R. 1332-18 ;

4º Les résultats de l'analyse de risque effectuée pour chaque secteur d'activités d'importance vitale ;

5º Les directives nationales de sécurité, à l'exception de celles intéressant les secteurs d'activités d'importance vitale dont le ministre de la défense est le coordonnateur ;

6º Les plans de sécurité d'opérateurs d'importance vitale dont le périmètre dépasse celui de la zone de défense, à l'exception des plans d'opérateurs d'importance vitale relevant du ministre de la défense ;

7º La liste des points d'importance vitale annexée aux plans de sécurité mentionnés au 6º. La commission propose éventuellement des ajouts ou suppressions à cette liste.

II. La commission est également consultée sur :

1º Les plans particuliers de protection faisant l'objet d'un désaccord entre l'opérateur d'importance vitale et le préfet de département, à l'exception des plans des opérateurs d'importance vitale relevant du ministre de la défense ;

2º Le dossier mentionné à l'article R. 1332-34 qui peut valoir plan particulier de protection.

La commission entend l'opérateur d'importance vitale qui en fait la demande, lorsqu'elle examine le plan de sécurité de cet opérateur afin d'émettre l'avis mentionné à l'article R. 1332-21, ou, en cas de désaccord avec le préfet de département, l'avis mentionné au II de l'article R. 1332-26.

La commission peut être saisie par un ministre de toute question relative à la sécurité dans les secteurs d'activités d'importance vitale. Elle peut également contrôler sur place les mesures prises pour la sécurité des points d'importance vitale. Elle en fait rapport au ministre coordonnateur.

III. - La commission établit un rapport annuel adressé au Premier ministre.

Sous-section 3

Commission zonale de défense et de sécurité

des secteurs d'activité d'importance vitale

Article R1332-13

Dans chaque zone de défense, une commission zonale de défense et de sécurité des secteurs d'activités d'importance vitale est présidée par le préfet de zone ou son représentant.

Cette commission comprend :

1º Le procureur général près la cour d'appel dans le ressort de laquelle se trouve la préfecture de la zone de défense ou son représentant ;

2º L'officier général de la zone de défense ou son représentant ;

3º L'officier commandant la région de gendarmerie situé au siège de la zone de défense ou son représentant ;

4º Le délégué de zone du ministre chargé de l'économie ou son représentant ;

5º Sur convocation du président, les préfets de départements, les chefs des services déconcentrés de l'Etat, le délégué de zone de défense et de sécurité du ministre, intéressés par les questions traitées, ou leurs représentants.

(Al. 8 de l'article 9 du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.)

Article R1332-14

La commission se réunit sur convocation de son président, qui établit l'ordre du jour de la réunion. Son secrétariat est assuré par l'état-major de la zone de défense.

Article R1332-15

La commission est chargée d'une mission générale de coordination, d'assistance et de contrôle de la mise en œuvre des plans particuliers de protection, à l'exception de ceux dépendant d'opérateurs d'importance vitale relevant du ministre de la défense. Elle donne un avis sur :

1º La désignation des opérateurs d'importance vitale mentionnés au deuxième alinéa de l'article R. 1332-3 ;

2º Les plans de sécurité des opérateurs d'importance vitale dont le périmètre ne dépasse pas le ressort de la zone de défense et de sécurité. Tout opérateur d'importance vitale présent dans la zone est entendu lors de l'examen de son plan par la commission, s'il en fait la demande ;

3º La liste des points d'importance vitale annexée aux plans de sécurité mentionnés au 2º. Elle propose éventuellement des ajouts ou suppressions à cette liste ;

4º La désignation et le périmètre des zones d'importance vitale mentionnées aux articles R. 1332-35 à R. 1332-38 ;

5º Le plan particulier de protection de zone d'importance vitale prévu à l'article R. 1332-38. Tout opérateur d'importance vitale présent dans la zone est entendu lors de l'examen de ce plan par la commission, s'il en fait la demande.

La commission est saisie de toute question jugée utile par son président ou par un préfet de département.

Elle peut également contrôler sur place, à son initiative ou sur demande d'un ministre ou d'un préfet de département, les mesures prises pour la sécurité des points d'importance vitale.

Section 4

Directives nationales de sécurité

Article R1332-16

Le ministre coordonnateur d'un secteur d'activités d'importance vitale procède à l'analyse de risque de ce secteur en tenant compte des scénarios de menaces mentionnés au 2º de l'article R. 1332-18.

Les résultats de l'analyse de risque sont soumis à l'avis de la commission mentionnée à l'article R. 1332-10, à l'exception des résultats intéressant les secteurs d'activités d'importance vitale dont le ministre de la défense est le coordonnateur.

Article R1332-17

La ou les directives nationales de sécurité sont fondées sur l'analyse de risque mentionnée à l'article R. 1332-16. Elles s'appliquent à un secteur d'activités d'importance vitale et précisent les objectifs et les politiques de sécurité du secteur.

Elles définissent des mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre toute menace, notamment à caractère terroriste.

Elles sont approuvées, après avis de la commission mentionnée à l'article R. 1332-10, à l'exception de celles intéressant les secteurs dont le ministre de la défense est le coordonnateur, par arrêté du Premier ministre sur proposition du ministre coordonnateur du secteur d'activités d'importance vitale. Cet arrêté est protégé dans les conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale. Il est notifié à chaque opérateur d’importance vitale ainsi qu’à toutes les autorités administratives qui ont à en connaître.

Article R1332-18

Pour l'application des dispositions de la présente section, le Premier ministre, après avis de la commission mentionnée à l'article R. 1332-10, fixe par arrêtés :

1º La méthode d'analyse et de gestion du risque ;

2º La méthode à suivre 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 ;

3º Les plans types des plans de sécurité d'opérateurs d'importance vitale, des plans particuliers de protection et des plans de protection externe.

Section 5

Mesures de protection

Sous-section 1

Plan de sécurité d'opérateur

Article R1332-19

L'opérateur d'importance vitale qui, pour l'exercice de son activité, gère ou utilise plus d'un établissement, ouvrage ou installation mentionné au 2º du II de l'article R. 1332-1, élabore un plan de sécurité d'opérateur d'importance vitale qui a pour objet de définir la politique générale de protection pour l'ensemble de ces établissements, ouvrages ou installations, notamment ceux organisés en réseau.

Ce plan est conforme au plan type mentionné au 3º de l'article R. 1332-18.

Le plan de sécurité d'opérateur d'importance vitale prévoit, s'il y a lieu, les délais de réalisation des mesures de protection permanentes et des mesures temporaires et graduées qu'il prescrit. Ces délais courent pour les mesures de protection permanentes, à compter de la date d'entrée en vigueur du plan particulier de protection prévue à l'article R. 1332-28 et, pour les mesures temporaires et graduées, à compter de la transmission d'un message d'alerte à l'opérateur d'importance vitale par l'autorité administrative dont il relève.

Le plan de sécurité d'opérateur d'importance vitale, ainsi que tous les documents qui s'y rattachent, sont protégés dans les conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale. Le plan comporte un rapport de présentation qui ne contient aucune information classifiée.

(Art. 14 du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.)

Article R1332-20

Dans les six mois qui suivent la notification de la ou des directives nationales de sécurité intéressant un secteur d'activités d'importance vitale :

1º Les opérateurs d'importance vitale transmettent leur plan de sécurité d'opérateur d'importance vitale au ministre coordonnateur du secteur d'activités d'importance vitale dont ils relèvent ;

2º Les opérateurs d'importance vitale mentionnés au deuxième alinéa de l'article R. 1332-3 transmettent leur plan de sécurité au préfet de département compétent ;

Article R1332-21

En fonction du périmètre géographique du plan de sécurité d'opérateur d'importance vitale, l'autorité administrative mentionnée au 1º ou 2º de l'article R. 1332-20 soumet ce plan pour avis à la commission mentionnée à l'article R. 1332-10 ou à l'article R. 1332-13, sauf s'il s'agit du plan de sécurité d'un opérateur d'importance vitale relevant du ministre de la défense.

La commission s'assure notamment que :

1º Les mesures proposées répondent de manière satisfaisante aux directives nationales de sécurité ;

2º La liste des points d'importance vitale mentionnés à l'article R. 1332-4 est pertinente ;

3º La politique générale de sécurité définit des mesures spécifiques graduées de vigilance, de prévention, de protection et de réaction à une menace.

La commission émet dans un délai de trois mois à compter de la date de réception du plan un avis qui est notifié à l'opérateur. Cet avis est protégé dans les conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale.

Article R1332-22

Dès réception de l'avis mentionné à l'article R. 1332-21, le ministre coordonnateur ou le préfet de département pour les opérateurs d'importance vitale mentionnés au deuxième alinéa de l'article R. 1332-3, désigne le ou les points d'importance vitale devant figurer en annexe du plan de sécurité d'opérateur d'importance vitale.

La décision de l'autorité administrative n'est pas publiée. Elle est notifiée à l'opérateur d'importance vitale et est protégée dans les conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale.

Sous-section 1 bis

Accès aux points d'importance vitale

Article R1332-22-1

(Modifié par Décret n°2017-282 du 2 mars 2017 - art. 6)

Avant d'autoriser l'accès d'une personne physique ou morale à tout ou partie d'un point d'importance vitale qu'il gère ou utilise, l'opérateur d'importance vitale peut demander par écrit l'avis du préfet de département dans le ressort duquel se situe le point d'importance vitale ou, pour les opérateurs d'importance vitale relevant du ministre de la défense, l'avis de celui-ci.

Cette demande peut justifier que soit diligentée sous le contrôle de l'autorité concernée une enquête administrative destinée à vérifier que les caractéristiques de la personne physique ou morale intéressée ne sont pas incompatibles avec l'accès envisagé et pouvant donner lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 26 de la loi n° 78-17 du 6 janvier 1978.

La demande d'avis mentionnée aux alinéas précédents concerne l'accès aux parties des points d'importance vitale déterminées à cette fin dans les plans particuliers de protection.

Article R1332-22-2

(Créé par Décret n°2012-491 du 16 avril 2012 - art. 2)

La procédure prévue à l'article R. 1332-22-1 ne s'applique pas aux personnes appartenant à l'une des deux catégories suivantes :

1° Celles mentionnées au décret n° 2005-1124 du 6 septembre 2005 pris pour l'application de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 et fixant la liste des enquêtes administratives donnant lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 230-6 du code de procédure pénale, soumises à une obligation d'agrément ou d'habilitation par une autorité administrative ou judiciaire ;

2° Celles dont l'accès au point d'importance vitale fait l'objet, en raison notamment de la nature et de la durée de leur visite, de mesures de prévention et de sécurité suffisantes précisées dans le plan particulier de protection.

Article R1332-22-3

(Créé par Décret n°2012-491 du 16 avril 2012 - art. 2)

L'opérateur d'importance vitale informe par écrit la personne concernée de la demande d'avis formulée auprès de l'autorité administrative et lui indique que, dans ce cadre, elle fait l'objet d'une enquête administrative conformément aux dispositions de l'article L. 1332-2-1 du présent code.

Sous-section 2

Elaboration et approbation du plan particulier de protection

(Art. 17 du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale.)

Article R1332-23

A compter de la date de notification des directives nationales de sécurité à l'opérateur d'importance vitale, celui-ci dispose d'un délai maximal de deux ans pour présenter le plan particulier de protection de chaque point d'importance vitale au préfet du département dans le ressort duquel se trouve ce point.

Les opérateurs d'importance vitale relevant du ministre de la défense présentent le plan particulier de protection de chaque point d'importance vitale à l'autorité désignée par le ministre de la défense dans des délais identiques à ceux de l'alinéa précédent.

Les directives nationales de sécurité peuvent prévoir un délai différent de celui mentionné au premier alinéa.

Article R1332-24

Le plan particulier de protection de chaque point d'importance vitale est établi à partir du plan de sécurité d'opérateur d'importance vitale qui lui est annexé, conformément au plan type mentionné au 3º de l'article R. 1332-18.

Il comporte des mesures permanentes de protection et des mesures temporaires et graduées.

Il prévoit les délais de réalisation de ces mesures. Ces délais courent à compter de dates identiques à celles mentionnées au troisième alinéa de l'article R. 1332-19.

Le plan particulier de protection et tous les documents qui s'y rattachent sont protégés dans les conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale. Il comporte un rapport de présentation qui ne contient aucune information classifiée.

Article R1332-25

Les opérateurs d'importance vitale transmettent pour approbation le projet de plan particulier de protection au préfet du département dans le ressort duquel se trouve le point d'importance vitale.

Les opérateurs d'importance vitale relevant du ministre de la défense transmettent pour approbation le projet de plan particulier de protection à l'autorité désignée par le ministre de la défense.

Le préfet de département ou l'autorité désignée par le ministre de la défense statue dans un délai de six mois à compter de la date de réception du plan.

La décision portant approbation du plan particulier de protection est notifiée à l'opérateur d'importance vitale intéressé et est protégée dans les conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale.

Article R1332-26

I. - Au cours du délai mentionné au troisième alinéa de l'article R. 1332-25, le préfet de département ou l'autorité désignée par le ministre de la défense peut enjoindre l'opérateur d'importance vitale de compléter ou de modifier son plan particulier de protection s'il estime, notamment :

1º Qu'il n'a pas été suffisamment tenu compte de l'avis de la commission mentionné à l'article R. 1332-21 relatif au plan de sécurité de l'opérateur d'importance vitale ;

2º Ou qu'une mesure au moins ne répond pas de manière satisfaisante à la directive nationale de sécurité ou au plan de sécurité de l'opérateur d'importance vitale ou aux caractéristiques locales du point d'importance vitale.

Dans ce cas, un délai, compris entre trois et six mois, est fixé à l'opérateur d'importance vitale pour présenter un nouveau plan. L'injonction du préfet de département ou de l'autorité désignée par le ministre de la défense indique les mesures du plan qui ne peuvent être approuvées, précise en quoi elles doivent être modifiées ou complétées et invite l'opérateur à présenter ses éventuelles observations.

II. - Si le nouveau plan ne peut être approuvé pour les motifs énoncés au I, le préfet de département, après avis de la commission mentionnée à l'article R. 1332-10, ou l'autorité désignée par le ministre de la défense adopte par décision notifiée à l'opérateur d'importance vitale un plan complété ou modifié par ses soins.

III. - La décision de l'autorité mentionnée au II peut faire l'objet d'un recours devant le tribunal administratif, qui statue d'urgence. Le tribunal peut apprécier la nécessité des travaux exigés et substituer sa propre décision à celle de cette autorité.

Article R1332-27

Si, à l'expiration du délai mentionné au premier alinéa de l'article R. 1332-23, l'opérateur d'importance vitale n'a pas présenté au préfet de département ou à l'autorité désignée par le ministre de la défense le plan particulier de protection d'un point d'importance vitale, le préfet de département ou cette autorité désignée par le ministre de la

défense le met en demeure d'établir un tel plan dans un délai de trois mois à compter de la date de réception de la notification de l'arrêté de mise en demeure.

Si l'opérateur d'importance vitale n'a pas établi le plan particulier de protection à l'expiration de ce nouveau délai, le préfet de département ou l'autorité désignée par le ministre de la défense saisit l'autorité judiciaire aux fins de poursuites de l'auteur du délit prévu par les dispositions du premier alinéa de l'article L. 1332-7.

Sous-section 3

Mise en œuvre du plan particulier de protection

Article R1332-28

Le plan particulier de protection entre en vigueur à compter du lendemain de la date de notification de la décision d'approbation mentionnée à l'article R. 1332-25.

Article R1332-29

Le préfet du département dans le ressort duquel se trouve un point d'importance vitale veille à la réalisation du plan particulier de protection de ce point.

L'autorité désignée par le ministre de la défense procède de même pour les points d'importance vitale qui dépendent d'un opérateur d'importance vitale relevant du ministre de la défense.

Article R1332-30

Si, à l'expiration des délais prévus au troisième alinéa de l'article R. 1332-19 ou au troisième alinéa de l'article R. 1332-24, l'opérateur d'importance vitale n'a pas réalisé une mesure de protection prévue au plan particulier de protection, le préfet de département ou l'autorité désignée par le ministre de la défense le met par arrêté en demeure d'exécuter cette mesure dans un délai compris entre un mois et trois mois selon la nature de la mesure. Ce délai commence à courir à compter de la date de réception de la notification de l'arrêté de mise en demeure.

Si la mesure prévue n'a pas été réalisée à l'expiration de ce nouveau délai, le préfet de département ou l'autorité désignée par le ministre de la défense saisit l'autorité judiciaire aux fins de poursuite de l'auteur du délit prévu par les dispositions du premier alinéa de l'article L. 1332-7.

Sous-section 4

Révision du plan de sécurité et du plan particulier de protection

Article R1332-31

Un plan de sécurité d'opérateur d'importance vitale est révisé, selon la procédure prévue par les dispositions des articles R. 1332-19 à R. 1332-22, notamment en cas de modification d'une directive nationale de sécurité ou de changement d'activité de l'opérateur d'importance vitale.

Un plan particulier de protection peut être révisé, selon la procédure prévue par les dispositions des articles R. 1332-23 à R. 1332-28, notamment à la suite d'un contrôle portant sur la mise en œuvre du plan ou à l'initiative de l'opérateur d'importance vitale. Des audits internes doivent être conduits périodiquement par l'opérateur d'importance vitale pour apprécier la validité du plan.

Sous-section 5

Plan de protection externe

Article R1332-32

Pour chaque point d'importance vitale doté d'un plan particulier de protection, le préfet de département établit, en liaison avec le délégué de l'opérateur d'importance vitale pour la défense et la sécurité de ce point, un plan de protection externe conforme au plan type mentionné au 3º de l'article R. 1332-18.

Le plan de protection externe qui précise les mesures planifiées de vigilance, de prévention, de protection et de réaction prévues par les pouvoirs publics est protégé dans les conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale. Il comporte un rapport de présentation qui ne contient aucune information classifiée.

Sous-section 6

Contestation des actes pris par l'autorité administrative

Article R1332-33

Préalablement à l'introduction d'un recours contentieux contre tout acte administratif pris en application du présent chapitre, à l'exception de la décision mentionnée au II de l'article R. 1332-26 ou de toute décision mentionnée à la section 7 bis du présent chapitre, le requérant adresse un recours administratif au ministre coordonnateur du secteur d'activités dont il relève. Le ministre statue dans un délai de deux mois. En l'absence de décision à l'expiration de ce délai, le recours est réputé être rejeté.

Sous-section 7

Dispositions diverses

Article R1332-34

Lorsqu'en application d'accords internationaux régulièrement ratifiés ou approuvés, de lois ou de règlements, ou à l'initiative de l'opérateur d'importance vitale, un point d'importance vitale fait déjà l'objet de mesures de protection consignées dans un dossier particulier et qui répondent aux prescriptions prévues par les dispositions du présent chapitre, le préfet de département ou l'autorité désignée par le ministre de la défense dont relève ce point peut décider que ce dossier vaut plan particulier de protection, après avis de la commission mentionnée à l'article R. 1332-10.

Section 6

Zone d'importance vitale

Article R1332-35

Lorsque dans une zone géographique continue sont implantés plusieurs points d'importance vitale relevant d'opérateurs différents et interdépendants, le préfet du département dans le ressort duquel se situe cette zone peut la désigner zone d'importance vitale, par arrêté pris après avis de la commission mentionnée à l'article R. 1332-13.

L'arrêté délimite la zone et identifie les opérateurs d'importance vitale. Il est notifié à chacun des opérateurs d'importance vitale ainsi qu'à l'officier général de la zone de défense et de sécurité et est protégé dans les conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale.

L'arrêté mentionné aux premier et deuxième alinéas est pris par le ministre de la défense pour les zones d'importance vitale composées de points d'importance vitale relevant de sa responsabilité.

Article R1332-36

Lorsqu'une zone géographique, répondant aux conditions de l'article R. 1332-35, s'étend sur plus d'un département au sein d'une même zone de défense et de sécurité ou sur plusieurs zones de défense et de sécurité, un arrêté du Premier ministre, pris après avis de la commission mentionnée à l'article R. 1332-13, la qualifie de zone d'importance vitale et désigne un préfet de département coordonnateur.

Le préfet coordonnateur, en concertation avec les préfets de départements intéressés, arrête le périmètre de la zone, identifie les opérateurs d'importance vitale et exerce les attributions dévolues au préfet de département par les dispositions des articles R. 1332-23 à R. 1332-28.

Article R1332-37

Les opérateurs d'importance vitale désignent en commun un délégué pour la défense et la sécurité de la zone d'importance vitale, dont ils communiquent le nom au préfet de département mentionné à l'article R. 1332-35 ou au préfet de département coordonnateur mentionné à l'article R. 1332-36. Cette personne est habilitée dans les

conditions prévues par les articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale.

Le délégué pour la défense et la sécurité de la zone d'importance vitale exerce pour cette zone les fonctions prévues au deuxième alinéa de l'article R. 1332-5.

Tant qu'il n'a pas été désigné un délégué pour la défense et la sécurité de la zone d'importance vitale, les opérateurs d'importance vitale de cette zone exercent en commun cette fonction.

Article R1332-38

Le délégué pour la défense et la sécurité d'une zone d'importance vitale élabore, en liaison avec les opérateurs d'importance vitale présents dans la zone, un plan particulier de protection de zone qui prévoit des mesures communes de protection.

Les opérateurs d'importance vitale doivent veiller à la cohérence des plans particuliers de protection des points d'importance vitale situés dans une zone d'importance vitale avec le plan particulier de protection de cette zone.

Les dispositions des articles R. 1332-23 à R. 1332-28 sont applicables au plan particulier de protection de la zone d'importance vitale.

Section 7

Zones civiles sensibles

Article D1332-39

Les zones protégées situées dans les établissements, installations et ouvrages des opérateurs publics ou privés intéressant la défense et qui relèvent du ministre de la défense conformément aux dispositions de l'article D. 1142-19 peuvent être érigées en zones civiles sensibles par arrêté de ce ministre.

NOTA : Au lieu de lire « l’article D. 1142-19 », il convient de lire « l’article R. 1142-19 ».

Article D1332-40

La zone civile sensible est matérialisée par la mise en place de panneaux portant la mention " Défense de pénétrer, danger de mort ".

Article D1332-41

La protection matérielle des zones civiles sensibles est assurée notamment par des dispositifs dangereux, permanents ou temporaires.

La liste des dispositifs de protection dangereux et les conditions d'installation et d'emploi de chacun d'eux sont fixées par arrêté du ministre de la défense.

Section 7 bis : Dispositions spécifiques à la sécurité des systèmes d'information

Sous-section 1 : Règles de sécurité

Article R1332-41-1

L'Agence nationale de la sécurité des systèmes d'information élabore et propose au Premier ministre les règles de sécurité prévues à l'article L. 1332-6-1. Ces règles sont établies par arrêté du Premier ministre pris après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernés. Lorsque l'arrêté n'est pas publié, il est notifié aux personnes ayant besoin d'en connaître.

Les arrêtés mentionnés au premier alinéa peuvent prévoir des règles de sécurité différentes selon le secteur ou le type d'activité de l'opérateur. Ils fixent les délais dans lesquels les opérateurs d'importance vitale sont tenus d'appliquer les règles de sécurité. Ces délais peuvent être différents selon les règles de sécurité, le type de systèmes d'information concernés ou la date de mise en service de ces systèmes.

Article R1332-41-2

Chaque opérateur d'importance vitale établit et tient à jour la liste des systèmes d'information mentionnés à l'article L. 1332-6-1, y compris ceux des opérateurs tiers qui participent à ces systèmes, auxquels s'appliquent les règles de sécurité prévues au même article.

Les systèmes d'information figurant sur la liste mentionnée au premier alinéa sont dénommés “ systèmes d'information d'importance vitale ”.

La liste est établie selon des modalités fixées par arrêté du Premier ministre pris après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernés. Ces arrêtés peuvent prévoir des modalités différentes selon le secteur ou le type d'activité de l'opérateur. Lorsque l'arrêté n'est pas publié, il est notifié aux personnes ayant besoin d'en connaître.

Chaque opérateur communique sa liste de systèmes d'information d'importance vitale et les mises à jour de celle-ci à l'Agence nationale de la sécurité des systèmes d'information selon des modalités et dans des délais fixés par l'arrêté mentionné au troisième alinéa.

L'Agence nationale de la sécurité des systèmes d'information peut, après avis des ministres coordonnateurs concernés, faire des observations à l'opérateur sur sa liste. Dans ce cas, l'opérateur modifie sa liste conformément à ces observations et communique la liste modifiée à l'Agence nationale de la sécurité des systèmes d'information dans un délai de deux mois à compter de la réception des observations.

La liste des systèmes d'information d'importance vitale est couverte par le secret de la défense nationale.

Sous-section 2 : Détection des événements de sécurité

Article R1332-41-3

Les règles de sécurité prévues à l'article L. 1332-6-1 fixent les conditions et les délais dans lesquels les opérateurs d'importance vitale mettent en œuvre des systèmes de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information d'importance vitale. Elles déterminent également le type de système de détection utilisé.

Article R1332-41-4

Lorsque l'opérateur d'importance vitale est une administration de l'Etat, le Premier ministre, après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernés, décide, en fonction des risques particuliers encourus par les systèmes d'information en cause, si les systèmes de détection sont exploités par l'Agence nationale de la sécurité des systèmes d'information, par un autre service de l'Etat ou par un prestataire de service qualifié.

Dans les autres cas, les systèmes de détection sont exploités exclusivement par un prestataire de service qualifié.

Lorsque les systèmes de détection sont exploités par un prestataire de service qualifié, l'opérateur choisit le prestataire sur la liste prévue à l'article R. 1332-41-9.

Article R1332-41-5

L'opérateur d'importance vitale conclut une convention avec le service de l'Etat ou le prestataire de service chargé d'exploiter les systèmes de détection. Cette convention précise :

1° Les systèmes d'information de l'opérateur qui font l'objet du service de détection ;

2° Les fonctionnalités du service de détection et le type de système de détection utilisé ;

3° Les systèmes de détection qualifiés utilisés et leurs modalités d'installation et d'exploitation par le service de l'Etat ou le prestataire ;

4° La nature des informations échangées entre l'opérateur et le service de l'Etat ou le prestataire, les conditions dans lesquelles elles sont utilisées et protégées ainsi que les moyens de communication sécurisés nécessaires à ces échanges ;

5° Les moyens techniques et humains nécessaires à l'opérateur pour la mise en œuvre du service de détection.

La convention est conclue dans des délais compatibles avec ceux prévus pour la mise en service des systèmes de détection.

Une copie de la convention signée est adressée sans délai par l'opérateur à l'Agence nationale de la sécurité des systèmes d'information.

Article R1332-41-6

Afin de rechercher et d'analyser des événements susceptibles d'affecter la sécurité des systèmes d'information d'importance vitale, l'Agence nationale de la sécurité des systèmes d'information peut demander aux services de l'Etat et aux prestataires de service chargés d'exploiter les systèmes de détection d'utiliser dans ces systèmes des données techniques qu'elle leur fournit.

L'utilisation de ces données techniques est soumise à des conditions particulières définies par l'Agence nationale de la sécurité des systèmes d'information, en particulier lorsque les données sont couvertes par le secret de la défense nationale.

Sous-section 3 : Qualification des systèmes de détection et des prestataires de service exploitant ces systèmes

Article R1332-41-7

Les systèmes de détection et les prestataires de service mentionnés à l'article L. 1332-6-1 sont qualifiés dans les conditions prévues respectivement par les chapitres II et III du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

Article R1332-41-8

Un opérateur d'importance vitale peut agir comme prestataire de service exploitant des systèmes de détection au profit d'autres opérateurs d'importance vitale ou pour ses besoins propres sous réserve d'être qualifié dans les conditions prévues à l'article R. 1332-41-7.

Article R1332-41-9

L'Agence nationale de la sécurité des systèmes d'information met à la disposition du public par voie électronique la liste des systèmes de détection et des prestataires de service exploitant ces systèmes, qualifiés dans les conditions prévues à l'article R. 1332-41-7.

Sous-section 4 : Déclaration des incidents de sécurité

Article R1332-41-10

En application de l'article L. 1332-6-2, les opérateurs d'importance vitale communiquent à l'Agence nationale de la sécurité des systèmes d'information les informations relatives aux incidents affectant la sécurité ou le fonctionnement de leurs systèmes d'information d'importance vitale.

Les opérateurs communiquent les informations dont ils disposent dès qu'ils ont connaissance d'un incident et les complètent au fur et à mesure de leur analyse de l'incident. Ils répondent aux demandes d'informations complémentaires de l'Agence nationale de la sécurité des systèmes d'information concernant l'incident.

Le Premier ministre précise par arrêté, en distinguant le cas échéant selon le secteur ou le type d'activité de l'opérateur, les informations qui doivent être communiquées, les modalités de leur transmission ainsi que les types d'incident auxquels s'applique l'obligation prévue à l'article L. 1332-6-2. Lorsque l'arrêté n'est pas publié, il est notifié aux personnes ayant besoin d'en connaître.

Article R1332-41-11

L'Agence nationale de la sécurité des systèmes d'information transmet aux ministres coordonnateurs des secteurs d'activités d'importance vitale concernés, lorsque son analyse de l'incident le justifie, une synthèse des informations recueillies relatives à cet incident.

Sous-section 5 : Contrôles de sécurité

Article R1332-41-12

Le Premier ministre, après avis des ministres coordonnateurs des secteurs d'activités d'importance vitale concernés, notifie aux opérateurs d'importance vitale sa décision d'imposer un contrôle prévu à l'article L. 1332-6-

3. Il précise les objectifs et le périmètre du contrôle et fixe le délai dans lequel le contrôle est réalisé. Il précise, en fonction de la nature des opérations à mener, si ce contrôle est effectué par l'Agence nationale de la sécurité des systèmes d'information, par un autre service de l'Etat ou par un prestataire de service qualifié. Dans ce dernier cas, l'opérateur choisit le prestataire sur la liste prévue à l'article R. 1332-41-16.

Le Premier ministre ne peut imposer à un opérateur plus d'un contrôle par année civile d'un même système d'information, sauf si les systèmes d'information de cet opérateur sont affectés par un incident de sécurité ou si des vulnérabilités ou des manquements aux règles de sécurité ont été constatés lors d'un contrôle précédent subi par l'opérateur.

Article R1332-41-13

L'opérateur d'importance vitale fournit au service de l'Etat ou au prestataire de service chargé du contrôle :

1° Les informations nécessaires pour évaluer la sécurité de ses systèmes d'information, notamment la documentation technique des équipements et des logiciels utilisés dans ses systèmes ainsi que les codes sources de ces logiciels ;

2° Les moyens nécessaires pour accéder à ses systèmes d'information et à l'ensemble de leurs composants afin de permettre au service de l'Etat ou au prestataire de réaliser des analyses sur les systèmes, notamment des relevés d'informations techniques.

Article R1332-41-14

L'opérateur d'importance vitale conclut une convention avec le service de l'Etat ou le prestataire de service chargé d'effectuer le contrôle. Cette convention précise :

1° Les systèmes d'information qui font l'objet du contrôle ;

2° Les objectifs et le périmètre du contrôle ;

3° Les modalités de déroulement du contrôle, notamment les conditions d'accès aux sites et aux systèmes d'information de l'opérateur ;

4° Les informations nécessaires à la réalisation du contrôle, fournies par l'opérateur, et les conditions de leur protection ;

5° Les modalités selon lesquelles sont effectuées les analyses techniques sur les systèmes d'information de l'opérateur.

La convention est conclue dans des délais compatibles avec le délai fixé par le Premier ministre pour la réalisation du contrôle.

Une copie de la convention signée est adressée sans délai par l'opérateur à l'Agence nationale de la sécurité des systèmes d'information.

Article R1332-41-15

Le service de l'Etat ou le prestataire ayant réalisé le contrôle rédige un rapport exposant ses constatations, au regard de l'objectif du contrôle, sur le niveau de sécurité des systèmes d'information contrôlés et le respect des règles de sécurité prévues à l'article L. 1332-6-1. Les vulnérabilités et les manquements aux règles de sécurité constatés lors du contrôle sont indiqués dans le rapport, qui formule le cas échéant des recommandations pour y remédier. Le rapport est couvert par le secret de la défense nationale.

Après avoir mis l'opérateur en mesure de faire valoir ses observations, le service de l'Etat ou le prestataire remet, dans le délai fixé pour la réalisation du contrôle, le rapport à l'Agence nationale de la sécurité des systèmes d'information.

L'Agence nationale de la sécurité des systèmes d'information peut auditionner, dans un délai de deux mois à compter de la remise du rapport, le service de l'Etat ou le prestataire ayant réalisé le contrôle, le cas échéant en présence de l'opérateur, aux fins d'examiner les constatations et les recommandations figurant dans le rapport. Elle peut inviter les ministres coordonnateurs des secteurs d'activités d'importance vitale concernés à assister à cette audition.

L'Agence nationale de la sécurité des systèmes d'information communique aux ministres coordonnateurs des secteurs d'activités d'importance vitale concernés les conclusions du contrôle.

Article R1332-41-16

Les prestataires de service mentionnés à l'article L. 1332-6-3 sont qualifiés dans les conditions prévues par le chapitre III du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

L'Agence nationale de la sécurité des systèmes d'information met à la disposition du public par voie électronique la liste des prestataires de service qualifiés mentionnés au premier alinéa.

Article R1332-41-17

Le coût des contrôles effectués par un service de l'Etat en application de l'article L. 1332-6-3 est calculé en fonction du temps nécessaire à la réalisation du contrôle et du nombre d'agents publics qui y participent. Un arrêté du Premier ministre fixe le coût d'un contrôle mobilisant un agent public pendant une journée.

Le coût des contrôles effectués par un prestataire de service est déterminé librement par les parties.

Sous-section 6 : Réponse aux crises majeures

Article R1332-41-18

L'Agence nationale de la sécurité des systèmes d'information propose au Premier ministre les mesures mentionnées à l'article L. 1332-6-4.

Sous-section 7 : Dispositions diverses

Article R1332-41-19

Les opérateurs d'importance vitale prennent les mesures nécessaires, notamment par voie contractuelle, pour garantir l'application des dispositions prévues à la présente section aux systèmes d'information des opérateurs tiers mentionnés au premier alinéa de l'article R. 1332-41-2.

Article R1332-41-20

Chaque opérateur d'importance vitale désigne une personne chargée de le représenter auprès de l'Agence nationale de la sécurité des systèmes d'information pour toutes les questions relatives à l'application des dispositions prévues à la présente section. Nul ne peut être désigné s'il n'est titulaire de l'habilitation mentionnée à l'article R. 2311-7.

Article R1332-41-21

L'Agence nationale de la sécurité des systèmes d'information peut imposer aux opérateurs d'importance vitale et aux prestataires de service mentionnés aux articles L. 1332-6-1 et L. 1332-6-3 l'utilisation d'un moyen particulier pour protéger les échanges d'information prévus à la présente section lorsqu'ils sont effectués par voie électronique.

Article R1332-41-22

Les services de l'Etat et les prestataires de service mentionnés aux articles L. 1332-6-1 et L. 1332-6-3 accèdent aux systèmes d'information des opérateurs d'importance vitale et, le cas échéant, aux informations qu'ils contiennent dans le respect des secrets protégés par la loi.

Article R1332-41-23

Si un opérateur d'importance vitale ne satisfait pas aux obligations prévues aux articles L. 1332-6-1 à L. 1332-6-4, l'Agence nationale de la sécurité des systèmes d'information saisit l'autorité judiciaire aux fins de poursuite de l'auteur du délit prévu au troisième alinéa de l'article L. 1332-7. Hormis le cas d'un manquement à l'article L. 1332-6-2, cette saisine est précédée d'une mise en demeure adressée à l'opérateur par l'Agence nationale de la sécurité des systèmes d'information.

Section 8

Dispositions pénales

Article R1332-42

Le fait de faire obstacle à l'accomplissement des missions des fonctionnaires chargés de vérifier l'état des établissements mentionnés aux articles L. 1332-1 et L. 1332-2 et de constater les infractions est puni de l'amende prévue pour les contraventions de la 5e classe.

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs

NOR : *PRMX0609332A*

Le Premier ministre, le ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire, la ministre de la défense, le ministre de l'économie, des finances et de l'industrie, le ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche, le garde des sceaux, ministre de la justice, le ministre des transports, de l'équipement, du tourisme et de la mer, le ministre de la santé et des solidarités, le ministre de l'agriculture et de la pêche, le ministre de la culture et de la communication, la ministre de l'écologie et du développement durable, le ministre de l'outre-mer, le ministre délégué à l'enseignement supérieur et à la recherche et le ministre délégué à l'industrie,

Vu le décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale, notamment son article 2 ;

Vu l'avis de la commission interministérielle de défense et de sécurité des secteurs d'activités d'importance vitale en date du 28 avril 2006,

Arrêtent :

Art. 1er. – La liste des secteurs d'activités d'importance vitale prévue à l'article 2 du décret du 23 février 2006 susvisé et de leurs ministres coordonnateurs est fixée conformément au tableau annexé au présent arrêté.

Art. 2. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait à Paris, le 2 juin 2006.

Le Premier ministre,
DOMINIQUE DE VILLEPIN

Le ministre d'Etat,
ministre de l'intérieur
et de l'aménagement du territoire,
NICOLAS SARKOZY

La ministre de la défense,
MICHÈLE ALLIOT-MARIE

Le ministre de l'économie,
des finances et de l'industrie,
THIERRY BRETON

Le ministre de l'éducation nationale,
de l'enseignement supérieur
et de la recherche,
GILLES DE ROBIEN

Le garde des sceaux, ministre de la justice,
PASCAL CLÉMENT

Le ministre des transports, de l'équipement,
du tourisme et de la mer,
DOMINIQUE PERBEN

Le ministre de la santé et des solidarités,
XAVIER BERTRAND

Le ministre de l'agriculture et de la pêche,
DOMINIQUE BUSSEREAU

Le ministre de la culture
et de la communication,
RENAUD DONNEDIEU DE VABRES

La ministre de l'écologie
et du développement durable,
NELLY OLIN

Le ministre de l'outre-mer,
FRANÇOIS BAROIN

Le ministre délégué
à l'enseignement supérieur
et à la recherche,
FRANÇOIS GOULARD

Le ministre délégué à l'industrie,
FRANÇOIS LOOS

ANNEXE

À L'ARRÊTÉ DU 2 JUIN 2006 FIXANT LA LISTE DES SECTEURS D'ACTIVITÉS D'IMPORTANCE VITALE ET DÉSIGNANT LES MINISTRES COORDONNATEURS DESDITS SECTEURS

SECTEURS	MINISTRES COORDONNATEURS
Activités civiles de l'Etat.	Ministre de l'intérieur.
Activités judiciaires.	Ministre de la justice.
Activités militaires de l'Etat.	Ministre de la défense.
Alimentation.	Ministre chargé de l'agriculture.
Communications électroniques, audiovisuel et information.	Ministre chargé des communications électroniques.
Energie.	Ministre chargé de l'industrie.
Espace et recherche.	Ministre chargé de la recherche.
Finances.	Ministre chargé de l'économie et des finances.
Gestion de l'eau.	Ministre chargé de l'écologie.
Industrie.	Ministre chargé de l'industrie.
Santé.	Ministre chargé de la santé.
Transports.	Ministre chargé des transports.

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Arrêté du 3 juillet 2008 portant modification de l'arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs

NOR : *PRMD0813724A*

Le Premier ministre, le ministre d'Etat, ministre de l'écologie, de l'énergie, du développement durable et de l'aménagement du territoire, et la ministre de l'économie, de l'industrie et de l'emploi,

Vu le code de la défense, notamment son article R. 1332-2 ;

Vu l'arrêté interministériel du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs,

Arrêtent :

Art. 1er. – Le tableau annexé à l'arrêté du 2 juin 2006 susvisé est ainsi modifié :

A la ligne « Energie », dans la colonne « ministres coordonnateurs », remplacer : « ministre chargé de l'industrie » par : « ministre chargé de l'énergie ».

Art. 2. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait à Paris, le 3 juillet 2008.

Le Premier ministre,
Pour le Premier ministre et par délégation :
Le secrétaire général du Gouvernement,
SERGE LASVIGNES

Le ministre d'Etat, ministre de l'écologie, de l'énergie, du développement durable et de l'aménagement du territoire,
JEAN-LOUIS BORLOO

La ministre de l'économie, de l'industrie et de l'emploi,
CHRISTINE LAGARDE

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE LA DÉFENSE

Arrêté du 31 mars 2017 relatif au secteur d'activité d'importance vitale dont le ministre de la défense est ministre coordonnateur

NOR : *DEFD1710382A*

Le ministre de la défense,

Vu le code de la défense, notamment le chapitre II du titre III du livre III de sa première partie ;

Vu le décret n° 2009-1178 du 5 octobre 2009 modifié portant organisation de l'administration centrale du ministère de la défense ;

Vu le décret n° 2015-1029 du 19 aout 2015 modifié relatif à la direction de la protection des installations, moyens et activités de la défense,

Arrête :

Art. 1er. – Pour l'application de l'article R. 1332-6 du code de la défense, le nom du délégué pour la défense et la sécurité désigné pour chaque point d'importance vitale est communiqué aux autorités suivantes, agissant au nom du ministre de la défense :

1° Les chefs d'état-major d'armée, les directeurs généraux, directeurs et chefs de services du ministère de la défense et les commandants supérieurs des forces armées, pour les points d'importance vitale relevant de leur autorité respective ;

2° Le délégué général pour l'armement, pour les points d'importance vitale relevant des opérateurs d'importance vitale autres que ceux mentionnés au 1°, à l'exception de ceux constituant des installations nucléaires intéressant la dissuasion ;

3° Le directeur de la protection des installations, moyens et activités de la défense pour les points d'importance vitale relevant d'opérateurs d'importance vitale autres que ceux mentionnés au 1° et constituant des installations nucléaires intéressant la dissuasion.

Les autorités mentionnées au 1° et 2° en tiennent informé le directeur de la protection des installations, moyens et activités de la défense.

Art. 2. – Pour l'application des dispositions des articles R. 1332-23, R. 1332-25, R. 1332-26, R. 1332-27, R. 1332-29, R. 1332-30 et R. 1332-34 du code de la défense, les autorités mentionnées à l'article 1er agissent, chacune en ce qui la concerne, pour ces mêmes points d'importance vitale, en qualité d'autorité désignée par le ministre de la défense.

Conformément au IV de l'article 5 du décret du 19 août 2015 susvisé, les autorités mentionnées aux 1° et 2° de l'article 1er doivent recueillir, selon le cas, l'avis ou l'avis favorable du directeur de la protection des installations, moyens et activités de la défense avant de prendre la décision d'approbation prévue à l'article R. 1332-25 du code de la défense.

Art. 3. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait le 31 mars 2017.

JEAN-YVES LE DRIAN

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

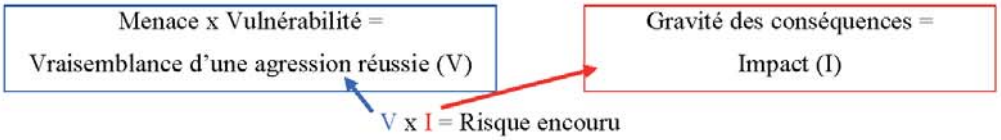
L'étape finale de l'évaluation vise à hiérarchiser les risques encourus. Elle peut se faire de la manière suivante, présentée à titre d'illustration.

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

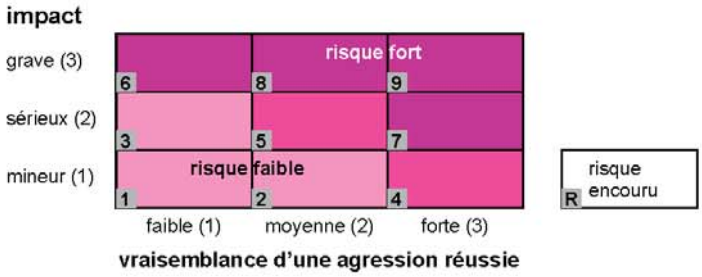
impact	niveau	description
grave	3	- dangerosité élevée pour la population - effet important sur l'activité du pays
sérieux	2	- dangerosité sérieuse pour la population - effet sensible sur l'activité du pays
mineur	1	- dangerosité faible pour la population - effet faible sur l'activité du pays

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.

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Arrêté du 2 juillet 2018 portant approbation du plan type des plans de sécurité d'opérateurs d'importance vitale

NOR : *PRMD1818234A*

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, R. 1332-12 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. – Le plan type des plans de sécurité d'opérateurs d'importance vitale, annexé au présent arrêté, est approuvé.

Art. 2. – L'arrêté du 27 avril 2007 fixant le plan type des plans de sécurité d'opérateurs 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

PLAN-TYPE – PLAN DE SÉCURITÉ D'OPÉRATEUR

Préambule. Rapport de présentation (non classifié)

Introduction. Champ d'application du plan de sécurité d'opérateur d'importance vitale

Chapitre 1. Analyse des risques

1.1. Scénarios de menace
1.2. Evaluation des risques
1.3. Etudes de vulnérabilités spécifiques aux établissements, ouvrages ou installations gérés par l'opérateur prises en compte pour la détermination du ou des points d'importance vitale
1.4. Autres vulnérabilités à prendre en compte (notamment pour les organisations en réseau)

Chapitre 2. Mesures destinées à réduire les risques - mise en œuvre du plan VIGIPIRATE

2.1. Mesures spécifiques permanentes de vigilance, de prévention, de protection et de réaction
2.2. Mesures spécifiques temporaires et graduées de vigilance, de prévention, de protection et de réaction
2.3. Développement de dispositifs particuliers (politique de sécurité informatique, mesures de protection spécifique du système d'acquisition et de contrôle de données (SCADA)…)

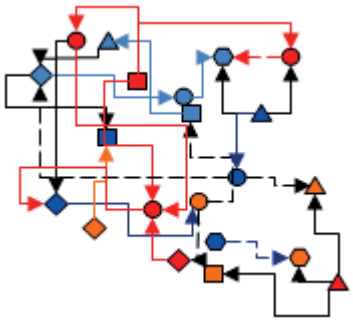
Chapitre 3. Dispositif d'alerte et de gestion de crise

3.1. Prévention des crises
3.2. Dispositifs d'alerte et de déclenchement de l'organisation de crise
3.3. Organisation des cellules de crise
3.4. Plans de continuité et de reprise d'activité
3.5. Exercices de simulation

SECURITE DES ACTIVITES D'IMPORTANCE VITALE



GUIDE
POUR L'ELABORATION D'UN PLAN DE SECURITE D'OPERATEUR

VIGIPIRATE

Edition juillet 2018

SGDSN

En contribuant aux besoins essentiels des populations, à leur sécurité ou au fonctionnement de l'économie, de nombreux opérateurs publics et privés revêtent un caractère indispensable pour la Nation.

Ces opérateurs d'importance vitale (OIV) sont ainsi des acteurs majeurs du dispositif de sécurité des activités d'importance vitale (SAIV) dont l'objectif est de les protéger plus efficacement contre une menace terroriste élevée et multiforme, des aléas climatiques, des risques technologiques ou des attaques de plus en plus fréquentes et agressives contre les systèmes d'information.

Le dispositif SAIV doit ainsi permettre aux opérateurs d'analyser leurs risques et d'appliquer les mesures en cohérence avec les décisions des pouvoirs publics.

Le présent guide propose des conseils aux opérateurs d'importance vitale en vue de l'élaboration et de la mise en œuvre de leur plan de sécurité d'opérateur. Il fournit les éléments généraux facilitant l'élaboration du plan et cerne les points à considérer. Il n'a pas de valeur contraignante pour les opérateurs.

Il complète et précise les éléments fournis par la réglementation et par l'instruction générale interministérielle N° 6600/SGDSN/PSE/PSN du 7 janvier 2014.

Table des matières

INTRODUCTION : QU'EST-CE QU'UN PSO ?

Le plan de sécurité d'opérateur définit la politique et l'organisation de la sécurité de l'opérateur. Il précise, de façon générique, les mesures à mettre en œuvre pour chaque point d'importance vitale (PIV) tant sur le plan organisationnel (organiser l'alerte et gérer la crise), qu'en matière de prévention (réduire les vulnérabilités) et de protection (réduire les conséquences).

Il est fondé sur une analyse de risque prenant en compte notamment les scénarios de la ou les directives nationales de sécurité (DNS).

Il s'appuie sur le dispositif de sécurité existant et sur l'expérience acquise par l'opérateur dans la gestion de la sécurité et de la sûreté.

Quelle commission rend un avis sur le PSO ?

- Le périmètre du PSO dépasse celui de la zone de défense : la commission interministérielle de défense de sécurité (CIDS).
- Le périmètre du PSO ne dépasse pas le ressort de la zone de défense : la commission zonale de défense et de sécurité (CZDS).
- Les PSO relevant du ministère de la défense ne font pas l'objet d'un avis de la CIDS ou de la CZDS.

Il est rédigé par l'opérateur et fait l'objet d'un avis de la commission interministérielle ou zonale de défense et de sécurité (CIDS ou CZDS) selon le cas, après instruction par le ministre coordonnateur du secteur. L'avis rendu porte aussi bien sur les mesures de sécurité proposées par l'opérateur que sur la liste des PIV.

Pour chaque PIV, l'opérateur est tenu de rédiger un plan particulier de protection (PPP) qui adapte, aux conditions locales de chaque site, les principes du PSO. Le préfet de département approuve le PPP et élabore pour chaque PIV un plan de protection externe (PPE) comportant les mesures de surveillance et d'intervention de la force publique.

Document structurant pour la sécurité de l'OIV, le PSO doit être pensé comme un instrument stratégique qui assiste l'opérateur dans la gestion de sa sécurité. Il doit permettre à l'opérateur de s'interroger sur des scénarios majeurs et, le cas échéant, de repenser certains dispositifs opérationnels. Il doit également amener à une connaissance partagée de ces enjeux avec les pouvoirs publics.

Le PSO, ainsi que tous les documents qui s'y rattachent, sont protégés par le secret de la défense nationale. Ils ne sont communiqués qu'aux personnes ayant à en connaître (SGDSN, ministère coordonnateur, préfets de la zone de défense et de sécurité et du département concerné).

1. DESCRIPTION DE L'ATTENDU

1.1. Principes généraux

Les articles R. 1332-19 et suivants du code de la défense prévoient que l'opérateur élabore un plan de sécurité d'opérateur à partir d'une ou plusieurs directives nationales de sécurité qui lui ont été notifiées.

Le PSO décrit l'organisation et la politique de sécurité de l'opérateur. Il lui permet, en outre, de s'assurer d'une cohérence dans l'organisation de la sécurité de ses différents points d'importance vitale. Ainsi, le plan particulier de protection de chaque PIV se conforme à la politique globale de sécurité définie préalablement dans le PSO. Par ailleurs, le PSO étant

établi sur un plan-type, il assure un niveau d'exigence commun entre les opérateurs d'un même secteur d'activités.

Le PSO permet également de constituer un référentiel pour la sécurité des sites qui n'ont pas été retenus comme point d'importance vitale.

1.2. Cadre d'élaboration

Le plan du PSO doit respecter le modèle type annexé à l'arrêté du Premier ministre du 2 juillet 2018. Ce plan-type doit permettre à l'opérateur de ne rien omettre dans la rédaction du PSO et assure, pour les pouvoirs publics, un canevas commun pour l'ensemble des OIV.

L'opérateur prend en compte la ou les DNS qui lui ont été notifiées. Il définit sa politique de sécurité en intégrant, d'une part, les objectifs généraux de sécurité énoncés dans la DNS et, d'autre part, en déclinant les scénarios de menace listés dans celles-ci.

Il mentionne les autres obligations juridiques éventuelles ou conventions de service public pouvant exister.

Cas d'un opérateur intéressant plusieurs DNS

- Les ministères concernés et la CIDS se concertent pour définir un correspondant privilégié pour l'OIV.
- Le correspondant privilégié transmet à l'opérateur les DNS nécessaires à l'élaboration du PSO.
- L'opérateur rédige son PSO à partir des DNS qui lui ont été notifiées et le transmet au ministère retenu comme « correspondant privilégié ».

L'OIV peut, s'il le souhaite, solliciter son ministère coordonnateur pour l'aider dans la rédaction du PSO.

La rédaction du PSO se fera sur un poste informatique sécurisé.

1.3. Base documentaire

Pour l'accompagner dans la rédaction de son PSO, l'opérateur dispose des documents suivants :

- articles L. 1332-1 à L. 1332-7 du code de la défense ;
- articles R. 1332-1 à R. 1332-45 du code de la défense ;
- le plan VIGIPIRATE du 1er décembre 2016 (parties publique et confidentielle) ;
- l'instruction générale interministérielle relative à la sécurité des activités d'importance vitale n° 6600/SGDSN/PSE/PSN du 7 janvier 2014 ;
- l'instruction méthodologique d'analyse de risque fixée par arrêté du Premier ministre du 2 juillet 2018 ;
- le plan-type du PSO annexé à l'arrêté du Premier ministre du 2 juillet 2018 ;
- la ou les directives nationales de sécurité qui lui ont été notifiées ;
- le présent guide d'élaboration du plan de sécurité d'opérateur.

1.4. Articulation avec les plans et règlementations existants

1.4.1. Le plan VIGIPIRATE

L'opérateur décline et adapte dans son PSO les mesures sectorielles et les mesures des domaines transverses du plan VIGIPIRATE qui lui sont applicables et qu'il est susceptible de mettre en œuvre pour atteindre les objectifs de sécurité fixés par la DNS.

Le PSO permet une forte collaboration entre l'État et l'ensemble des opérateurs désignés d'importance vitale afin de prendre des dispositions cohérentes avec celles que le Gouvernement aura arrêtées ou recommandées au niveau national.

1.4.2. Le plan de continuité d'activité (PCA)

Le PCA décrit la stratégie adoptée par une organisation pour rétablir et reprendre son activité à la suite d'une perturbation importante. En listant et hiérarchisant l'ensemble des scénarios de risque et de menace pour un secteur donné, la directive nationale de sécurité constitue un référentiel pour le PCA et le PSO. Si ce dernier insiste sur les actes de malveillance (terrorisme, sabotage etc.), le PCA doit tenir compte de l'ensemble des scénarios.

Les OIV sont désormais tenus de rédiger un plan de continuité d'activité (article L. 2151-1 du code de la défense). Ils ont la possibilité de le décliner pour chacun de leur PIV.

Il est recommandé pour l'élaboration de ce plan de continuité d'activité, d'utiliser le guide méthodologique proposé par le secrétariat général de la défense et de la sécurité nationale (SGDSN) intitulé *Guide pour réaliser un plan de continuité d'activité.* Il est disponible sur le site internet www.sgdsn.gouv.fr/.

1.4.3. La sécurité des systèmes d'information, l'application des articles L. 1332-6-1 à L. 1332-6-6 du code de la défense

Les dispositions réglementaires issues de l'article 22 de la loi de programmation militaire du 18 décembre 2013 imposent de nouvelles obligations aux opérateurs d'importance vitale en matière de sécurité de leurs systèmes d'information. Elles comprennent la désignation des systèmes d'information d'importance vitale (SIIV), la déclaration d'incidents et la mise en œuvre de règles fixées par l'ANSSI. Les mesures SSI décrites dans le PSO doivent être cohérentes avec les arrêtés sectoriels pris en application de l'article L. 1332-6-1 du code de la défense.

L'identification des SIIV s'appuie sur les missions et activités essentielles définies dans la DNS.

Bien que n'étant pas soumis à l'avis de la CIDS ou CZDS, la liste des systèmes d'information d'importance vitale peut figurer dans le PSO.

1.4.4. La révision des directives nationales de sécurité (DNS)

Le processus de révision des DNS lancé en 2013 à trois objectifs principaux : prendre en compte le nouveau plan VIGIPIRATE, renforcer la sécurité des systèmes d'information et adopter une approche tous risques afin d'inciter les opérateurs à se préparer à faire face à toutes sortes de crises affectant leurs ressources (humaines, immobilières, réseaux...), en élaborant des plans de continuité d'activité (PCA).

Quand réviser son PSO ?

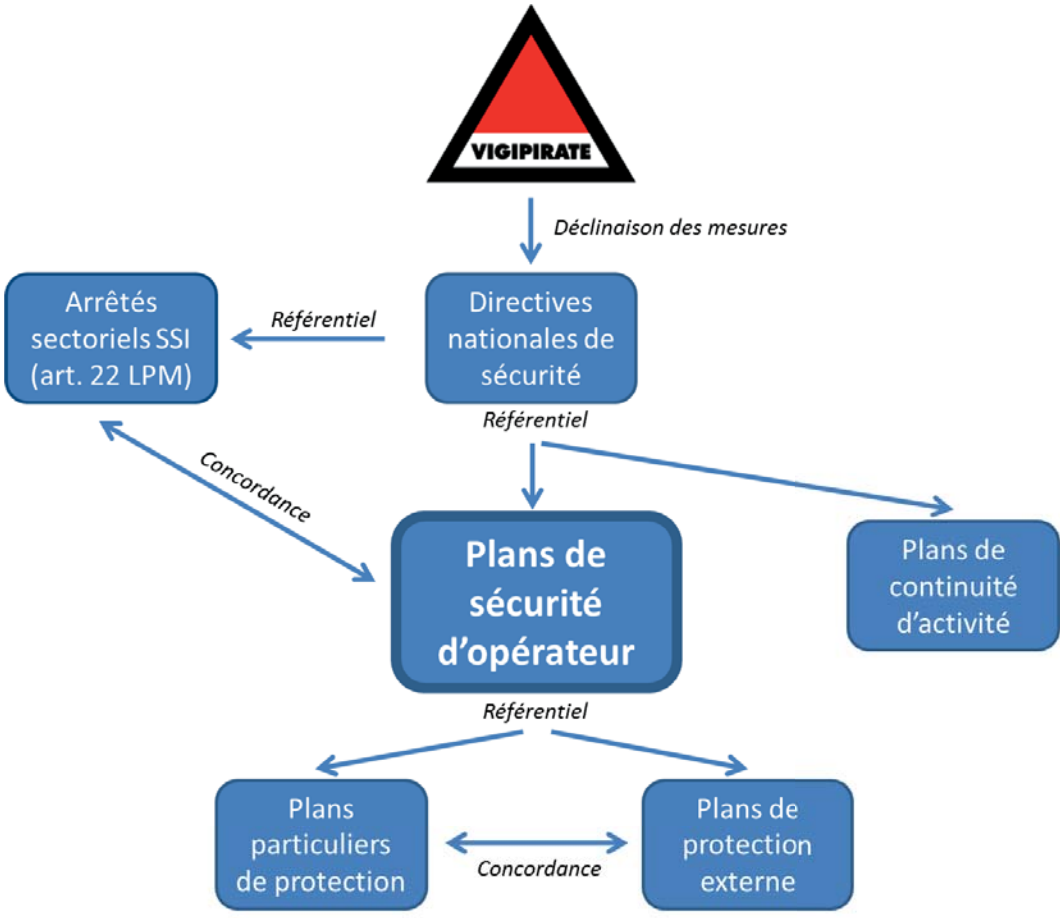
- En cas de notification d'une DNS révisée.
- Sur initiative de l'opérateur, en cas de modification majeure de son organisation ou de sa politique de sécurité.

Les DNS, qui constituaient déjà un référentiel pour les PSO, le seront dorénavant pour les PCA.

1.4.5. La révision des plans de sécurité d'opérateur (PSO)

La révision du plan VIGIPIRATE en 2016, l'application des articles L. 1332-6-1 à L. 1332-6-6 du code de la défense et la révision des DNS induisent une nécessaire actualisation du PSO pour tenir compte de ces évolutions. Cette révision doit également permettre à l'opérateur de considérer de nouvelles menaces ou qui se sont accentuées depuis la précédente version du PSO (exemples : attaques cyber, survols de drones, radicalisation…).

1.4.6. Schéma de synthèse



2. COMMENT ELABORER UN PSO ? PRINCIPES DIRECTEURS PAR CHAPITRE

Cette section présente des lignes directrices des étapes à réaliser en mettant l'accent sur la cohérence entre la politique de protection des points d'importance vitale, le dispositif VIGIPIRATE et les mesures de renforcement de la sécurité des systèmes d'information.

Elle suit les chapitres du plan-type du PSO assurant à l'opérateur la prise en compte des principaux enjeux de sécurité.

2.1. Préambule : rapport de présentation (non classifié)

Le préambule doit rappeler les principales dispositions du PSO : la méthodologie d'élaboration, les différents acteurs, les objectifs du plan, l'articulation avec les plans et réglementations en vigueur.

Le contenu du rapport de présentation doit être pensé pour pouvoir s'adresser à une population restreinte, interne à l'entreprise, mais pas nécessairement habilitée au niveau « confidentiel défense » (exemple : membres du conseil d'administration, instances représentatives du personnel, etc.).

2.2. Introduction. Champ d'application du plan de sécurité d'opérateur d'importance vitale

L'opérateur présente succinctement son activité, son organisation interne, les missions qu'il considère d'importance vitale au regard de la DNS.

Il peut préciser également les limites éventuelles de la démarche d'élaboration du plan de sécurité d'opérateur (interdépendances, implantations en dehors du territoire national).

2.3. Analyse de risque

Objectif

L'analyse de risque doit permettre à l'opérateur de définir les priorités de sa politique de sécurité en s'appropriant la DNS (notamment en reprenant les scénarios de menace qui y sont présentés). Il complète ces scénarios par ceux qu'il estime pertinents au regard de son activité.

L'analyse de risque doit également tenir compte de l'appréciation des impacts, de l'analyse des vulnérabilités propres à l'opérateur, de la probabilité d'occurrence (dans le cas d'aléas naturels) et de l'attractivité (dans le cas de malveillances).

L'appréciation de ces éléments (menace, impact, vulnérabilité, occurrence, attractivité) permet d'évaluer le risque pour chacun des points qu'il souhaite qualifier d'importance vitale. Ainsi, la hiérarchisation des scénarios peut varier en fonction des spécificités locales des PIV retenus.

Exemple : le risque cyclonique sera élevé dans une zone intertropicale comme la Polynésie et nul en métropole.

Méthode

Aucune méthode d'analyse de risque n'est imposée dans la rédaction du PSO. Le ministère coordonnateur en charge de l'instruction du dossier, ainsi que la commission interministérielle ou zonale de défense et de sécurité, jugeront de la pertinence et des résultats de la méthode.

Comme référence, l'opérateur peut utiliser l'instruction méthodologique d'analyse de risque fixée par arrêté du Premier ministre du 2 juillet 2018.

2.4. Mesures destinées à réduire les risques – mise en œuvre du plan VIGIPIRATE

Objectifs

Les mesures décrites dans le PSO doivent permettre à chaque délégué pour la défense et la sécurité d'un point d'importance vitale de décliner localement, en fonction de son contexte spécifique, le dispositif de sécurité global et les mesures opérationnelles. L'ensemble étant regroupé dans le plan particulier de protection (PPP).

Les délais de réalisation des mesures de protection permanentes et des mesures temporaires et graduées sont indiqués.

Les mesures de sécurité du plan de sécurité d'opérateur s'appuient sur les dispositifs existants.

Mise en œuvre du plan VIGIPIRATE

Les mesures de sécurité prises par l'opérateur doivent être cohérentes avec les objectifs et les exigences de sécurité de la DNS. En effet, la DNS précise les mesures du plan VIGIPIRATE applicables au secteur ou sous-secteur. Le PSO décline ces mesures qui doivent être classées en :

- **mesures socles**, correspondant aux investissements indispensables et aux actions permanentes de vigilance ;
- **mesures additionnelles** activables en fonction des consignes transmises à l'opérateur dans le cadre de l'activation de mesures spécifiques du plan VIGIPIRATE. Ces mesures peuvent être techniques, organisationnelles ou comportementales.

Les mesures du plan VIGIPIRATE, volontairement larges, doivent être adaptées et déclinées au contexte de l'entreprise. C'est l'objet du PSO et des PPP.

Exemple : la mesure additionnelle BAT 31-01 « renforcer la surveillance interne et limiter les flux (dont interdiction de zone) » peut se décliner concrètement en contrôlant et limitant l'accès aux zones névralgiques des PIV (relevé des identités de chaque personne qui accède à la zone, interdire l'accès en dehors des heures d'ouverture du PIV, s'assurer que les personnes soient accompagnées…).

2.5. Dispositif d'alerte et de gestion de crise

Cette partie traite des procédures spécifiques à la gestion des situations d'urgence :

- prévention de crise (veille, gestion des signaux faibles) ;
- gestion de l'alerte (schéma d'alerte, gestion des astreintes, remontée d'incidents) ;

- organisation de la cellule de crise (fonctionnement de la cellule de crise, liaison avec les autres cellules de crise et les centres opérationnels des pouvoirs publics) ;
- continuité et reprise d'activité (description succincte de la stratégie de continuité d'activité, gestion du mode dégradé, liste des scénarios retenus dans le PCA) ;
- formations, entrainements, exercices (typologie, périodicité, retour d'expérience).

NB. Certaines procédures décrites dans cette partie peuvent être redondantes avec la description de mesures VIGIPIRATE du chapitre précédent (exemple : les objectifs de sécurité du domaine « alerte-intervention »). Aussi faut-il décrire les mesures qu'une seule fois et faire des références si besoin.

Exemple : les procédures d'alerte et de gestion de crise existent souvent dans les entreprises de manière formelle ou informelle. Il n'y a pas de format à privilégier, l'essentiel étant que ces procédures soit applicables et facilement assimilables par l'organisation. L'opérateur peut s'en assurer à travers des exercices réguliers.

2.6. Dispositions de sauvegarde des personnes et des biens - plans de secours

Les plans de secours déjà réalisés comme le plan de sauvegarde en cas de crue, le plan d'organisation interne (POI) peuvent être intégrés ou rappelés dans cette partie par l'opérateur. L'articulation avec le dispositif ORSEC est également à prévoir.

Exemple : une société concessionnaire d'autoroutes va rappeler les plans d'intervention et de sécurité (PIS) qui la concerne. Elle peut en expliquer les grands principes, les obligations auquel elle est assujettie (surveillance des installations, interventions…) et qui auraient un intérêt dans le cadre du PSO.

2.7. Mesures génériques de protection par type de point d'importance vitale

L'opérateur détaille, par type de PIV, les mesures de protection génériques (passives et actives, techniques et organisationnelles : types de clôtures, d'éclairage, de surveillance, de contrôles, de protection de son système d'information, etc.) qui seront effectivement retenues et déclinées de façon plus précise dans chaque plan particulier de protection de point d'importance vitale.

Obligations en matière de SSI

Les mesures de sécurité du plan de sécurité d'opérateur répondent directement de la spécificité des fonctions concernées au regard de leurs vulnérabilités, des menaces particulières auxquelles elles sont exposées et des conséquences pouvant en résulter. Les mesures génériques de SSI doivent être cohérentes avec les obligations liées à l'application des articles L. 1332-6-1 à L. 1332-6-6 du code de la défense.

Les délais de réalisation des mesures de protection sont indiqués.

Bien que n'étant pas soumis à l'avis de la CIDS ou CZDS, la liste des systèmes d'information d'importance vitale peut figurer dans le PSO.

Exemple : selon la stratégie de sécurité de l'opérateur, les mesures génériques peuvent être très précises (« tous les PIV devront être équipés d'une clôture périmétrique de 3 mètres minimum et ils devront disposer d'un système de vidéosurveillance ») ou ne se limiter qu'à des mesures organisationnelles (« tous les PIV devront rendre le port du badge obligatoire »). Le degré de précision est défini par l'opérateur.

2.8. Relations avec les services de l'Etat - délégué pour la défense et la sécurité

L'opérateur décrit ses relations avec les pouvoirs publics, notamment dans le cadre du plan VIGIPIRATE (à l'échelle nationale, zonale ou locale).

Il porte une attention particulière aux mesures dont l'application relève d'actions conjointes de l'opérateur et des pouvoirs publics. En effet, l'opérateur reçoit directement de son ministère de tutelle des instructions classifiées qui doivent être transmises et déclinées pour ses PIV. Les préfets s'assurent ensuite, auprès des opérateurs de leur département, de la cohérence des mesures adoptées. La mise en œuvre concrète de ce circuit d'information doit être précisée.

Les coordonnées du DDS et éventuellement des correspondants locaux, habilités au niveau confidentiel défense, sont indiquées.

Exemple : pour un établissement de santé qui interagit à différents niveaux avec les services de l'Etat, un schéma peut illustrer le mécanisme de déclenchement des mesures du plan VIGIPIRATE. Il précisera ainsi les relations avec le centre de crise du ministère de la santé (CORRUS), avec le centre opérationnel zonal (COZ) et le centre opérationnel départemental (COD).

Le rôle du DDS

Le délégué pour la défense et la sécurité joue un rôle prépondérant au sein du dispositif SAIV. Interlocuteur privilégié des autorités publiques, il coordonne la rédaction du PSO et des PPP, il reçoit, adapte et diffuse les postures VIGIPIRATE. Il participe ainsi la planification de défense et de sécurité nationale.

2.9. Dépendances vis-à-vis d'autres secteurs d'activités d'importance vitale

Les dépendances amont envers d'autres systèmes (énergie, télécommunications…) doivent être prises en compte dans l'analyse globale de sécurité.

De la même manière, les dépendances aval (conséquences de l'arrêt de l'opérateur pour d'autres secteurs d'activités d'importance vitale) doivent être décrites.

Enfin, les aspects internationaux doivent également être considérés (dépendance envers d'autres pays).

La description des interdépendances doit permettre à l'opérateur de s'assurer que ces vulnérabilités sont correctement identifiées et, au besoin, redondées. De la même façon, cette information permet aux pouvoirs publics d'identifier d'éventuels opérateurs qui répondraient aux critères d'un OIV.

Exemple : un laboratoire pharmaceutique précisera, dans la mesure du possible, son niveau de dépendance en matières premières importées de l'étranger.

2.10. Annexe : liste des points d'importance vitale

Cette liste énumère les points d'importance vitale retenus par l'opérateur. Elle doit préciser succinctement la nature de l'activité de chacun des points. Un point d'importance vitale peut être constitué de composants essentiels appelés alors points névralgiques[1].

Le choix d'un PIV est fait à partir :

- des critères qui peuvent être définis dans la ou les DNS qui concernent l'opérateur ;
- de l'analyse de risque réalisée par l'opérateur ;
- des sites difficilement remplaçables ou substituables qui participent aux activités essentielles de l'opérateur ;
- des sites dont la destruction ou l'avarie peut présenter un danger grave pour la population.

Le fait qu'un site dispose de moyens de protection et prévention efficaces ne lui retire pas son caractère indispensable à l'échelle de la Nation. Il ne peut donc s'agir d'un critère pour écarter un site de la liste des PIV.

[1] Point névralgique : point à la fois vital et vulnérable, qui peut n'être qu'un composant d'un point d'importance vitale.

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Arrêté du 2 juillet 2018 portant approbation du plan type des plans particuliers de protection des points d'importance vitale

NOR : *PRMD1818233A*

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, R. 1332-12 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 21 décembre 2017,

Arrête :

Art. 1er. – Le plan type des plans particuliers de protection, annexé au présent arrêté, est approuvé.

Art. 2. – L'arrêté du 27 septembre 2007 fixant le plan type des plans particuliers de protection des points 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 : Plan-type – Plan particulier de protection

SECURITE DES

ACTIVITES D'IMPORTANCE VITALE



GUIDE D'AIDE

A L'ELABORATION ET L'EXAMEN

D'UN PLAN PARTICULIER DE PROTECTION


VIGIPIRATE

2 juillet 2018

SGDSN

Ce guide a pour objet de constituer une aide à l'élaboration et à l'examen du *plan particulier de protection* (PPP). Il donne des indications et recommandations qui n'ont pas une valeur contraignante.

Le PPP doit se conformer au plan-type fixé par arrêté du Premier ministre. Si, lors de la rédaction du PPP, l'opérateur constate qu'un chapitre n'est pas applicable pour son *point d'importance vitale* (PIV), il peut indiquer la mention « néant » ou « non applicable ».

Pour faciliter la lecture, le PPP doit être paginé et le sommaire doit figurer au début du document.

Rappel de la procédure d'approbation du PPP

La décision d'approbation du préfet de département se fonde sur une évaluation qualitative du PPP soumis par l'opérateur. Cette évaluation prend en compte :

- *l'avis de la CZDS s'il a été sollicité ;*
- *la conformité du plan particulier de protection par rapport au plan-type ;*
- *la cohérence du dispositif proposé au regard de la politique générale de protection définie par le PSO ;*
- *la prise en compte des prescriptions de la DNS qui s'appliquent au PIV, notamment les scénarios de menace et les objectifs de sécurité ;*
- *l'adéquation du dispositif proposé aux infrastructures et aux modalités d'exploitation du PIV.*

Instruction générale interministérielle relative à la sécurité des activités d'importance vitale n° 6600/SGDSN/PSE/PSN du 7 janvier 2014

Suivi des modifications

Date	Version n°	Auteur / service	Commentaires

Préambule

Le préambule vise à rappeler les enjeux du dispositif SAIV et l'objectif attendu du PPP. S'il ne contient aucune information classifiée, le préambule peut être extrait du PPP et déclassifié de manière à présenter la démarche du PPP auprès de personnels non-habilités (membres du comité exécutif, instances représentatives du personnel, *etc.*).

Le préambule peut également indiquer le circuit de validation du document, sa version et la dernière mise à jour.

Les documents ressources dans la rédaction ou l'examen du PPP

Plusieurs documents peuvent faciliter la rédaction, la compréhension et l'instruction du PPP :

- l'instruction générale interministérielle relative à la sécurité des activités d'importance vitale n° 6600/SGDSN/PSE/PSN du 7 janvier 2014 ;
- le plan de sécurité d'opérateur (pour la compréhension de l'activité de l'opérateur, les scénarios retenus, les objectifs de sécurité, le choix du PIV, *etc.*) ;
- la directive nationale de sécurité du secteur (pour les scénarios notamment) ;
- le plan VIGIPIRATE (pour les mesures applicables) ;
- les éventuels comptes rendus de visites de la commission zonale de défense et de sécurité.

1. Présentation du point d'importance vitale

1.1. Désignation du PIV

Critères de désignation du PIV

Les critères peuvent figurer dans le PSO de l'opérateur.

- Nom de la société et adresse complète.
- N° de triplet attribué par le SGDSN et figurant dans l'arrêté de désignation du PIV.
- Nature des activités.
- Secteur(s) et *directive(s) nationale(s) de sécurité* (DNS) de rattachement.
- Lien avec l'opérateur d'importance vitale (filiale, *etc.*).
- Critères retenus pour la désignation du site comme PIV.
- Classement éventuel du site au titre d'autres réglementations et plans applicables (installation classée pour la protection de l'environnement, Seveso, installations portuaires relevant du code ISPS, site abritant des matières nucléaires, IGH, ERP, *etc.*).
- Surface totale du PIV.

1.2. Localisation du PIV

- Plan d'accès lisible et pratique pour des interventions externes (routes d'accès, différentes entrées, *etc.*).
- Plan de masse du site.
- Site situé en zone police ou gendarmerie.
- Description de l'environnement (urbain ou rural, zone résidentielle ou industrielle, proximité d'axes routiers et/ou ferroviaires).
- Zonage spécifique au titre d'autres réglementations (existence d'une zone protégée, d'une zone à régime restrictif, d'une zone de défense hautement sensible, d'une zone nucléaire à accès réglementé, *etc.*).

1.3. Organisation générale du PIV

- Site ouvert ou fermé au public.
- Effectifs employés sur le site (salariés, prestataires, *etc.*).
- Présence sur le site 24/7.
- Organisation hiérarchique (avec un organigramme).
- Rôle et responsabilités du délégué à la défense et à la sécurité du site.

2. Analyse de risque

2.1. Cartographie des risques

> ***Analyse de risque du PPP et du PSO***
> Si l'analyse de risque spécifique au PIV est déjà menée dans le PSO de l'opérateur, ce dernier peut la copier à cet emplacement ou renvoyer au document.

L'analyse de risque doit permettre à l'opérateur d'identifier les scénarios les plus pertinents pour son site au regard de sa situation, son environnement, ses retours d'expérience, ses vulnérabilités. Il définit ainsi les priorités de sa politique de sécurité en s'appropriant la DNS et son PSO (notamment en reprenant les scénarios de menace qui y sont présentés). Il complète ces scénarios par ceux qu'il estime pertinents au regard de son activité, de sa situation.

NB. L'analyse de risque doit notamment tenir compte des nouvelles orientations de la DNS en intégrant les risques de cybersécurité et les risques naturels, technologiques, pandémiques, *etc*.

2.2. Vulnérabilités spécifiques du site

Vulnérabilités propres à l'activité et l'environnement du site (exemples : site ouvert au public, proximité de grands axes de circulations, de sites industriels, zones de fragilités, bâtiments mitoyens).

2.3. Interdépendances

Mise en évidence des interdépendances (exemple : nécessité de disposer d'une alimentation électrique permanente pour assurer le fonctionnement des systèmes de sécurité, recours à des prestataires essentiels, à des matières premières non substituables).

2.4. Points névralgiques

Identification des points névralgiques du PIV par leur importance, leur sensibilité. L'arrêt ou la destruction du point névralgique peut conduire à un arrêt des activités du site et/ou à un problème de sécurité. Il s'agit, par définition, d'un élément difficilement substituable.

Donner la justification du choix des points névralgiques.

Cartographie des points névralgiques

Le fait de matérialiser les points névralgiques sur une carte permet de se rendre compte du périmètre concerné et également du respect du principe de défense en profondeur.

Ces points névralgiques peuvent également correspondre aux parties que l'opérateur souhaite soumettre à une enquête administrative préalable (*cf.* article R. 1332-22-1 du code de la défense).

3. Dispositifs de sûreté en place ou prévus

3.1. Moyens humains

3.1.1. Service de sécurité/sûreté

- Nom de la société.
- Missions des agents (exemples : contrôle et surveillance des entrées/sorties, de la circulation interne, de la sécurité technique, *etc.*).
- Effectifs employés.
- Présence sur le site.
- Rythme des rondes.
- Qualité des agents (internes ou prestataires).
- Qualifications et formations particulières (emploi de chiens de défense, de chiens pour la détection d'explosifs, port d'armes, *etc.*).

3.1.2. PC de sécurité et sûreté (PCS)

- Description du PC : localisation (sur le site ou distant), dispositifs de secours, site de secours.
- Nombre d'agents présents (jour/nuit/week-end).
- Outils de communication et moyens de supervision à disposition.
- Autres moyens matériels.
- Rôle du PCS en en cas de crise (armement spécifique).

3.2. Dispositifs de protection physique

3.2.1. Protection des points névralgiques et respect du principe de « défense en profondeur »

Stratégie de protection des points névralgiques dans le respect du principe de défense en profondeur et de l'équation de protection.

Orientations principales de la stratégie de protection (détection, dissuasion, protection, dissimulation, *etc.*).

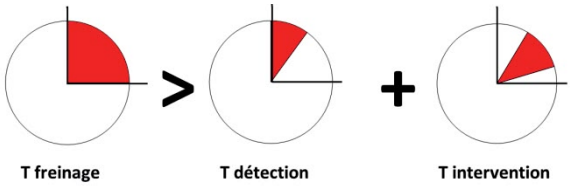
Le principe de défense en profondeur, avec la sectorisation générale du PIV en nombre de « couches » successives, doit être décrit de façon à expliciter l'articulation des dispositifs de protection, de la périphérie aux points névralgiques. Si ça s'avère pertinent, les différents dispositifs de protection peuvent figurer sur un ou plusieurs plans et être joints au PPP.

La défense en profondeur

La défense en profondeur consiste en la superposition de plusieurs lignes de défense, composées d'un ensemble de mesures de sécurité, chaque ligne devant contribuer à affaiblir l'attaque et à permettre aux suivantes de se renforcer en vue soit d'empêcher la destruction ou la prise de contrôle des composants névralgiques du PIV, soit d'en limiter les effets.

L'équation de protection

Le temps de résistance mécanique des dispositifs installés doit être supérieur au temps de détection de l'attaque (et de transmission de l'information) ajouté au temps d'intervention.



3.2.2. Clôtures, murs, portes, portails d'accès, obstacles retardateurs

- Clôture périmétrique (hauteur, résistance, *etc.*).
- Dispositif masquant la vue depuis l'extérieur (éléments naturels, *etc.*).
- Sécurisation des ouvrants (fenêtres, portes, *etc.*).
- Obstacles retardateurs (concertina, *etc.*).
- Sas d'entrée.
- Parking.
- Panneautage signalant une zone protégée ou un site sensible.
- Fonctions principales des dispositifs (freiner, dissuader, dissimuler, tromper, *etc.*).

3.2.3. Vidéoprotection

- Politique de vidéoprotection (aux entrées, à l'intérieur des bâtiments, pour les points névralgiques identifiés, donnant sur la voie publique, *etc.*)
- Spécificités techniques (enregistrement, qualité, détecteur de mouvement, caméras discrètes, infrarouge, *etc.*).
- Fonctions principales du dispositif de vidéoprotection (détecter, surveiller, lever de doute, dissuader, *etc.*).

Vidéoprotection de la voie publique

La vidéoprotection de la voie publique aux abords immédiats d'un site privé, peut être mise en œuvre par les autorités publiques aux fins de prévention d'actes de terrorisme. Cette mise en œuvre répond à des règles strictes (*cf.* code L. 223-1 du code de la sécurité intérieure).

3.2.4. Contrôle d'accès

- Badges (caractéristiques de la politique de gestion des badges, accès restrictifs par lieux/plages horaires, passage unique, technologie utilisée pour les badges, *etc.*).
- Biométrie (existence de contrôle biométrique, localisation, *etc.*).

- Clés (politique de gestion des clés, clés non copiables, *etc*.).
- Contrôle des véhicules.
- Fonctions principales du dispositif de contrôle d'accès (détecter, recenser, freiner, sectoriser, *etc.*).

3.2.5. Eclairage

- Efficacité des installations choisies : surface éclairée, déclenchement automatique.
- Fonctions principales du dispositif d'éclairage (dissuader, détecter, intervenir, *etc.*).

3.2.6. Protection des approches terrestres

- Ralentisseur, chicanes, barrières anti-véhicules bélier, *etc.*

3.2.7. Détection d'intrusion

- Contacteurs de porte, détecteurs bris de vitre, détecteurs volumétriques, détecteurs thermiques, gestion des alarmes, *etc.*

3.2.8. Protection des systèmes de sécurité

- Exemples de protections techniques : gaines spéciales, autonomie des systèmes, vérification de l'inviolabilité des badges, *etc.*

3.2.9. Systèmes de secours

- Moyens de production autonomes prévus permettant la continuité des systèmes de sécurité (description des moyens, autonomie).

3.3. Audits et contrôle

Vérification des dispositifs de sécurité, du respect des règles et procédures de sécurité (catégorie de l'audit/contrôle, périodicité, prise en compte des conclusions).
Prise en compte de tout élément utile tiré d'autres évaluations de sûreté (exemple : réglementation ISPS, évaluation de sûreté bâtimentaire réalisée par la DGSI, audit interne de l'opérateur).

3.4. Gestion des colis et du courrier

Procédure spécifique en matière de sûreté pour la gestion des colis et courrier entrants.

3.5. Gestion et stockage de l'information classifiée

- Conservation des documents classifiés selon les dispositions de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale du 30 novembre 2011 (coffre, local protégé, *etc*.).
- Mise en place d'une zone protégée.
- Définition des responsabilités.

> ***La zone protégée***
> L'objet de la zone protégée est d'assurer, aux lieux intéressant la défense nationale, une protection juridique contre les intrusions, complémentaire d'une protection physique (*cf. article 413-7 du code pénal*).

4. Sécurité des systèmes d'information

- Existence d'une *politique de sécurité des systèmes d'information* (PSSI). PSSI locale ou « groupe ».
- Autres documents d'application.
- Liste des principaux systèmes d'information du site, décrits de la façon synthétique suivante :
    - SI métier, SI bureautique, SI de sécurité/sûreté, SI industriel.
    - Indication de la criticité du système pour l'entreprise / pour les impacts sur les populations / *etc*.
    - Où est hébergé le système (à distance, localement) ?
    - Responsabilités :
        - Qui gère/administre le système ?
        - Le cas échéant, qui est en charge de la cybersécurité du système (éventuellement, distinguer l'aspect « gouvernance » et l'aspect « opérationnel ») ?
        - Y a-t-il un ou plusieurs prestataires « clés » dont la mise en œuvre du SI dépend fortement ?
- Description des dispositifs de sauvegarde des données existants.
- Dispositifs de secours permettant la continuité des systèmes métiers (description des moyens, autonomie).

> ***L'analyse de risque SSI***
> L'analyse de risque menée dans le cadre d'un PPP n'a pas vocation à aborder le sujet des systèmes d'information autrement que de façon synthétique, sans rentrer dans le détail technique. La DNS inclut des scénarios cyber qui sont ensuite repris dans le PSO ou le PPP.

5. Lien avec le plan VIGIPIRATE

Les OIV font apparaître dans leurs PSO et PPP les mesures qu'ils sont susceptibles de mettre en œuvre pour atteindre les objectifs de sécurité de leur domaine d'action, qui figurent dans la ou les directives nationales de sécurité qui leur sont applicables.

Le principe est que l'activation nationale de n'importe laquelle des mesures VIGIPIRATE puisse donner lieu immédiatement à une action concrète au sein du PIV, décrite dans le PPP. D'une manière générale, la déclinaison peut rester succincte mais il faut que l'opérateur ait anticipé sa réaction.
La déclinaison des mesures permet de s'assurer qu'il les a bien intégrées en amont et ainsi qu'il a prévu une application graduée de ces mesures.

NB. Toutes les mesures ne nécessitent pas une déclinaison concrète par l'opérateur. En effet, certaines mesures peuvent être suffisamment explicites pour ne pas à avoir à être déclinées (exemple : « ALR 20-01 Elaborer et mettre à jour un plan de continuité d'activité »).
Ou bien, une déclinaison serait redondante avec les mesures décrites par ailleurs dans le PPP (exemple : « BAT 10-02 Surveiller les abords des installations et bâtiments »).

Exemples de déclinaison de mesures du plan VIGIPIRATE :

Numéro de mesure	Mesures	Type de mesure	Prise en compte par l'opérateur : Oui/Non/Non applicable	Précisions sur les dispositions prises par l'opérateur
BAT 31-01	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	additionnelle	*Oui*	*En cas d'activation de cette mesure, un seul des deux accès du PIV est maintenu et le contrôle visuel des bagages est systématisé. Un agent privé de sécurité vient renforcer l'accueil et participe aux contrôles.*
ALR 11-04	Rappeler les conduites à tenir en réponse à la menace d'actions terroristes (fusillade, colis abandonné, alerte à la bombe)	additionnelle	*Oui*	*En cas d'activation de cette mesure et en complément des mesures de sensibilisation décrites en 7.1, une session de sensibilisation du personnel peut être organisée par notre personnel de sûreté et un message de sensibilisation est diffusé sur nos panneaux d'affichage.*

6. Procédure d'alerte et de gestion de crise

6.1. Astreinte

- Rôles et fonctions du personnel d'astreinte.
- Fonctionnement (H24 ? délai d'intervention sur site ?)

NB. Les numéros peuvent figurer en annexe.

Missions de l'astreinte

Selon les organisations, une astreinte peut avoir été constituée pour répondre à des événements spécifiques (ex. : maintenance, incident sanitaire, etc.)
Néanmoins, l'opérateur doit s'interroger si ce dispositif est également efficace face à tout type de scénario susceptible d'interrompre ses activités (ex. : acte de malveillance, arrêt des activités, panne des SI, etc.).

6.2. Schéma d'alerte

Chaîne de remontée de l'alerte vers :

- les autorités de décision interne ;
- les autorités administratives (services préfectoraux, forces de sécurité intérieure, service du haut fonctionnaire de défense et de sécurité du ministère coordonnateur) ;
- les populations, les abonnés prioritaires si nécessaire.

Description de la procédure de « levée de doute ».

6.3. Outils d'alerte et de gestion de crise (hors salle de crise)

- Moyens de communications (téléphones filaires, mobiles, radios, haut-parleurs, interphones, internet ou intranet).

- Fiche de réaction/d'intervention spécifique à un risque encouru (pour le service de sécurité/sûreté, pour les membres de la cellule de crise).
- Consignes en cas d'alerte (consignes générales et dispositifs spécifiques selon les catégories de personnels ou d'emplois).
- Malette de crise à disposition pour le personnel d'astreinte, en salle de crise.
- Véhicule de fonction.

6.4. Organisation de crise

- Rôle et fonctionnement de la cellule de crise du PIV.
- Composition des membres de la cellule de crise (par fonction).

6.5. Salle de crise

- Localisation.
- Outils à disposition (manuel de gestion de crise, plans, *etc.*).
- Moyens de communication (dont moyens sécurisés pour les services de l'Etat).
- Existence d'un site de repli.
- Modification des consignes en cas d'alerte.

6.6. Exercices et entrainements

- Réalisation d'exercices (sur table, mise en situation). Périodicité.
- Agents concernés (cellule de crise, personnel de sûreté, ensemble du personnel, *etc.*).
- Scénarios (sécurité, sûreté, continuité d'activité, *etc.*).

6.7. Continuité d'activité

- PCA groupe, PCA de site.
- PCA abordant :
  - les scénarios d'indisponibilité du personnel, indisponibilité du site, indisponibilité du réseau informatique, indisponibilité des prestataires essentiels.
  - l'identification des missions prioritaires ;
  - les solutions de secours.
- Test du PCA (périmètre et périodicité des tests).

Continuité des activités

La continuité d'activité est un des objectifs de la révision des DNS (approche « tous risques ») et il convient donc d'y apporter une attention toute particulière. Par exemple, un PCA ne doit pas couvrir uniquement les questions de pandémie mais aussi aborder les problématiques d'indisponibilité du réseau SI, indisponibilité du bâtiment, indisponibilité des prestataires.

NB. Cette partie peut être facultative pour les opérateurs désignés au titre de l'article L. 1332-2 du code de la défense (opérateurs qui « peuvent présenter un danger grave pour la population »).

6.8. Retour d'expérience

Politique de retour d'expérience après une crise réelle, un exercice, un incident.

7. Gestion du personnel

7.1. Sensibilisation et formation

Sensibilisation

Une sensibilisation sur les questions de sûreté peut être facilement mise en œuvre à moindre coût (exemple : diffusion de l'affiche « comment réagir face à une attaque terroriste », guides de bonnes pratiques, etc.). Ces documents sont disponibles sur le site www.risques.gouv.fr

7.1.1. Sensibilisation

Sensibilisation des agents, de l'ensemble du personnel, du public, des visiteurs occasionnels.

7.1.2. Formation

- Formation des agents à la sûreté (catégorie ciblée).
- Formation à la gestion de crise (catégorie ciblée).
- Maintien des acquis (périodicité).
- Existence d'un plan de formation.

7.2. Postes sensibles et criblages

7.2.1. Postes sensibles

- Identification de postes sensibles (personnes « clés » du PIV).
- Politique pour l'attribution de postes « sensibles ».

7.2.2. Criblage

Organisation du criblage.

Criblage

Bien que le criblage ne soit pas une obligation, il représente une sécurité supplémentaire pour les PIV. Notamment pour des personnels susceptibles d'accéder seuls à des points névralgiques. (Ex. personnel de maintenance, société de gardiennage).

7.3. Services prestataires, sous-traitants

Gestion des personnels prestataires et sous-traitants (accès restreints, accompagnés sur le site, dans les points névralgiques uniquement). Information sur les règles de sécurité/sûreté.

7.4. Visiteurs

Gestion des visiteurs (accompagnés, port du badge apparent).

Annexes

A. Annuaires

Fonction	Nom	Prénom	Courriel	Numéro de téléphone fixe	Numéro de téléphone mobile	Autre fonction exercée
Poste de sécurité (joignable 24/7)						
DDS du PIV						
DDS du PIV suppléant						
DDS de l'OIV						
Directeur ou responsable du site						

Personnes à contacter

- Des adresses électroniques et des numéros de téléphone génériques limitent le risque d'avoir des annuaires obsolètes.
- En cas de changement important, l'annexe seule peut être envoyée à la préfecture pour mise à jour du PPP.

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Arrêté du 2 juillet 2018 portant approbation du plan type des plans de protection externe des points d'importance vitale

NOR : *PRMD1818235A*

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, R. 1332-12 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 21 décembre 2017,

Arrête :

Art. 1er. – Le plan type des plans de protection externe, annexé au présent arrêté, est approuvé.

Art. 2. – L'arrêté du 27 septembre 2007 fixant le plan type des plans de protection externe des points 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

Annexe : Plan-type – Plan de protection externe

1. Caractéristiques générales du point d'importance vitale
   - **1.1. Désignation ou raison sociale du point d'importance vitale et numéro de triplet**
   - **1.2. Classement du (des) site(s) selon les réglementations concernant la sécurité**
   - **1.3. Zone de compétence**
   - **1.4. Secteur(s) d'activités d'importance vitale concerné(s)**
   - **1.5. Effectifs employés dans le point d'importance vitale**
   - **1.6. Liste des points névralgiques identifiés dans le plan particulier de protection (PPP)**
2. Localisation du point d'importance vitale
   - **2.1. Adresse complète**
   - **2.2. Environnement/alentours**
3. Caractéristiques internes du point d'importance vitale
   - **3.1. Surface totale du point d'importance vitale**
   - **3.2. Eléments particuliers à signaler à l'attention des forces de sécurité**
     - 3.2.1. Dispositifs de protection périmétrique du site
     - 3.2.2. Vulnérabilités
     - 3.2.3. Eléments objectifs de nature à compliquer l'intervention des forces de sécurité
     - 3.2.4. Matériels pouvant être détournés par l'agresseur
   - **3.3. Moyens humains de protection**
4. Intervention
   - **4.1. Moyens d'intervention**
   - **4.2. Modalités de prise de contact avec l'opérateur**
     - 4.2.1. Lieux de contact
     - 4.2.2. Procédure de contact
5. Exercices et retours d'expérience
   - **5.1. Exercices**
   - **5.2. Retours d'expérience**

Annexes
- **A. Cartes et plans**
- **B. Annuaire**

SECURITE DES

ACTIVITES D'IMPORTANCE VITALE



GUIDE D'AIDE

A L'ELABORATION

D'UN PLAN DE PROTECTION EXTERNE


2 juillet 2018

SGDSN

Le plan de protection externe définit les modalités d'intervention des forces de sécurité en cas d'agression sur le PIV. Il décrit et planifie les moyens humains et matériels à mettre en œuvre. A ce titre :

- sa rédaction doit associer les principaux acteurs concernés (groupement de gendarmerie départemental ou direction départementale de la sécurité publique) ;
- il doit tenir compte des éléments du *plan particulier de protection* (PPP) sans pour autant être redondant ;
- il doit être testé et compléter en tant que de besoin ;
- il doit, dans la mesure du possible, faire l'objet d'une déclinaison par fiche d'intervention, fiches réflexes ou dossiers d'objectifs.

Suivi des modifications

Date	Version n°	Auteur / service	Commentaires

1. Caractéristiques générales du point d'importance vitale

1.1. Désignation ou raison sociale du point d'importance vitale et numéro de triplet

Nom de la société et type d'entreprise.

1.2. Classement du site selon les réglementations concernant la sécurité

Mentionnez de manière succincte la ou les réglementation(s) qui justifient des mesures de sécurité ou sûreté spécifiques (ICPE dont SEVESO, ERP, IGH, PPST, etc.).

1.3. Zone de compétence

Police et/ou gendarmerie.

1.4. Secteur(s) d'activités d'importance vitale concerné(s)

Précisez si besoin le sous-secteur ainsi que la ou les directives nationales de sécurité (DNS) applicables au PIV.

1.5. Effectifs employés dans le point d'importance vitale

Précisez l'effectif total et éventuellement la répartition civil/militaire, salariés de l'OIV/prestataires, sous-traitants.

1.6. Liste des points névralgiques identifiés dans le *plan particulier de protection* (PPP)

Rappelez de façon précise et exhaustive les points névralgiques identifiés par l'opérateur. Ces points peuvent figurer également sur une carte en annexe.

2. Localisation du point d'importance vitale

2.1. Adresse complète

Dont le code postal.

2.2. Environnement/alentour

Précisez notamment si le site est situé en ville ou campagne, en zone résidentielle ou industrielle, proche d'axes routiers et/ou ferroviaires importants.
Une représentation cartographique de l'environnement peut figurer en annexe.

3. Caractéristiques internes du point d'importance vitale

3.1. Surface totale du point d'importance vitale

3.2. Eléments particuliers à signaler à l'attention des forces de sécurité

3.2.1. Dispositifs de protection périmétrique du site
Clôtures, présence de barreaux, dispositif d'alarme, poste(s) de garde, portes blindées, éclairage, caméras, etc.

3.2.2. Vulnérabilités
Enumérez notamment les points défaillants ou franchissables facilitant l'accès aux points névralgiques (hauteur des murs insuffisantes, présence d'un bâtiment contigüe, etc.).

3.2.3. Eléments objectifs de nature à compliquer l'intervention des forces de sécurité
Mentionnez les différents risques tenant à la nature de l'activité (NRBC, risque électrique, zone explosive ATEX, dégagement de monoxyde de carbone) et/ou à la configuration des lieux (immeubles de grande hauteur, établissement recevant du public, zones à accès contrôlé par badge, biométrie, et/ou accompagnement obligatoire.).

3.2.4. Matériels pouvant être détournés par l'agresseur
Exemple : armement, produits NRBC-E, etc.

3.3. Moyens humains de protection

Distinguez les agents privés de sécurité de l'opérateur, les agents prestataires et les agents de l'Etat.
Préciser éventuellement l'armement des agents.
Précisez le type de surveillance et d'intervention (sur site et/ou à distance, délais d'intervention) ainsi que l'amplitude horaire (jour/nuit/week-end).

4. Intervention

4.1. Moyens d'intervention

Décrivez les unités primo-intervenantes concernées, leurs effectifs (patrouilles, équipages) et leurs moyens de transmissions (y compris sécurisés) ainsi que les unités de renforts des services spécialisés (RAID, GIGN, DCIT, etc.). Précisez les délais d'intervention (même seulement à titre indicatif).

4.2. Modalités de prise de contact avec l'opérateur

4.2.1.Lieux de contact
Précisez le mode habituel et le mode dégradé. Indiquez les lieux sur les plans figurant en annexe.

4.2.2.Procédure de contact
Précisez le point de contact (les coordonnées pouvant figurer dans l'annuaire de l'annexe 2).

5. Exercices et retour d'expérience

5.1. Exercices

Précisez la politique d'exercice (périodicité, typologie, acteurs, scenarios). Les exercices peuvent se décliner sous plusieurs formes :

- *simple test de la chaîne d'alerte (inopiné ou non) ;*
- *visite exploratoire (avec l'opérateur : identification des cheminements, de l'agencement des bâtiments, des obstacles éventuels, etc.).*
- *exercice sur table, exercice sur carte ;*
- *exercice de mise en situation. Sur une procédure donnée (exemple : plan de bouclage) ou un exercice*

avec mobilisation de tous les acteurs.

5.2. Retour d'expériences

Politique de retour d'expérience après une crise réelle, un exercice, un incident.

Annexes

A. Cartes et plans

Exemples de cartes et plans pouvant intéresser le PPE : plans des itinéraires et accès ; plan du site ; plan de bouclage (si pertinent) ; cartographie des points névralgiques ; plan avec les zones de rassemblement en cas d'évacuation)

B. Annuaire

Indiquez ici la date de mise à jour de l'annuaire. Complétez l'annuaire par les numéros utiles (ex. : unités de renfort, etc.).

Fonction / service	Numéro	Nom/prénom
Personne à contacter en cas d'intervention sur le site : *A préciser*		
DDS du PIV		
DDS suppléant du PIV		
DDS de l'OIV		
Directeur/responsable du site		
Groupement de gendarmerie départementale		
Directeur départemental de la sécurité publique		
SIDPC/SIRACEDPC		

DISPOSITIONS CONNEXES A LA SAIV

Installations prioritaires de défense

Service de sécurité nationale

Enquêtes administratives

Sécurité des systèmes d’informations

Investissements étrangers

Règlementation Européenne

CODE DE LA DEFENSE

DISPOSITIONS CONNEXES A LA SAIV

I - INSTALLATIONS PRIORITAIRES DE DEFENSE

(partie législative)

Section 5 : Secteurs de sécurité des installations prioritaires de défense

Article L1321-2

(Modifié par LOI n°2009-928 du 29 juillet 2009 - art. 5)

Le ministre de l'intérieur reçoit du ministre de la défense, pour le développement et la mise en œuvre de ses moyens, le soutien des services et de l'infrastructure des armées et, notamment pour le maintien de l'ordre public, l'appui éventuel de forces militaires.

Dans les zones où se développent des opérations militaires et sur décision du Gouvernement, le commandement militaire désigné à cet effet devient responsable de l'ordre public et exerce la coordination des mesures de défense civile avec les opérations militaires.

En cas de menace portant sur une ou plusieurs installations prioritaires de défense, le commandement militaire désigné à cet effet peut être chargé, par décret en conseil des ministres, de la responsabilité de l'ordre public et de la coordination des mesures de défense civile avec les mesures militaires de défense à l'intérieur du ou des secteurs de sécurité délimités autour de ces installations par le Président de la République en conseil de défense et de sécurité nationale.

Des décrets en Conseil d'Etat définissent les modalités d'application des dispositions du présent article.

(partie règlementaire)

Section 5 : Secteurs de sécurité des installations prioritaires de défense

Article R*1311-39

Dans les secteurs de sécurité des installations prioritaires de défense mentionnés au troisième alinéa de l'article L. 1321-2, des mesures de protection ou de défense, nécessitées par la sûreté de ces installations, sont prises à titre permanent ou temporaire dans le cadre de la législation en vigueur.

Article R*1311-40

Lorsqu'un secteur de sécurité d'une installation prioritaire de défense est situé sur plusieurs départements limitrophes, il est appelé " secteur de sécurité interdépartemental ". Dès que ce secteur est délimité, l'un des préfets des départements concernés est chargé par décret de coordonner en tout temps la recherche et l'exploitation du renseignement relatif à la sécurité de cette installation.

Article R*1311-41

Dans les secteurs mentionnés à l'article R. * 1311-40, les pouvoirs de police nécessaires au maintien de l'ordre détenus par les préfets des départements concernés peuvent, lorsque les circonstances l'exigent, être transférés au préfet désigné pour coordonner le renseignement.

Un décret pris en conseil des ministres fixe la date de ce transfert.

Article R*1311-42

Les pouvoirs dont le transfert est opéré par le décret mentionné à l'article R. * 1311-41 comprennent les pouvoirs généraux de police que les préfets tiennent du code général des collectivités territoriales ainsi que, lorsque l'état d'urgence est déclaré, les pouvoirs exceptionnels qu'ils tiennent de la loi n° 55-385 du 3 avril 1955 instituant un état d'urgence.

Article R*1311-43

Lorsque les pouvoirs dont l'autorité civile est investie sont transférés à l'autorité militaire par application des dispositions de l'article L. 2121-2, relatives à l'état de siège, ou des dispositions des deuxième et troisième alinéas de l'article L. 1321-2, relatives au commandement militaire, les pouvoirs définis aux articles R. * 1311-41 et R. * 1311-42 sont transférés à une autorité unique.

Un décret pris en conseil des ministres fixe la date d'effet et détermine l'autorité militaire au profit de laquelle ce transfert est opéré.

CODE DE LA DEFENSE

DISPOSITIONS CONNEXES A LA SAIV

II – SERVICE DE SECURITE NATIONALE

(partie législative)

Chapitre unique

Article L2151-1

(Modifié par LOI n°2011-892 du 28 juillet 2011 - art. 3)

Le service de sécurité nationale est destiné à assurer la continuité de l'action de l'Etat, des collectivités territoriales, et des organismes qui leur sont rattachés, ainsi que des entreprises et établissements dont les activités contribuent à la sécurité nationale.

Le service de sécurité nationale est applicable au personnel, visé par un plan de continuité ou de rétablissement d'activité, d'un des opérateurs publics et privés ou des gestionnaires d'établissements désignés par l'autorité administrative conformément aux articles L. 1332-1 et L. 1332-2.

Seules les personnes majeures de nationalité française, ressortissantes de l'Union européenne, sans nationalité ou bénéficiant du droit d'asile peuvent être soumises aux obligations du service de sécurité nationale.

Article L2151-2

(Modifié par LOI n°2011-892 du 28 juillet 2011 - art. 3)

Dans les circonstances prévues aux articles L. 1111-2 et L. 2171-1 ou à l'article 1er de la loi n° 55-385 du 3 avril 1955, le recours au service de sécurité nationale est décidé par décret en conseil des ministres.

Article L2151-3

(Modifié par LOI n°2011-892 du 28 juillet 2011 - art. 3)

Lors du recours au service de sécurité nationale, les personnes placées sous ce régime sont maintenues dans leur emploi habituel ou tenues de le rejoindre.

Elles continuent d'être soumises aux règles de discipline et aux sanctions fixées par les statuts ou les règlements intérieurs de leur organisme d'emploi.

Article L2151-4

(Modifié par LOI n°2011-892 du 28 juillet 2011 - art. 3)

Les employeurs mentionnés au deuxième alinéa de l'article L. 2151-1 sont tenus d'élaborer des plans de continuité ou de rétablissement d'activité et de notifier aux personnes concernées par ces plans qu'elles sont susceptibles d'être placées sous le régime du service de sécurité nationale.

Article L2151-5

(Modifié par LOI n°2011-892 du 28 juillet 2011 - art. 3)

Les modalités d'application du présent titre sont déterminées par décret en Conseil d'Etat.

(partie règlementaire)

Section 1 : Obligations permanentes

Article R. 2151-1

Les employeurs mentionnés au deuxième alinéa de l'article L. 2151-1 mettent à jour les renseignements relatifs à l'identité et à la fonction de leur personnel susceptible d'être placé sous le régime du service de sécurité nationale. Ils tiennent ces renseignements à la disposition des hauts fonctionnaires de défense et de sécurité compétents.

Article R. 2151-2

Les employeurs mentionnés au deuxième alinéa de l'article L. 2151-1 sont tenus d'informer les personnes désignées par leurs plans de continuité ou de rétablissement d'activité dès qu'elles ne sont plus susceptibles d'être placées sous le régime du service de sécurité nationale.

Section 2 : Mise en œuvre du service de sécurité nationale

Article R. 2151-3

Le décret par lequel le recours au service de sécurité nationale est instauré peut en limiter la mise en œuvre à une partie du territoire ou au personnel de certains des employeurs mentionnés au deuxième alinéa de l'article L. 2151-1. Il en fixe également la durée.

Article R. 2151-4

Les ministres coordonnateurs compétents, tels que définis à l'article R. 1332-2, notifient le recours au service de sécurité nationale aux employeurs concernés. Ceux-ci en informent sans délai leurs employés placés sous le régime du service de sécurité nationale.

Article R. 2151-5

Les personnes placées sous le régime du service de sécurité nationale sont tenues de rejoindre leur emploi habituel dans un délai maximum de trois jours à compter de leur information.

Article R. 2151-6

Les ministres coordonnateurs compétents informent les employeurs concernés de la fin de la mise en œuvre du service de sécurité nationale. Les employeurs en informent les personnels placés sous le régime du service de sécurité nationale.

Section 3 : Dispositions pénales

Article R. 2151-7

Est puni de l'amende prévue pour les contraventions de 5e classe le fait de faire obstacle à l'accomplissement des obligations imposées par les articles L. 2151-3 et L. 2151-4 et par le présent titre.

Est puni de la même amende le fait de faire obstacle à l'accomplissement, par un agent de l'autorité publique, des fonctions tendant à assurer l'exécution ou le contrôle des obligations mentionnées à l'alinéa précédent.

La récidive des contraventions prévues aux alinéas précédents est réprimée conformément à l'article 132-11 du code pénal.

CODE DE LA SECURITE INTERIEURE

Chapitre IV : Enquêtes administratives

(partie législative)

Article L114-1

(Modifié par LOI n°2018-778 du 10 septembre 2018 - art. 5)

I. – Les décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux, peuvent être précédées d'enquêtes administratives destinées à vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées.

Ces enquêtes peuvent donner lieu à la consultation de traitements automatisés de données à caractère personnel relevant de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'exception des fichiers d'identification. Les conditions dans lesquelles les personnes intéressées sont informées de cette consultation sont précisées par décret.

II. – Il peut également être procédé à de telles enquêtes administratives en vue de s'assurer que le comportement des personnes physiques ou morales concernées n'est pas devenu incompatible avec les fonctions ou missions exercées, l'accès aux lieux ou l'utilisation des matériels ou produits au titre desquels les décisions administratives mentionnées au I ont été prises.

III. – Lorsque le résultat de l'enquête fait apparaître que le comportement de la personne bénéficiant d'une décision d'autorisation, d'agrément ou d'habilitation est devenu incompatible avec le maintien de cette décision, il est procédé à son retrait ou à son abrogation, dans les conditions prévues par les dispositions législatives ou réglementaires qui lui sont applicables ou, à défaut, dans les conditions prévues au chapitre Ier du titre II du livre Ier du code des relations entre le public et l'administration. En cas d'urgence, l'autorisation, l'agrément ou l'habilitation peuvent être suspendus sans délai pendant le temps strictement nécessaire à la conduite de cette procédure.

IV. – Lorsque le résultat de l'enquête fait apparaître que le comportement d'un fonctionnaire occupant un emploi participant à l'exercice de missions de souveraineté de l'Etat ou relevant du domaine de la sécurité ou de la défense est devenu incompatible avec l'exercice de ses fonctions, l'administration qui l'emploie procède à son affectation ou à sa mutation dans l'intérêt du service dans un emploi comportant l'exercice d'autres fonctions. En cas d'impossibilité de mettre en œuvre une telle mesure ou lorsque le comportement du fonctionnaire est incompatible avec l'exercice de toute autre fonction eu égard à la menace grave qu'il fait peser sur la sécurité publique, il est procédé à sa radiation des cadres.

Ces décisions interviennent après mise en œuvre d'une procédure contradictoire. A l'exception du changement d'affectation, cette procédure inclut l'avis d'un organisme paritaire dont la composition et le fonctionnement sont fixés par décret en Conseil d'Etat.

Lorsque le résultat de l'enquête fait apparaître que le comportement d'un agent contractuel de droit public occupant un emploi défini au premier alinéa du présent IV est devenu incompatible avec l'exercice de ses fonctions, son employeur lui propose un emploi comportant l'exercice d'autres fonctions et correspondant à ses qualifications. En cas d'impossibilité de mettre en œuvre une telle mesure, en cas de refus de l'agent ou lorsque son comportement est incompatible avec l'exercice de toute autre fonction eu égard à la menace grave qu'il fait peser sur la sécurité publique, il est procédé, après mise en œuvre d'une procédure contradictoire, à son licenciement.

Les décisions prises en application du présent IV, auxquelles l'article L. 411-2 du code des relations entre le public et l'administration n'est pas applicable, peuvent être contestées devant le juge administratif dans un délai de quinze jours à compter de leur notification et faire l'objet d'un appel et d'un pourvoi en cassation dans le même

délai. Les juridictions saisies au fond statuent dans un délai de deux mois. En cas de recours, la décision contestée ne peut prendre effet tant qu'il n'a pas été statué en dernier ressort sur ce litige.

L'employeur peut décider, à titre conservatoire, et pendant la durée strictement nécessaire à la mise en œuvre des suites données au résultat de l'enquête, d'écarter sans délai du service le fonctionnaire ou l'agent contractuel de droit public, avec maintien de son traitement, de l'indemnité de résidence, du supplément familial de traitement et des prestations familiales obligatoires.

V. – Il peut être procédé à des enquêtes administratives dans les conditions prévues au second alinéa du I du présent article pour la délivrance, le renouvellement ou le retrait d'un titre ou d'une autorisation de séjour sur le fondement des articles L. 121-4, L. 122-1, L. 311-12, L. 313-3, L. 314-3 et L. 316-1-1 du code de l'entrée et du séjour des étrangers et du droit d'asile ou des stipulations équivalentes des conventions internationales ainsi que pour l'application des articles L. 411-6, L. 711-6, L. 712-2 et L. 712-3 du même code.

NOTA :

Conformément au III de l'article 71 de la loi n° 2018-778 du 10 septembre 2018, ces dispositions entrent en vigueur à une date fixée par décret en Conseil d'Etat, au plus tard le 1er janvier 2019 et sont applicables aux demandes déposées postérieurement à cette dernière.

Le décret n° 2018-1159 du 14 décembre 2018 en son article 23 a fixé cette date au 1er janvier 2019.

(partie règlementaire)

Article R114-1

(Modifié par Décret n°2018-141 du 27 février 2018 - art. 3)

La liste des décisions pouvant donner lieu, en application de l'article L. 114-1, à des enquêtes administratives est fixée aux articles R. 114-2 à R. 114-5.

Article R114-4

Peuvent donner lieu aux enquêtes mentionnées à l'article R. 114-1 les autorisations d'accès aux lieux suivants protégés en raison de l'activité qui s'y exerce :

1° Zones militaires ou placées sous le contrôle de l'autorité militaire ;

2° Zones protégées intéressant la défense nationale mentionnées à l'article 413-7 du code pénal ;

3° Etablissements, installations ou ouvrages d'importance vitale, mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ;

4° Zones non librement accessibles des aérodromes, aux zones d'accès restreint, délimitées à l'intérieur des zones portuaires de sûreté et aux installations à usage aéronautique ou d'assistance météorologique mentionnées à l'article L. 6332-1 du code des transports ;

5° Lieux de préparation, de traitement, de conditionnement et de stockage des expéditions de fret et de colis postaux ainsi que des biens et produits destinés à être utilisés à bord des aéronefs, au sein des entreprises ou organismes agréés au sens des articles L. 6342-1 et L. 6343-1 du code des transports ;

6° Etablissements pénitentiaires, pour les personnes autres que les conseils des détenus.

Article R114-6

(Modifié par Décret n°2018-141 du 27 février 2018 - art. 3)

Les personnes qui font l'objet d'une enquête administrative en application de l'article L. 114-1 sont informées de ce que cette enquête donne lieu à la consultation des traitements automatisés de données personnelles relevant de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'exception des fichiers d'identification.

Lorsque l'enquête administrative qui donne lieu à la consultation fait suite à une demande de décision de l'intéressé, celui-ci en est informé dans l'accusé de réception de sa demande prévu aux articles L. 112-3 et L. 112-6 du code des relations entre le public et l'administration.

Dans les autres cas, l'intéressé est informé lors de la notification de la décision administrative le concernant.

Lors de la notification de la décision administrative mentionnée à l'article L. 114-1 du présent code le concernant, l'intéressé est également informé qu'il peut, dans ce cadre, faire l'objet d'une enquête administrative conformément aux dispositions du premier alinéa du présent article.

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'INTÉRIEUR

Décret n° 2017-668 du 27 avril 2017 portant création d'un service à compétence nationale dénommé « service national des enquêtes administratives de sécurité »

NOR : *INTC1710988D*

Publics concernés : *administrations de l'Etat (ministère de l'intérieur, ministère des transports).*

Objet : *création d'un service à compétence nationale dénommé « service national des enquêtes administratives de sécurité ».*

Entrée en vigueur : *le texte entre en vigueur le lendemain de sa publication.*

Notice : *le décret crée un service à compétence nationale, relevant du ministre de l'intérieur et rattaché au directeur général de la police nationale, qui a pour mission de contribuer à la prévention du terrorisme, des atteintes à la sécurité et à l'ordre publics et à la sûreté de l'Etat en diligentant des enquêtes administratives pour le compte du ministre de l'intérieur.*

Références : *le décret peut être consulté sur le site Légifrance (http://www.legifrance.gouv.fr).*

Le Premier ministre,

Sur le rapport du ministre de l'intérieur,

Vu le code de la sécurité intérieure, notamment ses articles L. 114-2 et L. 211-11-1 ;

Vu le décret n° 87-389 du 15 juin 1987 modifié relatif à l'organisation des services d'administration centrale ;

Vu le décret n° 97-464 du 9 mai 1997 modifié relatif à la création et à l'organisation des services à compétence nationale ;

Vu le décret n° 2005-850 du 27 juillet 2005 modifié relatif aux délégations de signature des membres du Gouvernement ;

Vu le décret n° 2013-728 du 12 août 2013 modifié relatif à l'organisation de l'administration centrale du ministère de l'intérieur et du ministère des outre-mer, notamment son article 6 ;

Vu le décret n° 2015-510 du 7 mai 2015 portant charte de la déconcentration ;

Vu le décret n° 2017-588 du 20 avril 2017 portant création d'un service à compétence nationale dénommé « commandement spécialisé pour la sécurité nucléaire » ;

Vu l'avis du comité technique ministériel unique du ministère de l'intérieur et du ministère des outre-mer en date du 28 février 2017,

Décrète :

Art. 1er. – Il est créé, au ministère de l'intérieur, un service à compétence nationale dénommé « service national des enquêtes administratives de sécurité », rattaché au directeur général de la police nationale.

Art. 2. – A la demande du ministre de l'intérieur, le service réalise, sous réserve des compétences du commandement spécialisé pour la sécurité nucléaire, des enquêtes administratives destinées à vérifier, au regard de l'objectif de prévention du terrorisme et des atteintes à la sécurité et à l'ordre public et à la sûreté de l'État, que le comportement de personnes physiques ou morales n'est pas incompatible avec l'autorisation d'accès à des sites sensibles ou l'exercice de missions ou fonctions sensibles dont elles sont titulaires ou auxquelles elles prétendent.

Dans ce cadre, le service :

– consulte de manière directe ou indirecte des traitements de données à caractère personnel relatifs à la prévention du terrorisme ou des atteintes à la sécurité et à l'ordre publics et évalue, exploite et analyse les informations ainsi recueillies afin d'émettre un avis, le cas échéant par délégation du ministre de l'intérieur, sur la compatibilité entre le comportement de la personne et l'exercice des missions ou fonctions envisagées ou l'accès aux sites concernés au regard du risque d'atteinte à la sécurité et à l'ordre publics que celle-ci représente ;

– élabore une doctrine en matière d'enquêtes administratives pour homogénéiser les pratiques dans les domaines qui lui sont confiés ;

– assure le traitement des recours administratifs diligentés à l'encontre de ses avis.

Art. 3. – Le chef du service est nommé par arrêté du ministre de l'intérieur. Il exerce son autorité sur l'ensemble des personnels affectés dans le service.

Art. 4. – Le service comprend :

– le bureau chargé de la supervision et de la coordination ;
– le bureau chargé des affaires juridiques ;
– le bureau chargé du recueil et de l'analyse de l'information ;
– le bureau chargé du soutien et de la sécurité informatique.

Art. 5. – Le ministre de l'intérieur et le secrétaire d'Etat chargé de la réforme de l'Etat et de la simplification sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait le 27 avril 2017.

BERNARD CAZENEUVE

Par le Premier ministre :

Le ministre de l'intérieur,
MATTHIAS FEKL

Le secrétaire d'Etat
chargé de la réforme de l'Etat
et de la simplification,
JEAN-VINCENT PLACÉ

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'INTÉRIEUR

Décret n° 2017-588 du 20 avril 2017 portant création d'un service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire »

NOR : *INTJ1702733D*

Publics concernés : *administrations de l'Etat (ministère de l'intérieur, ministère de la défense et ministère chargé de l'énergie) ; opérateurs d'importance vitale.*

Objet : *création d'un service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire ».*

Entrée en vigueur : *le décret entre en vigueur le lendemain de sa publication.*

Notice : *le décret crée un service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire » relevant conjointement du ministre chargé de l'énergie et du ministre de l'intérieur et rattaché au directeur général de la gendarmerie nationale. Il exerce, en lien avec le ministère chargé de l'énergie, notamment avec les services du haut fonctionnaire de défense et de sécurité, la coordination de l'ensemble des mesures prises par le ministère de l'intérieur destinées à assurer la protection des installations et matières nucléaires contre tout acte de malveillance ou menace. Concernant la protection des installations nucléaires intéressant la dissuasion, le Commandement spécialisé pour la sécurité nucléaire centralise, exploite et assure la diffusion des informations et renseignements intéressant la sécurité nucléaire.*

Références : *le décret peut être consulté sur le site Légifrance (http://www.legifrance.gouv.fr).*

Le Premier ministre,

Sur le rapport de la ministre de l'environnement, de l'énergie et de la mer, chargée des relations internationales sur le climat et du ministre de l'intérieur,

Vu le code de la défense ;

Vu le code de l'environnement, notamment les articles L. 591-1, L. 592-25 et L. 592-26 ;

Vu le code pénal ;

Vu le code de la sécurité intérieure, notamment les articles L. 114-1, L. 421-1, L. 421-2, R. 114-4 et R. 114-5 ;

Vu le décret n° 87-389 du 15 juin 1987 modifié relatif à l'organisation des services de l'administration centrale ;

Vu le décret n° 97-464 du 9 mai 1997 modifié relatif à la création et à l'organisation des services à compétence nationale ;

Vu le décret n° 2005-850 du 27 juillet 2005 modifié relatif aux délégations de signature des membres du Gouvernement ;

Vu le décret n° 2008-680 du 9 juillet 2008 modifié portant organisation de l'administration centrale du ministère de l'écologie, de l'énergie, du développement durable et de l'aménagement du territoire ;

Vu le décret n° 2013-728 du 12 août 2013 modifié portant organisation de l'administration centrale du ministère de l'intérieur et du ministère des outre-mer ;

Vu le décret n° 2015-510 du 7 mai 2015 portant charte de la déconcentration ;

Vu l'avis n° 2017-AV-0284 de l'Autorité de sûreté nucléaire en date du 24 janvier 2017 ;

Vu l'avis du comité technique ministériel unique du ministère de l'intérieur et du ministère des outre-mer en date du 28 février 2017,

Décrète :

Art. 1er. – Il est créé un service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire » relevant du ministre chargé de l'énergie et du ministre de l'intérieur.

Il est rattaché au directeur général de la gendarmerie nationale.

Il apporte également son concours au ministre de la défense.

Art. 2. – I. – Au titre de la préservation des intérêts fondamentaux de la Nation, le Commandement spécialisé pour la sécurité nucléaire, sans préjudice des compétences des services mentionnés aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure, coordonne la réponse des forces et services concourant à la sécurité intérieure, placés sous l'autorité du ministre de l'intérieur, dans le domaine de la protection des matières nucléaires

non affectées aux moyens nécessaires à la mise en œuvre de la politique de dissuasion, de leurs installations et de leurs transports contre tout acte de malveillance, agression ou menace, notamment à caractère terroriste.

A ce titre, il est chargé :

– d'améliorer, harmoniser et coordonner les concepts opérationnels ;
– de centraliser, exploiter, analyser et synthétiser le renseignement relatif aux menaces à la sécurité nucléaire, en lien avec les services mentionnés aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure ;
– d'assurer le contrôle et le suivi administratif des personnes accédant aux installations ;
– de développer l'expertise des personnels de la gendarmerie et de la police nationales impliqués dans ces missions.

Ses domaines de compétence recouvrent, dans la limite des missions définies aux articles 3 à 5 :

– la protection du secret de la défense nationale portant sur les activités des opérateurs d'importance vitale du sous-secteur nucléaire, de leurs sous-traitants et de leurs prestataires de services ;
– la protection des points d'importance vitale du sous-secteur nucléaire ;
– la protection des installations et matières nucléaires, y compris lors de leurs transports.

II. – Il apporte son concours au ministre de la défense dans l'exercice de ses responsabilités en matière de protection des installations nucléaires intéressant la dissuasion mentionnées à l'article L. 1411-1 du code de la défense.

Art. 3. – I. – Dans les domaines relevant de la compétence du ministre de l'intérieur, au titre de la prévention, de l'anticipation ainsi que de la réponse opérationnelle de l'Etat, sans préjudice des compétences des services mentionnés aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure, le Commandement spécialisé pour la sécurité nucléaire est le référent pour le ministère de l'intérieur au titre des missions définies à l'article 2.

II. – A ce titre, en lien avec les ministères, l'Autorité de sûreté nucléaire, les directions, les services compétents et les opérateurs, il est chargé :

1° De centraliser, exploiter, analyser et synthétiser le renseignement relatif aux menaces à la sécurité nucléaire, en lien avec les services mentionnés aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure ;

2° D'analyser les risques au regard des menaces et d'évaluer les modalités de la réponse apportée par les forces et services mentionnés au I de l'article 2 ;

3° De proposer des recommandations sur les évolutions de concepts opérationnels envisagées par les directions du ministère de l'intérieur ;

4° D'instruire, à la demande des autorités compétentes, les demandes d'avis en application de l'article R. 1332-22-1 du code de la défense, en vue d'autoriser une personne à accéder à tout ou partie d'un point d'importance vitale ;

5° D'instruire, à la demande des opérateurs concernés ou des autorités compétentes, les enquêtes administratives liées aux procédures administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation en application de l'article L. 114-1 du code de la sécurité intérieure ;

6° De coordonner, en lien avec les services enquêteurs, les enquêtes administratives d'habilitation des personnes physiques et morales réalisées au titre de la protection du secret de la défense nationale conformément aux dispositions de l'article R. 2311-7 du code de la défense ;

7° De suivre et centraliser les avis émis au titre de l'article R. 1332-22-1 du code de la défense ainsi que les décisions prises sur le fondement de l'article L. 114-1 du code de la sécurité intérieure et de l'article R. 2311-7 du code de la défense ;

8° En matière de transports :

a) De recueillir, auprès de l'autorité compétente, la planification des transports de matières nucléaires non affectées aux moyens nécessaires à la mise en œuvre de la politique de dissuasion sur le domaine public ;

b) D'apporter aux autorités administratives une expertise sur les opérations de sécurité assurées par les forces et services concourant à la sécurité intérieure mentionnés au I de l'article 2 ;

9° De concevoir et proposer les mesures de protection destinées au personnel des forces de sécurité intérieure contre les risques inhérents au domaine nucléaire ;

10° D'émettre l'avis prévu à l'article R. 1333-3 du code de la défense ;

11° De conseiller les autorités nationales et locales dans l'élaboration de la planification de défense et de sécurité nationale ;

12° De conseiller les délégués pour la défense et la sécurité des opérateurs du sous-secteur nucléaire désignés à l'article R. 1332-37 du code de la défense, de leurs sous-traitants et de leurs prestataires de services, en coordination avec les services enquêteurs, en matière de sécurité économique.

III. – Pôle d'expertise pour le ministère de l'intérieur, le Commandement spécialisé pour la sécurité nucléaire est associé à tous travaux relatifs aux domaines d'attributions mentionnés au présent article.

Art. 4. – Dans les domaines relevant de la compétence du ministre chargé de l'énergie, le Commandement spécialisé pour la sécurité nucléaire est chargé :

1° De centraliser les demandes d'habilitation, saisir les services enquêteurs et délivrer aux personnes physiques et morales les décisions d'habilitation au titre de la protection du secret de la défense nationale, conformément aux dispositions de l'article R. 2311-7 du code de la défense ;

2° De vérifier la mise en œuvre des règles ayant conduit à la délivrance de l'aptitude technique des locaux abritant des éléments couverts par le secret de la défense nationale.

Art. 5. – I. – Dans les domaines relevant de la compétence du ministre de la défense pour la protection des installations nucléaires intéressant la dissuasion, le Commandement spécialisé pour la sécurité nucléaire, sans préjudice des compétences des services mentionnés aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure, centralise, exploite, analyse et synthétise le renseignement relatif aux menaces à la sécurité nucléaire, en lien avec les services précités et le diffuse à la direction de la protection des installations, moyens et activités de la défense et à la direction du renseignement et de la sécurité de la défense.

II. – Pour la protection des installations nucléaires intéressant la dissuasion ne relevant pas du ministre de la défense au sens de l'article R.* 1411-9 du code de la défense :

1° Le Commandement spécialisé pour la sécurité nucléaire procède aux enquêtes administratives relatives aux personnes physiques accédant aux installations et communique les avis en résultant aux organismes demandeurs ;

2° Le Commandement spécialisé pour la sécurité nucléaire est informé :

a) Par le service enquêteur, des demandes d'habilitation des personnes physiques et morales au titre de la protection du secret de la défense nationale et du résultat des enquêtes ;

b) Par l'autorité d'habilitation du ministère de la défense, des décisions d'habilitation des personnes physiques et morales au titre de la protection du secret de la défense nationale.

Art. 6. – Le Commandement spécialisé pour la sécurité nucléaire est dirigé par un directeur nommé par arrêté conjoint du ministre chargé de l'énergie et du ministre de l'intérieur.

Le directeur peut déléguer sa signature à ses collaborateurs pour signer tous actes, décisions ou conventions, dans la limite de leurs attributions.

Il a autorité sur l'ensemble des personnels affectés dans le service.

Art. 7. – Le Commandement spécialisé pour la sécurité nucléaire est constitué de trois départements chargés :

– d'harmoniser et de coordonner les principes et concept opérationnels des forces et services concourant à la sécurité intérieure mentionnés au I de l'article 2 ;
– d'assurer le contrôle et le suivi administratif des personnes accédant aux installations concernées ;
– de développer l'expertise des personnels de la gendarmerie et de la police nationales impliqués dans ces missions.

Art. 8. – Un protocole conclu entre le ministère de l'intérieur et le ministère chargé de l'énergie, d'une part, et le ministère de la défense, d'autre part, fixe leurs obligations respectives en moyens et en personnels pour le fonctionnement du Commandement spécialisé pour la sécurité nucléaire et l'accomplissement de ses missions ainsi que les conditions du suivi annuel de ses actions et résultats.

Art. 9. – La ministre de l'environnement, de l'énergie et de la mer, chargée des relations internationales sur le climat, le ministre de la défense et le ministre de l'intérieur sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait le 20 avril 2017.

BERNARD CAZENEUVE

Par le Premier ministre :

Le ministre de l'intérieur,
MATTHIAS FEKL

La ministre de l'environnement,
de l'énergie et de la mer,
chargée des relations internationales
sur le climat,
SÉGOLÈNE ROYAL

Le ministre de la défense,
JEAN-YVES LE DRIAN

CODE DE LA DEFENSE

SÉCURITÉ DES SYSTÈMES D'INFORMATION

(partie législative)

Chapitre Ier : Responsabilités

Article L2321-2-1

(Créé par LOI n°2018-607 du 13 juillet 2018 - art. 34)

Lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques, des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 ou des opérateurs mentionnés à l'article 5 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, l'autorité nationale de sécurité des systèmes d'information peut mettre en œuvre, sur le réseau d'un opérateur de communications électroniques ou sur le système d'information d'une personne mentionnée aux 1 ou 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des dispositifs mettant en œuvre des marqueurs techniques aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information des autorités publiques et opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du présent code ou à l'article 5 de la loi n° 2018-133 du 26 février 2018 précitée. Ces dispositifs sont mis en œuvre pour la durée et dans la mesure strictement nécessaires à la caractérisation de la menace.

Les agents de l'autorité nationale de sécurité des systèmes d'information individuellement désignés et spécialement habilités sont autorisés, aux seules fins de prévenir et de caractériser la menace affectant les systèmes d'information des autorités publiques ou des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du présent code ou des opérateurs mentionnés à l'article 5 de la loi n° 2018-133 du 26 février 2018 précitée, à procéder au recueil et à l'analyse des seules données techniques pertinentes, à l'exclusion de toute autre exploitation.

Les données techniques recueillies directement par l'autorité nationale de sécurité des systèmes d'information en application du premier alinéa du présent article ou obtenues en application du deuxième alinéa de l'article L. 2321-3 ne peuvent être conservées plus de dix ans.

Les données recueillies autres que celles directement utiles à la prévention et à la caractérisation des menaces sont immédiatement détruites.

Un décret en Conseil d'Etat définit les modalités d'application du présent article

Article L2321-2-2

(Créé par LOI n°2018-607 du 13 juillet 2018 - art. 34)

Est puni de 150 000 € d'amende le fait, pour un opérateur de communications électroniques ou ses agents ou pour une personne mentionnée au premier alinéa de l'article L. 2321-2-1, de faire obstacle à la mise en œuvre, par l'autorité nationale de sécurité des systèmes d'information, des dispositifs mentionnés au même premier alinéa.

Les personnes physiques coupables de cette infraction encourent également l'interdiction, pour une durée de cinq ans au plus, d'exercer l'activité professionnelle à l'occasion de l'exercice de laquelle l'infraction a été commise

Article L2321-3

(Modifié par LOI n°2018-607 du 13 juillet 2018 - art. 34)

Pour les besoins de la sécurité des systèmes d'information des autorités publiques, des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et des opérateurs mentionnés à l'article 5 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, les agents de l'autorité nationale de sécurité des systèmes d'information, habilités par le Premier ministre et assermentés dans des conditions fixées par décret en Conseil d'Etat, peuvent obtenir des opérateurs de communications électroniques, en application du III de l'article L. 34-1 du code des postes et des communications électroniques, l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou l'atteinte de leur système.

Lorsque l'autorité nationale de sécurité des systèmes d'information est informée, en application de l'article L. 33-14 du même code, de l'existence d'un événement affectant la sécurité des systèmes d'information d'une autorité publique ou d'un opérateur mentionné aux articles L. 1332-1 et L. 1332-2 du présent code ou d'un opérateur mentionné à l'article 5 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, les agents mentionnés au premier alinéa du présent article peuvent obtenir des opérateurs de communications électroniques les données techniques strictement nécessaires à l'analyse de cet événement. Ces données ne peuvent être exploitées qu'aux seules fins de caractériser la menace affectant la sécurité de ces systèmes, à l'exclusion de toute autre exploitation.

Les surcoûts identifiables et spécifiques des prestations assurées par les opérateurs de communications électroniques à la demande de l'autorité nationale de sécurité des systèmes d'information en application du premier alinéa du présent article sont compensés selon les modalités prévues au III de l'article L. 34-1 du code des postes et des communications électroniques.

Article L2321-4

(Créé par LOI n°2016-1321 du 7 octobre 2016 - art. 47)

Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.

L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.

L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information

Article L2321-5

(Créé par LOI n°2018-607 du 13 juillet 2018 - art. 34)

L'Autorité de régulation des communications électroniques et des postes est chargée de veiller au respect par l'autorité nationale de sécurité des systèmes d'information des conditions d'application de l'article L. 2321-2-1 et du deuxième alinéa de l'article L. 2321-3.

(partie réglementaire)

Article R2321-1-1

(Créé par Décret n°2018-1136 du 13 décembre 2018 - art. 1)

La décision de mettre en œuvre les dispositifs mentionnés au premier alinéa de l'article L. 2321-2-1 sur les réseaux et les systèmes d'information des personnes mentionnées au même alinéa leur est notifiée par l'Agence nationale de la sécurité des systèmes d'information.

Cette notification est accompagnée d'un cahier des charges élaboré, le cas échéant, après concertation avec les personnes destinataires. Ce document précise les conditions techniques d'organisation et de fonctionnement nécessaires à la mise en œuvre de ces dispositifs ainsi que le délai dans lequel ils sont mis en œuvre et la durée de leur mise en œuvre. Il prévoit, le cas échéant, une phase de test préalable sur les réseaux ou systèmes d'information concernés.

La décision mentionnée au premier alinéa est communiquée sans délai à l'Autorité de régulation des communications électroniques et des postes

Article R2321-1-2

(Créé par Décret n°2018-1136 du 13 décembre 2018 - art. 1)

Les dispositifs mentionnés au premier alinéa de l'article L. 2321-2-1 sont mis en œuvre pour une période maximale de trois mois, prorogeable en cas de persistance de la menace et dans cette limite. Toute prorogation fait l'objet d'une décision de l'Agence nationale de la sécurité des systèmes d'information notifiée aux personnes mentionnées au premier alinéa de l'article R. 2321-1-1 et communiquée à l'Autorité de régulation des communications électroniques et des postes

Article R2321-1-3

(Créé par Décret n°2018-1136 du 13 décembre 2018 - art. 1)

Les marqueurs techniques exploités par les dispositifs mentionnés au premier alinéa de l'article L. 2321-2-1 sont des éléments techniques caractéristiques d'un mode opératoire d'attaque informatique, permettant de détecter une activité malveillante ou d'identifier une menace susceptible d'affecter la sécurité des systèmes d'information. Ils visent à détecter les communications et programmes informatiques malveillants et à recueillir et analyser les seules données techniques nécessaires à la prévention et à la caractérisation de la menace.

Article R2321-1-4

(Créé par Décret n°2018-1136 du 13 décembre 2018 - art. 1)

Les dispositifs de traçabilité des données collectées mentionnés au 2° de l'article L. 36-14 du code des postes et des communications électroniques garantissent notamment l'identification des agents mentionnés au deuxième alinéa de article L. 2321-2-1 et au premier alinéa de l'article L. 2321-3. Ces dispositifs enregistrent les opérations effectuées sur les données, dont leur suppression à l'issue du délai mentionné au troisième alinéa de l'article L. 2321-2-1

Article R2321-1-5

(Créé par Décret n°2018-1136 du 13 décembre 2018 - art. 1)

Les modalités de la compensation des prestations assurées par les personnes mentionnées au premier alinéa de l'article R. 2321-1-1 au titre de l'article L. 2321-2-1 et du deuxième alinéa de l'article L. 2321-3 sont fixées par arrêté conjoint du Premier ministre et du ministre chargé des communications électroniques

CODE MONETAIRE ET FINANCIER

(partie législative)

Chapitre Ier : Dispositions générales

Article L151-3

(Modifié par Loi n°2004-1343 du 9 décembre 2004 - art. 30 JORF 10 décembre 2004)

I. – Sont soumis à autorisation préalable du ministre chargé de l'économie les investissements étrangers dans une activité en France qui, même à titre occasionnel, participe à l'exercice de l'autorité publique ou relève de l'un des domaines suivants :

a) Activités de nature à porter atteinte à l'ordre public, à la sécurité publique ou aux intérêts de la défense nationale ;

b) Activités de recherche, de production ou de commercialisation d'armes, de munitions, de poudres et substances explosives.

Un décret en Conseil d'Etat définit la nature des activités ci-dessus.

II. – L'autorisation donnée peut être assortie le cas échéant de conditions visant à assurer que l'investissement projeté ne portera pas atteinte aux intérêts nationaux visés au I.

Le décret mentionné au I précise la nature des conditions dont peut être assortie l'autorisation.

III. – Le ministre chargé de l'économie, s'il constate qu'un investissement étranger est ou a été réalisé en méconnaissance des prescriptions du I ou du II, peut enjoindre à l'investisseur de ne pas donner suite à l'opération, de la modifier ou de faire rétablir à ses frais la situation antérieure.

Cette injonction ne peut intervenir qu'après l'envoi d'une mise en demeure à l'investisseur de faire connaître ses observations dans un délai de quinze jours.

En cas de non-respect de l'injonction précitée, le ministre chargé de l'économie peut, après avoir mis l'investisseur à même de présenter ses observations sur les faits qui lui sont reprochés dans un délai minimum de quinze jours, sans préjudice du rétablissement de la situation antérieure, lui infliger une sanction pécuniaire dont le montant maximum s'élève au double du montant de l'investissement irrégulier. Le montant de la sanction pécuniaire doit être proportionnel à la gravité des manquements commis. Le montant de la sanction est recouvré comme les créances de l'Etat étrangères à l'impôt et au domaine.

Ces décisions sont susceptibles d'un recours de plein contentieux.

Le décret mentionné au I détermine les modalités d'application du III.

(partie réglementaire)

Chapitre III : Investissements étrangers soumis à autorisation préalable.

Section 1 : Dispositions relatives aux investissements étrangers en provenance de pays tiers

Article R153-1

(Modifié par Décret n°2012-691 du 7 mai 2012 - art. 1)

Constitue un investissement au sens de la présente section le fait pour un investisseur :

1° Soit d'acquérir le contrôle, au sens de l'article L. 233-3 du code de commerce, d'une entreprise dont le siège social est établi en France ;

2° Soit d'acquérir tout ou partie d'une branche d'activité d'une entreprise dont le siège social est établi en France ;

3° Soit de franchir le seuil de 33,33 % de détention du capital ou des droits de vote d'une entreprise dont le siège social est établi en France.

Article R153-2

(Modifié par Décret n°2018-1057 du 29 novembre 2018 - art. 1)

Relèvent d'une procédure d'autorisation au sens du I de l'article L. 151-3 les investissements étrangers mentionnés à l'article R. 153-1 réalisés par une personne physique qui n'est pas ressortissante d'un Etat membre de l'Union européenne ou d'un Etat partie à l'accord sur l'Espace économique européen ayant conclu une convention d'assistance administrative avec la France en vue de lutter contre la fraude et l'évasion fiscale, par une entreprise dont le siège social ne se situe pas dans l'un de ces mêmes Etats ou par une personne physique de nationalité française qui n'y est pas résidente, dans les activités suivantes :

1° Activités dans les secteurs des jeux d'argent à l'exception des casinos ;

2° Activités réglementées de sécurité privée ;

3° Activités de recherche, de développement ou de production relatives aux moyens destinés à faire face à l'utilisation illicite, dans le cadre d'activités terroristes, d'agents pathogènes ou toxiques et à prévenir les conséquences sanitaires d'une telle utilisation ;

4° Activités portant sur les matériels ou dispositifs techniques de nature à permettre l'interception des correspondances ou conçus pour la détection à distance des conversations ou la captation de données informatiques, définis à l'article 226-3 du code pénal ;

5° Activités de services dans le cadre de centres d'évaluation agréés dans les conditions prévues au décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;

6° Activités de production de biens ou de prestation de services dans le secteur de la sécurité des systèmes d'information exercées, y compris en qualité de sous-traitant, au profit d'un opérateur mentionné aux articles L. 1332-1 ou L. 1332-2 du code de la défense ;

7° Activités relatives aux biens et technologies à double usage énumérés à l'annexe IV du règlement (CE) n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage ;

8° Activités relatives aux moyens de cryptologie et les prestations de cryptologie mentionnés aux paragraphes III, IV de l'article 30 et I de l'article 31 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;

9° Activités exercées par les entreprises dépositaires de secrets de la défense nationale notamment au titre des marchés classés de défense nationale ou à clauses de sécurité conformément aux articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale ;

10° Activités de recherche, de développement et activités mentionnées à l'article L. 2332-1 du code de la défense relatives aux armes, munitions, poudres et substances explosives destinées à des fins militaires ou aux matériels de guerre et assimilés, réglementés par le titre III ou le titre V du livre III de la deuxième partie du code de la défense ;

11° Activités exercées par les entreprises ayant conclu un contrat d'étude, de prestation de services ou de fourniture d'équipements au profit du ministère de la défense, soit directement, soit par sous-traitance, pour la réalisation d'un bien ou d'un service relevant d'un secteur mentionné aux points 7° à 10° ci-dessus ;

12° Autres activités portant sur des matériels, des produits ou des prestations de services, y compris celles relatives à la sécurité et au bon fonctionnement des installations et équipements, essentielles à la garantie des intérêts du pays en matière d'ordre public, de sécurité publique ou de défense nationale énumérés ci-après :

a) Intégrité, sécurité et continuité de l'approvisionnement en électricité, gaz, hydrocarbures ou autre source énergétique ;

b) Intégrité, sécurité et continuité de l'approvisionnement en eau dans le respect des normes édictées dans l'intérêt de la santé publique ;

c) Intégrité, sécurité et continuité d'exploitation des réseaux et des services de transport ;

c bis) Intégrité, sécurité et continuité des opérations spatiales mentionnées au 3° de l'article 1er de la loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales ;

d) Intégrité, sécurité et continuité d'exploitation des réseaux et des services de communications électroniques ;

d bis) Intégrité, sécurité et continuité d'exploitation des systèmes électroniques et informatiques spécifiques nécessaires pour l'exercice des missions de la police nationale, de la gendarmerie nationale, des services de sécurité civile ou pour l'exercice des missions de sécurité publique de la douane ;

e) Intégrité, sécurité et continuité d'exploitation d'un établissement, d'une installation ou d'un ouvrage d'importance vitale au sens des articles L. 1332-1 et L. 1332-2 du code de la défense et des systèmes d'information mentionnés à l'article L. 1332-6-1 du code de la défense ;

f) Protection de la santé publique.

13° Activités de recherche et de développement relatives à des moyens destinés à être mis en œuvre dans le cadre d'une activité définie aux 4°, 8°, 9° et 12° et portant sur les domaines suivants :

a) Cybersécurité, intelligence artificielle, robotique, fabrication additive, semi-conducteurs ;

b) Biens et technologies à double usage énumérés à l'annexe I du règlement (CE) du Conseil du 5 mai 2009 précité ;

14° Activités d'hébergement de données dont la compromission ou la divulgation est de nature à porter atteinte à l'exercice des activités ou aux intérêts relevant des 11° à 13°.

NOTA : Conformément à l'article 10 du décret n° 2018-1057 du 29 novembre 2018, ces dispositions s'appliquent aux demandes présentées à compter du 1er janvier 2019.

Section 2 : Dispositions relatives aux investissements en provenance des Etats membres de l'Union européenne

Article R153-3

(Modifié par Décret n°2012-691 du 7 mai 2012 - art. 3)

Constitue un investissement au sens de la présente section le fait pour un investisseur :

1° Soit d'acquérir le contrôle, au sens de l'article L. 233-3 du code de commerce, d'une entreprise dont le siège social est établi en France.

2° Soit d'acquérir tout ou partie d'une branche d'activité d'une entreprise dont le siège social est établi en France.

Article R153-4

(Modifié par Décret n°2018-1057 du 29 novembre 2018 - art. 2)

Sont soumis à une procédure d'autorisation au sens de l'article L. 151-3, s'ils relèvent de l'article R. 153-3, les investissements réalisés dans les activités énumérées du 8° au 14° de l'article R. 153-2 par une personne physique ressortissante d'un Etat membre de l'Union européenne ou d'un autre Etat partie à l'accord sur l'Espace économique européen ayant conclu une convention d'assistance administrative avec la France, en vue de lutter contre la fraude et l'évasion fiscale par une entreprise dont le siège social se situe dans l'un de ces mêmes Etats ou par une personne physique de nationalité française qui y est résidente.

NOTA : Conformément à l'article 10 du décret n° 2018-1057 du 29 novembre 2018, ces dispositions s'appliquent aux demandes présentées à compter du 1er janvier 2019.

Article R153-5

(Modifié par Décret n°2018-1057 du 29 novembre 2018 - art. 3)

Sont soumis à une procédure d'autorisation au sens de l'article L. 151-3, s'ils relèvent du 2° de l'article R. 153-3, les investissements réalisés par une personne physique ressortissante d'un Etat membre de l'Union européenne ou d'un autre Etat partie à l'accord sur l'Espace économique européen ayant conclu une convention d'assistance administrative avec la France, en vue de lutter contre la fraude et l'évasion fiscale par une entreprise dont le siège social se situe dans l'un de ces mêmes Etats ou par une personne physique de nationalité française qui y est résidente, dans les activités suivantes :

1° (alinéa abrogé) ;

2° Activités de sécurité privée, au sens des titres Ier et II du livre VI du code de la sécurité intérieure, lorsque les entreprises qui les exercent :

a) Fournissent une prestation à un opérateur public ou privé d'importance vitale, au sens de l'article L. 1332-1 du code de la défense ;

b) Ou participent directement et spécifiquement à des missions de sécurité définies aux articles L. 6342-4 et L. 5332-6 du code des transports ;

c) Ou interviennent dans les zones protégées ou réservées, au sens de l'article 413-7 du code pénal et des textes pris en application des articles R. 2311-1 et suivants du code de la défense relatifs à la protection du secret de la défense nationale ;

3° Activités de recherche, de développement ou de production, lorsqu'elles intéressent exclusivement :

a) Les agents pathogènes, les zoonoses, les toxines et leurs éléments génétiques ainsi que leurs produits de traduction mentionnés aux alinéas 1C351 et 1C352a. 2 de l'annexe I du règlement (CE) n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage ;

b) Les moyens de lutte contre les agents prohibés au titre de la convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et de leur destruction, faite à Paris le 13 janvier 1993,

et que le contrôle de l'investissement est exigé par les nécessités de la lutte contre le terrorisme et de la prévention des conséquences sanitaires de celui-ci ;

4° Activités de recherche, développement, production ou commercialisation portant sur les matériels ou dispositifs techniques de nature à permettre l'interception des correspondances ou conçus pour la détection à distance des conversations ou la captation de données informatiques, définis à l'article 226-3 du code pénal, dans la mesure où le contrôle de l'investissement est exigé par les nécessités de la lutte contre le terrorisme et la criminalité ;

5° Activités de services dans le cadre de centres d'évaluation agréés dans les conditions prévues au décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, lorsque les entreprises qui les exercent fournissent ces prestations au profit de services de l'Etat, dans la mesure où le contrôle de l'investissement est exigé par les nécessités de la lutte contre le terrorisme et la criminalité ;

6° Activités de production de biens ou de prestation de services dans le secteur de la sécurité des systèmes d'information exercées, y compris en qualité de sous-traitant, au profit d'un opérateur mentionné aux articles L. 1332-1 ou L. 1332-2 du code de la défense pour protéger un établissement ou une installation visés par ces dispositions ;

7° Activités relatives aux biens et technologies à double usage énumérés à l'annexe IV du règlement du 5 mai 2009 précité exercées au profit d'entreprises intéressant la défense nationale.

NOTA : Conformément à l'article 10 du décret n° 2018-1057 du 29 novembre 2018, ces dispositions s'appliquent aux demandes présentées à compter du 1er janvier 2019.

DIRECTIVE 2008/114/CE DU CONSEIL

du 8 décembre 2008

concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection

(Texte présentant de l'intérêt pour l'EEE)

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité instituant la Communauté européenne, et notamment son article 308,

vu la proposition de la Commission,

vu l'avis du Parlement européen [1],

vu l'avis de la Banque centrale européenne [2],

considérant ce qui suit:

(1) En juin 2004, le Conseil européen a demandé qu'une stratégie globale de protection des infrastructures critiques soit élaborée. En réponse, la Commission a adopté, le 20 octobre 2004, une communication intitulée «Protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme», dans laquelle elle a proposé des mesures en vue de renforcer la prévention, la préparation et la réponse de l'Union européenne face aux attaques terroristes contre des infrastructures critiques.

(2) Le 17 novembre 2005, la Commission a adopté un *Livre vert sur un programme européen de protection des infrastructures critiques*, présentant différents scénarios pour la mise en place de ce programme et du réseau d'alerte concernant les infrastructures critiques. Les réponses à ce livre vert ont mis en exergue la valeur ajoutée d'un cadre communautaire en matière de protection des infrastructures critiques. La nécessité de renforcer la capacité de protection des infrastructures critiques en Europe et de réduire les vulnérabilités de ces infrastructures a été reconnue. L'importance des principes clés de subsidiarité, de proportionnalité et de complémentarité ainsi que du dialogue avec les acteurs concernés a été soulignée.

(3) En décembre 2005, le Conseil «Justice et affaires intérieures» a demandé à la Commission de présenter une proposition de programme européen de protection des infrastructures critiques (EPCIP) et a décidé que ce programme devait être fondé sur une approche tous risques conjuguée avec la priorité donnée à la lutte contre la menace terroriste. Cette approche tient compte des risques d'origine humaine, des menaces technologiques et des catastrophes naturelles dans le processus de protection des infrastructures critiques, mais donne la priorité à la menace terroriste.

(4) En avril 2007, le Conseil a adopté des conclusions sur l'EPCIP, dans lesquelles il souligne que c'est aux États membres qu'incombe en dernier ressort la gestion de dispositifs de protection des infrastructures critiques sur leur territoire national, tout en se félicitant des efforts déployés par la Commission en vue d'élaborer une procédure à l'échelle européenne aux fins du recensement et de la désignation des infrastructures critiques européennes (ICE) ainsi que de l'évaluation de la nécessité d'améliorer leur protection.

(5) La présente directive constitue la première étape d'une approche progressive visant à recenser et désigner les ICE, ainsi qu'à évaluer la nécessité d'améliorer leur protection. Cette directive se concentre sur le secteur de l'énergie et sur celui des transports, et devrait être réexaminée en vue d'en évaluer les effets et d'apprécier la nécessité d'inclure d'autres secteurs dans son champ d'application, notamment le secteur des technologies de l'information et de la communication (TIC).

(6) La responsabilité de la protection des infrastructures critiques européennes incombe essentiellement et en dernier ressort aux États membres et aux propriétaires/opérateurs de ces infrastructures.

(7) Il existe un certain nombre d'infrastructures critiques dans la Communauté, dont l'arrêt ou la destruction aurait un impact transfrontalier significatif. Il pourrait s'agir d'effets intersectoriels transfrontaliers résultant des dépendances entre infrastructures interconnectées. Il convient de recenser ces ICE et de les désigner comme telles selon une procédure commune. L'évaluation des impératifs de sécurité concernant ces infrastructures devrait être effectuée selon des critères minimaux communs. Les programmes bilatéraux de coopération entre États membres dans le domaine de la protection des infrastructures critiques constituent un moyen bien établi et efficace de protéger les infrastructures critiques transfrontalières. L'EPCIP devrait s'appuyer sur cette forme de coopération. Les informations relatives à la désignation d'une infrastructure donnée comme ICE devraient recevoir un niveau de classification approprié, conformément à la législation communautaire et nationale applicable.

[1] Avis du Parlement européen du 10 juillet 2007 (non encore paru au Journal officiel).

[2] JO C 116 du 26.5.2007, p. 1.

(8) Dans la mesure où différents secteurs possèdent une expérience, une expertise et des exigences particulières en matière de protection des infrastructures critiques, il convient d'élaborer et de mettre en œuvre une approche communautaire dans ce domaine, en tenant compte des spécificités et des mesures sectorielles existantes, notamment celles en vigueur au niveau communautaire, national ou régional, y compris où il existe déjà des accords transfrontaliers d'assistance mutuelle entre propriétaires/opérateurs d'infrastructures critiques. Compte tenu du rôle très important joué par le secteur privé dans la surveillance et la gestion des risques, la planification de la continuité de l'exploitation et la reprise d'activité après une catastrophe, l'approche communautaire doit encourager une participation pleine et entière de ce secteur.

(9) En ce qui concerne le secteur de l'énergie, et plus particulièrement les procédés de production et de transport de l'électricité (en ce qui concerne la fourniture d'électricité), il est entendu que, lorsque cela est jugé nécessaire, la production d'électricité peut englober les éléments des centrales nucléaires servant au transport de l'électricité, tout en excluant les éléments strictement nucléaires, qui relèvent de la réglementation pertinente en matière nucléaire, notamment les traités et le droit communautaire.

(10) La présente directive complète les mesures sectorielles existant au niveau communautaire et dans les États membres. Dans les cas où des mécanismes communautaires sont déjà en place, ils devraient continuer à être utilisés et ainsi à contribuer à la mise en œuvre globale de la présente directive. Il y a lieu d'éviter les doubles emplois, voire les contradictions, entre différents actes ou différentes dispositions.

(11) Toutes les ICE désignées comme telles devraient être dotées de plans de sécurité d'opérateurs (PSO) ou de mesures équivalentes comportant un recensement des points importants, une évaluation des risques, ainsi que l'identification, la sélection et le classement par ordre de priorité des contre-mesures et des procédures. Afin d'éviter des travaux inutiles ou les doubles emplois, chaque État membre devrait en premier lieu établir si les propriétaires/opérateurs d'ICE désignées comme telles disposent de PSO ou de mesures similaires. En l'absence de tels plans, chaque État membre devrait prendre les dispositions nécessaires afin que des mesures appropriées soient prévues. Il appartient à chaque État membre de décider de la forme d'action la plus opportune en ce qui concerne l'établissement de PSO.

(12) Les mesures, principes et orientations, y compris des mesures communautaires, ainsi que les programmes de coopération bilatéraux et/ou multilatéraux qui prévoient un plan similaire ou équivalent à un PSO ou la présence d'un correspondant pour la sécurité ou d'une personne ayant une fonction équivalente, devraient être réputés satisfaire aux obligations imposées par la présente directive en ce qui concerne respectivement le PSO ou la présence d'un correspondant pour la sécurité.

(13) Des correspondants pour la sécurité devraient être désignés pour chaque ICE désignée comme telle afin de faciliter la coopération et la communication avec les autorités nationales compétentes en matière de protection des infrastructures critiques. Afin d'éviter des travaux inutiles ou les doubles emplois, chaque État membre devrait en premier lieu établir si les propriétaires/opérateurs d'ICE désignées comme telles disposent déjà d'un correspondant pour la sécurité ou d'un équivalent. En l'absence d'un correspondant, chaque État membre devrait prendre les dispositions nécessaires afin que des mesures appropriées soient prévues. Il appartient à chaque État membre de décider de la forme d'action la plus opportune en ce qui concerne la désignation de correspondants pour la sécurité.

(14) Une détermination efficace des risques, des menaces et des vulnérabilités dans les différents secteurs exige une communication à la fois entre les propriétaires ou opérateurs d'ICE et les États membres, et entre les États membres et la Commission. Chaque État membre devrait recueillir des informations sur les ICE qui se trouvent sur son territoire. La Commission devrait recevoir des informations génériques des États membres sur les risques, menaces et vulnérabilités qui existent dans les secteurs où ont été recensées des ICE, y compris, le cas échéant, des informations sur les améliorations pouvant éventuellement être apportées aux ICE et les éventuelles dépendances intersectorielles, qui pourraient au besoin servir de base à l'élaboration de propositions spécifiques de la Commission en vue d'améliorer la protection des ICE.

(15) Afin de faciliter l'amélioration de la protection des ICE, des méthodes communes de recensement et de désignation des risques, menaces et vulnérabilités touchant les points d'infrastructure peuvent être définies.

(16) Il y a lieu de donner aux propriétaires/opérateurs d'ICE accès, principalement par l'intermédiaire des autorités compétentes des États membres, aux bonnes pratiques et méthodes en matière de protection des infrastructures critiques.

(17) Une protection efficace des ICE exige une communication, une coordination et une coopération au niveau national et au niveau communautaire. Le meilleur moyen d'y parvenir consiste à désigner des points de contact pour la protection des infrastructures critiques européennes (ci-après dénommés «points de contact PICE»), dans chaque État membre, chargés de coordonner les questions européennes liées à la protection de ces infrastructures au niveau national, ainsi qu'avec les autres États membres et la Commission.

(18) Afin de développer les mesures de protection des infrastructures critiques européennes dans les domaines qui requièrent un certain degré de confidentialité, il convient de veiller à ce qu'un échange d'informations cohérent et sûr s'effectue dans le cadre de la présente directive. Il est important que les règles de confidentialité prévues par le droit national applicable ou le règlement (CE) nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission [1] soient appliquées aux informations spécifiques sur des points d'infrastructure critique qui pourraient être utilisées pour planifier et mettre en œuvre des actions visant à entraîner des conséquences inacceptables pour les installations concernées. Les informations classifiées devraient être protégées conformément à la législation communautaire et nationale applicable. Chaque État membre et la Commission devraient respecter la classification de sécurité attribuée à un document par son émetteur.

(19) Le partage des informations sur les ICE devrait s'effectuer dans un climat de confiance et de sécurité. Le partage des informations exige en effet une relation de confiance dans laquelle les entreprises et organisations savent que leurs données sensibles et confidentielles seront suffisamment protégées.

(20) Étant donné que les objectifs de la présente directive, à savoir l'instauration d'une procédure de recensement et de désignation des ICE et la définition d'une approche commune pour évaluer la nécessité d'améliorer la protection de ces infrastructures, ne peuvent pas être réalisés de manière suffisante par les États membres et peuvent donc, en raison des dimensions de l'action, être mieux réalisés au niveau communautaire, la Communauté peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(21) La présente directive respecte les droits fondamentaux et observe les principes reconnus notamment par la charte des droits fondamentaux de l'Union européenne,

A ARRÊTÉ LA PRÉSENTE DIRECTIVE:

Article premier

Objet

La présente directive établit une procédure de recensement et de désignation des infrastructures critiques européennes, ci-après dénommées «ICE», ainsi qu'une approche commune pour évaluer la nécessité d'améliorer leur protection, afin de contribuer à la protection des personnes.

Article 2

Définitions

Aux fins de la présente directive, on entend par:

a) «infrastructure critique»: un point, système ou partie de celui-ci, situé dans les États membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif dans un État membre du fait de la défaillance de ces fonctions;

b) «infrastructure critique européenne» ou «ICE»: une infrastructure critique située dans les États membres dont l'arrêt ou la destruction aurait un impact considérable sur deux États membres au moins. L'importance de cet impact est évaluée en termes de critères intersectoriels. Cela inclut les effets résultant des dépendances intersectorielles par rapport à d'autres types d'infrastructures;

c) «analyse de risques»: examen des scénarios de menace pertinents destiné à évaluer les vulnérabilités d'infrastructures critiques et les impacts potentiels de leur arrêt ou destruction;

d) «informations sensibles relatives à la protection des infrastructures critiques»: les informations sur une infrastructure critique qui, en cas de divulgation, pourraient être utilisées pour planifier et mettre en œuvre des actions visant à provoquer l'arrêt ou la destruction d'installations d'infrastructures critiques;

e) «protection»: l'ensemble des activités visant à garantir le bon fonctionnement, la continuité et l'intégrité d'une infrastructure critique afin de prévenir, d'atténuer ou de neutraliser une menace, un risque ou une vulnérabilité;

f) «propriétaires/opérateurs d'ICE»: les entités responsables des investissements relatifs à / de la gestion quotidienne d'un point, d'un système ou d'une partie de celui-ci, désigné comme ICE en vertu de la présente directive.

Article 3

Recensement des ICE

1. Conformément à la procédure prévue à l'annexe III, chaque État membre recense les ICE potentielles qui satisfont à la fois aux critères intersectoriels et sectoriels et qui répondent aux définitions énoncées à l'article 2, points a) et b).

[1] JO L 145 du 31.5.2001, p. 43.

La Commission peut, à leur demande, aider les États membres à recenser les ICE potentielles.

La Commission peut attirer l'attention des États membres concernés sur l'existence d'infrastructures critiques potentielles dont on pourrait considérer qu'elles satisfont aux critères pour être désignées comme ICE.

Il appartiendra à chaque État membre et à la Commission de poursuivre en permanence le recensement des ICE potentielles.

2. Les critères intersectoriels visés au paragraphe 1er sont notamment les suivants:

a) le nombre de victimes (nombre potentiel de morts ou de blessés);

b) l'incidence économique (ampleur des pertes économiques et/ou de la dégradation de produits ou de services, y compris l'incidence potentielle sur l'environnement);

c) incidence sur la population (incidence sur la confiance de la population, souffrances physiques et perturbation de la vie quotidienne, y compris disparition de services essentiels).

Les seuils des critères intersectoriels sont fondés sur la gravité de l'impact de l'arrêt ou de la destruction d'une infrastructure donnée. Les seuils précis applicables aux critères intersectoriels sont établis au cas par cas par les États membres concernés par une infrastructure critique donnée. Chaque État membre notifie chaque année à la Commission le nombre d'infrastructures par secteur pour lesquelles les seuils relatifs aux critères intersectoriels ont fait l'objet de discussions.

Les critères sectoriels tiennent compte des caractéristiques des différents secteurs d'ICE.

La Commission élabore, avec les États membres, des lignes directrices concernant l'application des critères intersectoriels et sectoriels et des seuils approximatifs à utiliser pour recenser les ICE. Ces critères font l'objet d'une classification. L'utilisation de telles lignes directrices est laissée à l'appréciation des États membres.

3. Les secteurs retenus pour la mise en œuvre de la présente directive sont ceux de l'énergie et des transports. Les sous-secteurs sont répertoriés à l'annexe I.

À l'occasion du réexamen de la présente directive prévu à l'article 11, de nouveaux secteurs peuvent, si cela s'avère opportun, être retenus pour la mise en œuvre de la présente directive. Il y a lieu d'accorder la priorité au secteur TIC.

Article 4

Désignation des ICE

1. Chaque État membre informe les autres États membres susceptibles d'être affectés considérablement par une ICE potentielle de l'existence de cette infrastructure et des raisons de sa désignation en tant qu'ICE potentielle.

2. Chaque État membre sur le territoire duquel est située une ICE potentielle engage des discussions bilatérales et/ou multilatérales avec les États membres susceptibles d'être affectés considérablement par ladite ICE potentielle. La Commission peut prendre part à ces discussions mais elle n'aura pas accès aux informations précises qui permettraient d'identifier sans équivoque une infrastructure déterminée.

Un État membre qui a des raisons de croire qu'il pourrait être affecté considérablement par une ICE potentielle mais qui n'a pas été identifiée comme telle par l'État membre sur le territoire duquel cette infrastructure est située peut faire part à la Commission de son souhait d'engager des discussions bilatérales et/ou multilatérales sur ce sujet. La Commission communique sans tarder ce souhait à l'État membre sur le territoire duquel l'ICE potentielle est située et œuvre pour faciliter un accord entre les parties.

3. L'État membre sur le territoire duquel se situe une ICE potentielle la désigne en tant qu'ICE après accord entre cet État membre et les États membres qui sont susceptibles d'être affectés considérablement par l'infrastructure.

L'accord de l'État membre sur le territoire duquel se situe l'infrastructure à désigner comme ICE est requis.

4. L'État membre sur le territoire duquel se situe une ICE désignée comme telle informe chaque année la Commission du nombre d'ICE désignées comme telles par secteur et du nombre d'États membres concernés par chacune d'entre elles. Seuls les États membres qui sont susceptibles d'être affectés considérablement par une ICE sont en possession des informations permettant de l'identifier.

5. L'État membre sur le territoire duquel l'ICE est située informe le propriétaire/opérateur de l'infrastructure de la désignation de celle-ci comme ICE. Les informations relatives à la désignation d'une infrastructure comme ICE reçoivent un niveau de classification approprié.

6. Le processus de recensement et de désignation des ICE en application de l'article 3 et du présent article est mené à terme au plus tard le 12 janvier 2011 et fait l'objet d'un réexamen régulier.

Article 5

Plans de sécurité d'opérateur

1. La procédure d'élaboration du plan de sécurité d'opérateur, ci-après dénommé «PSO», recense les différents points de l'ICE, ainsi que les mesures de sécurité appliquées ou en cours de mise en œuvre pour leur protection. Le contenu minimum d'un PSO ICE est exposé à l'annexe II.

2. Chaque État membre apprécie si chaque infrastructure classée comme ICE établie sur son territoire est dotée d'un PSO ou a mis en place des mesures équivalentes répondant aux points figurant à l'annexe II. Si un État membre estime qu'un PSO ou une mesure équivalente existe et est mis à jour régulièrement, aucune autre mesure d'exécution n'est nécessaire.

3. Si un État membre constate qu'un PSO ou une mesure équivalente n'a pas été élaboré, il prend toutes les dispositions qu'il juge appropriées pour que soit établi un tel PSO ou un plan équivalent répondant aux points figurant à l'annexe II.

Chaque État membre s'assure qu'un PSO ou une mesure équivalente est établi et que, dans un délai d'un an à compter de la désignation de l'infrastructure critique comme ICE, il fait l'objet d'un réexamen. Ce délai peut être prorogé dans des circonstances exceptionnelles, avec l'accord de l'autorité compétente de l'État membre et avec notification à la Commission.

4. Lorsque des dispositions en matière de vérification ou de surveillance sont déjà applicables à une ICE, ces dispositions ne sont pas affectées par le présent article, et la surveillance prévue par ces dispositions est assurée par l'autorité compétente de l'État membre visée au présent article.

5. Dès lors que des mesures, y compris des mesures communautaires, qui, dans un secteur déterminé, exigent un plan similaire ou équivalent à un PSO et le contrôle de ce plan par l'autorité compétente, ou font référence à la nécessité de disposer d'un tel plan et d'exercer un tel contrôle, sont respectées, toutes les obligations incombant aux États membres en vertu du présent article ou adoptées en application de celui-ci, sont également réputées respectées. Les lignes directrices relatives à la mise en œuvre visées à l'article 3, paragraphe 2, comportent une liste indicative de ces mesures.

Article 6

Correspondants pour la sécurité

1. Le correspondant pour la sécurité exerce la fonction de point de contact pour les questions liées à la sécurité entre le propriétaire/opérateur de l'ICE et l'autorité compétente de l'État membre.

2. Chaque État membre apprécie si chaque infrastructure classée comme ICE établie sur son territoire est dotée d'un correspondant pour la sécurité ou d'un équivalent. Si un État membre constate qu'un tel correspondant pour la sécurité est en place ou qu'une fonction équivalente existe, aucune autre mesure d'exécution n'est nécessaire.

3. Si un État membre constate que, pour une ICE désignée comme telle, il n'y a pas de correspondant pour la sécurité ou d'équivalent, il prend toutes les dispositions qu'il juge appropriées pour qu'un tel correspondant ou personne exerçant une fonction équivalente soit désigné.

4. Chaque État membre met en œuvre un mécanisme de communication approprié entre l'autorité compétente de l'État membre et le correspondant pour la sécurité ou la personne occupant un poste équivalent, dans le but d'échanger les informations utiles concernant les risques et les menaces identifiés qui pèsent sur l'ICE concernée. Ce mécanisme de communication s'exerce sans préjudice des obligations nationales applicables en matière d'accès aux informations sensibles et classifiées.

5. Dès lors que des mesures, y compris des mesures communautaires, qui, dans un secteur déterminé, exigent la présence d'un correspondant pour la sécurité ou d'un poste équivalent, ou font référence à la nécessité d'une telle présence, sont respectées, toutes les obligations incombant aux États membres en vertu du présent article ou adoptées en application de celui-ci, sont également réputées respectées. Les lignes directrices relatives à la mise en œuvre, visées à l'article 3, paragraphe 2, comportent une liste indicative de ces mesures.

Article 7

Rapports

1. Chaque État membre réalise une évaluation de la menace pesant sur les sous-secteurs d'ICE dans un délai d'un an à compter de la désignation d'une infrastructure critique située sur son territoire comme ICE au sein de ces sous-secteurs.

2. Chaque État membre présente à la Commission, tous les deux ans, des données génériques synthétisées sur les types de risques, menaces et vulnérabilités rencontrés dans chacun des secteurs d'ICE comptant une ICE désignée comme telle, conformément à l'article 4, et située sur son territoire.

Un modèle commun de rapport peut être élaboré par la Commission, en coopération avec les États membres.

Chaque rapport reçoit le niveau de classification jugé nécessaire par l'État membre qui l'a émis.

3. Sur la base du rapport visé au paragraphe 2, la Commission et les États membres apprécient secteur par secteur s'il y a lieu d'envisager des mesures de protection supplémentaires au niveau communautaire pour les infrastructures critiques européennes. Ce processus d'évaluation se déroule à l'occasion du réexamen de la présente directive prévu à l'article 11.

4. Des lignes directrices communes pour les méthodes d'analyse des risques touchant les ICE peuvent être élaborées par la Commission, en coopération avec les États membres. L'utilisation de telles lignes directrices est laissée à l'appréciation des États membres.

Article 8

Soutien de la Commission aux ICE

La Commission soutient, par l'intermédiaire de l'autorité compétente de l'État membre, les propriétaires ou opérateurs d'ICE désignées comme telles en leur donnant accès aux bonnes pratiques et méthodes existantes ainsi qu'en facilitant la formation et l'échange d'informations sur les nouvelles évolutions techniques liées à la protection des infrastructures critiques.

Article 9

Informations sensibles relatives à la protectiondes infrastructures critiques européennes

1. Toute personne traitant des informations classifiées en application de la présente directive pour le compte d'un État membre ou de la Commission est soumise à une enquête de sûreté adéquate.

Les États membres, la Commission et les instances de surveillance compétentes veillent à ce que les informations sensibles relatives à la protection des infrastructures critiques européennes communiquées à d'autres États membres ou à la Commission ne soient pas utilisées à d'autres fins que la protection de ces infrastructures.

2. Le présent article s'applique aussi aux informations échangées oralement durant les réunions au cours desquelles des questions sensibles sont examinées.

Article 10

Points de contact pour la protectiondes infrastructures critiques européennes

1. Chaque État membre désigne un point de contact pour la protection des infrastructures critiques européennes (ci-après dénommé «point de contact PICE»).

2. Ce point de contact PICE coordonne les questions liées à la protection des infrastructures critiques européennes tant à l'intérieur de l'État membre qu'avec les autres États membres et la Commission. La désignation d'un point de contact PICE ne fait pas obstacle à ce que d'autres autorités d'un État membre soient associées aux questions relatives à la protection des infrastructures critiques européennes.

Article 11

Réexamen

Un réexamen de la présente directive commencera le 12 janvier 2012.

Article 12

Mise en œuvre

Les États membres adoptent les dispositions nécessaires pour se conformer à la présente directive au plus tard le 12 janvier 2011. Ils en informent immédiatement la Commission et lui communiquent le texte de ces dispositions ainsi qu'un tableau de correspondance entre celles-ci et la présente directive.

Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

Article 13

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Article 14

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le 8 décembre 2008.

Par le Conseil

Le président

B. KOUCHNER

ANNEXE I

Liste des secteurs d'ICE

Secteur	Sous-secteurs	
I Énergie	1. Électricité	Infrastructures et installations permettant la production et le transport d'électricité, en ce qui concerne la fourniture d'électricité
	2. Pétrole	Production pétrolière, raffinage, traitement, stockage et distribution par oléoducs
	3. Gaz	Production gazière, raffinage, traitement, stockage et distribution par gazoducs Terminaux GNL
II Transports	4. Transports par route 5. Transport ferroviaire 6. Transport aérien 7. Navigation intérieure 8. Transport hauturier et transport maritime à courte distance (cabotage) et ports	

Le recensement des infrastructures critiques pouvant être désignées comme ICE est effectué par les États membres conformément à l'article 3. Par conséquent, la liste des secteurs d'infrastructures ne génère pas en soi une obligation générale de désigner une ICE dans chaque secteur.

ANNEXE II

PROCÉDURE D'ÉLABORATION DU PSO ICE

Le PSO recense les points de l'infrastructure critique, ainsi que les mesures de sécurité appliquées ou en cours de mise en œuvre pour leur protection. La procédure d'élaboration du PSO ICE comprendra au moins:

1. le recensement des points d'infrastructure importants;

2. la conduite d'une analyse de risques fondée sur les principaux scénarios de menace, les vulnérabilités de chaque point d'infrastructure et les impacts potentiels, et

3. l'identification, la sélection et la désignation par ordre de priorité des contre-mesures et des procédures en établissant une distinction entre:

   — les mesures de sécurité permanentes, qui précisent les investissements et les moyens nécessaires en matière de sûreté qui sont susceptibles d'être utilisés en toutes circonstances. Cette catégorie contiendra des informations relatives aux mesures générales, par exemple les mesures techniques (y compris l'installation de moyens de détection, de contrôle d'accès, de protection et de prévention), aux mesures de nature organisationnelle (y compris des procédures d'alerte et de gestion de crise), aux mesures de contrôle et de vérification; aux communications; à la sensibilisation et à la formation, ainsi qu'à la sécurité des systèmes d'information;

   — des mesures de sécurité graduées, qui peuvent être déclenchées en fonction de différents niveaux de menace.

ANNEXE III

Procédure applicable en ce qui concerne le recensement par les États membres des infrastructures critiques pouvant être désignées parmi les ICE au titre de l'article 3

L'article 3 exige que chaque État membre recense les infrastructures critiques pouvant être désignées comme ICE. Cette procédure est mise en œuvre par chaque État membre en respectant la série d'étapes consécutives reprises ci-après.

L'ICE potentielle qui ne satisfait pas aux exigences de l'une des étapes successives ci-après est considérée comme «non ICE» et est exclue de la procédure. L'ICE potentielle qui répond aux définitions est soumise aux étapes suivantes de la présente procédure.

Étape 1

Chaque État membre applique les critères sectoriels afin d'opérer une première sélection parmi les infrastructures critiques existant au sein d'un secteur.

Étape 2

Chaque État membre applique la définition des infrastructures critiques visée à l'article 2, point a), à l'ICE potentielle recensée lors de l'étape 1.

La gravité de l'impact sera déterminée par application des méthodes nationales de recensement des infrastructures critiques ou sur la base des critères intersectoriels, à l'échelon national approprié. En ce qui concerne les infrastructures qui offrent un service essentiel, il sera tenu compte de l'existence de solutions de remplacement ainsi que de la durée de l'arrêt/de la reprise d'activité.

Étape 3

Chaque État membre applique l'élément transfrontalier de la définition d'ICE visée à l'article 2, point b), à l'ICE potentielle qui a franchi les deux premières étapes de la procédure. Si l'ICE potentielle répond à la définition, elle est soumise à l'étape suivante de la procédure. En ce qui concerne les infrastructures qui offrent un service essentiel, il sera tenu compte de l'existence de solutions de remplacement ainsi que de la durée de l'arrêt/de la reprise d'activité.

Étape 4

Chaque État membre applique les critères intersectoriels aux ICE potentielles restantes. Les critères intersectoriels tiennent compte des éléments suivants: la gravité de l'impact et, pour les infrastructures qui offrent un service essentiel, l'existence de solutions de remplacement, ainsi que la durée de l'arrêt/de la reprise d'activité. Les ICE potentielles qui ne répondent pas aux critères intersectoriels ne seront pas considérées comme étant des ICE.

L'identification des ICE potentielles qui franchissent toutes les étapes de cette procédure n'est communiquée qu'aux États membres susceptibles d'être affectés considérablement par lesdites infrastructures.