PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Directive Générale Interministérielle relative à la Planification de **défense** et de **sécurité nationale**

N°320/SGDSN/PSE/PSN du date 23 janvier 2023

Secrétariat général de la défense et de la sécurité nationale

Référence	N°320/SGDSN/PSE/PSN
Date de signature	23 janvier 2023
Emetteur	Première ministre / Secrétariat général de la défense et de la sécurité nationale.
Objet	Directive générale interministérielle relative à la planification de défense et de sécurité nationale.
Commande	Cette directive vise à refondre la planification de défense et de sécurité nationale, avec pour objectif d'optimiser et de rationaliser les plans nationaux existants, dans une approche « tous risques et menaces ». Elle apporte davantage de modularité dans la planification et la gestion de crise, et prépare l'Etat à faire face à des crises plus transverses et protéiformes, en intégrant des fonctions de coordination renforcées.
Action(s) à réaliser	Mettre en œuvre cette directive dans le cadre de la planification sectorielle mise à jour par les ministères et les administrations déconcentrées.
Echéance	Effet immédiat.
Contact utile	courrier.sgdsn@sgdsn.gouv.fr
Nombre de pages et annexes	18 pages ; 8 annexes (104 pages annexes incluses).

SOMMAIRE

Champ de la planification de défense et de sécurité nationale

Le champ de la planification de défense et de sécurité nationale correspond à celui de l'article L1111-1 du code de la défense qui précise :

« ***La stratégie de sécurité*** *nationale a pour objet d'identifier* ***l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation****, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de* ***déterminer les réponses que les pouvoirs publics doivent y apporter.*** *L'ensemble des politiques publiques concourt à la sécurité nationale.*

La politique de défense *a pour objet d'assurer l'intégrité du territoire et la protection de la population contre les agressions armées.* ***Elle contribue à la lutte contre les autres menaces susceptibles de mettre en cause la sécurité nationale.*** *Elle pourvoit au respect des alliances, des traités et des accords internationaux et participe, dans le cadre des traités européens en vigueur, à la politique européenne de sécurité et de défense commune.* »

La planification de défense et de sécurité nationale contribue à renforcer la résilience, définie[1] comme la volonté et la capacité du pays, de la société et des pouvoirs publics de résister aux conséquences d'une agression ou d'une catastrophe majeure, puis de rétablir rapidement leur capacité de fonctionnement, du moins dans un mode socialement acceptable. Elle vise ainsi :

- en priorité, **à préparer la Nation à des crises majeures** dont l'intensité et le caractère multisectoriel imposent une réaction globale fondée sur une organisation cohérente. Elle s'applique donc, quoique non exclusivement, aux crises **justifiant la mise en place de la *cellule interministérielle de crise* (CIC)** et peut préparer la mise en œuvre progressive de mesures spécifiques ;
- plus généralement, à **assurer la continuité tant de l'État que des fonctions essentielles au fonctionnement de la Nation face à tous les types de risques et de menaces en s'appuyant sur les dispositifs de continuité d'activité ainsi que sur les dispositifs permanents qui assurent au quotidien la sécurité de la Nation**. Généralement interservices, ces derniers relèvent de la responsabilité des différents ministères dans le cadre des politiques publiques dont ils ont la charge et se déclinent à tous les niveaux territoriaux (représentants de l'État et collectivités territoriales[2]). Dans les différents champs de la sécurité (publique, civile, sanitaire, économique, environnementale, etc.) et de la défense, ils comprennent des mécanismes de surveillance, de détection, de contrôle, de protection, d'alerte et d'intervention.

La planification de défense et de sécurité nationale fixe ainsi un référentiel interministériel commun, tout en laissant à chaque ministère ses prérogatives. Cette approche facilite les déclinaisons territoriales, les réflexions transverses et la prise en compte d'enjeux émergents (conséquences du changement climatique, déplacement de population ou catastrophes Outre-mer).

1 - Livre Blanc de la défense et de la sécurité nationale de 2008.
2 - Notamment lorsque des services publics leur ont été confiés par la loi.

1. PRINCIPES GÉNÉRAUX

La planification de défense et de sécurité nationale vise à **faire face à tous les risques et toutes les menaces** susceptibles **d'affecter les activités clés de la vie de la Nation**. **Coordonnée au niveau interministériel**, sur la base d'une stratégie et d'un **processus décisionnel commun**, elle s'appuie sur les responsabilités de chaque ministère[3] .

Elle se décline en **trois niveaux** :

- la planification **gouvernementale** ;
- la planification **ministérielle et/ou sectorielle** ;
- leurs déclinaisons **territoriales**.

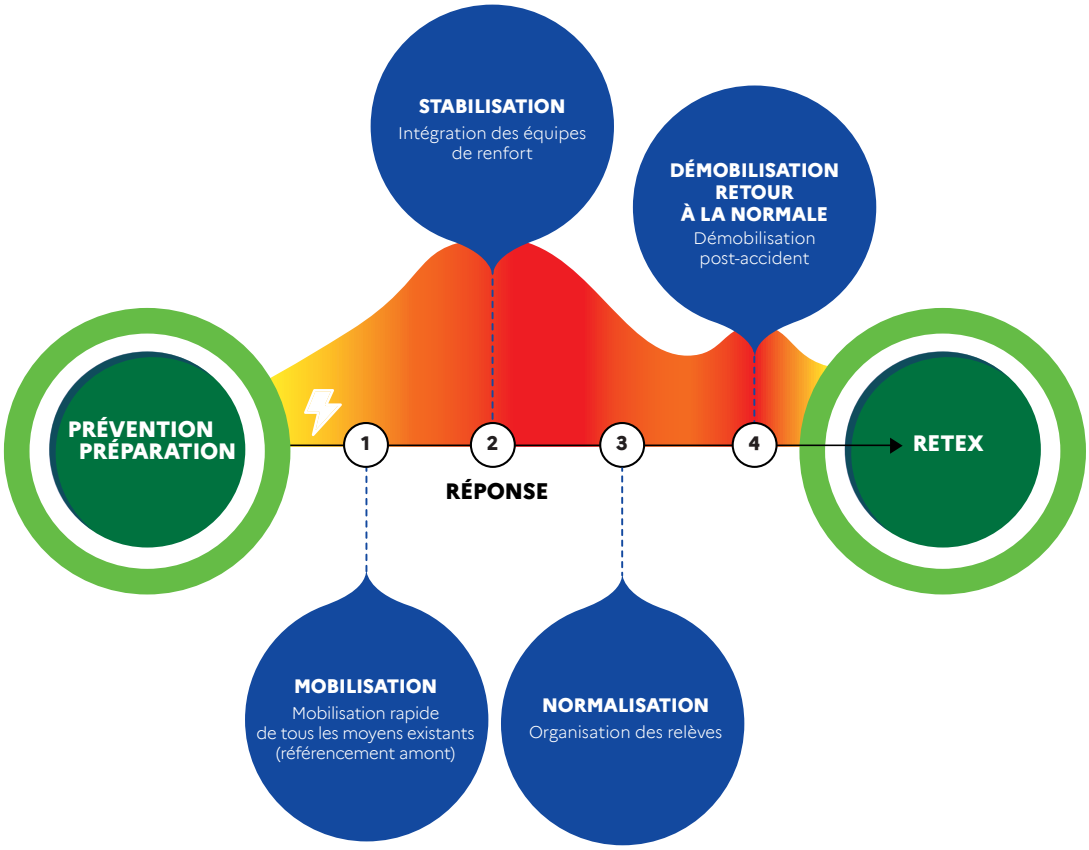
et s'appuie sur **quatre principes** :

1. **une analyse préalable des menaces et des risques** réalisée au niveau national et par grands bassins de risques, tous secteurs confondus, en y associant l'ensemble des acteurs (publics et privés) ;
2. **une approche capacitaire** qui s'appuie sur la connaissance des capacités de gestion de crise mobilisables (nationales, locales, ministérielles) ;
3. **la modularité** avec une base de mesures socles toujours actives et des mesures additionnelles pouvant être mises en œuvre en complément, indépendamment d'un déclenchement formel d'un plan ;
4. **la subsidiarité** avec une planification réalisée au niveau le plus pertinent, c'est-à-dire au plus petit niveau organisationnel capable d'apporter une réponse adaptée et d'en conduire la mise en œuvre.

La planification de défense et de sécurité nationale recouvre des logiques de :

- **prévention** : cartographies des risques et menaces, actions de réduction des vulnérabilités… ;
- **préparation** : planification, adaptation des outils, formation, entrainement… ;
- **réponse :** mise en œuvre et adaptation des mesures et outils associés, contrôle des actions, avec quatre phases qui se succèdent, quelle que soit la cinétique de l'évènement :
  - **la mobilisation** qui**,** conduite par les structures initialement chargées de la résolution et immédiatement disponibles, permet une réponse réflexe pendant la mobilisation d'éventuelles capacités supplémentaires ;
  - **la stabilisation** qui voit l'ordonnancement des capacités engagées pour contenir les effets de la crise, organise l'identification des besoins et suscite la fourniture de services dépassant les capacités et moyens des premiers intervenants ;
  - **la normalisation** qui voit réussir l'action coordonnée des capacités, mobilisées au juste besoin, pour atteindre une forme de routine ;
  - **le rétablissement d'un fonctionnement socialement acceptable** qui, par une adaptation continue, voit la démobilisation progressive des capacités complémentaires engagées pour tendre vers un « nouvel équilibre ».
- **retour d'expérience** : capitalisation de l'expérience, diffusion de l'information, réajustement *ex post*.

3 - article L1141-1 du code de la défense.



Cette démarche de planification globale qui s'inscrit **dans le temps** permet de **préparer chacune des phases ainsi que les transitions entre elles.**

En conduite, l'adaptation de la posture globale de sécurité (ajout ou retrait de mesures additionnelles ou de capacités) devra être évaluée régulièrement pour ajuster la réponse au cours de phases qui peuvent s'avérer longues, notamment pour recouvrer des capacités d'agir en cas de résurgence ou d'émergence d'autres crises.

La réussite de chacune de ces phases est liée à une gouvernance adaptée et à l'atteinte de critères de succès (annexe 6).

2. ANALYSES PRÉALABLES

Une crise majeure est le produit **d'une menace ou d'un risque**, né d'un évènement déclencheur appliqué à une **vulnérabilité,** que les **capacités** de protection n'auront permis de contenir.

La planification de défense et de sécurité nationale décrite ici permet une analyse préalable cohérente de ces différents éléments quelle que soit la typologie de la crise et ses déclinaisons territoriales. Elle permet aux décideurs d'apporter la réponse la plus adaptée, tout en faisant preuve de réalisme au travers d'une priorisation.

A. TYPOLOGIE DES MENACES ET DES RISQUES

Les travaux de planification de défense et de sécurité répondent à plusieurs typologies de crises majeures, non exclusives, et décrites en annexe 3 :

Menaces

- *menace extérieure, agression*[4]
- *attentats, de nature NRBC ou non (terrorisme, tuerie de masse, prise d'otages…)*
- *troubles sociétaux graves (violences urbaines, migrations massives…)*
- *cyber*
- *hybrides*

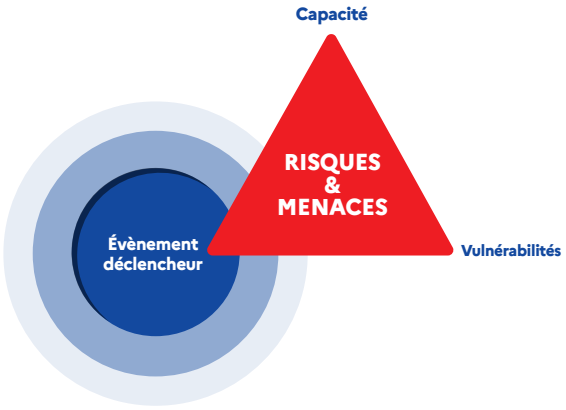
Risques

- *naturels*
- *technologiques ou industriels*
- *sanitaires*

4 - article R1421-1 du code de la défense

a. TYPOLOGIES DES ÉVÉNEMENTS DÉCLENCHEURS

Ces typologies permettent de définir une liste non exhaustive d'acteurs ou d'évènements déclencheurs, susceptibles d'initier ces crises majeures et donc justifier leur prise en compte en planification. Cités en annexe 3, ils sont définis selon leur intensité ou leur probabilité d'occurrence spatiale (bassins de risques) et temporelle.

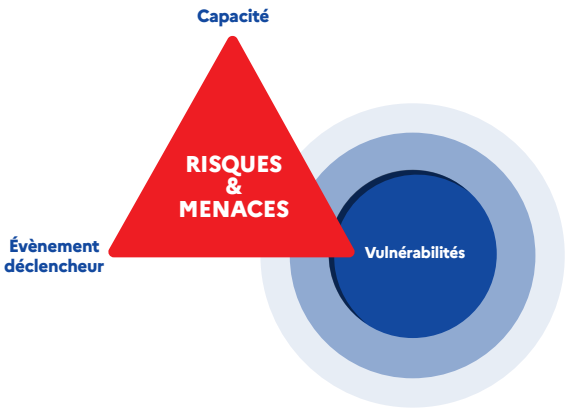


Cette démarche méthodologique permet :

- d'analyser une menace ou un risque à travers des situations de référence liées à la survenue d'un évènement déclencheur (plus probable au plus dangereux) ;
- d'identifier les effets amplificateurs en cas de concomitance des menaces et des risques ;
- de chercher à identifier les effets en cascade.

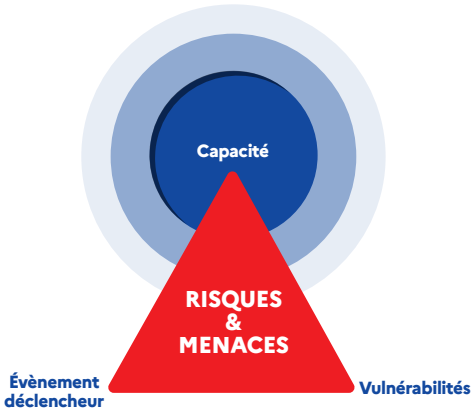
b. TYPOLOGIES DES ENJEUX ET VULNÉRABILITÉS

Les évènements déclencheurs impactent les intérêts et ressortissants français tant à l'étranger que sur le territoire national et concernent :



- les personnes (réunies ou isolées, représentatives d'une autorité, entité, communauté…) ;
- les flux :
  - rassemblements…
  - fret : transport de matières dangereuses (TMD)…
  - énergie, eau, télécommunications…
  - flux immatériels (données y compris financières, communication et réseaux sociaux) ;
- les infrastructures, en particulier :
  - les sites symboliques (établissements sanitaires et médico-sociaux, lieux de cultes, établissements d'enseignement, administrations, espaces publics) ;
  - les sites sensibles (industries, infrastructures de télécommunications…) ;
  - les sites de production et de stockage ;
- les ressources essentielles y compris économiques ;
- les vecteurs :
  - terrestres ;
  - aériens ;
  - maritimes ;
  - interfaces numériques…

Ces enjeux doivent faire l'objet de mesures de prévention et de protection, dans chacune des activités clés définies *infra*, afin de limiter tant la probabilité de survenue d'une crise majeure que son impact.



B. CAPACITÉS CRITIQUES

Pour chaque type de crise, la confrontation des risques/menaces avec les vulnérabilités, étayée par les déclinaisons territoriales existantes et les systèmes d'information dédiés, permet d'identifier **les capacités critiques** nécessaires à une réponse efficace.

Il s'agit de qualifier, pour chaque phase de la crise, les capacités nécessaires à sa résolution, que ces moyens soient détenus en propre ou fournis par des prestations contractuelles (moyens de transports, de protection, d'appui ou de soutien...).

Ils pourraient alors être :

- insuffisants ;
- indisponibles ;
- inexistants ;
- inadaptés.

Cette confrontation structurée des risques et des menaces aux crises vécues, enjeux, vulnérabilités et capacités critiques nécessaires, permet de fonder une première analyse, essentielle aux autorités responsables de la planification. Elle permet l'établissement de priorités et une réponse publique immédiate. L'articulation de cette réponse à une démarche d'anticipation permettra ensuite d'adapter les capacités à un horizon de sortie de crise établi.

La planification de défense et de sécurité nationale doit offrir, à chaque niveau de responsabilité, les moyens d'apporter une réponse ciblée et graduée permettant de revenir, quelle que soit la nature de l'évènement et pour chaque activité clé de la vie de la Nation à un niveau socialement acceptable. Ainsi, lorsqu'un évènement concerne plusieurs activités clés ou si plusieurs évènements se cumulent, le décideur dispose d'une vision globale de la crise et de sa gestion.

A. MODULARITÉ

Un référentiel de 12 activités clés et 8 fonctions de coordination, fixant une grille de lecture unifiée permet la cohérence d'ensemble des plans décrits en annexe 4 de la présente directive.

a. Activités clés et ossature de la planification de défense et de sécurité nationale

La continuité de la vie de la Nation dépend de la préservation de 12 activités clés :


sécurisation


défense militaire du territoire


sanitaire


économie


justice


social et sociétal


alimentation et eau


transports


énergies


poste et communications électroniques


numérique


international

Chaque activité clé fait l'objet d'une **stratégie de sécurité** spécifique fondée sur ses vulnérabilités propres qui vise à maintenir la continuité de l'activité, qu'elle soit concernée par l'origine de la crise ou qu'elle affronte les conséquences à titre collatéral.

Décrites en annexe 7, décomposées en sous-activités et en objectifs de sécurité à atteindre, ces stratégies élaborées par les ministères menants[5] en lien avec les ministères concourants s'appuient sur des comités existants pour faciliter leur préparation.

b. Fonctions de coordination interministérielle

En situation de crise majeure, par nature multisectorielle, ces stratégies de sécurité des activités clés sont portées par **8 fonctions de coordination,** communes à la gestion de chaque crise majeure et ainsi définies :

organisation

anticipation

gestion de l'information

logistique

juridique

finances

territoires

communication

Décrites en annexe 8, elles fondent le socle interministériel de toute réponse à une crise. Chacune dispose d'un référentiel propre pour en faciliter la compréhension commune. Ces référentiels seront adaptés en fonction des retours d'expérience.

L'ensemble, activités clés et fonctions de coordination interministérielles, permet de proposer une grille d'analyse facilitant la réponse à tous les risques et l'intégration éventuelle de nouveaux enjeux.

5 - L1141-1 du code de la défense.

B. SUBSIDIARITÉ : LES ACTEURS DE LA PLANIFICATION DE DÉFENSE ET DE SÉCURITÉ NATIONALE

Par nature interministérielle, la **planification de défense et de sécurité nationale est pilotée** :

- au **niveau national, par le secrétariat général de défense et de sécurité nationale**[6] **(SGDSN)** en coordination avec les ministères ou, en mer, avec le secrétariat général de la mer (SGmer)
- au **niveau territorial, par les préfets de zones de défense et de sécurité** en coordination avec les préfets de départements et, en mer, par le préfet maritime en coordination avec les préfets de zones et les préfets de départements (article R*122-3 du CSI) tel que décrit en annexe 5.

La planification des armées est conduite sous l'autorité du ministre des armées et du chef d'état-major des armées (CEMA) par les commandants militaires désignés, conformément au code de la défense.

Sous l'autorité du Premier ministre, qui dirige l'action du Gouvernement en matière de sécurité nationale et prépare l'action des pouvoirs publics en cas de crise majeure (article L1131-1 du code de la défense), le **SGDSN élabore la planification interministérielle de défense et de sécurité nationale et veille à son application**, notamment *via* des exercices interministériels.

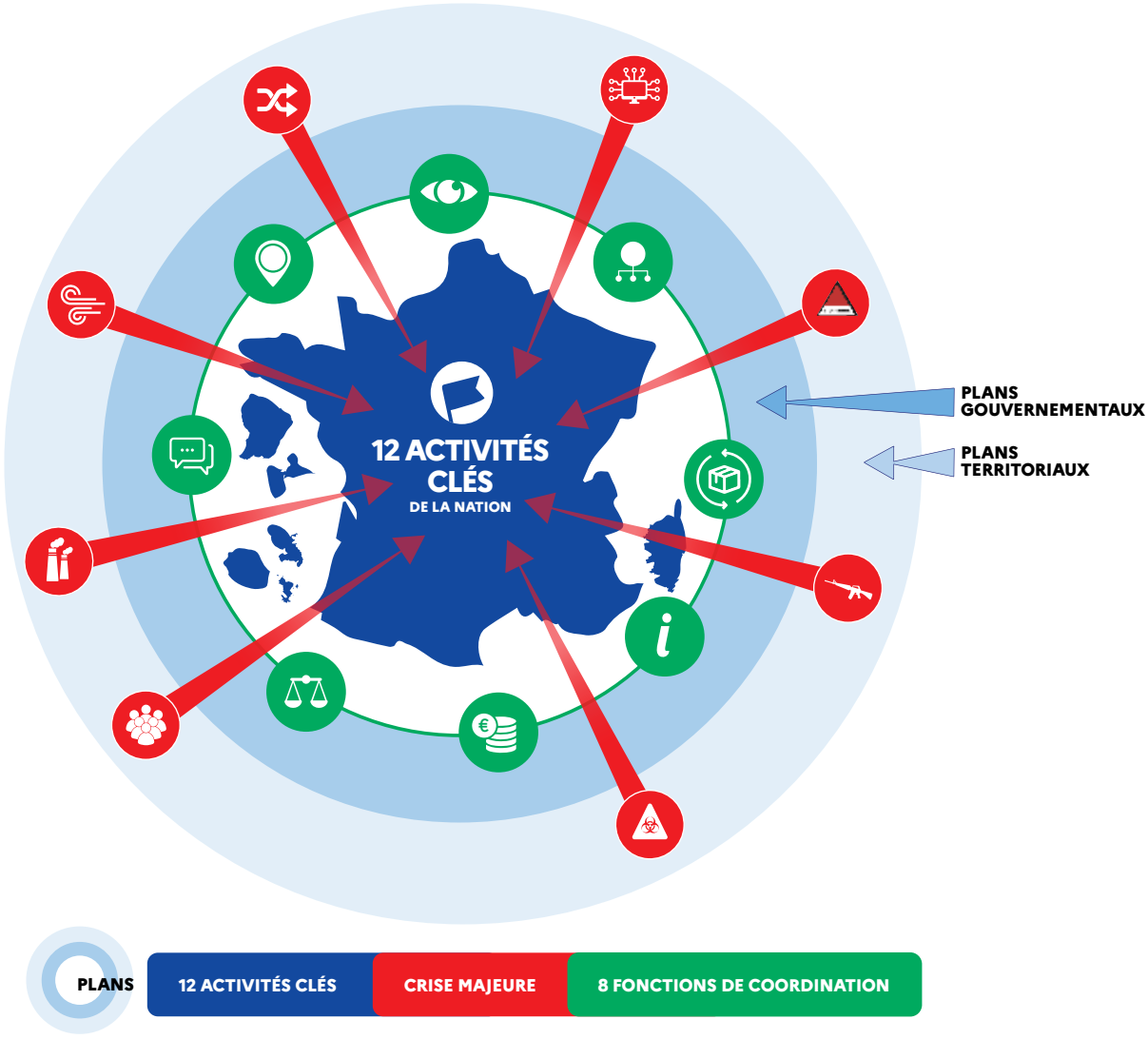
Il coordonne la préparation et la mise en œuvre des mesures de défense et de sécurité nationale incombant aux divers départements ministériels et s'assure de la coordination des moyens civils et militaires prévus en cas de crise majeure (article R*1132-3 du code de la défense).

Chaque ministre est responsable, sous l'autorité du Premier ministre, de la préparation et de l'exécution des mesures de défense et de sécurité nationale incombant au département dont il a la charge (article L1141-1 du code de la défense). Associé à la rédaction des documents établis par le SGDSN, il contribue à la planification, notamment en coordonnant celle relatives aux activités clés et aux sous-activités qui en découlent.

6 - article L1111-1 du code de la défense.

SCHÉMA DE SYNTHÈSE

La planification de défense et de sécurité nationale vise à faire face à **tous les risques et toutes les menaces** susceptibles d'affecter la **vie de la Nation. Coordonnée au niveau interministériel,** elle s'appuie sur les responsabilités et les compétences de chaque ministre.



TYPOLOGIE DES MENACES ET DES RISQUES

Menaces extérieures ou agressions armées · Attentats · Naturels · Troubles sociétaux graves (violences urbaines, migrations massives,...) · Technologiques ou industriels · Sanitaire · Cyber · Hybrides

12 ACTIVITÉS CLÉS

Poste et communication électronique · Numérique · Énergies · International · Économie · Social et sociétal · Alimentation et eau · Sécurisation · Transports · Justice · Sanitaire · Défense militaire du territoire

8 FONCTIONS DE COORDINATION

Anticipation · Organisation · Logistique · Gestion de l'information · Finances · Juridique · Communication · Territoire

Les efforts de prévention pour réduire les menaces et les risques ou les vulnérabilités face à des évènements catastrophiques majeurs, s'ils sont absolument nécessaires, ne sauraient cependant les interdire. La réponse à ces catastrophes, quant à elle, impose toujours un engagement massif de l'ensemble des ressources mobilisables ainsi qu'une méthodologie d'anticipation.

En application du principe de subsidiarité, la planification de défense et de sécurité nationale est établie par l'autorité immédiatement responsable de sa mise en œuvre, en liaison avec les principaux acteurs concernés[7]. Elle décrit l'organisation à mettre sur pied et les stratégies préventives, réactives, curatives et proactives à développer. Elle fixe un vocabulaire commun quant aux objectifs à atteindre à chaque phase selon un modèle préalablement défini.

Elle est un outil d'aide à la décision, qui doit à la fois être synthétique et couvrir l'ensemble du spectre des réponses à une crise. Elle s'articule en deux parties[8] :

- une analyse des enjeux :
  - étude préalable pour identifier les enjeux et vulnérabilités associés à un évènement déclencheur ou une crise majeure (annexes 2 et 3) ;
  - identification des ressources, des capacités initiales et de leur disponibilité à l'emploi ;
  - éléments de compréhension de cette situation lorsqu'elle survient ;
  - cartographie des acteurs, clarifiant notamment la répartition des responsabilités (annexe 5).
- un guide d'aide à la décision :
  - formulation d'une stratégie de réponse, y compris pour la communication publique ;
  - élaboration des objectifs à atteindre et des mesures associées, par phase, en fonction des options retenues, sur la base d'une posture globale de sécurité (annexes 7 et 8).

A. LA STRATÉGIE DE RÉPONSE

La stratégie de réponse d'ensemble à une crise majeure consiste à :

- agir sur sa cause, quand cela est possible, pour contenir l'intensité, l'étendue géographique ou temporelle de l'évènement ;
- gérer les impacts sur le fonctionnement des activités clés et en assurer *in fine*, un fonctionnement socialement acceptable avec l'adhésion de la population.

Elle peut être complétée par les planifications *ad hoc* en fonction de leurs enjeux spécifiques, en particulier quant aux moyens à mettre en œuvre pour obtenir les effets escomptés.

Les objectifs de sécurité de chacune des activités clés sont déclinés en mesures destinées à faire face à un évènement ou à la survenue d'une crise majeure et sont consultables

7 - Notamment selon les limites de délégations de service public.

8 - Cette structuration vaut pour la planification interministérielle. Les planifications sectorielles, en particulier militaires, suivent leurs contraintes propres quant à la forme à adopter.

dans le « **catalogue unifié des objectifs de défense et de sécurité** ». Ces mesures peuvent être déclinées dans le temps par :

- ***Secteur :* avec une réponse par secteur d'activité.** La mise en œuvre de ce levier relève du seul ministère de tutelle.
- ***Catégorie :* avec une réponse liée aux catégories de personnes** (personnes vulnérables, enfants, actifs, cas contact, etc…).
- ***Géographie :* avec une adaptation de la réponse aux spécificités des territoires** (réponse nationale, régionale, départementale, ultramarine, insulaire). L'activation de ce levier est souvent laissée à l'appréciation des autorités locales (maire, préfets…).

Ainsi, les mesures prises participent à l'amélioration de la situation initiale et tentent d'en limiter l'impact sur les autres activités clés au travers de décisions fondées sur :

- **des indicateurs** sectoriels, catégoriels et/ou géographiques constatant le besoin et/ou l'efficacité des mesures ;
- **des évaluations régulières** pour pondérer les éventuels impacts inédits.

B. UNE POSTURE GLOBALE DE SÉCURITÉ

L'ensemble des mesures activées constitue la posture globale de sécurité. Elle se structure autour :

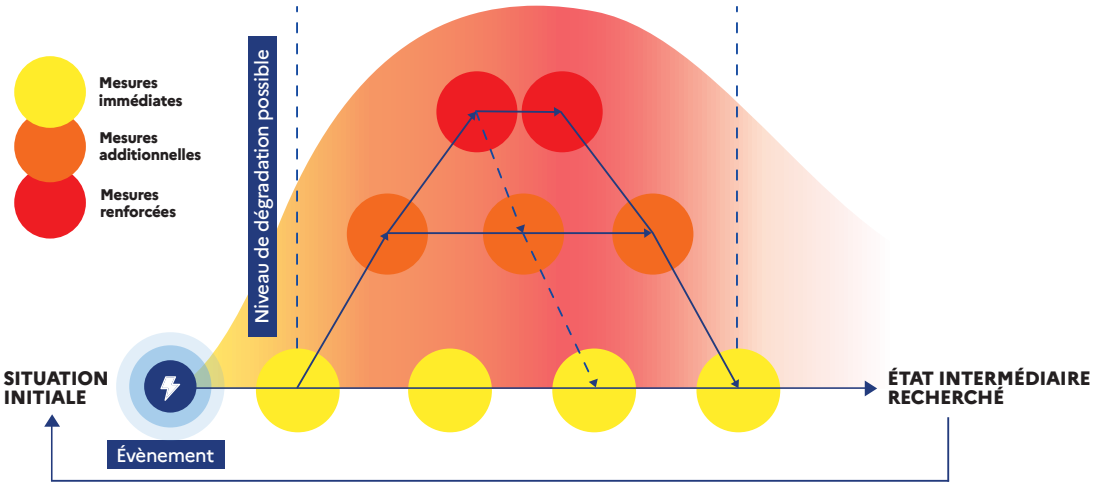
- d'une **posture socle de sécurité**, qui regroupe des mesures de prévention soutenables, destinée à entretenir la vigilance sans perturber les activités administratives, économiques et sociales usuelles ;
- de **mesures additionnelles** activées en fonction de l'état des risques et des menaces.

4. STRATÉGIE ET PROCESSUS DÉCISIONNEL

C. PROCESSUS DÉCISIONNEL

Au sein de chaque phase de la réponse à une crise, des situations envisageables sont alors établies par anticipation, le cas échéant avec le concours d'un collège d'experts pluridisciplinaires.

La révision des mesures, aux niveaux départemental, zonal et/ou national, s'apprécie **avec un pas de temps fixé préalablement en fonction de la nature de la crise et de sa cinétique.** En cas d'évolution des indicateurs permettant d'objectiver un changement de situation, une adaptation de la planification et/ou des mesures doit être proposée. Cette démarche prend alors la forme suivante :



Fait à Paris le 23 Janvier 2023

La Première ministre
Élisabeth BORNE

ANNEXES

ANNEXE 1 : GLOSSAIRE

***Activité clé* :** activité essentielle à la continuité de la vie de la nation.

***Aléa* :** manifestation d'un phénomène naturel ou anthropique.

***Capacités critiques* :** capacités humaines, matérielles ou immatérielles, indispensables pour apporter une réponse efficace lors de la survenue d'un évènement déclencheur. **Détenues en propre ou par des prestations contractuelles (moyens de transports, de protection, d'appui ou de soutien…) elles peuvent être identifiées et différenciées pour chaque phase de la crise**.

***Crise* :** la crise désigne un ensemble de phénomènes plus ou moins intenses et durables qui met en danger ou en péril les organisations, dont elle perturbe le fonctionnement normal ou interrompt des activités essentielles, en y provoquant des pertes et des dommages inacceptables. Pour ces organisations, la crise met en tension quatre capacités :

- la compréhension et le discernement d'une situation complexe ou inédite ;
- la conception d'une réponse adaptée ;
- la disposition à temps des ressources nécessaires en qualité et en quantité ;
- la mise en œuvre de ces ressources dans des conditions anormalement contraignantes et leur contrôle.

***Crise majeure* :** une crise est qualifiée de majeure lorsque l'étendue des phénomènes qui la caractérisent et l'intensité des troubles et transformations qui en résultent conduisent à des pertes et des dommages socialement inacceptables. Les seuils correspondants en termes d'étendue, d'intensité et d'acceptabilité sociale relèvent d'une appréciation à la fois technique (nombre ou dimension des collectivités territoriales concernées, quantité de victimes, pertes matérielles et économiques constatées et prévisibles, caractère vital des activités ou du secteur d'activité concerné, mise en jeu d'interdépendances, dépassement des capacités locales de gestion de crise…) et politique (réaction des populations, engagements vis-à-vis des partenaires, position de principe des pouvoirs publics…) de l'État.

***Elément déclencheur / source* :** tout élément qui, seul ou combiné à d'autres, présente un potentiel intrinsèque susceptible de concrétiser un risque ou une menace.

***Enjeux* :** Intérêts humains, politiques, environnementaux, culturels, économiques et sociaux menacés par un risque ou une menace.

***Impact* :** effet d'un évènement affectant les objectifs.

***Menace* :** manifestation signifiant une intention hostile, le projet de nuire.

ANNEXE 1 : GLOSSAIRE

Objectif de sécurité : effet à obtenir en termes de vigilance et de protection contre les risques ou les menaces pour réduire les vulnérabilités dans un domaine d'activité particulier.

Risque : probabilité d'occurrence d'un évènement ayant des conséquences positives ou négatives sur l'atteinte des objectifs qu'une organisation poursuit. Il est souvent exprimé en termes d'impact et de probabilité d'occurrence. Il s'agit de l'exposition à un aléa.

Risque majeur : on parle de risque majeur face à un risque dont les effets peuvent mettre en jeu un grand nombre de personnes, occasionner des dommages importants et dépasser les capacités de réaction de la société. Un risque majeur est caractérisé par sa faible fréquence et par son énorme gravité. L'existence d'un risque majeur est liée :

- d'une part, à la présence d'un évènement, qui est la manifestation d'un phénomène naturel ou anthropique dit aléa ;
- d'autre part, à l'existence d'enjeux, qui représentent l'ensemble des personnes et des biens (ayant une valeur monétaire ou non monétaire) pouvant être affectés par un phénomène. Les conséquences d'un risque majeur sur les enjeux se mesurent en termes de vulnérabilité.

Stratégie de sécurité : elle vise à organiser un dispositif garantissant pour chaque activité clé une action de maintien de sa continuité quelles que soient les circonstances, en s'appuyant sur des moyens techniques et une planification adaptée. Pour cela, il s'agit d'identifier les vulnérabilités et de définir les objectifs à atteindre. Chaque objectif est décrit dans des fiches présentant des mesures à mettre en place.

Vulnérabilité : sensibilité à un risque ou une menace.

ANNEXE 2 : RÉPARTITION DES RESPONSABILITÉS DE L'ÉVALUATION DES PRINCIPAUX RISQUES ET MENACES

Liste des principaux risques et menaces	Responsabilités	Évaluation nationale	Planification nationale (coord. SGDSN)
1. Menaces			
▷ **Agressions armées d'origine étatique**	MINARM (menant) et ensemble des ministères (concourant)[9]	Services	*Planification qui relève du MINARM*
▷ **Menaces pouvant conduire à une atteinte grave à l'ordre public et à la continuité de l'État (émeutes, troubles graves, dégradation ou interruption d'une activité essentielle)**	MIOM (menant)[10] et ensemble des ministères (concourant)	Services du premier et du deuxième cercle dont DCSP/SCRT[11]	Guide dédié à la constitution des plans de continuité d'activité ministériels, plans spécifiques consacrés à la continuité de l'État et à l'action gouvernementale
▷ **Terrorisme de toutes natures**	CNRLT[12], SGDSN[13] et ensemble des ministères	Évaluation de la menace terroriste, postures Vigipirate Évaluations du MIOM Groupes spécifiques	Famille Pirate NRBC
▷ **Menaces touchant les ressortissants français à l'étranger**	MEAE[14], MINARM	Plans de sécurité des postes à l'étranger en lien avec la planification MINARM/CPCO et le CDCS	Piratext

9 - Le ministre de la défense est responsable de la préparation et de la mise en œuvre de la politique de défense. Il est également chargé de l'anticipation et du suivi des crises intéressant la défense (article L1142-1 du code de la défense).

10 - Le MIOM est chargé de l'anticipation et du suivi des crises susceptibles d'affecter la sécurité intérieure et la sécurité civile. Il contribue à la planification interministérielle en matière de sécurité nationale. Il prépare les plans à dominante d'ordre public, de protection et de sécurité civiles. Il est responsable du renseignement intérieur, sans préjudice des compétences des ministres chargés de l'économie et du budget (article L1142-2 du code de la défense).

11 - Dans le cadre de sa mission de renseignement, la direction centrale de la sécurité publique est chargée, sur l'ensemble du territoire national à l'exception de Paris et des départements des Hauts-de-Seine, de la Seine-Saint-Denis et du Val-de-Marne, de la recherche, de la centralisation et de l'analyse des renseignements destinés à informer le Gouvernement et les représentants de l'État dans les collectivités territoriales de la République dans les domaines institutionnel, économique et social ainsi que dans tous les domaines susceptibles d'intéresser l'ordre public, notamment les phénomènes de violence. En lien avec les services chargés de la lutte contre le terrorisme et sans préjudice de leurs attributions, la direction centrale de la sécurité publique contribue à la mission de prévention du terrorisme. Ces missions s'exercent sur l'ensemble du territoire des départements et collectivités, en coordination avec la gendarmerie nationale. La direction centrale de la sécurité publique concourt, à ce titre, à l'exercice des missions de renseignement et d'information confiées aux forces de sécurité intérieure (article 21 du décret n° 2013-728 du 12 août 2013 portant organisation de l'administration centrale du ministère de l'intérieur et du ministère des outre-mer).

12 - La CNRLT est chargé de l'analyse globale de la menace et propose sur cette base au Président de la République les orientations du renseignement et de la lutte contre le terrorisme, et les priorités d'actions coordonnées, que celui-ci fixe aux services (article R*1122-8-1 du code de la défense).

13 - L'article R*1132-3 du code de la défense dispose : « En appui du coordonnateur national du renseignement et de la lutte contre le terrorisme, [le SGDSN] concourt à l'adaptation du cadre juridique dans lequel s'inscrit l'action des services de renseignement et à la planification de leurs moyens et assure l'organisation des groupes interministériels d'analyse et de synthèse en matière de renseignement ».

14 - Le MEAE coordonne la gestion des crises extérieures ainsi que la planification civile de celles-ci avec le concours de l'ensemble des ministères et des services de l'État concernés (article L1142-6 du code de la défense).

ANNEXE 2 : RÉPARTITION DES RESPONSABILITÉS DE L'ÉVALUATION DES PRINCIPAUX RISQUES ET MENACES

Liste des principaux risques et menaces	Responsabilités	Évaluation nationale	Planification nationale (coord. SGDSN)
▷ **Cyber menaces**	ANSSI	Services, ANSSI, MIOM	Piranet
▷ **Menaces hybrides**	SGDSN (point de contact national)	CNRLT, MEAE, MINARM, MIOM, ANSSI, VIGINUM	Document de référence interministériel sur les stratégies hybrides
▷ **Manipulation de l'information**	SGDSN	CNRLT, MEAE, MINARM, MIOM	Doctrine « lutte contre les manipulations de l'information »
2. Risques			
▷ **Naturels (cyclone, inondation, séisme, etc.)**	MTE (menant)[15] MIOM, MINARM, MASA (concourant)	Missions de la direction générale de la prévention des risques du MTE[16] *(pollutions chimiques, biologiques et radioactives ; risques liés à l'activité humaine et aux aléas naturels et à la prévision des crues). Elle exerce la coordination interministérielle des politiques de prévention des risques majeurs, de lutte contre le bruit et de gestion des déchets)*	Plan gouvernemental Crue de Seine
▷ **Technologiques et industriels (accident nucléaire, rupture de barrage, pollution maritime, etc.)**	MTE (menant) MIOM, MINARM (concourant)	Missions de la direction générale de la prévention des risques du MTE	Plan accident nucléaire ou radiologique majeur Plan continuité électrique
▷ **Sanitaires (épidémie, épizootie, etc.).**	MSP[17]	Missions de la direction générale de la prévention des risques du MTE Ministère de la Santé et des solidarités	Plan Ebola Plan Pandémie grippale Plan Variole Futur plan « pandémies générique »

15 - Les ministres chargés de l'environnement, des transports, de l'énergie et de l'industrie sont responsables, chacun en ce qui le concerne, en matière de maîtrise des risques naturels et technologiques, de transports, de production et d'approvisionnements énergétiques ainsi que d'infrastructures, de la satisfaction des besoins de la défense et de la sécurité nationale et, en toutes circonstances, de la continuité des services (article L1142-9 du code de la défense).

16 - Cf. article 8 du décret n° 2008-680 du 9 juillet 2008 portant organisation de l'administration centrale du ministère de l'écologie, de l'énergie, du développement durable et de l'aménagement du territoire : « *la direction générale de la prévention des risques est chargée de l'élaboration et de la mise en œuvre de la politique relative : à la connaissance, l'évaluation, la prévention et la réduction des pollutions chimiques, biologiques et radioactives, et des diverses nuisances sur l'environnement, notamment du bruit ; à la connaissance, l'évaluation et la prévention des risques liés à l'activité humaine et aux aléas naturels et à la prévision des crues ; aux conditions d'évaluation de la qualité écologique des sols et de l'atmosphère et à la prévention de la production de déchets, à leur valorisation et à leur traitement. Elle exerce la coordination interministérielle des politiques de prévention des risques majeurs, de lutte contre le bruit et de gestion des déchets* ».

17 - Le ministre chargé de la santé est responsable de l'organisation et de la préparation du système de santé et des moyens sanitaires nécessaires à la connaissance des menaces sanitaires graves, à leur prévention, à la protection de la population contre ces dernières, ainsi qu'à la prise en charge des victimes. Il contribue à la planification interministérielle en matière de défense et de sécurité nationale en ce qui concerne son volet sanitaire (article L1142-8 du code de la défense).

ANNEXE 3 : TYPOLOGIE DES MENACES ET DES RISQUES[18]

MENACE : MENACE EXTÉRIEURE, AGRESSION — TM1

1. Nature

La menace extérieure et l'agression peuvent se matérialiser dans tout ou partie des milieux et champs. Elles peuvent appeler une réponse d'abord militaire de l'État. En cas de difficulté d'attribution ou de caractérisation (notamment en cas de mise en œuvre d'une stratégie hybride), elles devront être préalablement reconnues en conseil de défense et de sécurité nationale (CDSN).

2. Acteurs défavorables

Acteur extérieur, qu'il soit ou non étatique, soutenant ou conduisant des actions hostiles contre le territoire national, y compris les outremers, et ses approches.

3. Vulnérabilités

- L'ennemi cherchant à atteindre nos instruments de puissance, en exploitant nos vulnérabilités matérielles et immatérielles. l'ensemble des secteurs d'activité d'importance vitale, au premier rang desquels ceux intéressant la défense, peut donc faire l'objet d'actions militaires ciblées. L'ennemi peut également viser des cibles seulement symboliques, dans le cadre d'une manœuvre stratégique d'influence.

4. Gradation possible et modes opératoires

Les modes opératoires envisageables couvrent un spectre allant de l'intimidation à la guerre ouverte.

La crise peut se matérialiser, en métropole comme en outre-mer, dans les milieux terrestre, maritime, aérien, exo-atmosphérique, et les champs immatériels (cyber, informationnel et électromagnétique).

5. Conséquences possibles

Acteurs publics

- Les conséquences de cette crise sont susceptibles d'affecter tous les acteurs publics et peuvent nécessiter la mise en œuvre coordonnée de tout ou partie des mesures prévues au titre des douze activités-clés décrites en annexe 7.
- En fonction de la menace, des mesures de mobilisation et d'adaptation du cadre juridique peuvent s'avérer nécessaires, notamment pour amoindrir les vulnérabilités identifiées (occurrence et conséquence). Ainsi, cette crise peut entraîner la déclaration des régimes d'application de circonstances exceptionnelles listés au point 6 et/ou la mise en œuvre de mesures particulières de défense du territoire. Dans le milieu terrestre, la responsabilité de l'ordre public et de la coordination des mesures de défense civile avec les mesures militaires de défense pourrait être transférée, dans les seules zones où se développeraient des opérations militaires et pour la durée de ces opérations, à une autorité militaire. Le reste des activités resterait sous la responsabilité de l'autorité civile compétente.

Opérateurs

Les conséquences de cette crise sont susceptibles d'affecter tous les opérateurs et de nécessiter le renforcement des mesures de protection (dont les PPP/PPE) et la mise en œuvre des PCA. L'État pourra appuyer sa réponse sur des réquisitions, voire des mesures de mobilisation.

6. Cadre juridique et référence documentaire

18 - Les fiches de cette annexe sont remplies sur la base des responsabilités décrites en annexe 2.

Constitution : article 16, guerre (article 35), état de siège (article 36).

Code de la défense : état de siège (articles L.2121-1 à L.2121-8), état d'urgence (article L.2131-1), mise en garde (articles L.2141-1 et L.1311-1), mobilisation (articles L.2141-1 à L.2141-4), défense opérationnelle du territoire (articles R.*1422-1 à R.*1422-4), défense maritime du territoire (articles D.*1431-1 à D.*1432-5), défense aérienne (articles D.*1441-1 à D.*1442-6), caractérisation et réaction à une crise cyber (article L.2321-4).

7. Indicateurs et contrôles de l'exécution

Pour prévenir ce type de crise, la DRM assure un dispositif de veille-alerte à l'étranger, en coordination avec la DGSE, en employant des capteurs nationaux et par le biais de partenariats « renseignement », notamment avec les alliés de l'OTAN.

8. Planifications en lien

Plans particuliers de protection (PPP), plans de protection externe (PPE), plan de continuité d'activité (PCA).

Plans de défense opérationnelle du territoire (DOT), plans de défense maritime du territoire (DMT), plan militaire de défense aérienne (PMDA), plan militaire de défense cybernétique (PMDC).

9. Commentaires

ANNEXE 3 : TYPOLOGIE DES MENACES ET DES RISQUES

MENACE : ATTENTATS POSSIBLEMENT NRBC — TM2

1. Nature

La France est confrontée à un niveau de menace à l'intensité durablement élevée, émanant de groupes extrémistes de toutes natures. À la fois diffuse et omniprésente, agissant à l'extérieur comme à l'intérieur du territoire national, cette menace est ponctuée de pics de crise constitués par les attaques majeures.

2. Acteurs défavorables

Les mouvements extrémistes de toutes natures :

- djihadisme (projet commandité ou acteurs isolés) ;
- mouvements ultras (droites, gauches, veggie-pirates…) ;
- mouvements séparatistes (groupes régionalistes indépendantistes français voire étrangers) ;
- mais aussi les personnes atteintes de troubles psychologiques.

3. Vulnérabilités

Les mouvements extrémistes visent une multitude de cibles potentielles au caractère symbolique :

- les représentants de l'État, dépositaires de l'autorité publique, et les représentants des cultes ;
- l'espace public fortement fréquenté, notamment les espaces commerciaux, les lieux de culte, d'enseignement, les tribunaux, les administrations ou les rassemblements ;
- les infrastructures critiques ;
- les moyens ou les infrastructures de transports ;
- les établissements sanitaires et médico-sociaux.

Mais aussi tout citoyen de manière aléatoire.

4. Gradation possible et modes opératoires

- Détournement d'un moyen de transport (train, bateau à passagers, avion).
- Tuerie de masse.

Les modes d'action suivants peuvent également être utilisés :

- artisanaux (véhicule bélier/arme blanche/arme à feu/ explosif de fabrication artisanale) ;
- NRBC ;
- prise d'otage ;
- attaque ciblée sur des personnes ou des lieux symboliques.

5. Impacts possibles

Acteurs publics

- engagement de l'ensemble des forces de sécurité intérieure, des moyens de la sécurité civile, des armées, de la santé et des partenaires internationaux ;
- réorganisation des services (renforts, rappel de personnels) ;
- nécessité de prioriser et de communiquer.

Opérateurs

- policiers municipaux / acteurs de la sécurité privée.
- responsables des ERP.

6. Cadre juridique et référence documentaire

- article L 1142-2 du code de la défense : **le ministre de l'intérieur** est chargé de l'anticipation et du suivi des crises susceptibles d'affecter la sécurité intérieure et la sécurité civile ;
- code pénal et de procédure pénale ;
- état d'urgence ;
- mesures loi SILT.

7. Indicateurs et contrôles de l'exécution

- dispositif Vigipirate fixant le niveau d'alerte associé à cette menace ;
- informations provenant de la communauté du renseignement (CNRLT).

8. Planifications en lien

- plans de la famille PIRATE.
- plan NRBC.
- schéma national d'intervention SNI.
- plan ORSEC/ COTRRiM.
- plan ORSAN / Situations Sanitaires Exceptionnelles.
- plan de gestion des décès massifs.
- bilan victimaire.

9. Commentaires

CCI NRBC

ANNEXE 3 : TYPOLOGIE DES MENACES ET DES RISQUES

MENACE : TROUBLES SOCIÉTAUX GRAVES — TM3

1. Nature

Les tendances observées au repli communautaire ou identitaire, pouvant aller qu'au séparatisme, ainsi que les revendications sociales violentes, combinées à des activités délinquantes, déstabilisent certaines zones du territoire national. Les phénomènes de contestation violente qui y ont cours sont susceptibles de dégénérer en émeute.

2. Acteurs défavorables

- groupes mettant en œuvre des stratégies de black bloc.
- mouvements contestataires extrémistes.
- mouvements identitaires.
- bandes violentes.

3. Vulnérabilités

Les symboles institutionnels pourraient être visés et les forces de sécurité prises à partie de façon délibérée. En outre un nombre de grands évènements au sens de l'article L 211-11-1 du CSI[19] médiatisés, rassemblant d'importantes foules, à caractère culturel, sportif ou politique (sommets de chefs d'État, de gouvernements ou internationaux), susceptibles de se produire sur plusieurs sites géographiques peuvent également faire l'objet de menaces spécifiques donnant lieu à des troubles à l'ordre public avec potentielle atteinte aux flux économiques.

4. Gradation possible et modes opératoires

- manifestations et grands évènements à risque : des manifestations sociales d'ampleur nationale ou régionale à répétition peuvent générer un risque de paralysie voire de contagion et de convergence des luttes. La cinématique rapide de la détérioration de la situation peut s'inscrire dans le temps long ;
- troubles de type insurrectionnel : des contestations violentes sur certaines zones du territoire national (quartiers sensibles, revendications autonomistes parfois aggravées par une tendance au repli communautaire). Ces troubles s'inscrivent dans une cinématique relativement lente avec des pics de violence ;
- flux migratoires massifs : un afflux majeur, à l'intérieur du territoire, de populations immigrées en situation irrégulière est susceptible de susciter des tensions avec les forces de sécurité parallèlement à une crise humanitaire. Ces flux s'inscrivent dans le temps long ;
- à l'étranger : la situation internationale pourrait localement mettre en cause l'intégrité des ressortissants ou des intérêts français à l'étranger.

5. Impacts possibles

Acteurs publics

- sous l'autorité des préfets, engagement de l'ensemble des forces de sécurité intérieure, des moyens de la sécurité civile et des services de renseignement territoriaux :
  - réorganisation des services (renforts, rappel de personnels) ;
  - activation si nécessaire des PCA.
- collectivités territoriales

Opérateurs

- policiers municipaux / acteurs de la sécurité privée.
- responsables d'ERP. Fédérations et associations professionnelles de commerçants.
- associations.

19 - La notion de « grands événements » s'entend au sens MI avec une programmation dans le temps (G7, Euro16, JOP24, etc.)

6. Cadre juridique et référence documentaire

- article L 1142-2 du code de la défense : le ministre de l'intérieur est chargé de l'anticipation et du suivi des crises susceptibles d'affecter la sécurité intérieure et la sécurité civile.
- état d'urgence.

7. Indicateurs et contrôles de l'exécution

- informations des services de renseignements, notamment du renseignement territorial (SCRT).
- réseaux des attachés de sécurité intérieure (ASI) de la DCIS dans le cadre du suivi des événements à l'étranger.

8. Planifications en lien

- schéma national de maintien de l'ordre.
- plan de gestion des désordres intérieurs graves.
- plan de déplacement massif de population.
- plan PIRATEXT.

9. Commentaires

ANNEXE 3 : TYPOLOGIE DES MENACES ET DES RISQUES

MENACE : CYBER — TM4

1. Nature

La multiplication des cyberattaques se révèle être une nouvelle source de vulnérabilité en raison de la dépendance généralisée des organisations aux outils numériques et systèmes d'information.

L'atteinte au fonctionnement des systèmes numériques des acteurs privés comme publics est rapidement visible et pose des enjeux de continuité d'activité. Les cyberattaques majeures peuvent ainsi perturber voire désorganiser les activités essentielles de la société (communication numérique, santé, chaines d'approvisionnements, etc.).

La gravité d'une crise peut être accentuée par l'effet de dysfonctionnements en cascade, lié à l'interconnexion des systèmes.

2. Eléments déclencheurs possibles

- forces étrangères.
- cybercriminels.
- « hacktivistes ».

3. Vulnérabilités

- les cibles varient en fonction du profil et des objectifs des attaquants.
- cybercriminalité : mise à mal du fonctionnement des systèmes d'information de toute organisation privée/publique et récupération des données hébergées sur ces systèmes.
- destruction et déstabilisation : mise à mal du fonctionnement des systèmes d'information des secteurs d'importance vitale et des institutions publiques et récupération ou destruction des données hébergées sur ces systèmes.
- espionnage étatique : récupération des données hébergées sur les systèmes d'information des secteurs d'importance vitale et des institutions publiques.

4. Gradation possible et modes opératoires

- des attaques, motivées par l'argent et organisées par des groupes de cybercriminalité, qui peuvent préfigurer des crises ou avoir un effet aggravant sur d'autres crises.
- des tentatives de pénétration de systèmes d'information à des fins d'espionnage conduites par des forces étrangères.
- des attaques visant la prise de contrôle et la mise à mal du fonctionnement de systèmes d'information d'importance vitale.
- des attaques rendant indisponibles les services d'institutions à des fins activistes.
- des attaques de grande ampleur contre les systèmes d'information nationaux, dans un scenario de guerre informatique mettant à mal la continuité des services rendus à la Nation et la confiance dans l'utilisation des outils numériques.

5. Impacts possibles

Acteurs publics

- les conséquences d'une ou plusieurs cyberattaques (arrêt des systèmes, données indisponibles) sont susceptibles d'affecter la continuité des services rendus par chaque acteur public et ainsi impacter la confiance citoyenne dans les institutions. L'interconnexion des systèmes peut accentuer le périmètre d'impact de l'attaque.
- tout ministère impacté par une cyberattaque est chargé via son centre opérationnel, de remonter des informations et prendre les mesures nécessaires pour assurer la continuité de ses activités.
- l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) est notamment en charge d'apporter des éléments de compréhension sur l'attaque et d'orienter et piloter la stratégie de réponse cyber auprès des victimes.
- Le COMCYBER des armées et le COMCYBERGEND peuvent contribuer à l'action de l'ANSSI.
- les fonctionnaires de sécurité des systèmes d'information (FSSI) sont notamment chargés d'apporter des éléments de compréhension sur le périmètre et les impacts de l'attaque et de coordonner la stratégie de réponse cyber de leur ministère de tutelle.
- en parallèle, le centre de coordination contre les cyberattaques (C4) est chargé d'assurer la réponse à la cause des incidents cyber.

Opérateurs

- les conséquences d'une ou plusieurs cyberattaques (arrêt des systèmes, données indisponibles) sont susceptibles d'affecter la continuité d'activité de tout opérateur, avec des impacts particuliers dans les secteurs d'importance vitale. L'interconnexion des systèmes peut accentuer le périmètre d'impact de l'attaque.
- les opérateurs victimes d'une cyberattaque sont chargés de mettre en place un plan de remédiation cyber et d'assurer la continuité de leur activité, en lien avec la chaine étatique.
- les opérateurs d'un secteur ciblé peuvent décider d'actions annexes afin de renforcer la sécurité de leurs systèmes.

6. Cadre juridique et référence documentaire

- article L.1332-6-1 et suivants du code de la défense.
- article R.1132-3 du code la défense.
- article L.2321-1 du code de la défense Article 3 du décret n° 2009-834 du 7 juillet 2009.
- article R.1132-3.
- article D98-7 du code des postes et des communications électroniques.
- loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 (LPM 2014-2019) et portant diverses dispositions concernant la défense et la sécurité nationales, notamment les articles 21 et 22 de la LPM 2014-2019.

7. Indicateurs et contrôles de l'exécution

/

8. Planifications en lien

- plan PIRANET
- plan VIGPIRATE

9. Commentaires

ANNEXE 3 : TYPOLOGIE DES MENACES ET DES RISQUES

MENACE : HYBRIDE — TC 5

1. Nature

Une stratégie hybride s'entend comme le recours par un acteur étatique ou non à une combinaison intégrée et volontairement ambiguë de modes d'actions militaires et non militaires, directs et indirects, légaux ou illégaux, difficilement attribuables. Jouant avec les seuils estimés de riposte et de conflit armé, cette combinaison est conçue pour contraindre et affaiblir l'adversaire, voire créer chez lui un effet de sidération.

Par ces méthodes, nos compétiteurs stratégiques continuent les combats sous une autre forme (terrorisme, harcèlement, cyberattaques, guerre informationnelle et division de nos opinions publiques), allant jusqu'à préparer les conditions de réussite des opérations futures (potentiellement de guerre) qu'ils auront à mener. Cette action peut passer par l'affaiblissement de la résolution adverse à agir/intervenir, la contradiction légale/juridique de l'action adverse, des capacités d'entrave multi-domaines — cyber, paramilitaire, spatial, informationnel, économique — en parallèle de moyens d'action plus conventionnels (déni d'accès, technologies défensives). À certains égards, les stratégies mises en œuvre par des organisations criminelles ou terroristes fortement structurées relèvent d'une logique hybride (actions combinant moyens civils et militaires, implantation transrégionale, concurrence à l'action de l'État, objectifs de déstabilisation).

2. Eléments déclencheurs possibles

- acteurs étatiques.
- organisations criminelles.
- organisations terroristes.

3. Vulnérabilités

Plusieurs vulnérabilités peuvent être identifiées comme susceptibles d'être ciblées par des stratégies hybrides :

- la légitimité, le fonctionnement des institutions politiques démocratiques ainsi que les valeurs qui les fondent : l'adversaire cherche à affaiblir en attaquant la légitimité de l'État et de ses institutions, en affaiblissant la souveraineté (notamment par prédation dans les DROM/COM et dans notre ZEE), en sapant les processus de décision et d'action publique, et en perturbant les processus électoraux.
- la cohésion sociale et les équilibres sociétaux : il s'agit de miner la cohésion de la société et des modes de vie par l'exploitation, voire l'aggravation, de clivages sociopolitiques, socio-économiques ou du communautarisme. Les acteurs hostiles peuvent viser à déstabiliser la société via la suggestion, le soutien, l'organisation ou la supervision d'actions troublant l'ordre public.
- la robustesse de l'économie nationale : acquisition d'entreprises dans des secteurs stratégiques, entraves à leurs activités, ou encore captations de ressources dans notre ZEE remettant en cause la capacité de l'État à assurer le contrôle de ses espaces souverains.
- la conduite de nos opérations extérieures et l'intégrité de nos dispositifs outre-mer et à l'étranger.

La menace hybride possède par nature un caractère global. Elle peut viser nos intérêts sur le territoire national comme hors des frontières et dans l'espace extra-atmosphérique. Elle multiplie les possibilités pour un adversaire, en recourant notamment aux nouvelles technologies, de provoquer le dysfonctionnement grave de plateformes portuaires/aéroportuaires, d'une place financière, d'un ministère, d'une compagnie de transport maritime, la rupture des chaînes logistiques d'approvisionnement, la destruction ou le pillage d'un serveur, voire l'isolement numérique total d'un pays. Si les attaques sont le plus souvent de basse intensité, elles peuvent malgré tout être graves et déstabilisantes.

De ce fait, la menace ne concerne pas exclusivement les ministères régaliens et ne doit pas être traitée uniquement en réaction à une agression manifeste.

4. Gradation possible et modes opératoires

Le cadre conceptuel sur les menaces hybrides, adopté au niveau européen en décembre 2020, recense de manière exhaustive les 13 domaines dans lesquels peuvent se déployer des stratégies hybrides et les vulnérabilités associées. Ces domaines sont les infrastructures, notamment critiques, le cyber, l'espace, l'économie, le domaine militaire et de défense, la culture, le domaine sociétal, l'administration publique, le champ légal et juridique, le renseignement, la diplomatie, le politique et la sphère informationnelle. La France identifie cinq domaines d'action prioritaire dans lesquels elle souhaite porter ses efforts :

- le cyber ;
- le champ informationnel ;
- l'utilisation stratégique de l'arme normative, notamment juridique (*lawfare*) ;
- le champ économique et financier ;
- le champ opérationnel.

5. impacts possibles

Acteurs publics

Si toutes les activités clés peuvent être plus particulièrement touchées par des attaques hybrides, l'ensemble des acteurs publics — y compris les opérateurs, entités déconcentrées et collectivités territoriales — peuvent faire face à une menace touchant leur activité.

Opérateurs

L'ensemble des opérateurs d'importance vitale, mais également les TPE/PME dans les secteurs-clés peuvent être cibles ou vecteurs à leur insu d'attaques hybrides.

6. Cadre juridique et référence documentaire

Publié en février 2021, le Document de Référence interministériel en matière de lutte contre les menaces hybrides est le fruit d'un travail interministériel piloté par le SGDSN. Il a pour vocation de constituer un point de référence sur le sujet à destination de l'ensemble des acteurs.

7. Indicateurs et contrôles de l'exécution

Dans les cinq domaines prioritaires identifiés par la France dans la lutte contre les menaces hybrides, des structures, des outils et une comitologie (la liste des acteurs est classifiée) sont dédiés au suivi de situation, à l'alerte et au contrôle de l'exécution des mesures décidées. L'approche interministérielle de ce suivi est assurée par le SGDSN, dans le cadre de ses prérogatives. Pour rappel, les champs d'action sont les suivants :

- cyber ;
- lutte contre la manipulation de l'information ;
- sécurité économique ;
- *lawfare* ;
- opérationnel.

8. Planifications en lien

La planification de la réaction globale à des attaques hybrides relève de la résilience de la Nation. À titre sectoriel, chacun des domaines prioritaires de la lutte contre la menace hybride fait l'objet d'une planification dédiée.

9. Commentaires

ANNEXE 3 : TYPOLOGIE DES MENACES ET DES RISQUES

RISQUE : NATUREL	TR 6

1. Nature

La prise en compte de la variété de ces risques repose avant tout sur une planification locale et la définition de « bassins de risques », de lieux clés, établie au regard de la sensibilité du territoire concerné. L'échelon national se conçoit en appui ou en pilotage en fonction de la situation.

2. Eléments déclencheurs possibles

- les évènements climatiques, comme les feux de forêt, peuvent être soumis à une saisonnalité. Mais leur prévisibilité, leur fréquence et leurs conséquences peuvent être modifiées par le changement climatique.
- leur déclenchement et leur intensité peuvent en outre être aggravés par l'intervention humaine (imprudences, pyromane, aménagements…).

3. Vulnérabilités

Ces divers phénomènes naturels portent une atteinte directe à l'intégrité physique et psychique des populations et ont un impact grave sur les infrastructures, les moyens de communication et les axes de circulation, imposant des mesures exceptionnelles de secours aux victimes (évacuation, hébergement d'urgence), ces dernières mesures de gestion de crise étant pilotées par le ministère de l'intérieur.

4. Gradation possible et modes opératoires

- épisodes climatiques exceptionnels : si l'évènement se produit généralement sur une faible période de temps et avec un préavis court (jusqu'à 72h), le retour à la normale s'inscrit dans le temps long, pouvant se compter en années ;
- feux de forêt dont l'ampleur peut imposer des évacuations de populations : cinématique rapide ;
- évènement d'origine tellurique (sismique, volcanique, effondrements…) ;
- éruption solaire du type « événement de Carrington » (tempête solaire de 1859).

5. Impacts possibles

Acteurs publics

Comme rappelé plus haut, il s'agit d'un enjeu particulièrement local (préfectures et collectivités territoriales, en lien le cas échéant avec les ARS).

Les autorités locales, notamment préfectorales, ont toute latitude pour engager l'ensemble des moyens de la force publique, et solliciter si nécessaire un engagement des armées.

Opérateurs

Météo-France et DGPR-Schapi, en amont des évènements, pour assurer la vigilance météorologique et hydrologique, et en liste non exhaustive : IGN pour des prises de vues immédiatement après la crise, ONF (tempêtes, feux de forêt) et au travers de la compétence de son service RTM (restauration des terrains en montagne) notamment pour les zones de montagne.

6. Cadre juridique et référence documentaire

- les ministres chargés de l'environnement et de l'industrie conduisent, chacun en ce qui le concerne, les travaux de planification sectoriels relatifs aux risques naturels ;
- instruction interministérielle relative à la vigilance météorologique et la vigilance crues.

7. Indicateurs et contrôles de l'exécution

8. Planifications en lien

Plans de prévention des risques naturels prévisibles (PPRN) :

- ORSAN
- ORSEC/COTRRiM

Instruction interministérielle de gestion sanitaire des vagues de chaleur

9. Commentaires

ANNEXE 3 : TYPOLOGIE DES MENACES ET DES RISQUES

RISQUES : TECHNOLOGIQUE ET INDUSTRIEL — TR 7

1. Nature

La prise en compte de la variété de ces risques repose avant tout sur la planification locale et la définition de « bassins de risques » et de lieux clés, établie au regard de la sensibilité du territoire concerné. L'échelon national se conçoit en appui ou en pilotage en fonction de la situation.

2. Eléments déclencheurs possibles

- agression externe (y compris catastrophe naturelle) ;
- agression interne (humaine, incendie…) ;
- accident.

3. Vulnérabilités

Cette crise porterait une atteinte directe à l'intégrité physique et psychique des populations et génèrerait un impact grave sur les établissements sanitaires et médico-sociaux, les infrastructures, les moyens de communication et les axes de circulation, imposant des mesures exceptionnelles de secours aux victimes (évacuation, hébergement d'urgence). Des impacts environnementaux sont également possibles. De plus, la combinaison risque naturel – risque technologique demeure possible (Fukushima).

4. Gradation possible et modes opératoires

- incident technologique ou industriel ;
- accident technologique ou industriel ;
- accident majeur au sens de la directive Seveso pour les ICPE ;
- accident nucléaire ;
- les exploitants ont des fiches réflexes pour réagir aux situations dégradées et mettent en place des plans d'urgence interne pour se préparer à gérer une crise (a minima les sites Seveso, les INB et les INBS).

5. Impacts possibles

Acteurs publics

- préfecture avec les différents services de l'État au COD dont (DREAL, SDIS, ASN et IRSN pour les événements sur les INB, ARS, Météo France…) ;
- CASU (cellule appui aux situations d'urgence de l'INERIS) ;
- IRSN pour les évènements nucléaires et radiologiques ;
- cellule interministérielle de crise pour les accidents importants avec le MTECT.
- Moyens des armées.

Opérateurs

Laboratoires de prélèvements environnementaux et de prélèvements sur les populations concernées.

6. Cadre juridique et référence documentaire

Les ministres chargés de l'environnement et de l'industrie conduisent, chacun en ce qui le concerne, les travaux de planification sectoriels relatifs aux risques technologiques.

7. Indicateurs et contrôles de l'exécution

/

8. Planifications en lien

Plans à vocation préventive en interface avec les plans opérationnels :

- plans de prévention des risques technologiques (PPRT)
- plan de prévention des risques miniers

Le plan de réponse à un accident nucléaire ou radiologique majeur (PNRANRM)/POI

Plans de prévention des risques naturels prévisibles (PPRN) :

- ORSAN
- ORSEC/COTRRiM

Plans relatifs à la sécurité des activités d'importance vitale et plans territoriaux :

- PPP pour l'opérateur
- PPE dans le cas d'agressions externes ou internes
- PPI pour les préfectures
- PCS pour les communes

9. Commentaires

ANNEXE 3 : TYPOLOGIE DES MENACES ET DES RISQUES

RISQUE : SANITAIRE — TR 8

1. Nature

Les épidémies sont caractérisées par l'apparition et la propagation d'une maladie infectieuse contagieuse qui frappe en même temps et en un même endroit un grand nombre de personnes. Le caractère pandémique se dit d'une épidémie (maladie humaine) ou d'une épizootie (maladie animale) qui se propage sur de très grandes distances et atteint successivement plusieurs continents.

De nombreuses pandémies, comme la Covid-19, le virus Ebola, la grippe aviaire ou encore le Sida, ont en commun de venir des animaux. Selon l'Organisation mondiale de la santé animale, 60% des maladies infectieuses humaines existantes sont zoonotiques et au moins 75% des agents pathogènes des maladies infectieuses humaines émergentes sont d'origine animale, imposant une approche globale entre santé humaine et santé animale (concept « One Health »). Les impacts directs et indirects d'une épidémie, *a fortiori* d'une pandémie, dépendent de la contagiosité, la létalité, la gravité des symptômes et des modes de contamination.

2. Eléments déclencheurs possibles

Le rythme d'émergence de nouveaux agents pathogènes, majoritairement issus de la faune sauvage, s'accélère compte tenu des pressions diverses de l'activité humaine sur les écosystèmes naturels. Les espèces sauvages occupent souvent un rôle prépondérant, d'une part en tant que réservoirs et d'autre part en tant que vectrices.

Le changement climatique est un autre facteur à l'origine de la multiplication des épidémies ainsi que de leur expansion géographique, et de l'aggravation de leur impact. Il rend l'environnement plus propice aux pathogènes et à leur prolifération ainsi qu'aux vecteurs de maladies infectieuses (tels les moustiques).

À ce contexte, s'ajoutent la globalisation et l'intensification des mouvements de personnes, de biens et d'animaux.

3. Vulnérabilités

L'enjeu est double :

- réduire le risque d'apparition d'une épidémie ou pandémie et en limiter les impacts sanitaires directs ;
- atténuer les effets indirects sur la vie économique et sociale.

Les vulnérabilités dépendent de la capacité du pays à faire face aux impacts sanitaires (notamment capacité de détection et de prise en charge des malades, infrastructures d'isolement adaptées et professionnels de santé formés et protégés), mise en œuvre de la stratégie de maitrise de l'épidémie (mesures barrières, vaccination), notamment de la stratégie « tester-alerter-protéger », adaptation du système de santé, contre-mesures médicales prenant en compte la production et la distribution de médicaments, d'équipements de protection individuelle, mobilisation de la recherche et de l'innovation mais aussi de l'efficience de la stratégie de continuité de la vie du pays et de l'activité économique (en particulier lié à l'absentéisme).

Une approche multidisciplinaire et intégrative peut aider à comprendre, prévenir et contrôler les phénomènes d'émergence ou de réémergence de maladies infectieuses en particulier zoonotique à potentiel épidémique et/ou pandémique afin d'en limiter les impacts sur notre société.

4. Gradation possible et modes opératoires

À partir de son lieu d'apparition, caractérisé par plusieurs foyers de transmission interhumaine, une pandémie mettrait au plus quelques semaines pour atteindre l'Europe et les collectivités d'outre-mer, sauf suspension totale des liaisons aériennes et maritimes ou efficacité des procédures de mise en quarantaine.

Sa durée serait de quelques semaines à quelques mois voire quelques années, l'éventualité d'une évolution en plusieurs vagues, espacées de quelques semaines à quelques mois, ne pouvant être exclue (ex. de la Covid-19).

ANNEXE 3 : TYPOLOGIE DES MENACES ET DES RISQUES

5. Impacts possibles

Acteurs publics

- système de santé (soins de ville, établissements de santé, établissements et services médico-sociaux) et tous les autres acteurs étatiques pouvant être impactés dans leur fonctionnement et leur continuité d'activité (EPA, EPIC, agences, administrations, collectivités, etc.).
- moyens des armées ;
- système vétérinaire (clinique, laboratoires, élevages, services déconcentrés…).

Opérateurs

- saturation de l'offre de soins notamment des établissements de santé avec impact sur les soins courants (déprogrammation) ;
- dépassement des capacités de production des moyens sanitaires nécessaires à la prise en charge des patients et à la lutte contre l'agent pathogène et le cas échéant, sa diffusion (contre-mesures médicales, équipements de protection individuelle, dispositifs médicaux, etc.) ;
- perturbation du fonctionnement des services étatiques ainsi que de la vie socio-économique.

6. Cadre juridique et référence documentaire

Article L.1142-8 du code de la défense : le ministre chargé de la santé est responsable de l'organisation et de la préparation du système de santé et des moyens sanitaires nécessaires à la connaissance des menaces sanitaires graves, à leur prévention, à la protection de la population contre ces dernières, ainsi qu'à la prise en charge des victimes.

7. Indicateurs et contrôles de l'exécution

- Ministère de la santé/CORRUSS-CCS : suivi de l'incidence et autres indicateurs épidémiques, suivi de l'activité du système de santé, suivi des mesures gouvernementales (vaccination, télétravail, etc.).
- Ministère de l'agriculture : mise en œuvre de la stratégie de prévention, de surveillance et de lutte contre les dangers sanitaires, qui sont de nature à porter atteinte à la santé des animaux et les végétaux ou à la sécurité sanitaire des aliments et les maladies d'origine animale ou végétale qui sont transmissibles à l'homme.
- opérateurs : ANSP (Santé Publique France ou SPF) ; ANSM, ANSES et autres agences sanitaires .

8. Planifications en lien

Plan national de préparation et de réponse à une pandémie Dispositif ORSAN :

- plan ORSAN REB (plan d'organisation de la réponse du système de santé face à un risque épidémique et biologique)

Plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles des établissements de santé.

Plan bleu des établissements et services médico-sociaux.

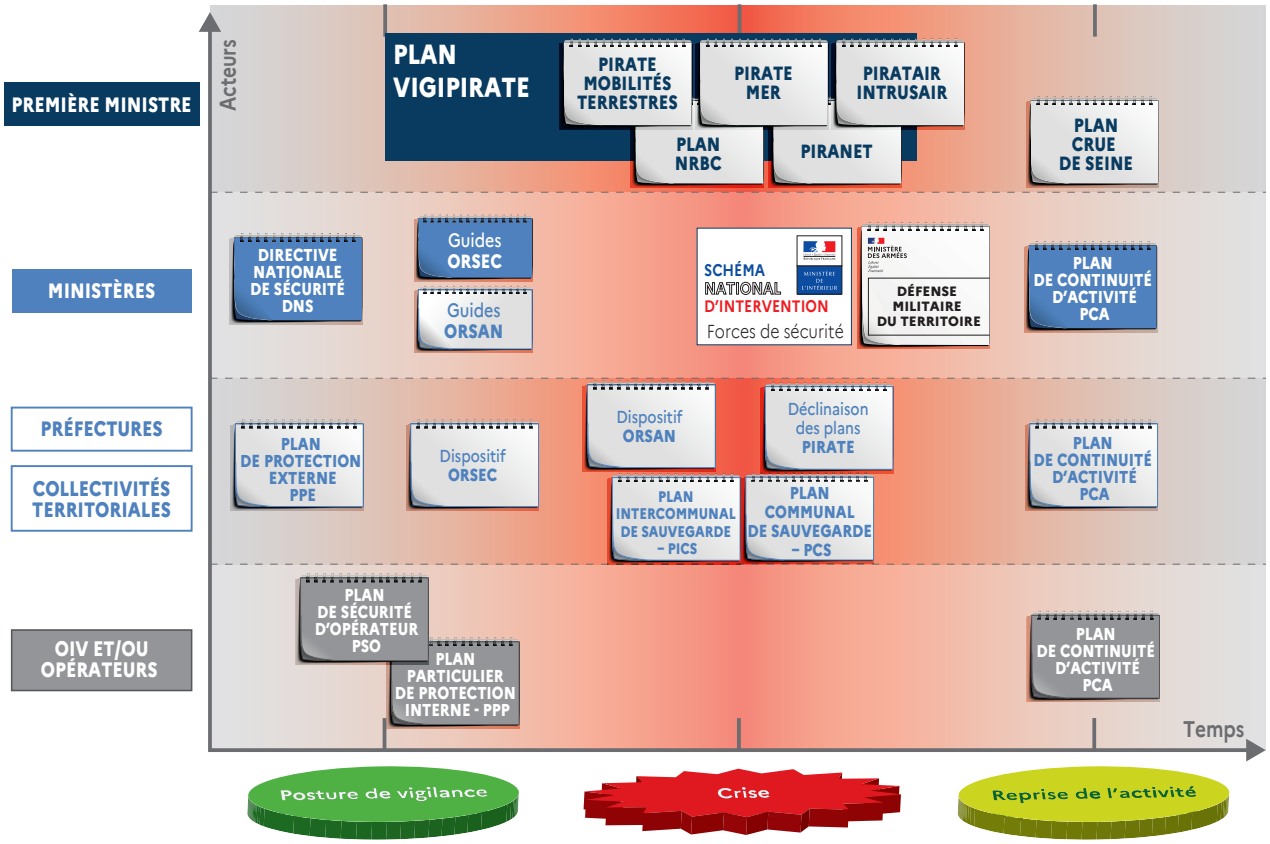
Tout autre plan de continuité d'activité.

Plan national d'intervention sanitaire d'urgence (PNISU – épizooties) :

- instruction interministérielle N° DGS/VSS2/DGOS/DGCS/DGT/DGSCGC/DGEC/DJEPVA/DS/ DGESC/DIHAL/2021/99 du 7 mai 2021 relative à la gestion sanitaire des vagues de chaleur en France métropolitaine.

9. Commentaires

ANNEXE 4 : PLANS NATIONAUX



Les plans nationaux sont construits en 2 parties :

- une première partie spécifiant les situations de référence et les enjeux spécifiques ;
- une seconde partie sous forme de guide d'aide à la décision.

A. LES PLANS GOUVERNEMENTAUX :

élaborés sous l'égide du SGDSN, ils sont destinés à :

- faire face à une menace ou à un risque particulier, identifié comme majeur sur le territoire national ;
- servir de cadre de référence à l'élaboration des plans territoriaux correspondants, déclinaisons adaptées aux caractéristiques locales (zone, département), le cas échéant en s'appuyant sur une déclinaison ministérielle.

B. LES PLANS MINISTÉRIELS SECTORIELS OU THÉMATIQUES[20] :

réalisés par les ministères, parfois sous l'égide du SGDSN et déclinés au niveau local, ils décrivent :

- des plans relatifs à un secteur d'activité (hydrocarbure, continuité électrique…) ;
- des plans relatifs à une thématique transversale particulière (rétablissement de réseau, évacuation de population… / plans ressources).

20 - Code de la défense articles L1141-1 à L1142-9.

C. LES DISPOSITIFS TERRITORIAUX :

Le dispositif ORSEC (départemental, zonal, maritime), relatif à l'organisation des secours (article L741-1 CSI), lie des dispositions générales applicables en toute circonstance et des dispositions spécifiques aux risques particuliers ou liés à l'existence et au fonctionnement d'installations ou d'ouvrages déterminés (PPI notamment).

Le contrat territorial de réponse aux risques et aux effets des menaces (CoTRRiM, dont le contenu est fixé par le décret n°2022-1316 du 13 octobre 2022)) est un document opérationnel qui vient s'ajouter aux documents de planification existants. Il est novateur car :

- il fournit une analyse multi-acteurs et multi-sectorielle des risques identifiés sur un territoire ;
- il est le seul document de planification qui va jusqu'à l'identification des éventuelles ruptures capacitaires ;
- son champ d'action est spécifique (planification capacitaire).

Le dispositif ORSAN organise la réponse du système de santé aux situations sanitaires exceptionnelles. Il constitue le cadre de préparation et de réponse opérationnelle du système de santé à ces situations. Il est élaboré dans chaque région par l'ARS et il comprend notamment des plans de réponse organisant la mobilisation, de façon coordonnée, des opérateurs de soins, des professionnels de santé et des moyens et matériels. Il définit les parcours de soins des patients et organise les filières de prise en charge. Il s'appuie notamment sur les plans blancs des établissements de santé et les plans bleus des établissements médico-sociaux. Le dispositif ORSAN s'articule avec le plan ORSEC pour la prise en charge des patients dans le système de santé.

D. LES PLANS RELATIFS À LA SÉCURITÉ DES ACTIVITÉS D'IMPORTANCE VITALE[21] :

- Visant à protéger les points d'importance vitale (PIV) contre toute menace et tout risque, il comprend des documents préparés par :
- les ministères coordinateurs des secteurs avec les directives nationales de sécurité (DNS) ;
- les opérateurs avec les plans de sécurité opérateur (PSO) et les plans particuliers de protection (PPP) ;
- les préfets de département avec les plans de protection externe (PPE).

E. LES PLANS DE CONTINUITÉ D'ACTIVITÉ (PCA) :

- élément central de la résilience, les secteurs fournissant des services vitaux doivent être en mesure de maintenir en permanence leurs activités à un niveau minimum socialement acceptable et le ramener à un niveau de fonctionnement normal le plus rapidement possible ;

21 - Code de la défense – articles L.1332-1 à L.1332-7, L.2151-1 à L.2151-5 et R.1332-1 à R.1332-42. •Instruction générale interministérielle n° 6600 relative à la sécurité des activités d'importance vitale du 7 janvier 2014. •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.

- le PCA a pour objet de décrire la stratégie de continuité à adopter par une organisation pour faire face, par ordre de priorité, à l'indisponibilité partielle ou durable d'une ou plusieurs capacités critiques. Il recense les ressources, moyens et procédures documentées à mettre en œuvre.

F. LES PLANS DE DÉFENSE :

Le ministre des armées, responsable de la politique de défense (article L 1131-1 du code de la défense), établit les plans de défense. La planification des armées vise à préparer l'engagement des moyens des armées que ce soit pour remplir leurs missions propres ou lorsqu'ils sont utilisés en appui ou en soutien des autres politiques publiques.

Répondant aux seules missions de défense militaire du territoire, les plans de défense sont de trois ordres :

les plans de défense opérationnelle du territoire (article R 1422-1)*

Sur la base des décisions prises en conseil de défense et de sécurité nationale (CDSN), le Premier ministre, ou par délégation le ministre des armées, établit les directives générales relatives à la préparation et à la mise en œuvre des mesures de défense opérationnelle du territoire (DOT) destinées à contrer une menace extérieure, une agression ou une invasion.

Le ministre des armées organise, met en condition et détermine les missions des forces prévues pour assurer la DOT. Chaque ministre intéressé, notamment le ministre de l'intérieur et les ministres chargés des finances et de l'outre-mer, définit en fonction des instructions reçues, les moyens de son ministère à mettre en œuvre.

Le chef d'état-major des armées adresse aux commandants de zone de défense et de sécurité les directives nécessaires à l'établissement des plans de DOT. Ces plans, élaborés en accord avec les préfets de zone ou les hauts fonctionnaires de zone sont arrêtés par le Premier ministre ou, par délégation, par le ministre des armées.

*les plans de défense maritime du territoire (article D*1432-2 et suivants) :*

Les directives générales relatives à la préparation et à la mise en œuvre des plans de défense maritime du territoire (PDMT) sont établies par le Premier ministre ou, par délégation, par le ministre des armées, sur la base des décisions arrêtées en conseil de défense et de sécurité nationale (CDSN).

Les PDMT, soumis pour approbation au chef d'état-major des armées, sont rédigés par les commandants de zone maritime, en liaison avec les préfets de zones riveraines et les commandants désignés de ces zones. Ils prévoient, à tous les échelons, des mesures de coordination avec le plan de défense aérienne du territoire.

*les plans de défense aérienne du territoire (article D*1442-1 et suivants) :*

Dans le cadre des plans et des décisions arrêtés en CDSN, le Premier ministre fixe les objectifs généraux à atteindre par les départements ministériels qui concourent à la défense aérienne.

Le ministre des armées fait établir et arrête le plan de défense aérienne. Compte tenu des priorités générales de défense, ce plan précise les menaces à prendre en considération et fixe les niveaux de capacité à atteindre. Il comprend les mesures de coordination avec les plans de sécurité intérieure et les autres plans de défense.

Le commandant de la défense aérienne et des opérations aériennes conduit l'exécution des plans d'opérations de défense aérienne, approuvés par le chef d'état- major des armées.

La planification de défense et de sécurité nationale

A. PLANIFICATION GOUVERNEMENTALE

- Directive générale interministérielle relative à la planification de défense et de sécurité nationale n°320 du 11 juin 2015 (abrogée par le présent document) ;
- instruction interministérielle relative à l'engagement des armées sur le territoire national en cas de crise majeure n° 10100/SGDSN/PSE/PSN/NP du 17 novembre 2017 ;
- circulaire relative à l'organisation gouvernementale pour la gestion des crises majeures n°5567/SG du 1er juillet 2019 ;
- instruction interministérielle provisoire de doctrine de sûreté maritime et portuaire n° 10056/SGDN/PSE/PPS/CD du 16 février 2006 ;
- instruction interministérielle relative à la fermeture de l'espace aérien n° 185/SGDSN/PSE/.. .. du 24 avril 2012 ;
- instruction relative à la prise en charge des victimes d'actes de terrorisme n°5358/SG du 19 décembre 2008 ;
- directive générale de mise en œuvre des mesures de défense opérationnelle du territoire n° 10200/SGDN/MPS/.. du 25 mars 1993 ;
- instruction interministérielle relative à la coordination et à l'optimisation des moyens aériens en cas de crise localisée sur le territoire national du 4 novembre 2013 ;
- instruction interministérielle relative au déclenchement et à la mise en place des dispositifs particuliers de sûreté aérienne n°1238/SGDN/PSE du 29 janvier 2008 ;
- circulaire interministérielle relative à la conduite des opérations de sûreté aérienne n°2000/SGDN/PSE/.. du 6 décembre 2006 ;
- instruction interministérielle relative à la sécurité de l'activité spatiale en Guyane n°4500/SGDN/PSE/PPS/..-.. du 22 mars 2007 ;
- guide pour réaliser un plan de continuité d'activité (dernière édition en 2022).
- thématique NRBC-E :
  - circulaire relative à la doctrine nationale d'emploi des moyens de secours et de soins face à une action terroriste mettant en œuvre des matières chimiques n° 700/SGDN/PSE/PPS du 7 novembre 2008 ;
  - circulaire relative à la découverte de plis, colis, contenants et substances suspectées de renfermer des agents radiologiques, biologiques ou chimiques dangereux n°750/SGDSN/PSE/PPS du 18 février 2011 ;
  - circulaire relative à la doctrine d'emploi des moyens de secours et de soins face à une action terroriste mettant en œuvre des matières radioactives n° 800/SGDSN/PSE/PPS du 18 février 2011 ;
  - directive interministérielle du 7 avril 2005 sur l'action des pouvoirs publics en cas d'événement entraînant une situation d'urgence radiologique ;
  - directive interministérielle du 30 novembre 2005 relative à l'application de la Convention internationale sur l'assistance en cas d'accident nucléaire ou de situation d'urgence radiologique ;

- circulaire relative à la doctrine de l'État pour la prévention et la réponse au terrorisme nucléaire, radiologique, biologique, chimique et par explosifs (NRBC-E) n°747/SGDSN/PSE/PPS du 30 octobre 2009 ;
- circulaire interministérielle relative au dispositif interministériel d'intervention face à la menace ou à l'exécution d'actes de terrorisme nucléaire, radiologique, biologique ou chimique (NRBC) n°007/SGDN/PSE/PPS du 8 octobre 2009.

- plan gouvernemental Vigipirate de vigilance, de prévention et de protection face aux menaces d'actions terroristes n° 650/SGDSN/PSE/PSN/CD du 17 janvier 2016 ;
- plan gouvernemental d'intervention Pirate-mer en cas de menace ou d'acte de terrorisme maritime ou de piraterie maritime n° 10070/SGDSN/PSE/PSN/.. de juillet 2017 ;
- plan gouvernemental de réponse Piratair-Intrusair n° 10104/SGDSN/PSE/PSN/.. du 07 septembre 2017 ;
- plan gouvernemental NRBC n° 10135/SGDSN/PSE/PPS/.. du 16 septembre 2016. Guide de déclinaison du plan gouvernemental NRBC ;
- plan gouvernemental de réponse aux actes de terrorisme dans le domaine des transports terrestres n°10124/SGDSN/PSE/PSN/.. du 05 octobre 2018 ;
- plan gouvernemental d'intervention Piranet contre une attaque terroriste sur les systèmes d'information n° 448/SGDSN/PSE/PSN/.. du 05/05/2017 ;
- plan gouvernemental d'intervention Piratex en cas de menace ou d'action terroriste contre des ressortissants ou des intérêts français à l'étranger n°10225/SGDN/PSE/PPS/.. du 25 juin 2004 ;
- plan gouvernemental « déplacements de populations » n°1670/SGDN/PSE/PPS du 26 août 2003 ;
- plan gouvernemental d'intervention « interception prolifération » en vue d'une interception de biens contribuant à des activités de prolifération d'armes de destruction massive n° 5366/SG du 9 février 2009 ;
- plan national de prévention et de lutte « pandémie grippale » n° 850/SGDSN/PSE/PSN du 30 novembre 2011 ;
- plan national de prévention et de lutte « maladie à virus Ébola » n°600/SGDSN/PSE/PSN du 24 novembre 2014 ;
- plan national de réponse à un accident nucléaire ou radiologique majeur n°200/SGDSN/PSE/PSN du 3 février 2014 ;
- plan gouvernemental crue de la Seine, édition novembre 2021 ;
- plan national de continuité électrique n° 600/SGDN/PSE/PPS du 18 septembre 2009.

B. PLANIFICATION RELATIVE AUX SECTEURS D'ACTIVITÉ D'IMPORTANCE VITALE (SAIV)

- Instruction générale interministérielle relative à la sécurité des activités d'importance vitale n°6600/SGDSN/PSE/PSN du 7 janvier 2014 ;
- directives nationales de sécurité (DNS) ;
- plans de sécurité d'opérateur (PSO) ;
- plans particuliers de protection (PPP) ;
- plans de protection externe (PPE) ;
- base DIVA des points d'importance vitale (PIV).

C. PLANIFICATION MINISTÉRIELLE SECTORIELLE ET THÉMATIQUE

- Plan ressources « Hydrocarbures » n° 0012/DGEMP/DIREM/PPS 2003-80/HFD/SIEN/DRD du 28 mars 2003 ;
- plan national d'urgence gaz (arrêté du 28 novembre 2013 portant adoption du plan d'urgence gaz pris en application du règlement (UE) n° 994/2010 du Parlement européen et du Conseil du 20 octobre 2010 concernant l'approvisionnement en gaz naturel et abrogeant la directive 2004/67/CE du Conseil) ;
- planification « troubles graves » ;
- guide méthodologique « évacuations massives » ;
- circulaire DGSNR/DHOS/DDS 11° 2005/1390 du 23 décembre 2005 relative aux principes d'intervention en cas d'événement susceptible d'entraîner une situation d'urgence radiologique hors situations couvertes par un plan de secours ou d'intervention ;
- instruction interministérielle N° DGS/VSS2/DGOS/DGCS/DGT/DGSCGC/DGEC/DJEPVA/DS/ DGESC/DIHAL/2021/99 du 7 mai 2021 relative à la gestion sanitaire des vagues de chaleur en France métropolitaine ;
- guide S5, plan d'intervention sanitaire d'urgence (zoonoses/épizooties).

D. PLANIFICATION DE DÉFENSE

- Plans de défense opérationnelle du territoire (PDOT). Plans de défense maritime du territoire ;
- plan de défense aérienne du territoire.

E. PLANIFICATION TERRITORIALE

- **Planification ORSEC : Le dispositif ORSEC se décline au niveau zonal et départemental :**
  - dispositions générales : méthode générale (G.1), Soutien des populations (G.2), la cellule d'information du public (G.3), alerte et information des populations (G.4), rétablissement et approvisionnement d'urgence des réseaux : électricité, communications électroniques, gaz, eau, hydrocarbures (G.5), secours à de nombreuses victimes dit « NOVI » (G.6), Organisation territoriale de gestion des crises (G.7).
  - dispositions spécifiques :
    - risques naturel : grand froid, gestion sanitaire des vagues de chaleur, inondation intempéries / évènements météorologiques dangereux, neige/verglas, avalanches, incendie, lutte contre les sargasses, séisme, volcan, tsunami, cyclone ;
    - risques technologiques : PPI installation nucléaire de base ,PPI installation classée seveso seuil haut, PPI stockage souterrain, PPI grand barrage, PPI établissement utilisant des microorganismes hautement pathogènes, PPI infrastructures liées aux transports des matières dangereuses dans les ports, PPI infrastructures liées aux transports des matières dangereuses dans les gares, PPI infrastructures liées aux transports des matières dangereuses dans les aires, PPI gestion des déchets de l'industrie extractive, accident nucléaire majeur (dont iode), transport de matières radioactives, transport de matières dangereuses,

pollution accidentelle des eaux intérieures, épisode pollution atmosphérique, NRBC ;
  - risque lié aux réseaux de transport : ferroviaire, POLMAR terre, POLMAR mer, sauvetage maritime de grande ampleur, plan de gestion du trafic (PGT) zonal, sauvetage aéroterrestre (SATER), accident d'aéronef sur aérodrome ou zone voisine, tunnels ;
  - risque sanitaire : épizootie, arbovirose, pandémie grippale, plan de mobilisation, plans d'intervention pour la gestion des urgences sanitaires ;
  - risque lié aux sites : grands sites (stades, parcs d'attractions…), grands évènements secours en montagne, spéléologie.
- plan ORSEC maritime défini par instructions du secrétariat général de la mer : dispositions générales (28 mai 2008), lieux refuges (24 avril 2012), secours maritime de grande ampleur (13 mai 2013), pollution maritime (4 mars 2002 et 11 janvier 2006), accident nucléaire maritime (7 septembre 1989) :
  - document d'interface mer/terre pour le secours maritime de grande ampleur ;
  - document d'interface mer/terre pour l'accueil des navires en difficulté.
- instructions diverses ORSEC :
  - plans de prévention des risques naturels prévisibles (PPRN). Plans de prévention des risques technologiques (PPRT) ;
  - plans de prévention des risques miniers.

- **planification ORSAN :**
  - dispositif ORSAN régional : plans ORSAN AMAVI, MEDICO-PSY, EPI-CLIM, NRC et REB ;
  - plans de réponse aux situations sanitaires exceptionnelles des opérateurs de soins : plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles des établissements de santé, plan bleu des établissements et services médico-sociaux, etc. ;
  - guide ORSAN ;
  - instructions diverses ORSAN.
- **plans d'urgence (plan d'opération interne (POI), plan d'urgence interne (PUI), plan particulier d'intervention (PPI), plan d'intervention et de sécurité (PIS), etc.) ;**
- **plans particuliers de mise en sûreté (établissements scolaires), plan communal de sauvegarde (PCS), plan intercommunal de sauvegarde (PICS), plan bleu ;**
- **instructions diverses relatives à la pollution du milieu marin (POLMAR) ;**
- **circulaire interministérielle n°DGS/DUS/2011/340 et n° DSC/2011/64 du 11 juillet 2011 relative au dispositif de stockage et de distribution des comprimés d'iodure de potassium hors des zones couvertes par un plan particulier d'intervention ;**
- **circulaire interministérielle n°DGS/DUS/DGSCGC/2013/374 du 26 septembre 2013 relative à l'élaboration du plan zonal de mobilisation des ressources sanitaires ;**
- **circulaire interministérielle n°DGS/DUS/BOP/DGAC/DGITM/DGSCGC/2014/249 du 18 août 2014 relative à la mise en œuvre du décret 11° 2013-30 du 9 janvier 2013 relatif à la mise en œuvre du règlement sanitaire international.**

ANNEXE 5 : ACTEURS DE LA PLANIFICATION

Sous l'autorité du Premier ministre, qui dirige l'action du Gouvernement en matière de sécurité nationale et prépare l'action des pouvoirs publics en cas de crise majeure (article L1131-1 du code de la défense), le **SGDSN élabore la planification interministérielle de défense et de sécurité nationale et veille à son application**, notamment *via* des exercices interministériels. **Il coordonne la préparation et la mise en œuvre des mesures de défense et de sécurité nationale incombant aux divers départements ministériels et s'assure de la coordination des moyens civils et militaires prévus en cas de crise majeure (article R*1132-3 du même code)**.

Chaque ministre est responsable, sous l'autorité du Premier ministre, de la préparation et de l'exécution des mesures de défense et de sécurité nationale incombant au département dont il a la charge (articleL1141-1 du même code). Elles sont précisées dans l'annexe 7. Il s'appuie à cet effet sur un service de haut fonctionnaire de défense et de sécurité (article R 1143-4 à R1143-8 du même code).

En particulier, conformément à l'article L1142-2 du code de la défense, « *le ministre de l'intérieur est responsable de la préparation et de l'exécution des politiques de sécurité intérieure et de sécurité civile qui concourent à la défense et à la sécurité nationale et il est, à ce titre, sur le territoire de la République, responsable de l'ordre public, de la protection des personnes et des biens ainsi que de la sauvegarde des installations et ressources d'intérêt général.*

À ce titre :

1° Il est chargé de l'anticipation et du suivi des crises susceptibles d'affecter la sécurité intérieure et la sécurité civile ;

2° Il contribue à la planification interministérielle en matière de sécurité nationale. Il prépare les plans à dominante d'ordre public, de protection et de sécurité civiles ;

3° Il assure la conduite opérationnelle des crises ;

***4° Il s'assure de la transposition et de l'application de l'ensemble de la planification gouvernementale par les représentants de l'État dans les zones de défense et de sécurité, les départements et les collectivités d'outre-mer. (…)* »**

Cette responsabilité du ministre de l'intérieur est régulièrement confirmée, notamment par la circulaire du Premier ministre n°6095/SG du 1er juillet 2019 relative à l'organisation gouvernementale pour la gestion des crises majeures (actualisant la circulaire PM du 2 janvier 2012).

A. LES ACTEURS INSTITUTIONNELS SUR LE TERRITOIRE NATIONAL :

a. Le préfet de zone de défense et de sécurité nationale

(article R*122-1 et suivants ; article R*1311-3 à R*1311-29-1 du code de la défense)

Le représentant de l'État dans la zone de défense et de sécurité **exerce le pilotage territorial de la planification de défense et de sécurité nationale.** Disposant à cet effet d'un état-major interministériel de zone de défense et de sécurité (EMIZDS), il est chargé, avec les acteurs concernés, de :

- la transposition au niveau zonal de l'ensemble de la planification interministérielle de défense et de sécurité nationale : il décline les plans établis par le SGDSN, sur

la base de l'analyse préalable des risques et des effets potentiels des menaces susceptibles de concerner sa zone (article R*122-4 du code de la sécurité intérieure) ;

- la préparation de l'ensemble des mesures à mettre en œuvre, en cas de crise intérieure, par les autorités civiles territoriales afin :
  - d'assurer en toutes circonstances la protection des points d'importance vitale (PIV) (article L1332-1 et suivants, article R1332-1 et suivants du code de la défense),
  - de maintenir et rétablir l'ordre public,
  - de garantir le fonctionnement des organismes essentiels à la vie de la Nation et à la sauvegarde de la population ;
- la cohérence de l'ensemble de la planification réalisée au sein de la zone, notamment des plans zonaux et départementaux. À ce titre, il prépare les mesures de coordination nécessaires, y compris avec les pays frontaliers lorsque cela est nécessaire.

En cas de crise majeure, il assure la répartition des moyens mobilisés au sein des ministères, des armées, des agences régionales de santé, des collectivités territoriales et des opérateurs d'importance vitale sur sa zone.

Dans cette optique, les travaux de planification doivent lui permettre d'avoir la connaissance des moyens, des capacités et des compétences disponibles ou mobilisables dans sa zone, qu'ils relèvent ou non de l'État, ainsi que des procédures pour les mobiliser.

Il est en particulier responsable de la coordination avec les autorités militaires et veille à ce titre à la cohérence entre les plans qui relèvent de sa compétence et les plans militaires de défense.

Le comité des préfets de zone de défense et de sécurité est présidé par le ministre de l'intérieur. Il comprend les préfets de zone de défense et de sécurité, les hauts fonctionnaires de défense et de sécurité et le secrétaire général de la défense et de la sécurité nationale. Il **a pour mission d'assurer les conditions de préparation de la chaîne territoriale de l'État à la gestion des crises majeures relevant de la sécurité nationale**. Les modalités de son fonctionnement sont arrêtées par le ministre de l'intérieur.

b. Le préfet de région

Même s'il n'a pas de rôle en matière de planification de défense et de sécurité nationale, les services régionaux de l'État apportent leur appui et leur expertise aux travaux territoriaux de planification maritimes, zonaux et départementaux (article R*1311-30 à R*1311-32).

c. Le préfet de département et le haut-commissaire de la République[22]

Il est **responsable de la gestion de crise au niveau territorial.** Il est directeur des opérations (DO). Selon les directives des niveaux national et zonal, **il transpose la planification de défense et de sécurité nationale au niveau départemental et veille à la cohérence avec les niveaux supérieurs**. Il dispose du service interministériel de défense et de protection civile (SIDPC), s'appuie sur les différents services de l'État, en particulier le commandant de groupement de gendarmerie départementale, le directeur départemental de la

22 - article R*122-52 du CSI, Décret n°2004-374 du 29 avril 2004 relatif aux pouvoirs des préfets, à l'organisation et à l'action des services de l'État dans les régions et départements, code de la défense article R*1311-33 à R1311-38-1.

sécurité publique, le directeur départemental d'incendie et de secours, le délégué militaire départemental et les agences régionales de santé, et associe les collectivités territoriales et les opérateurs de son département. **Cette planification intègre une démarche capacitaire visant à identifier les besoins à formuler (COTRRiM). Le préfet veille également à la réalisation des plans spécifiques à la sécurité des activités d'importance vitale (SAIV)** : les plans particuliers de protection (PPP) de la responsabilité des opérateurs et les plans de protection externe (PPE) de sa responsabilité.

d. Le représentant de l'État en mer (le préfet maritime en métropole, le préfet ou le haut-commissaire de la République délégué du Gouvernement pour l'action de l'État en mer en outre-mer)

Il conduit les travaux de planification appliqués aux zones maritimes.

e. Le Service d'Information du Gouvernement (SIG)

Sous l'autorité du Premier ministre, le SIG accompagne, coordonne et valorise la communication des services de l'État en matière de gestion de crise.

Au niveau stratégique, il veille à doter l'ensemble des acteurs de la communication d'outils adaptés, structure et anime le réseau des communicants de crise.

Sur le volet opérationnel, il agit en faveur d'une communication homogène des partenaires et services de l'État. Il coordonne leur action en vue d'optimiser l'impact et la compréhension de l'action gouvernementale.

f. Les collectivités territoriales

Responsables de services publics et disposant de nombreux moyens d'intervention et de gestion de crise, les collectivités territoriales appuient les préfets. Le maire, en particulier, dispose du pouvoir de police sur le territoire de sa commune.

Elles peuvent agir de la façon suivante :

- en matière de planification interne, elles doivent garantir, en toutes circonstances, un fonctionnement minimal et, à ce titre, élaborer des plans de continuité d'activité ;
- les communes, dotées d'un plan de prévention des risques naturels ou technologiques prévisibles (PPRN - PPRT) approuvé, ou comprises dans le champ d'application d'un plan particulier d'intervention doivent disposer d'un plan communal ou intercommunal de sauvegarde (PCS). Les conseils départementaux doivent également se doter d'une organisation de continuité d'activité et de gestion de crise pour assurer leurs services permanents (gestion de la voirie, action sociale, etc.) ;
- en matière de contribution à la planification de défense et de sécurité nationale, elles identifient les compétences, les moyens et les capacités qu'elles pourront mettre à disposition, en tant que concourant à l'action publique de l'Etat.

g. Les armées :

1/ défense militaire

La planification de la défense militaire du territoire est conduite, sous l'autorité du ministre des armées et du chef d'état-major des armées (CEMA), par les commandants militaires désignés (officiers généraux de zones de défense et de sécurité, commandants supérieurs outremer, délégués militaires départementaux), conformément au code de la défense.

2/ sécurité intérieure

Les armées peuvent être engagées dans des missions de sécurité nationale relevant d'autres ministères, au profit notamment de la sécurité publique et de la sécurité civile ou lorsque les moyens des autres ministères s'avèrent inexistants, insuffisants, inadaptés ou indisponibles[23] (règle des « 4i »).

Dans une situation de crise majeure, l'engagement des armées peut être nécessaire, en complément, en renforcement, en appui ou en soutien de l'action interministérielle. Cet engagement sur le territoire national, qui obéit à des règles strictes (article L1321-1 du code de la défense) est systématiquement envisagé dans les travaux de planification de défense et de sécurité nationale réalisés au sein du SGDSN.

L'engagement des armées doit être planifié conjointement par les autorités civiles et militaires territoriales. Le niveau privilégié de cette planification civilo-militaire est celui de la zone de défense et de sécurité. Ainsi, l'officier général de zone de défense et de sécurité (OGZDS) doit apporter son concours au préfet de zone de défense et de sécurité dans l'élaboration de toute planification zonale. Celle-ci permettra, en fonction de la typologie de crise, de définir les demandes d'effets susceptibles d'être adressés aux armées.

B. LES ACTEURS À L'INTERNATIONAL :

a. le chef de mission diplomatique :

Les missions diplomatiques sont des lieux de convergence des informations et capacités d'action en cas de menace à l'étranger. Elles apportent leur expertise du pays et assurent localement la liaison avec les ressortissants français, le réseau des établissements d'enseignement, les entreprises, les autorités politiques locales et les représentations diplomatiques des autres pays. Elles conduisent les travaux de planification nécessaires.

b. les acteurs internationaux :

Une crise sur le territoire national peut nécessiter pour sa résolution une action coordonnée des États ou des organisations internationales compétentes :

23 - Instruction interministérielle relative à l'engagement des armées sur le territoire national en cas de crise majeure n° 10100/SGDSN/PSE/PSN/NP du 17 novembre 2017.

- l'Union Européenne (UE) dispose d'un outil de coordination politique pour la gestion des crises majeures (*Integrated political response arrangements* ou IPCR) et d'un mécanisme européen de protection civile pour une réponse rapide si un État membre est frappé par une catastrophe majeure ;
- l'Organisation du Traité de l'Atlantique Nord (OTAN) dispose d'un système de réponse aux crises (*NATO crisis response system* ou NCRS) qui comporte un ensemble de mesures (*Crisis response measures* ou CRM) destiné à permettre à l'organisation et à ses alliés de réagir de manière coordonnée en cas d'opérations relevant ou non de l'article 5 du Traité. Par ailleurs, l'OTAN porte des plans civils d'urgence (PCU ou CEP : *civil emergency planning*) pour soutenir les autorités nationales en cas de catastrophe et assurer un soutien civil aux opérations militaires de l'organisation dans le cadre de son comité de résilience.

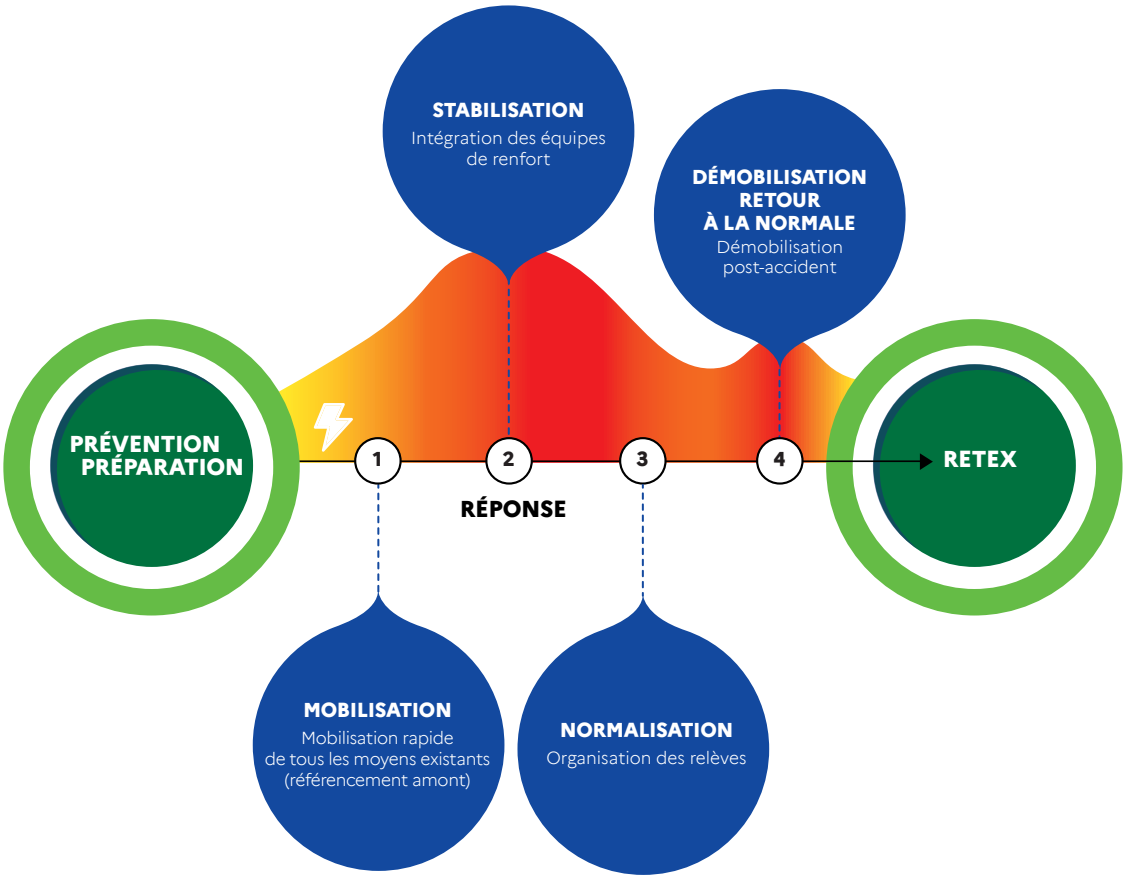
C. LES OPÉRATEURS :

Le dispositif de sécurité des activités d'importance vitale (SAIV) constitue le cadre permettant aux pouvoirs publics d'associer les opérateurs concernés aux dispositions mises en œuvre face aux risques et aux menaces.

Les opérateurs qui ne sont pas d'importance vitale sont aujourd'hui de fait associés à la gestion de crise puisque les capacités nécessaires sont de plus en plus souvent détenues par des opérateurs publics ou privés, notamment dans le cadre de délégation de service public (travaux publics, transports, énergie, etc.). Leur contribution potentielle doit donc être validée au plus tôt dans le processus de planification. Enfin, le rôle de l'ensemble des opérateurs est essentiel pour maintenir ou rétablir la continuité de l'activité économique.

Dans le cadre de la continuité d'activité, certains opérateurs ont l'obligation de se doter de plans de gestion de crise : plan de continuité d'activité pour les opérateurs d'importance vitale, plan d'opération interne pour certains opérateurs industriels, plan d'intervention et de sécurité pour les opérateurs de réseaux de circulation routière ou ferroviaire, plan interne de crise pour les opérateurs de réseau de fluides (électricité, eau, communications électroniques, gaz).

ANNEXE 6 : CRITÈRES DE SUCCÈS



PHASE 0 : PRÉVENTION ET PRÉPARATION :

- une sensibilisation par domaine et une capacité à détecter un évènement réalisées et maintenues ;
- des plans de mobilisation et de réponse fondés sur des scenarii réalistes ;
- des capacités et moyens à mobiliser correspondant aux besoins attendus ;
- les moyens nécessaires à une réponse initiale positionnés dans les zones à haut risque ;
- une coordination interministérielle planifiée avec des acteurs identifiés.

PHASE 1 : MOBILISATION ET RÉACTION IMMÉDIATE :

- un point de situation initial réalisé et partagé à travers un réseau organisé ;
- des ressources adaptées pour répondre aux besoins initiaux de protection des biens et des personnes ;
- une mobilisation qui s'appuie sur une estimation précise des besoins de la population en ressources financières et équipements ;
- une mobilisation menée par une organisation qui a planifié sa structure et ses processus, y compris pour l'anticipation.

PHASE 2 : STABILISATION :

- des ressources mobilisées rapidement intégrées dans une organisation de la réponse prédéterminée ;
- une coordination interministérielle établie ;
- une capacité à contrôler la collecte, la synthèse, l'analyse et la distribution interne et externe de l'information structurée ;
- une flexibilité organisationnelle et opérationnelle maintenue.a

PHASE 3 : NORMALISATION :

- des indicateurs mis en place, contrôlés et suivis ;
- une comptabilité établie ;
- les besoins nécessaires à un retour à la normale identifiés.

PHASE 4 : DÉMOBILISATION ET RETOUR À UN FONCTIONNEMENT NOMINAL

- des besoins permanents comblés ;
- un plan pour une transition vers les autorités locales développé et suivi ;
- des ressources extérieures démobilisées selon les plans et les processus ;
- des ressources de soutien à l'économie fournies ;
- un retour sur expérience effectué.

SÉCURISATION | SEC

Ministère menant : ministère de l'intérieur

Ministères concourants : les ministères chargés de l'agriculture, des armées, des transports et de la santé

1. Nature

La continuité de la sécurisation contribue à garantir la permanence du rôle protecteur de l'État envers les personnes, les biens et l'environnement. Elle concourt ainsi à la continuité de l'État en matière d'autorité et de sécurité de la Nation.

2. Enjeux

L'État se doit de garantir la « sécurisation » au risque de mettre en cause sa crédibilité. Il doit donc assurer l'ordre public, la protection et la sécurité civile des citoyens.

En outre, de manière exceptionnelle, des mesures de contrôles aux frontières intérieures peuvent être mises en œuvre. Elles concernent les frontières terrestres (routières et ferroviaires), y compris fluviales et lacustres, aériennes et les limites maritimes sous souveraineté française. Elles ne peuvent être mises en œuvre qu'en respectant les dispositions du règlement (CE) N° 2016/399 du Parlement européen et du Conseil du 9 mars 2016 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes dit « Code frontières Schengen » (CFS).

Le CFS distingue les frontières intérieures de l'espace Schengen, qui séparent les États membres entre eux, des frontières extérieures, qui séparent les États membres et les États tiers. Les frontières terrestres et aériennes de la France métropolitaine relèvent des deux types précités. Les frontières terrestres routières sont exclusivement des frontières intérieures au sens du CFS (à l'exception de la frontière extérieure avec l'Andorre sur laquelle se situe le PPF de Porta). En revanche, les limites maritimes sont exclusivement extérieures.

3. Acteurs

- autorité préfectorale ;
- forces de sécurité intérieure ;
- forces de sécurité civile ;
- autres acteurs privés.

En complément, pour le contrôle aux frontières :

- direction centrale de la police aux frontières (DCPAF) ;
- direction générale des douanes et des droits indirects (DGDDI) ;
- direction générale des infrastructures, des transports et de la mer (DGITM) ;
- directions régionales de l'environnement, de l'aménagement et du logement (DREAL) ;
- opérateurs portuaires et aéroportuaires.

4. Sous-activités et objectifs de sécurité

Intervention des forces spécialisées :

- mettre en œuvre des moyens d'intervention spécialisés des FSI ;
- agir contre les attentats (terrestre, maritime et aérien) ;
- agir contre les menaces NRBC-E.

Ordre public / police judiciaire :

- assurer le maintien de l'ordre public (manifestations, violences urbaines) ;
- réaliser les actes de surveillance et de renseignement (surveillance de personnes ou de frontières, cyber) ;
- identifier les auteurs des infractions.

Protection des institutions et de sites sensibles.

Contrôle des flux, les mobilités et des personnes :

- contrôler les mesures restrictives ;
- contrôler les flux et des frontières (contrôle des personnes, des biens et des vecteurs).

Protection des personnes et des biens :

- protéger la population y compris en outre-mer ;
- secourir les victimes ;
- protéger les biens ;
- mettre en œuvre des moyens de secours NRBC-E ;
- assurer la décontamination ;
- gérer les décès massifs.

Protection de l'environnement :

- protéger l'environnement des pollutions ;
- lutter contre les épizooties et les zoonoses.

5. Cadre juridique et références documentaires

Article L1142-2 : « *Le ministre de l'intérieur est responsable de la préparation et de l'exécution des politiques de sécurité intérieure et de sécurité civile qui concourent à la défense et à la sécurité nationale et il est, à ce titre, sur le territoire de la République, responsable de l'ordre public, de la protection des personnes et des biens ainsi que de la sauvegarde des installations et ressources d'intérêt général.*

À ce titre :

1° Il est chargé de l'anticipation et du suivi des crises susceptibles d'affecter la sécurité intérieure et la sécurité civile ;

2° Il contribue à la planification interministérielle en matière de sécurité nationale. Il prépare les plans à dominante d'ordre public, de protection et de sécurité civiles ;

3° Il assure la conduite opérationnelle des crises ;

4° Il s'assure de la transposition et de l'application de l'ensemble de la planification gouvernementale par les représentants de l'État dans les zones de défense et de sécurité, les départements et les collectivités d'outre-mer. (...) »

Cette responsabilité du ministre de l'intérieur est régulièrement confirmée, notamment par la circulaire du Premier ministre n°6095/SG du 1er juillet 2019 relative à l'organisation gouvernementale pour la gestion des crises majeures (actualisant la circulaire PM du 2 janvier 2012).

Autres textes d'intérêt :

- schéma national d'intervention (SNI) ;
- schéma national du maintien de l'ordre (SNMO) ;
- code pénal ;
- code de procédure pénale ;
- code de la sécurité intérieure ;
- code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA) ;
- loi n° 2009-971 du 3 août 2009 relative à la gendarmerie nationale.
- IM 10100 relative à l'engagement des armées sur le territoire national en cas de crise majeure

Le chapitre II du titre III du CFS dispose que la réintroduction temporaire du contrôle aux frontières intérieures ne peut être décidée qu'en dernier recours, de manière exceptionnelle et en cas de menace grave pour l'ordre public ou la sécurité publique. Elle est décidée par les plus hautes autorités de l'État, pour une durée déterminée et après concertation avec la Commission européenne et les États membres ou sur simple notification des institutions européennes et des États membres en fonction de la gravité des cas.

L'article 78-2 du code de procédure pénale permet aux forces de sécurité intérieure (à l'exclusion de la douane) de contrôler l'identité de toute personne en vue de vérifier le respect des obligations de détention, de port et de présentation des titres et documents prévues par la loi.

Dans ce cadre, le contrôle des obligations de détention, de port et de présentation des titres et documents prévus par la loi ne peut être réalisé que dans une durée n'excédant pas six heures consécutives dans un même lieu et ne peut consister en un contrôle systématique des personnes présentes ou circulant dans ces zones ou lieux. La fouille des bagages et des véhicules pourrait être mise en œuvre en revanche à tous les PPA terrestres.

Il existe des dispositions spécifiques, notamment prévues par les articles L812-1, L812-2, L812-3 et L812-4 du code de l'entrée et du séjour des étrangers et du droit d'asile pour les contrôles réalisés par la PAF dans son domaine de compétence aux frontières terrestres, pour les contrôles des véhicules.

Les fouilles de véhicules et de bagages ne peuvent être réalisées que dans le cadre des articles 78-2-2 et 78-2-4 du code de procédure pénale et ce en tout point du territoire y compris dans les zones frontalières. Les contrôles mentionnés au titre de l'article 78-2 du code de procédure pénale en zone frontalière le sont en vertu de l'alinéa 9 uniquement.

Deux administrations disposent au niveau national du statut de garde-frontières au sens du Code frontières Schengen qui prévoit le rétablissement des contrôles aux frontières intérieures : la DCPAF et la DGDDI. La mise en œuvre du rétablissement des contrôles en frontières intérieures s'inscrit dans le cadre d'une complémentarité étroite entre la douane et la police aux frontières pour la tenue des PPF et PPA. Les armées n'ont pas le statut communautaire de garde-frontières et ne peuvent mettre en application les dispositions du code frontières Schengen.

6. Indicateurs et contrôles de l'exécution

Définis avec les fiches mesures

7. Planifications en lien

- famille PIRATE
- plan troubles intérieurs graves
- plan gouvernemental NRBC
- SNI
- SNMO
- plans de sauvegarde des biens culturels
- POLMAR

8. Commentaires

SANTÉ | SAN

Ministère menant : le ministère de la santé

Ministères concourants : les ministères chargés de l'agriculture, de la recherche, des armées, de l'environnement

1. Nature

La continuité de cette activité doit garantir l'activité et la réactivité des acteurs de santé ainsi que la disponibilité des moyens pour permettre la meilleure prise en charge des victimes, y compris en cas d'afflux massif.

2. Enjeux

Les enjeux sociaux et humains associés au service public de la Santé sont primordiaux pour la société car l'activité santé doit rester ouverte sans interruption à toutes les personnes qui nécessitent des soins.

Le système de santé notamment les établissements de santé, doit donc garantir l'accessibilité et la continuité de l'offre de soin en préservant la qualité des soins.

Cette démarche s'inscrit dans un contexte international qu'il convient de veiller pour répondre aux attentes légitimes de protection de la population.

3. Acteurs

Au sein du ministère de la santé, la direction générale de la santé (DGS) assure le pilotage de la mobilisation du système de santé en lien avec les autres directions générales (DGOS, DGCS) et les agences et établissements sous tutelle.

Les acteurs de l'offre de soin :

Les établissements de santé publics ou privés ont une mission d'accueil permanent. Certains établissements de santé (CHU, CHR…) sont indispensables dans l'organisation de la réponse aux situations sanitaires exceptionnelles (établissements de santé de référence NRBC, spécialités peu fréquentes ou exclusives). Les professionnels de santé de ville (médecins, pharmaciens, infirmiers, biologistes, etc.) constituent un premier maillon indispensable de la chaine de soins et de veille sanitaire. Enfin, les établissements et services médico-sociaux, assurent l'accueil et la prise en charge des personnes fragiles.

Les acteurs du dispositif de veille et d'alerte :

Le dispositif repose sur le réseau des agences régionales de santé (ARS), sur le système de déclaration obligatoire de certaines maladies, sur l'agence nationale de santé publique (ANSP) et sur les laboratoires répartis sur le territoire. La France partage ses informations d'alerte et de veille avec l'Union Européenne et au niveau mondial avec l'organisation mondiale de la santé (OMS) dans le cadre du règlement sanitaire international (RSI)

Les laboratoires spécialisés d'analyse assurent l'identification d'éventuels agents NRBC afin d'orienter les mesures de prévention et de soin. Ils s'articulent autour de trois dispositifs :

- Les laboratoires du réseau BIOTOX-PIRATOX-PIRATOME, dont les laboratoires BIOTOX-eau ;
- les laboratoires hospitaliers équipés pour le diagnostic d'agents biologiques ou chimiques ;
- les centres nationaux de référence (CNR) pour la surveillance des maladies transmissibles.

Les dispositifs en matière d'épidémiosurveillance en santé animale et de surveillance sanitaire de la chaine alimentaire participent également à l'objectif global de veille, de prévention et d'alerte sanitaire. Ils mobilisent de nombreux acteurs, publics et privés, autour du ministère en charge de l'agriculture, dont les services de l'État (DRAAF, DDI), les laboratoires nationaux de référence et les laboratoires agréés ainsi que les vétérinaires sanitaires et les opérateurs de la chaine alimentaire.

Les acteurs majeurs de la fabrication et la distribution des produits de santé

La distribution des produits de santé, notamment de médicaments s'appuie sur un réseau de grossistes répartiteurs et de dépositaires qui approvisionnent les 26000 pharmacies et établissements de santé du territoire en flux tendu compte tenu du prix et de la péremption des produits.

Les agences sanitaires nationales concourent au dispositif d'autorisation, de fabrication, de distribution et de surveillance du marché (ANSM, ANSP, EFS, etc.)

Afin de produire de la connaissance et permettre l'activation des contremesures pour lutter contre les pandémies, le ministère chargé de la recherche scientifique met en alerte et mobilise la recherche et l'innovation d'urgence :

- développement et mise à disposition de méthodes et d'outils de diagnostic et d'investigation ;
- coordination de la mobilisation opérationnelle des laboratoires et personnels de recherche ;
- coordination et/ou participation aux travaux des groupes d'experts scientifiques, notamment pour la modélisation et l'information des médias.

Sous réserve de la réalisation de sa mission prioritaire au profit des armées, le service de santé des armées (SSA) et d'autres unités ou services des armées peuvent appuyer le dispositif civil de réponse à une crise sanitaire aigüe sur le territoire national.

4. Sous- activités et objectifs de sécurité

Offre de soins :

- assurer la prise en charge des patients ;
- assurer une régulation médicale ;
- maintenir une capacité de soins critiques et d'urgences médico-chirurgicales ;
- préserver le personnel de santé.

Veille sanitaire :

- assurer une veille épidémiologique dans une approche intégrée « une seule santé » (santé humaine, alimentation et santé animale) ;
- édicter une stratégie de lutte contre l'épidémie ;
- mobiliser les laboratoires ;
- mettre en œuvre et contrôler une stratégie de dépistage en mobilisant si besoin l'ensemble des capacités disponibles (dont les capacités analytiques vétérinaires) ;
- mettre en œuvre une campagne de vaccination.

Produits de santé, contremesures et protection :

- assurer la production des produits de santé ;
- garantir l'approvisionnement en produits de santé ;
- mettre en place une réserve de produits de santé.

Recherche et innovation en situation d'urgence :

- mobiliser l'expertise scientifique et de recherche adaptée à la nature de l'événement pour mise en œuvre d'une réponse d'urgence ;
- concourir à une information fondée.

5. Cadre juridique et références documentaires

Article L.1142-8 du code de la défense : « le ministre chargé de la santé est responsable de l'organisation et de la préparation du système de santé et des moyens sanitaires nécessaires à la connaissance des menaces sanitaires graves, à leur prévention, à la protection de la population contre ces dernières, ainsi qu'à la prise en charge des victimes ».

6. Indicateurs et contrôles de l'exécution

7. Planifications en lien

Plan national de préparation et de réponse à une pandémie.

Planification ORSAN.

8. Commentaires

SOCIAL ET SOCIÉTAL — SOC

Ministères menants : les ministères chargés des affaires sociales, de l'éducation nationale, de l'économie, de l'environnement, du travail, de la culture

Ministère concourant : le ministère des armées

1. Nature

La continuité de cette activité vise à maintenir une vie sociale et la permanence de l'exercice de la représentation et de l'administration de l'État.

2. Enjeux

Face aux forts enjeux sociaux et humains, l'État doit assurer la permanence de son fonctionnement et du soutien qu'il est en mesure d'apporter pour garantir en toutes circonstances l'accessibilité à ses services.

3. Acteurs

Compte tenu de l'étendue et de la diversité du spectre de cette activité clé, la cartographie des acteurs étatiques ou non sera précisée dans les fiches mesures associées.

4. Sous- activités et objectifs de sécurité

Résilience de la société civile :

- faire appel à la solidarité locale ;
- soutenir les acteurs de la gestion de crise ;
- associer la société civile à la gestion de crise.

Éducation :

- assurer la continuité de l'enseignement et de formation ;
- adapter les modalités d'accueil et de fonctionnement des établissements d'enseignement ;
- adapter les modalités d'accès aux activités scolaires, périscolaires et extrascolaires ;
- maintenir le lien avec les élèves/étudiants et personnel ;
- assurer l'accueil des enfants du personnel indispensable à la gestion de crise.

Hébergement :

- assurer l'hébergement des personnes vulnérables ;
- assurer l'hébergement des personnes en situation précaire ;
- mettre en place des structures de quarantaine ;
- mettre en place un hébergement d'urgence.

Déchets :

- assurer le traitement des eaux usées ;
- assurer l'évacuation et la collecte des déchets ;
- assurer l'évacuation et la collecte des déchets spécifiques (DASRI, NRBC…).

Organisation de la vie :

- organiser, contrôler les activités sociales (rassemblements, activités culturelles…) ou les espace publics ;
- avoir recours au télétravail ;
- réglementer les loisirs.

Emploi, chômage…

- garantir le versement des minima sociaux ;
- optimiser l'emploi des ressources critiques.

Administration publique :

- assurer une continuité de service des administrations ;
- organiser la continuité du fonctionnement démocratique (élections…).

5. Cadre juridique et référence documentaire

Article L.1141-1 du code de la défense : « chaque ministre est responsable, sous l'autorité du Premier ministre, de la préparation et de l'exécution des mesures de défense et de sécurité nationale incombant au département dont il a la charge ».

6. Indicateurs et contrôles de l'exécution

7. Planifications en lien

Plan gouvernemental « déplacement massif de population »

8. Commentaires

ALIMENTATION ET EAU — ALE

Ministère menant : ministères chargés de l'environnement, de la santé, de l'industrie, de l'économie
Ministères concourants : ministères chargés de l'intérieur et de l'outre-mer, et de l'agriculture et de l'alimentation

1. Nature :

Garantir pendant toute la durée de la crise un approvisionnement en produits de première nécessité (dont aliments et eau).

2. Enjeux

La stratégie vise à garantir à court terme l'approvisionnement des populations et de s'assurer de la continuité des approvisionnements à moyen et long termes.
En fonction des impacts directs et indirects de la crise et de ses caractéristiques, il s'agit donc de :

- sensibiliser les citoyens à la constitution d'un kit familial d'urgence pour faciliter la gestion de la phase d'extrême urgence (quelques heures ou quelques jours qui suivent l'évènement déclencheur) ;
- mobiliser les stocks facilement disponibles (notamment ceux détenus par les professionnels de la grande distribution et d'autres contributeurs tels que les associations agréées de sécurité civile et les banques alimentaires) et organiser leur acheminement (chaine logistique) et leur mise à la disposition des populations ;
- organiser le réapprovisionnement au moyen d'autres stocks ou de la mobilisation, et si nécessaire du renforcement, des capacités de production et de transformation ;
- mobiliser le cas échéant les stocks de réactifs consommables nécessaires aux différentes étapes de la production d'eau potable et au fonctionnement des usines de potabilisation.

Un haut niveau de sécurité sanitaire des produits (eau destinée à la consommation humaine et aliments) doit être garanti tout au long de la gestion de la crise.
Le rétablissement rapide des conditions normales d'approvisionnement et de distribution doit être recherché dans l'objectif d'une reconquête économique et sociale du territoire touché.

3. Acteurs

Acteurs étatiques :

- ministères chargés de l'économie et de l'industrie (protection économique des consommateurs / sécurité et conformité de tous les produits alimentaires et industriels / relation avec le secteur de la distribution et les organismes professionnels de la grande distribution) ;
- ministère chargé de l'agriculture (chaine alimentaire / contrôles sanitaires de la production à la distribution – SAIV / secteur « alimentation ») ;
- ministère chargé de l'environnement (SAIV / secteur « gestion de l'eau » / transports) ;
- ministère chargé de la santé (eau destinée à la consommation humaine, y compris les installations de production et de distribution / contrôles sanitaires) ;
- ministère de l'intérieur (organisation des secours / ordre public) ;
- services territoriaux en charge des contrôles officiels (DRAAF, DREETS, DREAL, ARS, DDI) et préfectures de départements.

Agences d'évaluation du risque, notamment :

- Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;
- Santé publique France (ANSP).

Collectivités territoriales (PCS / résilience individuelle et collective des citoyens).

Opérateurs de la chaine alimentaire : production agricole, transformation agroalimentaire, stockage, transport, distribution, consommation (responsables de la conformité des produits qu'ils mettent sur le marché / opérateurs particuliers : OIV - secteur « alimentation » et secteur « gestion de l'eau »).

4. Sous- activités et objectifs de sécurité

Les objectifs de sécurité principaux sont :

- renforcer la résilience individuelle et collective des populations, dont leur capacité de réponse en phase d'urgence ;
- prévenir les ruptures d'approvisionnement en eau ou en aliments de nature à mettre en péril la sécurité alimentaire des populations ;
- couvrir les besoins hydriques et énergétiques des populations sinistrées, dont les personnes vulnérables, en cas de dysfonctionnement des chaines habituelles d'approvisionnement ;
- garantir un haut niveau de sécurité sanitaire pendant la phase d'urgence et ce jusqu'au retour à la normale ;
- rétablir les conditions normales d'approvisionnement et de distribution en eau et en aliments.

Pour atteindre ces objectifs de sécurité, les actions mises en œuvre diffèrent en fonction :

- des caractéristiques intrinsèques de l'évènement déclencheur et sa localisation (tsunami, pandémie, accident nucléaire ou radiologique, attaque NRBC, etc.) ;
- de la temporalité de la crise et de ses impacts (actions à court, moyen et long termes) ;
- du positionnement et de la responsabilité des acteurs (échelons territorial et national).

L'atteinte des objectifs nécessite la mobilisation des fonctions de coordination, notamment les aspects financiers, la logistique et la communication.

5. Cadre juridique et références documentaires

Article L.1141-2 du code de la défense - Dans les cas prévus à l'article L.1111-2, un seul ministre est responsable, pour chacune des grandes catégories de ressources essentielles à la vie du pays telles que les matières premières et produits industriels, l'énergie, les denrées alimentaires, les transports, les entreprises de travaux publics et de bâtiments, les télécommunications, des mesures à prendre pour satisfaire au mieux les besoins des ministres utilisateurs.

Article R 1141.1 du code de la défense – Les ministres mentionnés à l'article L.1141-2 comme responsables en permanence des mesures à prendre pour assurer les besoins des ministres utilisateurs sont : [...] 3° Le ministre chargé de l'industrie, en ce qui concerne l'énergie, les matières premières et produits industriels. 4° Le ministre chargé de l'agriculture, en ce qui concerne les denrées et produits destinés à l'alimentation humaine et à la nourriture des animaux.

Article L 1142-3 du code de la défense - Le ministre chargé de l'économie prend les mesures de sa compétence garantissant la continuité de l'activité économique en cas de crise majeure et assure la protection des intérêts économiques de la Nation. Il oriente l'action des ministres responsables de la production, de l'approvisionnement et de l'utilisation des ressources nécessaire à la défense et à la sécurité nationale.

Article L 1142-8 du code de la défense - Le ministre chargé de la santé est responsable de l'organisation et de la préparation du système de santé et des moyens sanitaires nécessaires à la connaissance des menaces sanitaires graves, à leur prévention, à la protection de la population contre ces dernières, ainsi qu'à la prise en charge des victimes. Il contribue à la planification interministérielle en matière de défense et de sécurité nationale en ce qui concerne son volet sanitaire.

6. Indicateurs et contrôles de l'exécution

7. Planifications en lien

- dispositif ORSEC, dispositions générales, mode d'action « soutien des populations » ;
- plan communal de sauvegarde (PCS) ;
- plan intercommunal de sauvegarde (PICS).

8. Commentaires

Interactions avec les activités clés « Sécurisation », « Économie », « Social et sociétal ».

POSTE ET COMMUNICATIONS ELECTRONIQUES | PCE

Ministère menant : ministère chargé des communications électroniques et des postes

Ministères concourants : Premier ministre (ANSSI), ministère de l'intérieur

1. Nature

La continuité de ces activités doit permettre de maintenir la permanence des correspondances et des accès aux systèmes d'information, essentielle au fonctionnement de l'économie et à la vie de la Nation.

Ces activités sont portées par :

- les opérateurs de communications électroniques, c'est-à-dire les exploitants de réseaux ou services de communications électroniques ouverts au public ;
- les opérateurs de services postaux, tout particulièrement l'opérateur en charge du service postal universel.

2. Enjeux

L'enjeu principal consiste à éviter une interruption totale et durable :

- des communications électroniques, pour les services destinés tant au grand public qu'aux entreprises et administrations ;
- du service postal universel, pour les courriers et petits colis au profit du grand public et des entreprises et administrations.

Les axes d'effort portent sur :

- la protection des infrastructures et systèmes, avec une attention particulière portée à la sécurité physique et à la redondance des sites et artères majeurs, ainsi qu'à la sécurité logique des systèmes ;
- la capacité de détection et de réaction face aux alertes et incidents majeurs, tant en matière d'organisation que de compétences et moyens techniques.

La stratégie de sécurité retenue sera nécessairement fortement liée avec l'activité clé NUMERIQUE du fait de l'imbrication entre numérique et communications électroniques.

3. Acteurs

Ministère chargé des communications électroniques et des postes

Le Commissariat aux communications électroniques de défense (CCED), veille, au nom du ministre chargé des communications électroniques, à la satisfaction des besoins en communications électroniques liés à la défense et à la sécurité publique, ainsi qu'à l'application par les opérateurs des prescriptions du code des postes et des communications électroniques (CPCE) en matière de défense et de sécurité publique.

Le SHFDS des ministères économiques et financiers est en charge du pilotage du dispositif SAIV pour les secteurs couvrant les communications électroniques et les postes (directives nationales de sécurité « communications électroniques et internet » et « industrie »).

En outre, l'Agence nationale de fréquences (ANFR), établissement public sous tutelle du ministère, gère les fréquences radioélectriques en France et contrôle leur utilisation. Elle réalise des mesures permettant d'identifier les causes de brouillages.

Ministère de l'intérieur

Le Ministère de l'intérieur intervient au titre du dispositif ORSEC et de la mise en œuvre, au niveau local, du dispositif SAIV.

Premier ministre

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), en tant qu'autorité nationale en matière de cybersécurité et de cyberdéfense, est notamment en charge de piloter la partie cyber du dispositif SAIV.

Autorité indépendante - régulateur

L'autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), autorité administrative indépendante (AAI), est l'autorité de régulation nationale. Elle veille de manière générale au respect par les opérateurs de leurs obligations en matière de qualité de service.

Opérateurs :

- les opérateurs de communications électroniques et, indirectement, les hébergeurs ;
- la Poste, en tant que titulaire du service postal universel, mais aussi les autres opérateurs de services postaux d'information assurent un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État.

4. Sous- activités et objectifs de sécurité

Réseaux télécommunications :

- assurer la permanence et la sécurité des services des réseaux de téléphonie fixes et mobiles ;
- assurer la permanence et la sécurité du transport de données et de l'internet ;
- assurer la protection des réseaux satellitaires et des réseaux de câbles sous-marins.

« Service universel postal » : assurer « une offre de services postaux de qualité déterminée fournis de manière permanente en tout point du territoire à des prix abordables pour tous les utilisateurs » (Directive 97/67/CE).

5. Cadre juridique et références documentaires

Code de la défense

Articles L.1332-1 à L.1332-7 sur le dispositif de sécurité des activités d'importance vitale.

Article L.1334-1 sur les postes et communications électroniques.

Articles L.1332-1 et suivants pour le dispositif SAIV.

Article L.2151-4 sur la nécessité, pour les OIV, de disposer d'un PCA / PRA.

Code des postes et des communications électroniques

Article L.2 sur le service universel postal et les obligations du service postal.

Article L.33.-1 sur les règles applicables aux réseaux et services de communications électroniques.

Code de la sécurité intérieure

Articles L.732-1 à L.732-2-1 sur le maintien de la satisfaction des besoins prioritaires de la population.

6. Indicateurs et contrôles de l'exécution

Contrôles prévus par le cadre juridique susmentionné.

Retours d'expérience d'exercices ou d'incidents réels.

7. Planifications en lien

Dispositif SAIV (DNS secteur « communications électroniques et audiovisuel » et DNS du secteur industrie).

ORSEC « RETAP Réseaux ».

Contrat d'entreprise 2018-2022 entre l'État et La Poste – article 5 de la loi du 2 juillet 1990 n° 90-568 relative à l'organisation du service public de la poste et à France Télécom.

8. Commentaires

ACTIVITÉS ÉCONOMIQUES — ECO

Ministère menant : ministère chargé de l'économie

Ministères concourants : tous les ministères

1. Nature

Garantir la continuité économique de la Nation, limiter les effets de la crise (population, entreprises) et favoriser la relance économique.

2. Enjeux

- assurer une veille et disposer d'indicateurs sur les impacts économiques des crises ;
- apporter un soutien financier aux acteurs économiques et au grand public pendant les crises et pour la reprise de l'économie ensuite ;
- piloter la continuité d'activité du secteur des finance ;.

De manière transverse, les différents ministères soutiennent la continuité d'activité des secteurs relevant de leurs périmètres, et contribuent ainsi à la continuité de l'activité économique.

3. Acteurs

- Les MEF (COBER/CCE), tous ministères.
- ***COBER/CCE.***

Les MEF organisent un dispositif de veille et de suivi de tout événement, intervenant en France ou à l'étranger, susceptible d'avoir un impact sur la situation économique du pays. Chaque ministère et opérateur participe à enrichir le dispositif de veille en **adressant au centre opérationnel des ministères économiques et financiers (COBER)** l'évaluation des impacts économiques que l'évènement a générés ou est susceptible de générer sur son champ de compétence.

La circulaire du Premier ministre du 1er juillet 2019 prévoit que : « *Lorsque la crise risque d'avoir un impact économique important, le ministre de l'économie, qui est représenté en CIC, active* ***la cellule de continuité économique (CCE) composée des représentants des directions des ministères concernés et des opérateurs*** *des secteurs d'activité d'importance vitale concernés, en particulier ceux relevant de sa compétence. Cette cellule alimente le travail d'évaluation de la situation et d'anticipation de la CIC. Elle s'appuie sur les chargés de mission de sécurité économique auprès des préfets de zone de défense et de sécurité.* ». Cette structure permet également de dialoguer avec les fédérations professionnelles concernées.

Sur la base de l'analyse fournie dans ce cadre, le COBER procède à la synthèse des indicateurs de suivi de la situation économique et des mesures de soutien (aux entreprises, à la population) et la transmet à la CIC.

Pilotage des dispositifs SAIV et des dispositifs de continuité sectoriels

- **La Banque de France**

La Banque de France pilote notamment la continuité d'activité de la filière fiduciaire, et à travers le Groupe de Place Robustesse (GPR), les travaux relatifs à la continuité de la Place financière de Paris (constituée des principaux établissements de crédit et opérateurs d'infrastructures financières).

- **Les opérateurs**

Sont concernés les opérateurs des différents secteurs (OIV ou non), notamment ceux du secteur des finances : établissements de crédit (banques), organismes d'assurance, infrastructures de paiements, infrastructures de marché.

4. Sous-activités et objectifs de sécurité

capacité de production et fonctionnement de l'économie nationale :

- déployer un système de veille et d'indicateurs : évaluation de l'impact de l'évènement sur la situation économique ;
- soutenir les entreprises impactées (comité stratégique des filières industrielles, etc.) ;
- soutenir la population impactée ;
- suivre les prix ;
- assurer la continuité des marchés financiers ;
- assurer la promotion des Plans de Continuité d'Activité (public et privé) et anticiper le maintien des activités essentielles en outre-mer.

Secteur financier :

- assurer la continuité et l'intégrité des fonctions essentielles du secteur, notamment des flux financiers entre l'État et le reste de l'économie, des activités bancaires (en particulier l'approvisionnement fiduciaire), des infrastructures de marchés financiers et de paiement, des activités assurantielles.

5. Cadre juridique et référence documentaire

Article L.1142-3 du code de la défense :

- Le ministre chargé de l'économie est responsable de la préparation et de l'exécution de la politique de sécurité économique. Il prend les mesures de sa compétence garantissant la continuité de l'activité économique en cas de crise majeure et assure la protection des intérêts économiques de la Nation.
- Il oriente l'action des ministres responsables de la production, de l'approvisionnement et de l'utilisation des ressources nécessaires à la défense et à la sécurité nationale.
- Conjointement avec le ministre chargé du budget, il assure la surveillance des flux financiers.

Article L.1332-1 et suivants du code de la défense pour le dispositif SAIV.

Circulaire du 1er juillet 2019 relative à l'organisation gouvernementale pour la gestion des crises majeures.

6. Indicateurs et contrôles de l'exécution

Contrôles prévus par les différents dispositifs réglementaires, retours d'expérience d'exercices.

7. planifications en lien

Groupe de place robustesse.

Dispositif SAIV.

8. commentaires

ÉNERGIES — NRJ

Ministère menant : le ministère chargé de l'environnement et de l'énergie
Ministère concourant : le ministère chargé de l'économie et de l'industrie

1. Nature

La continuité de cette activité vise à maintenir la distribution des énergies, c'est-à-dire principalement l'électricité, le gaz et les hydrocarbures.

2. Enjeux

La **production électrique** française est principalement assurée par le parc nucléaire qui fournit l'électricité en base et par les centrales à gaz qui contribuent au réglage de la puissance.

Le réseau de transport d'électricité est organisé autour du grand réseau d'interconnexion composé essentiellement des ouvrages à 400 kV auquel sont raccordées toutes les principales centrales de production. Le réseau français est connecté aux réseaux de transport d'électricité de la plupart des pays européens continentaux au sein du réseau principal de l'UCTE (union for the coordination of transmission of electricity). Cette interconnexion permet à tous les pays associés de bénéficier d'un système de secours mutuel en cas d'incident important. Elle constitue un facteur essentiel pour la stabilité et la sécurité du système électrique français.

Au niveau régional, les réseaux de transport de répartition sont alimentés à partir du réseau à 400 kV par l'intermédiaire de postes de transformation du réseau de transport. Ces réseaux desservent à leur tour les postes sources des réseaux publics de distribution exploités par les distributeurs d'électricité et les distributeurs non nationalisés. Ces réseaux s'appuient sur des *dispatchings* régionaux correspondant aux zones de défense et sur un centre de *dispatching* national.

Contrairement au réseau de transport qui est maillé, le réseau de distribution d'ERDF n'est pas redondant, et la coupure d'une ligne de 20 000 volts ou d'un poste source affecte la totalité des clients jusqu'à sa réparation.

Le **secteur relatif à l'alimentation en gaz naturel** couvre l'acquisition des produits gaziers, la re-gazéification, le transport et le stockage de gaz.

Il est organisé autour des réseaux de transport et de distribution de gaz entre les points d'échanges avec les pays voisins, à l'amont, des terminaux et installations de stockage et les points de livraison aux utilisateurs. La particularité du système gazier est la possibilité de pouvoir stocker du gaz, soit sous forme liquide dans les terminaux méthaniers, soit sous forme gazeuse dans les stockages souterrains.

Le **secteur pétrolier** est constitué en chaînes logistiques entre les points d'importation et de raffinage et les points de distribution et de livraison des hydrocarbures liquides. Les hydrocarbures liquides d'origine pétrolière sont utilisés pour la production industrielle et énergétique, les transports, les activités économiques et sociales du secteur tertiaire et le secteur résidentiel. Une obligation de stocks stratégiques existe pour couvrir 29,5% des besoins annuels métropolitains, soit environ 90 jours. Le droit de réquisition et de répartition des ressources pétrolières est organisé par la loi en cas de crise ou de pénurie. En cas de crise, une réquisition de moyens des armées peut être effectuée.

3. Acteurs

La commission de régulation de l'énergie (CRE) est l'autorité administrative indépendante chargée de veiller au bon fonctionnement des marchés de l'*électricité* et du gaz en France. Elle régule les réseaux et les marchés et est garante de l'indépendance des gestionnaires. Les services de l'État délivrent les autorisations d'exploitation sur avis de la CRE.

Pour l'électricité : chaque opérateur est responsable dans son domaine de la continuité du service. La production d'électricité est principalement assurée par EDF, et par un grand nombre de petits producteurs. Le transport est entièrement assuré par RTE qui agit en tant que monopole sous le contrôle de la CRE. La distribution est assurée principalement par ERDF, filiale d'EDF et par des régies municipales ou des distributeurs privés.

Concernant le nucléaire civil, le contrôle est assuré par l'autorité de sûreté nucléaire (ASN), qui est une autorité indépendante. Le MIOM assure la protection opérationnelle des emprises concernées avec les pelotons spécialisés de protection de la gendarmerie (PSPG).

Pour le gaz : le transport est assuré par les seuls acteurs que sont GRT gaz et TIGF. Pour la distribution, GrDF est l'opérateur principal de distribution souvent par le biais de concessions, même si des entreprises locales de distribution existent.

Les services de l'État décident de l'utilisation éventuelle des stocks stratégiques dans le cadre des accords liant les États adhérents à l'agence internationale de l'énergie et conformément à la réglementation européenne[24]. Les opérateurs du secteur agissent dans le cadre de contrats qui définissent leurs obligations en matière de mise à disposition de produits pour la constitution des stocks stratégiques.

4. Sous- activités et objectifs de sécurité

Electricité :

- assurer l'approvisionnement en électricité ;
- intervenir en cas d'interruption ;
- réguler l'offre.

Nucléaire civil :

- assurer la production d'électricité ;
- assurer la production d'isotopes ;
- assurer le stockage et le transport de matières.

Hydrocarbure :

- permettre l'importation des hydrocarbures pétroliers ;
- assurer la disponibilité des produits raffinés ;
- permettre l'acheminement des hydrocarbures dans les ouvrages ;
- assurer le stockage stratégique.

Gaz :

- assurer l'approvisionnement en gaz ;
- intervenir en cas d'interruption ;
- réguler l'offre.

Énergies renouvelables

Chauffage urbain ;

Hydrogène.

5. Cadre juridique et références documentaires

Les ministres chargés de l'environnement, de l'énergie et de l'industrie conduisent les travaux de planification visant au maintien en toutes circonstances de la continuité dans les secteurs de la production et de l'approvisionnement énergétique (L1142-9).

IGI 6600.

6. Indicateurs et contrôles de l'exécution

/

7. Planifications en lien

Une planification européenne existe aussi pour la gestion européenne d'une crise, les réseaux électriques étant interconnectés et fortement interdépendants.

Plans ressources / PNRANRM / Continuité élec / Hydrocarbure / Gaz…

DNS/SAIV.

8. Commentaires

24 - Directive 68/414/CEE du 14 décembre 1968, modifiée par la directive 98/93/CE du 31 décembre 1998.

TRANSPORTS | MOB

Ministère menant : les ministères chargés des transports et de la mer
Ministère concourant : le ministère chargé des armées

1. Nature

La continuité de cette activité vise à garantir la liberté de circulation dans tous les milieux.

2. Enjeux

Ces secteurs d'activités concourent à la production de services indispensables au bon fonctionnement de l'économie et sont difficilement remplaçables ou substituables.

3. Acteurs

Les acteurs étatiques

- Le commissariat général aux transports (COMIGETRA) est un organisme de l'état-major des armées (EMA) hébergé au ministère chargé des transports qui assure la liaison entre les directions de transport [direction générale des infrastructures, des transports et maritime (DGITM) et direction générale de l'aviation civile (DGAC)] et le ministère des Armées.
- Il assure une veille stratégique de la politique générale des transports pour préserver les intérêts de la défense, notamment pour l'accès aux infrastructures civiles, routières, portuaires et aéroportuaires, et aux capacités civiles de transport multimodal (ferrées, routières, maritimes et aériennes).

Pour le milieu aérien :

- la direction générale de l'aviation civile (DGAC), par délégation du ministre chargé des transports, fait appliquer la réglementation européenne et nationale dans le domaine de la sûreté et est chargée de superviser l'obligation de moyens mis en œuvre par les opérateurs. Sa direction des services de navigation aérienne (DSNA), les services de contrôle aérien de la défense et Eurocontrol assurent le trafic dans l'ensemble de l'espace aérien français et plus généralement dans les régions d'information de vol (FIR) gérées par la France ;
- la surveillance de l'espace aérien national ainsi que de ses approches relève de la défense aérienne et est confiée au commandant de la défense aérienne et des opérations aériennes (COMDAOA). Sous l'autorité du Premier ministre, le COMDAOA est responsable en toutes circonstances de l'application des mesures de sûreté aérienne dans l'espace aérien national. Dans ce cadre, une haute autorité de défense aérienne (HADA), positionnée au centre national des opérations aériennes (CNOA), s'appuie sur un dispositif mobilisant des moyens au sol et en vol pour assurer le volet aérien de la posture permanente de sûreté ;
- les mesures de sûreté en vol sont effectuées, sous l'autorité de la HADA, par les unités militaires montant la permanence opérationnelle ; au sol, les mesures sont mises en œuvre par la gendarmerie des transports aériens (GTA), la police aux frontières et les douanes dans leurs périmètres respectifs.

Pour le milieu maritime :

- le cadre est celui de l'action de l'État en mer (AEM). Cette dernière s'exerce au sein des différentes zones maritimes. Une zone maritime comprend des espaces placés sous la souveraineté (eaux intérieures, mer territoriale) ou sous la juridiction de la France (zone contigüe, zone économique exclusive), mais aussi la haute mer sur laquelle la France peut exercer certaines attributions, soit à l'égard de ses propres navires, soit à l'égard des navires étrangers en vertu de conventions internationales ;
- la zone maritime est l'espace de compétence de l'autorité maritime unique (le préfet maritime en métropole, le délégué du gouvernement pour l'action de l'État en mer (DDG AEM) assisté du commandant de zone maritime (CZM) outre-mer) dont le rôle est la coordination des 45 missions AEM identifiées (réparties en 10 domaines) entre les administrations disposant de moyens d'intervention (principalement les affaires maritimes, les douanes, la gendarmerie et la Marine nationale). La sûreté maritime ainsi que la souveraineté et la protection des intérêts nationaux sont deux des domaines d'intervention de l'AEM.

Pour le milieu terrestre :

- la direction générale des infrastructures, des transports et de la mer (MTES/DGITM), gère et aménage le réseau routier national ;
- les conseils départementaux et les communes pour les réseaux routiers **départementaux et communaux**, conformément aux lois de décentralisation.

Les acteurs hors du périmètre de l'État

Pour le milieu aérien :

- les compagnies aériennes en particulier Air-France-KLM, ainsi que les grands opérateurs de fret.
- les plates-formes aéroportuaires, en particulier en outre-mer, essentielles pour la continuité territoriale.
- les opérateurs majeurs :
  - Météo France rend le service météorologique relatif à la navigation aérienne ;
  - les opérateurs, gestionnaires d'aéroports (Groupe aéroports de Paris, Société aéroportuaire aéroports de Lyon, SA Aéroports de la Côte d'Azur, etc.) assurant, dans leurs domaines de compétence, la gestion des passagers et des infrastructures des aéroports tant « côté piste » que « côté ville ».

Pour le milieu maritime :

- les compagnies maritimes pour le volet navires
- les infrastructures portuaires pour l'interface terre-navires :
  - les opérateurs d'infrastructure identifiée comme « grand port maritime » ;
  - les ports relevant des collectivités territoriales et outre-mer ;
  - les infrastructures portuaires de soutien (écluses, ponts etc.).

Pour le milieu fluvial :

- les opérateurs du transport fluvial sont les opérateurs de voies navigables et les opérateurs d'installations portuaires, dont :
  - l'établissement des voies navigables de France (6700 km de voies navigables) ;
  - la compagnie nationale du Rhône ;
  - les opérateurs d'infrastructures portuaires.

Pour le milieu terrestre :

- les opérateurs et gestionnaire des routes ;
- les opérateurs de tunnels (nationaux ou binationaux) ;
- les opérateurs de transports de voyageurs ;
- les opérateurs de transport de fret ;
- les opérateurs assurant, au bénéfice des acteurs du système ferroviaire, des missions communes essentielles dans les domaines de la sûreté ou du traitement des données ou de l'information ;
- les opérateurs d'infrastructures en charge du réseau ferré national ;
- les opérateurs desservant une agglomération ou une communauté de communes.

4. Sous- activités et objectifs de sécurité

Gestion des Flux :

- contrôler la liberté de circulation des biens et des personnes ;
- garantir les flux logistiques terrestres ;
- garantir les flux logistiques outremer.

Espace terrestre :

- contrôler les axes.

Espace aérien :

- garantir la liberté de l'espace aérien ;
- contrôler les vecteurs aériens, les infrastructures et les approches.

Espace maritime et fluviale :

- garantir la liberté de l'espace maritime ;
- contrôler les vecteurs maritimes, les infrastructures et les approches.

5. Cadre juridique et références documentaires

Les ministres chargés des transports et de la mer et le ministère des armées conduisent les travaux de planification visant à assurer le maintien en toutes circonstances de la continuité des transports.

Aérien : aa réglementation européenne est particulièrement exigeante et détaillée dans le domaine de la sûreté. Elle est transposée dans la législation et les réglementations nationales, en particulier dans le code des transports ainsi que dans le code de l'aviation civile. Celles-ci peuvent occasionnellement, en le justifiant auprès de l'agence de l'Union européenne pour la sécurité aérienne (AESA, rattachée à la Commission européenne), fixer des mesures plus strictes. Elles couvrent 12 domaines du secteur aérien : sûreté aéroportuaire, sûreté des aéronefs, sûreté des passagers, des bagages de cabine, des bagages de soute, du fret et du courrier, traitement du courrier et du matériel du transporteur, des approvisionnements de bord, des fournitures des aéroports, du recrutement et de la formation du personnel et de la conformité des équipements de sûreté des aéroports.

Maritime : code ISPS25 et son application européenne renforcée telle que définie par le règlement européen (CE) 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires et par la directive européenne 2005/65 26 octobre 2005 en matière de lutte contre les actes de malveillance et notamment les actes terroristes. L'arrêté interministériel du 4 juin 2008 qui décline au niveau national la réglementation européenne prévoit dans les installations portuaires la création de zones d'accès réservées à l'entrée desquelles peuvent être inspectés et filtrés les personnes et les véhicules.

Terrestre : pour la liaison fixe sous la Manche, les mesures font référence aux dispositions du traité de Cantorbéry et aux conclusions du comité de sûreté binational lié à ce traité. Elles assurent un contrôle systématique des passagers et de leurs bagages ainsi que des contrôles ciblés des véhicules et du fret. Des conventions binationales sont également en vigueur pour d'autres liaisons transfrontalières.

Les obligations faites aux opérateurs ne peuvent donc être décidées qu'en application de traités internationaux ou du code des transports, du code de la construction et des habitations pour ce qui concerne les infrastructures recevant du public, ou du code de la défense

Les contrôles et mesures restrictives éventuelles appliquées aux usagers ne peuvent être mis en œuvre qu'en application du code des transports ou le cas échéant du code de procédure pénale.

6. Indicateurs et contrôles de l'exécution

7. Planifications en lien

PIRATMER/PIRATAIR/PMT

8. Commentaires

25 - *International ship and port facility security* (code international pour la sûreté des navires et des installations portuaires).

JUSTICE — JUS

Ministère menant : le ministère chargé de la justice

1. Nature

Le maintien de cette activité clé doit permettre de garantir la continuité du traitement des conflits, du suivi des peines.

2. Enjeux

Cette activité est garante de l'égalité devant la loi. Une situation de crise peut mettre sous tension les institutions comme les procédures qu'il convient de préserver dans le respect des principes permettant de bénéficier d'une justice impartiale et de bonnes conditions d'exécution des peines.

3. Acteurs

- Direction des services judiciaires (DSJ / juridictions) ;
- Direction de la protection judiciaire de la jeunesse (DPJJ) ;
- Conseil d'État et juridictions administratives ;
- Direction de l'administration pénitentiaire (DAP).
- Unités de la gendarmerie nationale et de la police nationale exécutant des missions de police judiciaire.

4. Sous- activités et objectifs de sécurité

Activités juridictionnelles :

- assurer le traitement en temps réel, les instructions ;
- assurer la continuité du règlement des litiges ;
- tenir les permanences et les audiences ;
- mettre en œuvre les processus d'enquête.

Activités juridictionnelles administratives :

- assurer la continuité de l'activité consultative du CE, des jugements en référés statuant en urgence, et de l'activité des juridictions administratives.

Activités pénitentiaires :

- participer à l'exécution des décisions pénales ;
- surveiller, garder, contribuer à l'insertion ou à la réinsertion des personnes qui sont confiées par l'autorité judiciaire, à la prévention de la récidive et à la sécurité publique ;
- escortes judiciaires, hospitalières et transferts des personnes détenues, par les équipes de sécurité pénitentiaire (ESP/PREJ) et avec l'appui des ERIS en renfort d'escorte ou en escorte principale, pour assurer le transfert administratif de détenus signalés (profil violents ou sensibles).

Protection judiciaire de la jeunesse (DPJJ) : prise en charge des mineurs **:**

- mettre en œuvre les décisions des tribunaux pour enfants dans les établissements et services du secteur public et du secteur associatif habilité ;
- assurer la continuité des missions liées au service de placement et aux permanences éducatives, protection de l'enfance, suivi socio-éducatif pour les mineurs détenus.

5. Cadre juridique et références documentaires

- **le garde des Sceaux, ministre de la justice** conduit les travaux de planification relatifs au maintien en toute circonstance de la continuité du service public de la justice, en particulier de l'activité pénale et de l'exécution des peines (article L 1142-7 du code de la défense). Il est responsable de l'action et de la gestion des juridictions, nomme les officiers ministériels et présente au Parlement des projets de réforme. Le ministre conduit la politique d'action publique déterminée par le Gouvernement. Il veille à la cohérence de son application sur le territoire de la République.

- Placée auprès du garde des Sceaux, ministre de la justice, **la déléguée interministérielle à l'aide aux victimes** est chargée de coordonner l'action des différents ministères, d'une part en matière de suivi, d'accompagnement et d'indemnisation des victimes d'actes de terrorisme, d'accidents collectifs, de catastrophes naturelles, de sinistres sériels, et infractions pénales, et, d'autre part dans leurs relations avec les associations de victimes et d'aide aux victimes. Elle veille à l'efficacité ainsi qu'à l'amélioration des dispositifs d'aide aux victimes et prépare les réunions du comité interministériel de l'aide aux victimes.
- **L'Agence nationale des techniques d'enquêtes numériques judiciaires (ANTEN-J),** est chargée de coordonner les efforts de l'État en matière d'interceptions judiciaires de communications électroniques, de concevoir, de réaliser et d'assurer l'exploitation des outils permettant leur mise en œuvre et d'apporter un support aux utilisateurs de ces systèmes. Ce service est rattaché au secrétaire général du ministère de la justice. L'agence assure le pilotage de la **plate-forme nationale des interceptions judiciaires** (PNIJ) qui centralise l'ensemble des réquisitions judiciaires adressées aux opérateurs de communications électroniques et met les données reçues en réponse à disposition des magistrats et des services d'investigation.
- **Le Casier judiciaire national (CJN),** service à compétence nationale, rattaché à la direction des affaires criminelles et des grâces (DACG – Min justice), reçoit et mémorise les décisions principalement pénales, en gère la conservation et les effacements et délivre des extraits sous forme de bulletins, aux juridictions, aux administrations et aux particuliers. Ce service central automatisé est situé à Nantes. Autour du casier judiciaire proprement dit, de nouveaux fichiers judiciaires, FIJAIS (auteurs d'infractions sexuelles ou violentes), FIJAIT (auteurs d'infractions terroristes), REDEX (répertoire des expertises) et enfin l'interconnexion des casiers judiciaires des États de l'Union européenne, avec le projet ECRIS, complètent encore le service rendu.
- **Le Bureau de lutte contre la criminalité organisée, le terrorisme et le blanchiment (BULCO/DACG)** assure la permanence en cas d'attentat avec le PNAT (Parquet national antiterroriste) : permanence en matière anti-terroriste et permanence en matière de crimes contre l'humanité.

Textes de Références :

- décret n° 2008-689 du 9 juillet 2008 relatif à l'organisation du ministère de la justice ;
- loi n° 2009-1436 du 24 novembre 2009 pénitentiaire ;
- décret 9 octobre 2014 PNIJ ;
- décret n° 2017-614 du 24 avril 2017 – ANTENJ ;
- décret du 9 juillet 2008 modifié par le décret du 25 avril 2017 : DPJJ ;
- textes de référence pour le CJN : articles 768 à 781 de code de procédure pénale R.62 à 90 du code de procédure pénale, arrêté du 20 mars 2018 (JO du 23 mars 2018) ;
- loi n° 2019-1480 du 28 décembre 2019 visant à agir contre les violences au sein de la famille et décret n° 2020-1161 du 23 septembre 2020 relatif à la mise en œuvre d'un dispositif électronique mobile anti-rapprochement ;
- loi de programmation et de réforme pour la justice (LPJ) 2018-2022 - n° 2019 du 23 mars 2019 ;
- loi n° 2021-1729 du 22 décembre 2021 pour la confiance dans l'institution judiciaire.

6. Indicateurs et contrôles de l'exécution

Applications des articles des différents codes (pénal, code de procédure pénale) ou lois encadrant les procédures, les délais...

7. Planifications en lien

Chaque établissement pénitentiaire décline ses plans en fonction du degré de la crise et de la gravité de la situation : POI/PPI/PPP. Pour tous les services : mise en œuvre des PCA.

8. Commentaires

NUMÉRIQUE — NUM

Volet cyber - menant : ANSSI / concourant : tous ministères
Volet dysfonctionnement - menant : tous ministères

1. Nature

Le domaine numérique, *via* les systèmes d'information apporte un soutien permanent au fonctionnement et aux activités de la Nation, que ce soit pour les citoyens, les personnes publiques ou le secteur privé, en particulier les opérateurs d'importance vitale (OIV).

Les systèmes d'information critiques sont :

- les systèmes d'information d'importance vitale (SIIV), dont 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. Les critères d'appartenance des systèmes d'information à la catégorie des SIIV sont déterminés secteur d'activité par secteur d'activité ;
- les systèmes d'information essentiels (SIE), dont l'atteinte à la sécurité ou au fonctionnement aurait un effet disruptif important sur la fourniture du service essentiel au maintien d'activités sociétales et/ou économiques critiques. Les opérateurs de services essentiels (OSE) sont désignés par le Premier ministre en application de l'article 5 de la loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptations au droit de l'Union européenne dans le domaine de la sécurité. Ces OSE exercent une activité dans l'un des domaines mentionnés dans le décret N°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et des systèmes d'information des opérateurs de services essentiels et des fournisseurs de services numérique ;
- les atteintes au fonctionnement des systèmes critiques auront vraisemblablement des conséquences susceptibles d'interférer avec la vie ou la santé des citoyens, ou de perturber, voire de désorganiser, la société, avec un fort effet psychologique négatif.

Parallèlement, les systèmes d'information sont plus que jamais soumis à la menace d'attaques informatiques et aux dysfonctionnements majeurs, malgré les efforts nationaux et internationaux pour les en protéger. Les cyberattaques recouvrent les actions d'origine cyber dont les conséquences portent atteinte au bon fonctionnement ou à la disponibilité des systèmes d'information supportant des fonctions vitales pour la nation ou essentielles au bon fonctionnement de l'économie et/ou de la société. Elles intègrent les opérations préalables visant à repérer les caractéristiques et les vulnérabilités des systèmes ciblés.

Il convient de noter que la plupart des attaques cyber n'ont pas de visée terroriste mais que leurs effets sont identiques dans leurs capacités à nuire au bon fonctionnement des institutions de la Nation et de la vie des citoyens quelles que soient les motivations des attaquants.

Le dysfonctionnement majeur pourrait, lui, émaner d'une entité fournissant des services essentiels aux activités vitales de la Nation victime d'une panne / bug informatique, d'une destruction matérielle liée à un aléa naturel (inondation, feu, etc.), la vétusté ou l'obsolescence d'une infrastructure, ou bien une malveillance sur l'infrastructure physique (coupure électrique, section d'un câble, incendie, etc.) aux impacts importants.

2. Enjeux

L'enjeu principal consiste à éviter une interruption totale et durable des activités supportées par les systèmes d'information en sécurisant les infrastructures des systèmes d'information et les services numériques soutenus par ces systèmes d'information. L'espionnage et la compromission/corruption de données sont également deux enjeux de la sécurisation des systèmes d'information.

Il s'agit donc sur chacun de ces 2 axes :

- d'assurer la sécurité des infrastructures des systèmes d'information et de réagir aux incidents majeurs les affectant (supports physiques tels que les câbles, faisceau hertzien ou fibre optique, les datacenters, etc.) contre les pannes / bugs informatiques, les destructions matérielles liées à un aléa naturel (inondation, feu, etc.), la vétusté ou l'obsolescence, ou bien une malveillance sur l'infrastructure physique (coupure électrique, section d'un câble, incendie, etc.). Il s'agit donc de protéger les systèmes (restreindre les accès aux sites sensibles, renforcer la sécurité des terminaux, inspecter les sites sensibles, etc.) ;
- d'assurer la sécurité des systèmes d'information contre les actions volontaires et malveillantes afin de protéger les services numériques (y compris les données) et les systèmes sous-jacents.

La stratégie de sécurité retenue sera nécessairement fortement liée avec l'activité clé POSTE ET COMMUNICATIONS ELECTRONIQUES

3. Acteurs

- secrétariat général de la défense et de la sécurité nationale (SGDSN) et les ministères coordonnateurs : sous l'autorité du Premier ministre et à travers l'ANSSI, le SGDSN organise et coordonne la mise en œuvre du plan PIRANET et la partie sécurité du numérique du plan VIGIPIRATE qui s'appuie sur le ministère coordonnateur de chacun des secteurs d'activité d'importance vitale.
- Comité interministériel pour un numérique sécurisé (CINUS opérationnel) rassemblant l'ensemble des FSSI des ministères, mobilisé à l'invitation de ANSSI/SDO permet une coordination opérationnelle avec les ministères via une mobilisation à distance des FSSI lors d'une situation de crise majeure d'origine cyber. Complémentaire des dispositifs ministériels - notamment du Comité stratégique interministériel de la sécurité numérique (COSINUS) qui réunit périodiquement autour du SGDSN et du DG de l'ANSSI l'ensemble des HFDS ministériels - le CINUS opérationnel permet d'assurer un partage d'information vers le FSSI qui assure l'éclairage du CO Ministériel sur la crise d'origine cyber.
- opérateurs d'importance vitale et leurs sous-traitants : les OIV identifient leurs systèmes d'information d'importance vitale (SIIV)[26] et les déclarent à l'ANSSI. Les OIV doivent communiquer à l'ANSSI les informations relatives aux incidents de sécurité qui affectent leurs SIIV[27]. Ils doivent en outre appliquer à ces systèmes les règles de sécurité fixées par arrêté du Premier ministre pour leur secteur d'activité[28]. Ils déclinent et adaptent les mesures de sécurité du numérique du plan VIGIPIRATE qui leur sont applicables. Les OIV devront faire appliquer de manière appropriée les dispositions du dispositif SAIV à leurs sous-traitants. Les OIV ont obligation de mettre en œuvre les mesures du plan VIGIPIRATE.
- opérateurs de communication électroniques constituent une catégorie à part dans la mesure où ils constituent eux-mêmes des cibles mais peuvent également être les vecteurs des cyberattaques par le biais des infrastructures qu'ils opèrent. Les mesures du domaine communications électroniques (CEL) du plan Vigipirate, que reposent sur le code des postes et des communications électroniques, viennent compléter les mesures du domaine sécurité du numérique pour ces opérateurs.
- opérateurs de service essentiel (OSE)[29] doivent déclarer les incidents de sécurité ayant un impact significatif sur la continuité des services essentiels qu'ils fournissent[30]. Le Premier ministre pourra au besoin informer de ces incidents le public ou les États membres concernés. Si les OSE sont tenus d'appliquer les règles de sécurité fixées par le Premier ministre pour protéger les systèmes d'information nécessaires à la fourniture de leurs services essentiels, ils n'ont pas d'obligations spécifiques vis-à-vis des mesures Vigipirate.
- administrations d'État, en tant que responsables de systèmes d'information de l'État et propriétaires de systèmes essentiels, et les autorités administratives indépendantes (AAI), mettent en œuvre les dispositions du plan Vigipirate qui leur incombent, qu'elles soient ou non OIV ou OSE.
- collectivités territoriales et les entreprises non-OIV n'ont pas l'obligation d'appliquer les mesures Vigipirate. Les opérateurs non-OIV peuvent toutefois être liés à l'exécution des mesures, au cas par cas, selon la réglementation sectorielle en vigueur dans leur secteur d'activité.
- citoyens font l'objet d'un appel à la responsabilité les incitant à appliquer les recommandations proposées dans les mesures d'hygiène informatique, afin notamment que leurs systèmes informatiques et leurs objets connectés ne soient enrôlés à leur insu dans un groupe d'ordinateurs infectés (botnet) et contrôlés à distance par un pirate. À cette fin, des conseils et bonnes pratiques sont également rappelés dans la partie publique du plan Vigipirate.

4. Sous-activités et objectifs de sécurité

- assurer la continuité du système d'information ;
- assurer la sécurité du système d'information ;
- intervenir et coordonner les actions en cas d'attaques contre les systèmes d'information.

26 - article R.1332-41-2 du code de la défense.
27 - article R.1332-6-2 du code de la défense.
28 - article R.1332-6-1 du code de la défense.
29 - article 5, loi n°2018-133 du 26 février 2018.
30 - article 7, loi n°2018-133 du 26 février 2018.

5. Cadre juridique et références documentaires

- articles L.1332-6-4, L.2321-2 et R. 1332-41-18 du code de la défense ;
- article 3 du décret n° 2009-834 du 7 juillet 2009, qui prévoit que l'ANSSI propose au Premier ministre les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et coordonne, dans le cadre des orientations fixées par le Premier ministre, l'action gouvernementale en matière de défense des systèmes d'information ;
- article D98-7 du code des postes et des communications électroniques, qui dispose que, pour répondre aux menaces ou aux atteintes à la sécurité des systèmes d'information des autorités publiques et des OIV, les opérateurs de communications électroniques prennent les mesures utiles pour pouvoir répondre aux prescriptions de l'ANSSI ;
- politique de sécurité des systèmes d'information de l'État (PSSIE) pour les administrations de l'État et les AAI ;
- titre 1er de la loi n°2018-133 du 26 février 2018 susmentionnée et les mesures subséquentes pour les OSE ;
- décret 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics.

6. Indicateurs et contrôles de l'exécution

7. Planifications en lien

PIRANET
VIGIPIRATE

8. Commentaires

DÉFENSE MILITAIRE DU TERRITOIRE — DMT

Ministère menant : le ministère des armées

Ministère concourant : tous ministères

1. Nature

La **défense militaire** comprend la dissuasion nucléaire et la défense militaire du territoire. Relevant de la seule responsabilité des armées, **les missions de défense militaire sont prioritaires sur tout autre engagement des armées sur le territoire national.**

La **défense militaire du territoire** a pour objet d'assurer la liberté et la continuité d'action du gouvernement, la sauvegarde des organes essentiels à la défense de la Nation, l'intégrité du territoire et la protection de la population contre les agressions armées, dans tous les milieux. Elle s'exerce sur le territoire national et dans ses approches.

2. Enjeux

La **défense opérationnelle du territoire** [...] concourt au maintien de la liberté et de la continuité d'action du Gouvernement, ainsi qu'à la sauvegarde des organes essentiels à la défense de la nation (article R.*1421-1 du code de la d**éfense**) dans le milieu terrestre.

La **défense maritime du territoire** et la **défense aérienne** concourent, dans leurs milieux respectifs, à assurer la sécurité du territoire, et notamment la protection des installations prioritaires de défense (articles D. *1431-1 et D.*1441-1 du code de la d**éfense**).

La **cyberdéfense** est l'ensemble des moyens mis en place par l'État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité (JORF n°0219 du 19 septembre 2017). Le cyberespace souverain est défendu par l'ANSSI pour sa plus grande part, et par le commandement de la cyberdéfense dont le rôle est de préserver la liberté d'action des armées dans le cyberespace.

3. Acteurs

Acteurs des armées :

Le chef d'état-major des armées, responsable de l'emploi opérationnel des forces, en délègue le contrôle opérationnel :

- aux officiers généraux de zone de défense et de sécurité (OGZDS) et commandants supérieurs (COMSUP) pour la DOT dans leurs zones respectives ;
- aux commandants de zone maritime (CZM) et COMSUP pour la DMT dans leurs zones respectives ;
- au commandant de la défense aérienne et des opérations aériennes (COMDAOA) pour la défense aérienne ;
- au commandant de la cyberdéfense (OG COMCYBER) pour la cyberdéfense.

Coordination entre acteurs civils et militaires :

Les mesures de défense militaire du territoire doivent être coordonnées avec :

- les mesures relevant des secteurs d'activité d'importance vitale (SAIV) : protection interne et continuité de l'activité ;
- la défense non militaire (sécurité intérieure, sécurité civile), de la responsabilité des préfets ;
- les postures permanentes de sauvegarde maritime et de sûreté aérienne, qui relèvent à la fois de l'action de l'État en mer ou dans l'air et de la défense militaire du territoire.

Dans le milieu terrestre :

- le commandement militaire peut être chargé par le gouvernement de la responsabilité de l'ordre public et de la coordination des mesures de défense civile avec les mesures militaires de défense (article R.*1422-2 du code de la défense) ;
- les commandants de zone de défense et de sécurité expriment les besoins opérationnels primordiaux dont les préfets de zone de défense et de sécurité assurent en priorité la satisfaction (article R.*1422-2 du code de la défense).

4. Sous-activités et objectifs de sécurité

Défense opérationnelle du territoire (DOT) :

- en tout temps, participer à la protection des installations militaires et, en priorité, de celles de la dissuasion ;
- en présence d'une menace extérieure ou d'une agression, assurer la couverture générale du territoire national et s'opposer aux actions ennemies.

Défense maritime du territoire (DMT) :

- surveiller les espaces maritimes sous juridiction française et leurs approches ;
- renseigner les autorités sur les activités suspectes ou hostiles et sur les menaces contre les intérêts nationaux en mer ou depuis la mer ;
- s'opposer aux actions hostiles menées en mer ou depuis la mer contre les intérêts nationaux.

Défense aérienne (DA) :

- surveiller, déceler et évaluer la menace dans l'espace, les approches aériennes du territoire et l'espace aérien national ;
- faire respecter en tout temps la souveraineté nationale dans l'espace aérien français ;
- s'opposer à l'utilisation de l'espace aérien national par un agresseur éventuel ;
- concourir à la diffusion de l'alerte aux populations en cas de danger spatial ou aérien inopiné.

Cyberdéfense :

- surveiller les systèmes d'information du ministère des armées et mettre en œuvre les mesures de défense les concernant.

5. Cadre juridique et références documentaires

Les responsabilités du Premier ministre, des ministres concernés, des autorités préfectorales et militaires sont détaillées aux articles R.*1422-1 à R.*1422-4 (DOT) ; D.*1431-1 à D.*1432-5 (DMT) ; D.*1441-1 à D.*1442-6 (DA) ; L.2321-1 et 2, R*. 3121-2, D.3121-14-1 et D.3121-24-2 (cyberdéfense) du code de la défense.

Quoique la déclaration préalable ou simultanée de régimes d'application exceptionnelle ne soit pas requise, la mise en œuvre des mesures non permanentes de défense militaire du territoire pourrait être décidée dans le cadre des régimes juridiques définis par :

- la Constitution : article 16, guerre (article 35), état de siège (article 36) ;
- le code de la Défense : état de siège (articles L.2121-1 à L.2121-8), état d'urgence (article L.2131-1), mise en garde (articles L.2141-1 et L.1311-1), mobilisation (articles L.2141-1 à L.2141-4).

Exécutant des missions de défense militaire du territoire, **les armées interviennent hors du cadre de la réquisition.**

6. Indicateurs et contrôles de l'exécution

Trois niveaux d'alerte, internes aux armées et déterminés par milieu (terrestre, aérien, maritime et cybernétique), permettent de catégoriser la crise, d'adapter les mesures de veille et de protection des installations militaires, et d'adapter les postures permanentes de sauvegarde maritime (PPSM), de sûreté aérienne (PPSA) et de cyberdéfense (PPC).

La DRM assure un dispositif de veille-alerte à l'étranger, en coordination avec la DGSE, en employant des capteurs nationaux et par le biais de partenariats « renseignement », notamment avec les alliés de l'OTAN. La DRSD est un acteur de renseignement au profit de l'industrie de défense et des militaires. Hors état d'exception et mise en œuvre de dispositif particulier, le renseignement sur le territoire national est de la responsabilité du ministère de l'Intérieur, sous la coordination de la CNRLT.

Les contrats opérationnels, documents classifiés, établissent la nature, le volume et le niveau de disponibilité des capacités opérationnelles nécessaires à l'accomplissement des missions, en cohérence avec les ambitions et le format décrits dans les lois de programmation militaire (LPM) successives. Un emploi des armées dépassant ces contrats opérationnels est un indicateur au moins prévisionnel de dégradation de l'activité.

7. Planifications en lien

Directive générale de mise en œuvre des mesures de défense opérationnelle du territoire n° 10200/SGDN/MPS/CD du 25 mars 1993.

Plans de défense opérationnelle du territoire (DOT), plans de défense maritime du territoire (DMT), plan militaire de défense aérienne (PMDA), plan militaire de défense cybernétique.

8. Commentaires

Situés hors du champ de la défense militaire du territoire, **la dissuasion nucléaire** et la planification de **la défense militaire hors du territoire national ne relèvent pas de la présente directive.**

Conformément à l'IIM 10100 du 14/11/2017, dès lors que les moyens dont disposent les autorités civiles sont estimés *inexistants, insuffisants, inadaptés ou indisponibles,* les armées peuvent être sollicitées sous réquisition pour renforcer le dispositif de sécurité mis en œuvre sous la responsabilité du ministère de l'intérieur, mais **sont alors engagées hors du champ de la défense militaire.** Leur emploi doit alors être envisagé sur une durée courte et limitée, sans exclure une reconduction en fonction de la situation.

Toutes les missions des armées reposent enfin sur un réservoir unique de capacités militaires : un engagement accru, qu'il intervienne en matière de dissuasion nucléaire, hors du territoire ou en appui des autres ministères réduit d'autant les capacités disponibles pour la défense militaire du territoire. **Les éventuels arbitrages relèvent du président de la République** en CDSN.

INTERNATIONAL — INT

Ministère menant : le ministère des affaires étrangères

Ministères concourants : les ministères chargés de la santé, de l'économie, de l'industrie, de l'environnement, des transports, de la justice, des armées et de l'intérieur et de l'outre-mer

1. Nature

La continuité de cette activité doit permettre de prendre en compte le volet international tant pour :

- protéger les ressortissants et intérêts français à l'étranger ;
- mettre en œuvre la coopération internationale.

2. Enjeux

Le principal acteur de la sécurité des ressortissants français à l'étranger est l'État hôte qui est souverain sur son territoire. Il accorde par ailleurs une protection aux emprises représentatives des États accréditant en vertu de la convention de Vienne sur les relations diplomatiques de 1961[31].

Le rôle des pouvoirs publics français s'exerce donc dans le respect de la souveraineté de l'État hôte et du droit en vigueur. Il s'agit principalement de :

- d'informer les ressortissants français sur la situation sécuritaire, administrative et sanitaire ;
- d'orienter la recherche du renseignement ;
- de déterminer la menace et orienter la réponse (mesures de protection supplémentaires et/ou mesures d'intervention) ;
- de placer en alerte et au besoin prépositionner des moyens civils et militaires nécessaires à une éventuelle intervention.

3. Acteurs

Sur le volet international, le ministère de l'Europe et des affaires étrangères est responsable de la protection des représentations diplomatiques, des ressortissants et des intérêts français à l'étranger. Il tient donc un rôle central dans le dispositif général de protection. À cet effet,

- il établit l'analyse politique et sécuritaire des différents pays ;
- il définit et met en œuvre les mesures de sûreté qui s'appliquent aux postes diplomatiques et consulaires ;
- il coordonne la gestion des crises extérieures ainsi que la planification civile de celles-ci avec le concours de l'ensemble des ministères et des services de l'État concernés ;
- il informe — au travers de son centre de crise activé 24h/24 — les ressortissants français se trouvant à l'étranger ou comptant s'y rendre, de la situation en terme de sécurité et des recommandations à suivre.

Les missions diplomatiques — sur lesquelles il a autorité — sont les lieux de convergence de toutes les informations et capacités d'action en cas de menace à l'étranger. Elles apportent leur expertise sur chaque pays et assurent la liaison localement avec les ressortissants, avec le réseau des établissements d'enseignement, avec les entreprises, avec les autorités politiques locales et avec les représentations diplomatiques des autres pays.

31 - L'État accréditaire a l'obligation spéciale de prendre toutes mesures appropriées afin *« d'empêcher que les locaux de la mission ne soient envahis ou endommagés, la paix de la mission troublée ou sa dignité amoindrie »*. Article 22 de la convention de 1961 sur les relations diplomatiques.

4. Sous-activités et objectifs de sécurité

Diplomatie, coopération/Europe :

- mettre en œuvre les coopérations internationales et européennes.

Français à l'étranger :

- diffuser l'alerte ;
- mettre en œuvre des mesures de prévention ;
- prendre des mesures de fermetures et d'évacuations.

Expatriés :

- dispositif d'aide (dont médicale) ;
- prise en charge des ressortissants.

5. Cadre juridique et références documentaires

Le ministre des affaires étrangères conduit les travaux de planification civile relatifs aux crises extérieures avec le concours de l'ensemble des ministères et des services de l'État concernés (article L 1142-6 du code de la défense).

6. Indicateurs et contrôles de l'exécution

Nature de l'indicateur : document général de sécurité dans les postes, plan de sécurité de la communauté française et production d'un rapport annuel de sécurité.

7. Planifications en lien

PIRATEXT

8. Commentaires

ORGANISATION | ORG

Pilotes : SGDSN – ministère de l'intérieur

1. Nature

La gestion d'un évènement se structure autour d'une organisation dédiée capable de coordonner l'enchainement des actions lors des 4 phases génériques de la crise (prévention, intervention, mobilisation et normalisation).

2. Enjeux

Il s'agit de maintenir une structure opérationnelle et coordonnée ainsi que des procédures appropriées par acteur et situations critiques, afin d'optimiser la réponse aux crises, en :

- s'assurant de la mobilisation de toutes les ressources critiques par les corps responsables ;
- mettant en place une chaîne d'alerte efficiente.

Les structures et leur gouvernance peuvent varier au cours des 4 phases de la crise, en particulier lors du retour à la normale. Mais dans tous les cas, il conviendra de :

- synchroniser les efforts de planification et clarifier les rôles et les responsabilités de chacun (échelons nationaux, zonaux, régionaux, départementaux locaux et privés) ;
- déterminer quel acteur intervient à quelle phase de la crise et quels plans peuvent être déclenchés pour adapter au mieux la réponse à la situation.

3. Acteurs

- **SGDSN :** animateur et coordonnateur des travaux interministériels relatifs à la politique de défense et de sécurité nationale. Il élabore la planification interministérielle de défense et de sécurité nationale et veille à son application. Le SGDSN s'appuie sur un dispositif de veille et d'alerte ;
- **ministère de l'Intérieur et de l'Outre-mer :** responsable de l'anticipation et du suivi des crises susceptibles d'affecter la sécurité intérieure et la sécurité civile, il est responsable de la conduite opérationnelle des crises sur le territoire national, et s'assure de l'application déconcentrée des plans gouvernementaux. Le ministère de l'intérieur dispose également d'un dispositif de veille et d'alerte ;
- **autres ministères :** responsables de la gestion des crises et de la planification touchant à leur domaine de compétence, ils disposent aussi d'un dispositif de veille et d'alerte ;
- **réseau diplomatique et consulaire :** l'ambassadeur représentant la France dans le pays où il est accrédité, il est dépositaire de l'autorité de l'État dans ce pays. Préfecture de zone : responsable de la préparation et de l'exécution des mesures de sécurité nationale au sein de la zone de défense et de sécurité. Transpose la planification interministérielle au niveau zonal et les adaptes en fonction de la spécificité du territoire ;
- **préfecture de zone :** responsable de la préparation et de l'exécution des mesures de sécurité nationale au sein de la zone de défense et de sécurité, elle transpose la planification interministérielle au niveau zonal et l'adapte en fonction de la spécificité du territoire ;
- **préfecture de région :** responsable du respect par la région des sujétions imposées par la défense nationale et la sécurité, notamment en matière d'aménagement du territoire, d'urbanisme, de construction, d'investissement collectifs et de fonctionnement des services collectifs. Elle n'a pas de responsabilité spécifique en gestion de crise ;
- **préfecture de département :** responsable de la préparation et de l'exécution des mesures de sécurité intérieure, de sécurité civile et de sécurité économique qui concourent à la sécurité nationale. Le préfet est à ce titre directeur des opérations. Il a, à ce titre, un rôle prédominant dans la gestion de crise, dans l'organisation et l'action des services de l'État ;
- **collectivités territoriales :** l'échelon communal est primordial dans la gestion d'une situation de crise. Les maires sont chargés de la prévention des risques majeurs et de la gestion de crise sur le territoire de la commune ;

ANNEXE 8 : FONCTIONS DE COORDINATION

- **opérateurs :** ils sont tous concernés par la mise en œuvre des mesures et des plans gouvernementaux. Dans certaines situations, les opérateurs peuvent être sollicités pour concourir à la gestion d'une situation de crise. Certains désignés comme opérateurs d'importance vitale ont l'obligation légale de mettre en œuvre des mesures de protection spécifiques ;
- **industriels :** exceptionnellement, l'État peut ne pas disposer en propre d'expertise ou de moyens nécessaire à la gestion de crise. Les industriels peuvent donc apporter, idéalement à titre gracieux, des contributions exceptionnelles pour une durée limitée.

4. Vulnérabilités

- chaîne d'alerte inefficace ne permettant pas une mobilisation optimale des moyens, contraignant l'anticipation et aggravant potentiellement la situation de crise ;
- manque de coordination entre les acteurs n'optimisant pas la réponse aux crises ;
- manque de planification ou de synchronisation de la planification entre les échelons.

5. Objectifs de sécurité

Mobiliser :

- mettre en alerte les moyens disponibles lors d'une situation de crise ;
- mobiliser les moyens adéquats ;
- suivre et renforcer les effectifs si nécessaire afin d'apporter une réponse proportionnée à la crise ;
- assurer les relèves des équipes engagées.

Coordonner :

- activer des cellules de crise adaptées tant au niveau qu'au domaine de la crise rencontrée ;
- organiser la réponse à la situation de crise de sorte que chaque acteur agisse sur son seul domaine de compétence.

Décider :

- élaborer et faire prendre des décisions au bon niveau qu'il soit opérationnel ou stratégique.

6. Cadre juridique et références documentaires

- article L.1111-3 du code de la défense ;
- article L.1131-1 du code de la défense ;
- article L.1141-1 du code de la défense ;
- article L.1142-2 du code de la défense ;
- article 5 du décret du décret numéro 2010-146 du 16 février 2010 ;
- article 2215-1 du code général des collectivités territoriales ;
- article R*1311- 3du Code de la défense ;
- article 2212-2 du code général des collectivités territoriales ;
- circulaire du 10 octobre 2016 signée par le ministère de l'intérieur ;
- décret n°79-433 du 1er juin 1979.

7. Indicateurs et contrôles de l'exécution

8. Référentiel en lien

Memento de Gestion de Crise
Mémento COD (à venir)

9. Commentaires

GESTION DE L'INFORMATION — GIF

Pilotes : SGDSN – ministère de l'intérieur

1. Nature

L'information permet de lever le brouillard de la crise. Elle doit permettre, sur la base notamment d'indicateurs choisis, de fournir :

- aux autorités : des éléments descriptifs pour éclairer la situation ;
- aux acteurs : des décisions à mettre en œuvre.

2. Enjeux

De nombreux défis accompagnent la gestion de l'information :

- une disponibilité de l'information paradoxale : elle se caractérise souvent par un manque d'information robuste en début d'évènement et de trop nombreuses informations, passés les premiers instants ;
- une utilité de l'information : être capable d'identifier les informations réellement utiles ;
- une mise à jour à maîtriser : le rythme de remontée ou redescente de l'information doit être réinterrogé régulièrement pour éviter l'immobilisme comme l'agitation ;
- une cartographie des acteurs à préciser : la gestion de l'information doit permettre d'assurer la circulation de l'information tant horizontale que verticale pour prendre en compte la globalité de la crise.

3. Acteurs

L'anticipation s'adresse à tous les acteurs de la gestion de crise, quelles que soient la cinétique et la durée de la crise.

4. Risques

- incertitude sur le niveau de confiance à accorder aux données ;
- évènement trop rapide ou au contraire trop long et donc pas forcément compatible avec une bonne prise en compte ; évènement pouvant générer de la confusion ;
- difficulté à faire valoir certaines données.

5. Objectifs de sécurité

Collecter :

- établir les liaisons ;
- faire remonter les informations ;
- rechercher le renseignement ;
- tenir à jour une main courante.

Évaluer :

- les contours de l'évènement (assaillants, sites ...) ;
- les conséquences de l'évènement.

Synthétiser :

- les éléments (cartographie...) ;
- les besoins exprimés ;
- transmettre aux services concernés.

6. Cadre juridique et références documentaires

7. Indicateurs et contrôles de l'exécution

8. Référentiel en lien

9. Commentaires

ANNEXE 8 : FONCTIONS DE COORDINATION

ANTICIPATION — ANT

Pilote : SGDSN

1. Nature

Anticiper, c'est aider à une prise de décision menant à un nouvel équilibre socialement acceptable.

Se nourrissant de la planification, elle permet de présenter les principaux enjeux d'une crise à travers ce qui la singularise (cinétique, évènement déclencheur, conséquences). Pouvant potentiellement s'appuyer sur un plan préalablement édicté, elle peut l'adapter en fonction des écarts constatés.

2. Enjeux

1/ Fixer un nouvel équilibre acceptable.

L'anticipation doit permettre de viser un nouvel équilibre acceptable à travers une stratégie phasée dans le temps. Elle doit permettre de prioriser et pondérer les enjeux à considérer.

2/ Établir les situations envisageables.

Dans chaque phase, la situation peut évoluer favorablement ou défavorablement.

Pour formuler des réponses, l'anticipation doit s'appuyer sur des scenarii caractérisés et distincts, en particulier en faisant ressortir le plus probable comme le pire.

3/ Répondre aux autorités.

Elle guidera l'établissement d'une stratégie de sortie de crise, le cas échéant en adaptant une planification *a priori* conçue au contexte particulier de l'évènement.

En complément, et de manière asynchrone, les situations envisageables peuvent conduire à l'établissement de plans alternatifs, permettant de proposer des orientations possibles en cas d'émergence d'une situation inédite.

En fonction de la pression politique, sociale, économique ou médiatique, les autorités en charge de la gestion de crise peuvent en outre être amenées à interroger leur cellule de crise. Il revient, *a priori*, à l'anticipation d'y répondre.

3. Acteurs

L'anticipation s'adresse à tous les acteurs de la gestion de crise, quelles que soient la cinétique et la durée de la crise.

Pour remplir ses objectifs, la constitution d'une équipe dédiée est à privilégier, y compris quand la temporalité semble courte.

4. Risques

Processus permanent, l'anticipation en situation de crise s'effectue sous une **double contrainte de temps** :

- celle liée à la **cinétique de la crise** qui détermine l'échelle de l'horizon temporel à envisager ;
- celle liée à la **rapidité** avec laquelle **les premières décisions** vont devoir être prises.

À ce titre, le recours aux plans existants est un appui précieux a minima pour les réactions immédiates et une approche méthodologique doit permettre d'éviter des pièges, comme : prendre le plan pour ce qu'il n'est pas, s'enfermer dans les dires d'experts, répondre à la question au mauvais niveau, se concentrer uniquement sur les éléments les plus visibles (effet tunnel), ne pas consulter les premiers intéressés (exclus de proximité).

5. Objectifs de sécurité

1. Analyser la situation en temps réel :

- décrire l'évènement et ses évolutions ;
- décrire les enjeux liés et leurs évolutions ;
- décrire le cadre préétabli.

2. Etudier des évolutions envisageables par l'ensemble des acteurs :

- envisager des évolutions des différentes activités clés au cours du temps ;
- caractériser la situation la plus probable et la pire, au regard des critères établis ;
- identifier les indicateurs de suivi.

3. Trouver des options de réponses et les confronter aux évolutions possibles :

- apporter, dans la mesure du possible, une réponse aux causes de la crise, en particulier en recourant à des acteurs spécialisés le cas échéant ;
- contenir les conséquences de la crise en proposant des actions géographiques, sectorielles, catégorielles pour répondre à la crise ;
- confronter les actions aux différents scenarii, notamment aux moyens d'indicateurs croisés ;
- réinterroger ce processus itératif.

4. Présenter les propositions de décision :

- fixer le cadre espace-temps de la réflexion ;
- exposer les présuppositions et les incertitudes ;
- présenter les conclusions et les arbitrages ;
- présenter les étapes à venir, les éléments à compléter, à surveiller, les études supplémentaires.

6. Cadre juridique et références documentaires

Planification.

7. Indicateurs et contrôles de l'exécution

Plans nationaux.

8. Référentiel en lien

Référentiel interministériel relatif à l'anticipation opérationnelle.

9. Commentaires

ANNEXE 8 : FONCTIONS DE COORDINATION

LOGISTIQUE | LOG

Pilotes : SGDSN – ministère de l'intérieur

1. Nature

La logistique consiste à mettre à disposition un produit donné au bon moment, au bon endroit, au moindre coût et avec la meilleure qualité. À l'occasion d'une crise, le temps de réaction constitue l'enjeu majeur. Ainsi, la **planification hors crise** est incontournable, quel que soit l'échelon administratif.

2. Enjeux

1/ Maîtriser la ressource dans toutes ses composantes, dès l'origine de la crise.

Face à l'accumulation des crises et à leur concomitance, face aux effets du changement climatique, face à des crises à cinétique lente, la Nation doit se préparer à répondre à un ou plusieurs chocs majeurs par leurs conséquences intersectorielles, leur ampleur géographique, leur durée ou leur dimension internationale.

Ainsi, dès l'origine de la crise, il convient de maîtriser la consommation des capacités et des ressources, et de prévoir rapidement l'organisation des relèves selon le fondement de la maxime : « *faire que l'arrière tienne pour que les opérations de l'avant se poursuivent* ».

2/ Assurer la gestion de la crise dans le temps, constituer un vivier de logisticiens.

Hors crise, à chaque niveau de responsabilité, (interministériel, ministériel, zonal, départemental, communal), au travers des différents plans et dispositifs, il convient de préparer et de planifier la logistique de crise par l'animation d'un réseau de logisticiens civils et militaires, publics et privés, frontaliers et internationaux, nécessaires à la gestion de la crise. Ce vivier de logisticiens doit être en nombre suffisant pour assurer d'éventuelles relèves formées à la gestion de crise dans le domaine de la logistique.

3/ Anticiper les modalités de coopération et de mobilisation des moyens.

Les modalités de coopération et de mobilisation des moyens de ce réseau de logisticiens doivent être préalablement encadrées. En effet, le régime de la réquisition ne peut rester le seul mode opératoire à activer en temps de crise. De même, les contrats publics essentiels à la crise (ex : acheminement) doivent intégrer des clauses de « robustesse » notamment en matière de continuité d'activité.

4/ Assurer la continuité d'activité des services étatiques de gestion de crise et des entités vitales/critiques/essentielles.

La continuité d'activité des services étatiques de gestion de crise, des entités vitales/critiques/essentielles et du réseau des logisticiens constitue un impératif dans le cadre de la planification de réponse à la crise. *Pour mémoire, le rétablissement de l'ordre public constitue un préalable à l'action des opérateurs et des secours.*

5/ S'assurer de la résilience des moyens de télécommunication.

Essentiels, les moyens de télécommunication de crise (satellite, BLU, radio-amateurs, marine marchande…) doivent être régulièrement recensés, mis à jour et testés.

6/ Délivrer le juste besoin, coordonner l'action.

En crise, les moyens, qui sont comptés, doivent être mis en œuvre en recherchant prioritairement l'efficacité puis l'efficience, dans un souci d'optimisation des ressources et d'une empreinte logistique limitée au juste besoin. Anticipant un possible double choc, il est vital d'assurer une réaction coordonnée, afin d'économiser les capacités, de faire en sorte que l'aide soit fournie là où elle est nécessaire, d'éviter que les actions de secours ne fassent double emploi, d'éviter le chevauchement des moyens civils et militaires, de réduire au maximum les incohérences.

7/ La réactivité, mobilisation du réseau des logisticiens, anticipation de la manœuvre logistique.

Dès la survenue d'une crise (probable ou réelle), le responsable de la gestion de crise pré-alerte le réseau des logisticiens afin d'anticiper une montée en puissance rapide. Dès cet instant, la manœuvre logistique doit être anticipée, notamment le desserrement des moyens (aéronefs, navires…) pouvant être impactés par l'aléa et le choix de préacheminement ou de pré-déploiement des moyens doit être examiné.

8/ Le désengagement et le RETEX

Afin d'anticiper le RETEX, la mise en place, dès le début de la crise, d'une main courante pour le suivi des décisions, la centralisation de toutes les informations, la préparation des *reportings* sont essentiels. En sortie de crise, les flux de rapatriement et le désengagement doivent être anticipés et suivis.

9/ Intégrer dans la réflexion l'intelligence juridique et la maîtrise des circuits budgétaires (*cf. fiche transverses correspondantes*).

Si l'ingénierie logistique nécessite une très bonne connaissance des moyens capacitaires disponibles ou des modalités d'acheminement et de distribution, elle nécessite plus encore de parfaitement maîtriser les circuits décisionnels en matière d'autorisation budgétaire et comptable. L'intelligence juridique (connaissance de l'environnement juridique, anticipation et préservation des risques financiers, juridiques, réputationnels, mise en œuvre des instruments juridiques…) est également essentielle à la réussite des opérations.

3. Acteurs

Les acteurs peuvent être regroupés en quatre catégories : les responsables de la gestion de crise et de la coordination logistique, les « structures d'appui à la manœuvre logistique » et les « ressources mobilisables », ces deux derniers constituant le **réseau des logisticiens**.

Type de crise ⇨	Interministérielle	Ministérielle	Zonale	Départementale	Communale
Responsables gestion de crise	Premier ministre	Ministre	Préfet de zone	Préfet de département	Maire
Responsables cellule logistique	CCL interministérielle	CCL ministérielle	CCL zonale	CCL départementale	CCL locale
Structures d'appui à la manœuvre logistique	Les structures d'appui à la manœuvre logistique constituent des ressources, essentiellement publiques, assurant, au profit de la *cellule de coordination logistique* (CCL), le « **soutien administratif** » de la crise et certaines fonctions de « **soutien logistique** » lorsque celles-ci sont **internalisées**. Elles mettent en œuvre et conduisent les décisions de la cellule de crise dont elles dépendent.				
Ressources mobilisables	Les « **ressources mobilisables** » constituent l'ensemble des ressources (structures, personnels, matériels, stocks stratégiques…) civiles et militaires, publiques ou privées, nationales et internationales, nécessaires à la gestion de la crise pour assurer les secours et leur « **soutien logistique** ». Elles sont mobilisées au travers du réseau des logisticiens par les responsables de crise.				

CCL : Cellule de Coordination Logistique.

4. Risques

Impréparation dans la planification, y compris la continuité d'activité des entités vitales/critiques/essentielles et la formation des acteurs à la gestion de crise ; coût des clauses de « robustesse » dans les contrats publics ; retard dans la pré-alerte du réseau des logisticiens.

ANNEXE 8 : FONCTIONS DE COORDINATION

5. Objectifs de sécurité

Sous-fonctions		Objectifs	Responsabilité	Impact sur la manœuvre Logistique
Le terme générique de « secours » concerne ici les personnels projetés quelles que soient leurs fonctions (personnels hospitaliers, sécurité civile, sécurité publique…).				
Soutien logistique	Approvisionnements	• recenser les besoins (secours aux populations, administrations et soutien pétrolier conformément aux plans ressources), • les prioriser, • faire assurer les achats, • assurer la réception administrative du matériel, • assurer les groupages/dégroupages sur des bases logistiques, • assurer les livraisons sur les sites d'acheminement (port, aéroport), • assurer la distribution.	CCL (stratégie) et structures ad hoc (conduite)	Essentiel
	Acheminement (personnel et fret)	• assurer le transport des secours et de leurs soutiens, ainsi que des moyens déployés pour le secours à la population, par voies terrestre, aérienne ou maritime, • comprend également les opérations de transit, notamment la gestion des formalités douanières.	CCL (stratégie) et structures ad hoc (conduite)	Fort
	Soutien des secours	• maintenir la capacité opérationnelle des secours par la satisfaction des besoins vitaux (alimentation, hébergement, hygiène, santé) et, si besoin, la mise à disposition sur le site de la crise des moyens de mobilité.	CCL (stratégique) et hiérarchie (conduite)	Fort
Soutien Administratif	Financier	• engager, • liquider, • mandater, • payer, • nécessite au préalable de définir les structures en charge de ces fonctions.	CCL, Ministère des finances (stratégie) et Ministères concernés (conduite)	Fort Notamment vis-à-vis des opérateurs sollicités
	Achat	• en liaison étroite avec la fonction approvisionnement : – assurer les prospections puis les consultations, – élaborer les supports juridiques, – notifier les commandes.		

6. Cadre juridique et références documentaires

Planification ; finances publiques ; commande publique ; droit de la crise, droit du contentieux ; droit international

7. Indicateurs et contrôles de l'exécution

Constitution du réseau des logisticiens ; formation à la gestion de crise ; contrats cadre et contrats « robustes » ; exercices.

8. Référentiel en lien

Le référentiel LOGISTIQUE, à venir, précisera plus avant ces différents enjeux.

9. Commentaires

CADRE JURIDIQUE | JUR

/

1. Nature

La gestion de la crise s'inscrit dans un cadre juridique qui fait appel à des outils de droit commun mais peut également, au regard de la nature, de l'ampleur ou de la spécificité (pandémie, attentats terroristes) de la crise, nécessiter la mise en œuvre d'un cadre d'exception.

Afin d'accompagner tous les acteurs (essentiellement publics) de la crise dans la compréhension des impératifs juridiques qui s'imposent à eux, un guide du droit de la crise a été élaboré par le SGDSN. Il a été conçu dans une perspective théorique afin d'exposer les principales contraintes normatives qui pèsent sur les décisions mises en œuvre pour la résolution des origines et de conséquences des troubles. Il s'adresse aux acteurs juridiques mais également à tous ceux qui, non juristes, doivent comprendre l'environnement juridique dans lequel s'exerce la gestion de crise. Il doit être complété par un guide pratique comprenant les modèles d'actes réglementaires que les autorités centrales ou déconcentrés peuvent être amenés à prendre.

L'extrême complexité de ces mécanismes impose la création d'un véritable réseau de juristes compétents en « droit de la crise » et formés à cet effet.

2. Enjeux

1. Garantir la sécurité juridique des décisions, dès l'origine de la crise.

Face à l'accumulation des crises et à leur concomitance, face aux effets du changement climatique, face à des crises à cinétique longue, les acteurs en charge de la gestion de la crise doivent être en mesure d'adopter des dispositions en toute sécurité juridique.

Les décisions prises dans le cadre de la gestion de la crise doivent être mises en œuvre afin de garantir :

- le risque contentieux : il faut garantir la légalité des décisions prises ;
- le risque pénal : s'assurer que l'éventuelle mise en jeu de la responsabilité des décideurs n'aboutira pas à une condamnation.

2. Maîtriser les outils juridiques

Quel que soit le cadre dans lequel s'exerce la gestion de crise, l'identification des outils juridiques doit permettre d'optimiser la résolution de la crise : mise en œuvre des pouvoirs de police administrative dans le cadre du droit commun, réquisitions etc…

Le volet normatif de la gestion de crise se caractérise par la juxtaposition de deux cadres juridiques :

- le cadre juridique « de droit commun » de la crise : il est défini par les dispositions législatives et réglementaires codifiées principalement dans le :
  - code de la défense : menaces et risques (article L.1111-1 et suivants) ; compétences du Premier ministre et des ministres (article L.1131-1, L.1141-1 et suivants ; réquisition des forces armées pour les besoins de la défense et de la sécurité nationale (article L.1321-1) ; autres réquisitions (pour les besoins généraux de la Nation, militaires) ;
  - code général des collectivités territoriales : article L.2212-2 (pouvoirs de police du maire) et L.2215-1 (pouvoirs du préfet de département) ;
  - code de la sécurité intérieure : organisation des secours et gestion de crise (article L.741-1 à L.741-3, R.741.1 à R.741-17) ;
  - code de la santé publique : menaces sanitaires (article L.3131-1 à L.31313-11 et R.3131-1 à R.3131-17) ; situations sanitaires exceptionnelles : plan zonal de mobilisation : articles R.3131-4 à R.3131-9), Dispositif ORSAN (articles R.3131-10 à R.3131-10-2) ; Plan départemental de mobilisation (article R.3131-11), Plan blanc (article R.3131-13 à R.3131-14).

- des régimes d'exception sont organisés en fonction de la nature et de l'ampleur de la crise :
  - régimes d'exception autres que les états d'urgence : article 16 de la Constitution, état de siège, théorie jurisprudentielle des circonstances exceptionnelles ;
  - l'état d'urgence résultant de la loi du 3 avril 1955 modifiée ;
  - l'état d'urgence sanitaire : articles L.3131-12 à L.3131-20 et R.3131-18 à R.3131-25 du code de la santé publique.

Outre les dispositions législatives et réglementaires codifiées rappelées ci-dessus, il convient de prendre en compte notamment les dispositions suivantes :

- sur l'adaptation des modalités de travail (télétravail en temps de crise) : secteur privé (article L.1222-11 du code du travail) et secteur public (article 133 de la loi n° 2012-347 du 12 mars 2012 et décret n° 2016-151 du 11 février 2016 modifié) ;
- sur l'organisation de la planification :
  - Directive générale interministérielle n° 320/SGDSN/PSE/PSN du 11 juin 2015 relative à la planification de défense et de sécurité nationale.

Plans de continuité d'activité (article L.2151-4 du code de la défense), plans de lutte contre le terrorisme, plans de réponse à des risques particuliers, planification relative à la sécurité des activités d'importance vitale (article L.1332-1 et suivants du code de la défense), planification interministérielle de gestion de crise).

3. Acteurs

Déploiement de cellules juridiques dédiées à la gestion de crise (CIC…).

4. Risques

- impréparation dans la planification ;
- illégalité des décisions prises ;
- mise en jeu de la responsabilité des décideurs.

5. Objectifs de sécurité

- droit commun de la crise ;
- états d'urgence ;
- cas des outremers.

6. Cadre juridique et références documentaires

Guide « théorique » du droit de la crise ; guide pratique (pouvoirs de police administrative générale droit commun/droit d'exception ; commande publique ; réquisitions).

7. Indicateurs et contrôles de l'exécution

Constitution du réseau des juristes ; formation à la gestion de crise ; participation aux exercices.

8. Référentiel en lien

Guide juridique pratique (à venir).

9. Commentaires

FINANCIER | FIN

/

1. Nature

La présente activité clé a pour objectif, dès la survenance de la crise, voire en anticipation lorsque la crise est prévisible (exemple d'une crise cyclonique), et tout en assurant la maîtrise des dépenses :
de mobiliser les ressources budgétaires nécessaires pour faire face aux dépenses imprévues et dont l'engagement doit pouvoir être réalisé rapidement ;
de les positionner au plus près des besoins et en conformité avec les choix de la CIC décision ;
d'assurer la traçabilité de l'ensemble des ressources mobilisées et des dépenses réalisées sur l'ensemble des titres (T2, T3, T5, T6…) impactés ;
durant la crise, de renseigner (reporting), et après la crise d'assurer la clôture des comptes et de répondre aux autorités de contrôle.

2. Enjeux

1. Maîtrise des dépenses liées à la crise :
- mobiliser les ressources graduellement en fonction de la gravité de la crise :
  - mobiliser prioritairement les ressources ministérielles prévues à cet effet en programmation ;
  - puis dégeler les crédits des réserves de précaution ;
  - enfin mobiliser des ressources budgétaires exceptionnelles.

2. Définir la stratégie budgétaire de crise :
- décider de l'architecture budgétaire (responsables budgétaires, services exécutants et comptables de rattachement, centres de coût…) ;
- établir une charte de gestion budgétaire.

3. Mettre à disposition les crédits, dès le début de la crise, au plus près des centres de décision (engagement d'opportunité) :
- en conformité avec la stratégie budgétaire préalablement définie, éditer les décisions budgétaires (décret de virement, décret de transfert, décret d'avance, loi de finances rectificative…) ;
- nécessite une parfaite maîtrise des circuits décisionnels en matière d'autorisation budgétaire et de processus comptables.

4. Assurer la traçabilité exhaustive de l'ensemble des ressources mobilisées et des dépenses :
- en conformité avec la stratégie budgétaire de crise définie, décider de la codification CHORUS à retenir ;
- dès la survenance de la crise, voire en anticipation lorsque la crise est prévisible (exemple d'une crise cyclonique) ;
- concerne l'ensemble des titres mobilisés (T2, T3, T5, T6…) ;
- appliquer la codification ainsi retenue à l'ensemble des flux financiers afin de faciliter les restitutions, et d'en assurer leur fiabilité et leur sincérité.

5. Maîtriser les délais de paiement et limiter les contentieux :
- à l'instar de la chaîne budgétaire et financière, la chaîne « achat/approvisionnement » nécessite d'être clairement identifiée :
  - appliquer le processus décisionnel en matière d'opportunité définie par la charte de gestion budgétaire ;
  - appliquer la règlementation en matière de commande publique, désigner les représentants du pouvoir adjudicateur (qualité pour engager juridiquement l'État) ;
  - désigner les entités assurant la réception des commandes (biens ou services) et la certification du service fait.
- permet de :
  - fluidifier la chaîne d'exécution de la dépense de l'État ;
  - rassurer les partenaires de la crise (prestataires, fournisseurs, associations…) ;
  - anticiper la « reconstruction » dans les meilleures conditions, compte tenu de la confiance instaurée en amont.

6/ Renseigner tout au long de la crise :
- en assurant la fonction de reporting au profit des autorités et de la CIC ;
- en renseignant les services gestionnaires ou exécutants, voire certains opérateurs essentiels.

7/ Assurer la clôture des comptes et le RETEX
- afin d'anticiper le RETEX, mettre en place, dès le début de la crise, une main courante pour le suivi des décisions, la centralisation de toutes les informations, la préparation des reportings ;
- en sortie de crise, s'assurer de la clôture de l'ensemble des comptes, et être en mesure de renseigner les autorités de contrôle.

ANNEXE 8 : FONCTIONS DE COORDINATION

3. Acteurs

- services du ministère de l'économie et des finances (SCBCM, DB, DGFIP, DAE, AIFE…) ;
- services financiers des ministères (RFFIM, RPROG…) ;
- services gestionnaires (RBOP, RUO) et exécutants locaux (bureaux CHORUS), comptable public (DRFIP).

4. Risques

- impréparation dans la planification et, par voie de conséquence, dans la gestion de la crise ;
- mise sous tension des ministères, des autorités locales, des opérateurs, des partenaires, des associations… ;
- intervention des secours retardée ;
- contentieux inextricable.

5. fonction et Sous-fonctions

Fonctions	Définitions	Responsabilité	Impact sur la crise
Définir les stratégies budgétaires et achat	• identifier le cadre d'élaboration, de mise à disposition, de programmation, d'exécution et de suivi des ressources et des dépenses ; • définir la chaîne achat/approvisionnement ; • déterminer à chaque niveau les responsabilités des acteurs.	MEFR, RFFIM, RPROG	Fort
Codifications	• fixer la nomenclature et définir la codification de comptabilité analytique à enregistrer dans CHORUS pour l'ensemble des flux financiers afin de pouvoir les identifier et assurer un suivi et une restitution sincère et d'image fidèle.	MEFR, AIFE	Faible
Mobilisation et positionnement des ressources	• identifier les ressources mobilisables ; • assurer la programmation dans Chorus, tel que définie dans la charte de gestion.	MEFR, RFFIM, RPROG	Fort
Maîtrise de la dépense	• assurer la soutenabilité de la programmation et de l'exécution des budgets dédiés à la crise ; • s'assurer de pouvoir honorer les engagements souscrits.	RBOP et RUO en charge de la crise et réceptacles des ressources mobilisées	Faible
Exécution de la dépense	• veiller à l'exécution des dépenses dans des délais contraints, dans le respect des règles de comptabilité publique.	Services exécutants	Fort
Reporting	• suivre la mise en place des crédits et l'exécution des dépenses ; • être en mesure de restituer à tout moment des informations sincères, fiables, fidèles durant la crise et après crise, à l'ensemble des autorités y/c les autorités de contrôle.	MEFR, RFFIM, RPROG	Faible

6. Cadre juridique et références documentaires

Planification ; finances publiques ; commande publique ; droit de la crise, droit du contentieux ; droit international…

7. Indicateurs et contrôles de l'exécution

Élaboration d'une charte de gestion budgétaire et financière en matière de gestion de crise ; formation des cadres financiers du MEFR, des ministères et préfectures à la gestion de crise ; exercices.

8. Référentiel en lien

Recueil des règles de comptabilité budgétaire de l'État.

TERRITOIRES — TER

Pilote : ministère de l'intérieur

1. Nature

Les territoires sont à la fois le premier et l'ultime niveau de planification :

- le premier au titre du principe de subsidiarité ;
- l'ultime en ce qu'il lui revient de mettre en œuvre les mesures, quel que soit le niveau de décision.

L'objectif de la prise en compte par les territoires est donc de s'assurer de la bonne coordination et de la bonne cohérence de la planification et de sa mise en œuvre, le cas échéant.

2. Enjeux

Les aspects territoriaux relèvent de deux dynamiques :

Une conception centralisée :

- établir une bonne coordination et une cohérence d'action entre le territoire et les administrations centrales ;
- garantir une réponse efficiente aux événements sur le territoire et réagir à une dimension interministérielle ;
- identifier les possibles contradictions entre les mesures élaborées en planification et les procédures.

Une mise en œuvre décentralisée

- assurer la bonne continuité des services ;
- avoir une connaissance physique, humaine et économique du territoire, notamment pour éviter un décalage entre les demandes d'actions et les capacités opérationnelles d'un territoire ;
- **Identifier conséquemment les seuils de ruptures entre mesures et capacités.**

3. Acteurs

	Ministères	Préfets de zone	Préfets de département	Collectivités territoriales	Opérateurs
Planification Nationale					
Scénarios de crise générique	X	X	X		X
Planification zonale		X	X	X	
Objectifs de sécurités décentralisés		X	X	X	X
Planification Départementale			X		
PCA	X	X	X	X	X
Articulation entre planification nationale et ORSEC	X				
Vérification des capacités opérationnelles		X	X	X	X
Coordination avec les différents échelons administratifs	X	X	X	X	X

4. Risques

- si la coordination et la cohérence des actions entre les échelons centraux et déconcentrés ne sont pas harmonisées, l'action en période de crise risque d'être caduque. Autrement dit, sans coordination ni cohérence, le risque est celui **d'une rupture capacitaire**.
- la deuxième vulnérabilité, concomitante à la première, est la mauvaise gestion de l'information. La gestion et la transmission de l'information étant essentielles, il est nécessaire de s'assurer que l'information soit correctement gérée à tous les échelons, et correctement transmise du haut vers le bas et inversement.

5. Objectifs de sécurité

a. Objectif : déclinaison nationale :

Planification :

- décliner les plans sur la base d'une adaptation des situations de références nationales aux contraintes locales, sur la base d'une analyse locale des bassins de risques ;
- mettre en cohérence les priorités d'action afin de lisser la réponse à un événement sur l'ensemble du territoire, sans être trop contraignant pour les acteurs du territoire.

Capacités :

- répertorier les moyens de l'État ;
- engager les moyens centralisés de l'État dans les territoires.

b. Objectif : continuité d'activité :

PCA (au niveau local) :

- assurer la promotion des Plan de Continuité d'Activité (PCA), des Plan Communaux de Sauvegarde (PCS) et des Plans de Protection Externe (PPE) ;
- mettre à jour les mesures dans les Installations sensibles (PPP).

Collectivité :

- assurer la coordination avec les acteurs territoriaux dont les opérateurs ;
- mettre en œuvre les plans de portée territoriale ;
- engager les moyens des territoires dans les territoires ;
- maitriser les accès aux OM ;
- mettre à jour ses capacités opérationnelles ;
- identifier les points de ruptures avec les plans nationaux.

Opérateur :

- assurer la coordination entre les différents échelons administratifs et les opérateurs ;
- Identifier les points de ruptures avec les plans nationaux.

6. Cadre juridique et références documentaires

Le ministre des armées :

en matière de sécurité intérieure, l'engagement des armées doit être planifié conjointement par les autorités civiles et militaires territoriales. Le niveau privilégié de cette planification civilo-militaire est celui de la zone de défense et de sécurité. Ainsi, l'officier général de zone de défense et de sécurité (OGZDS) doit apporter son concours au préfet de zone de défense et de sécurité dans l'élaboration de toute planification zonale. Celle-ci permettra, en fonction des scénarios de crise, de définir les besoins à destination des armées. Elle procurera également à l'autorité préfectorale une meilleure connaissance des capacités militaires pouvant être mises à sa disposition en cas de crise.

Le ministre de l'intérieur (article L.1142-2) :

- s'assure de la transposition et de l'application au niveau territorial de la planification ;
- au titre de ses responsabilités en matière de sécurité civile, il veille à l'articulation entre la planification d'organisation des secours (ORSEC) et la planification de défense et de sécurité ;
- veille à l'articulation entre la planification ORSEC et la planification ORSAN (dispositif de planification du système de santé en cas de situation sanitaire exceptionnelle).

Le ministre chargé de la santé :

- veille à l'articulation entre la planification ORSAN (dispositif de planification du système de santé en cas de situation sanitaire exceptionnelle) et la planification ORSEC ;
- code de la défense : articles L1141-1 à L1142-9, articles L.1332-1 à L.1332-7, L.2151-1 à L.2151-5 et R.1332-1 à R.1332-42 ;
- article L.741-1 code de la sécurité intérieure ;
- circulaire relative à l'organisation gouvernementale pour la gestion des crises majeures n° 5567/SG du 1er juillet 2019 ;
- instruction générale interministérielle sur la planification de défense et de sécurité nationale ;
- instruction générale interministérielle relative à la sécurité des activités d'importance vitale n° 6600/SGDSN/PSE/PSN du 7 janvier 2014 ;
- planification ORSEC ;
- plan Particulier de Protection ;
- plan de protection externe.

7. Indicateurs et contrôles de l'exécution

8. Référentiels en lien

Guide de déclinaison territoriale NRBC
Guide ORSEC/ORSAN
Guide PCA/PCS
CoTTRim

ANNEXE 8 : FONCTIONS DE COORDINATION

COMMUNICATION — COM

Pilote : SIG

Contributeurs : tous ministères (DICOM)

1. Nature

En matière de gestion de crise, la communication des services de l'État quant aux dispositifs et mesures mis en œuvre contribue de manière décisive à l'adhésion de la population et le cas échéant à son implication. À ce titre, la clarté et la cohérence des messages portés par les différents acteurs d'une crise sont essentielles.

Afin de les soutenir dans leur mission, les acteurs étatiques chargés d'annoncer les actions engagées, les mesures activées et/ou renforcées mais également de sensibiliser la population, doivent disposer de modèles éprouvés, adaptés aux différents canaux de communication ainsi que d'éléments de langage ajustés aux situations et mesures concernées.

2. Enjeux

La communication constitue un élément central qui concoure à la réussite du processus de gestion de crise. Celle-ci repose sur la définition d'une stratégie unifiée, coordonnée et partagée, à l'échelle nationale et territoriale.

Elle s'appuie, en méthodologie, sur :

- des actions de communication accessibles qui s'inscrivent dans le registre de la preuve (partage de l'information et des résultats, mise en avant de la mobilisation de l'État) ;
- une coordination et une amplification ministérielle renforcée ;
- des actions de communication territorialisées ;
- un réseau de porte-paroles et d'experts thématiques identifiés et légitimes ;
- une prévention contre la manipulation de l'information.

Elle vise en particulier :

- le grand public et les citoyens directement impactés par la crise ;
- les responsables et communicants d'administrations, de services déconcentrés et des collectivités territoriales ;
- les agents/employés des structures impactées par la crise (ministères, opérateurs, institutions) ;
- les acteurs économiques et sociaux ;
- les journalistes et leaders d'opinion ;
- les partenaires publics et privés ;
- les partenaires étrangers.

Pour cela, une attention particulière sera apportée pour :

- simplifier les usages, harmoniser les pratiques, unifier la communication et renforcer sa cohérence (ton employé, message adressé, format utilisé) afin de garantir l'impact et la compréhension de l'action gouvernementale en temps de crise ;
- appuyer la formation et l'entraînement des communicants de crise grâce à l'utilisation et au maniement des outils mis à disposition.

3. Acteurs

Services centraux et déconcentrés de l'État (administrations centrales, cabinets ministériels, préfectures et collectivités territoriales).

4. Risques

Incompréhension de la population, absence d'adhésion, défiance.

ANNEXE 8 : FONCTIONS DE COORDINATION

5. Objectifs de sécurité

Externe :

- alerter ;
- diffuser les conduites à tenir ;
- obtenir l'adhésion de la population.

Interne :

- informer les autorités (EDL) ;
- informer les intervenants ;
- coordonner la communication entre acteurs étatiques et opérateurs.

6. Cadre juridique et références documentaires

- circulaire n° 6095/SG du 1er juillet 2019 relative à l'organisation gouvernementale pour la gestion des crises majeures ;
- circulaire n° 6120/SG du 14 octobre 2019 relative à l'organisation et à la coordination de la communication gouvernementale ;
- instruction conjointe du secrétaire général du ministère de l'intérieur et du directeur du service d'information du Gouvernement n° 18-5575 du 14 février 2018 relative à l'organisation et aux missions de la communication territoriale de l'État ;
- stratégie nationale de résilience.

7. Indicateurs et contrôles de l'exécution

- étude et analyse de l'opinion et du discours médiatique afin de mesurer la réception des communications par les citoyens et l'impact sur les comportements ;
- suivi des performances de l'écosystème numérique gouvernemental et des dispositifs de communication, notamment en ligne ;
- niveau d'appropriation et d'utilisation des ressources mises à disposition (plateforme dédiée aux communicants), notamment en cas de crise ou lors d'exercices ;
- suivi d'indicateurs sociétaux et économiques, notamment à travers la mise en œuvre de mesures barométriques.

8. Référentiels en lien

- une série d'outils est mobilisée pour déployer une approche unifiée et coordonnée de la communication de crise, à l'échelle nationale et territoriale (narratif commun, actions RP, dispositifs pluri-médias, contenus éditoriaux et productions digitales, partenariats institutionnels, canaux d'informations partagés, renforts ponctuels aux équipes territoriales) ;
- régulièrement actualisés et enrichis, les kits de communication concernés (éléments de langage, modèles de documents, gabarits digitaux) seront disponibles en ligne et déclinables selon les différents types de crise (terroriste, sanitaire, cyber, phénomènes météorologiques…).

9. Commentaires

SGDSN

SECRÉTARIAT GÉNÉRAL
DE LA DÉFENSE ET DE
LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
sgdsn.gouv.fr

Maquette : DSAF/DPSG/BAEC/Section Édition – Novembre 2022.