PREMIER
MINISTRE

Liberté
Égalité
Fraternité

Instruction interministérielle relative à l'organisation et à la coordination de la **sûreté maritime et portuaire**

N° 230/SGDSN/PSE/PSN/NP du 28 juin 2022.

Abroge et remplace l'instruction interministérielle n°230/SGDN/PSE/PSN/NP du 27 juin 2018 relative à l'organisation et à la coordination de la sûreté maritime et portuaire.

Cette instruction peut être consultée et téléchargée sur le site www.sgdsn.gouv.fr

Secrétariat général de la défense et de la sécurité nationale

La sûreté maritime et portuaire mobilise de multiples acteurs, publics comme privés. Elle requiert de leur part une étroite coordination ainsi qu'une information adéquate des usagers du transport maritime, des utilisateurs quotidiens des places portuaires et, plus largement, des populations susceptibles d'être impliqués par un événement résultant d'un acte illicite intentionnel.

A cet effet, l'instruction interministérielle relative à l'organisation et à la coordination de la sûreté maritime et portuaire met en lumière, au profit des acteurs publics et privés concernés, les principes de sûreté devant être mis en œuvre et leur permet d'avoir une connaissance claire de la gouvernance du dispositif national de sûreté maritime et portuaire.

Par sa large diffusion, elle vise à favoriser les bonnes pratiques au sein des administrations chargées de la réponse de l'État en cas d'événement affectant la sûreté maritime et portuaire, des administrations chargées du contrôle de la bonne application des exigences réglementaires, ainsi que des entités, publiques ou privées, soumises aux réglementations relatives à la sûreté maritime et portuaire.

Elle vise *in fine* à ce que l'action de tout acteur puisse se déployer de manière optimale et en cohérence avec celle des autres acteurs concernés, par une bonne compréhension des dispositifs mis en œuvre, en mer comme à terre, et par une adaptation permanente de tous aux risques et menaces ainsi qu'à la nature et à l'ampleur d'un événement résultant d'un acte illicite intentionnel.

En 2018, dans un contexte de menace terroriste élevée, le *secrétariat général de la défense et de la sécurité national* (SGDSN) avait fait le choix de réviser en profondeur cette instruction dont la précédente version datait de 2006.

À l'occasion de la neuvième commission interministérielle de sûreté maritime et portuaire du 28 février 2020, le cabinet du Premier ministre a souhaité que soit initiée une nouvelle mise à jour de ce document afin, notamment, de prendre en compte les évolutions de plusieurs références règlementaires et de l'organisation de certains services de l'Etat.

Cette nouvelle édition, réalisée en relation avec le secrétariat général de la mer (SGMer) et les ministères concernés, conforte, en premier lieu, les principes de sûreté et la gouvernance applicable. Elle présente des outils de compréhension afin que tous les acteurs publics et privés concernés puissent remplir efficacement la part des missions qui leur incombe.

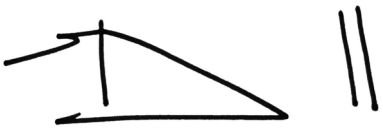
Elle précise, par ailleurs, l'organisation de la sûreté dans certains domaines tels que le zonage portuaire, la cybersécurité, la sécurité des activités d'importance vitale ainsi que la mise en œuvre des équipes de protections privées à bord des navires.

Elle abroge et remplace l'instruction interministérielle n°230/SGDSN/PSE/PSN/NP du 27 juin 2018.

Fait le 28 juin 2022

Le secrétaire général de la défense
et de la sécurité nationale

Stéphane Bouillon



SOMMAIRE

Objet et champ d'application de l'instruction 7

Titre I : Principes régissant la sûreté maritime et portuaire 9

Chapitre I : Enjeux 11

Chapitre II : Périmètre 12

Chapitre III : Menaces 13

Chapitre IV : Principes de sûreté 15

Titre II : Gouvernance de la sûreté maritime et portuaire 31

Chapitre I : Niveau international 33

Chapitre II : Niveau européen 34

Chapitre III : Niveau national 35

Chapitre IV : triple *continuum* 41

Annexes 45

Annexe 1 : Liste des sigles et des acronymes 47

Annexe 2 : Tableau de la chaine de remontée du renseignement, d'origine non étatique 51

Annexe 3 : Tableau des alertes et des intervenants 52

Annexe 4 : Corrélation entre le plan Vigipirate et le code *ISPS* 54

Annexe 5 : Principales références législatives et réglementaires 55

OBJET ET CHAMP D'APPLICATION DE L'INSTRUCTION

Les dispositifs de sûreté maritime et portuaire visent à fournir un cadre adapté pour d'une part, disposer de mesures dissuasives empêchant ou limitant la survenue d'actes malveillants et d'autre part, apporter une réponse, publique et privée, coordonnée, optimale et efficiente aux conséquences de ces actes. Il est primordial que les dispositions qui découlent des prescriptions de sûreté, définies aux niveaux international, national et local, s'articulent avec cohérence pour assurer une continuité au sein des flux portuaires et du trafic maritime. Ce principe implique un triple *continuum*, entre la mer et la terre, entre les pouvoirs publics et les opérateurs, mais également entre le niveau local et le niveau central.

Pour la présente instruction :

- la sûreté maritime renvoie aux missions relevant de la souveraineté et de la protection des intérêts nationaux, de la sûreté maritime à bord des navires et de la lutte contre les activités maritimes illicites[1] ;
- la sûreté portuaire renvoie aux dispositifs et mesures visant à dissuader, prévenir et limiter l'impact d'un acte malveillant contre les navires et les infrastructures portuaires, dans tous les ports comprenant au moins une installation portuaire fournissant des services à des navires à passagers, ou à des navires de charge de jauge égale ou supérieure à 500[2], qui effectuent des voyages internationaux, ainsi qu'aux navires à passagers effectuant une navigation nationale de plus de 20 milles marins[3] voire aux navires opérant des services intérieurs, à leur compagnies et aux installations portuaires desservies, selon les conclusions de l'évaluation quinquennale nationale obligatoire du risque de sûreté réalisée par l'autorité nationale de sûreté maritime compétente[4].

La présente instruction :

- ne s'applique pas aux ports militaires, aux installations couvertes par le secret de la défense nationale, ni aux navires de guerre ;
- n'aborde pas les actions à mener dans le domaine de la sûreté maritime et portuaire, par nature évolutives, qui relèvent de plans d'actions portés par ailleurs par les services du Premier ministre et les ministères concernés ;
- n'impose pas de procédures de sûreté, dont la définition et la mise en œuvre relèvent des ministères de tutelle.

Cette instruction s'adresse :

- aux administrations chargées de la réponse de l'État en cas d'événement affectant la sûreté maritime et portuaire ;
- aux administrations chargées du contrôle de la bonne application des exigences réglementaires ;
- aux entités, publiques ou privées, soumises aux réglementations relatives à la sûreté maritime et portuaire.

1 - Cf. en annexe 5, les arrêtés établissant la liste des missions en mer incombant à l'État.
2 - Conformément au règlement annexé à l'arrêté du 23 novembre 1987 modifié, la jauge d'un navire s'exprime sans unité.
3 - 1 mille équivaut à 1852 mètres.
4 - En application des dispositions du règlement (CE) n°725/2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires.

Enfin, pour favoriser la diffusion des bonnes pratiques, la présente instruction a valeur d'information pour toute autre entité maritime ou portuaire, publique ou privée, non soumise aux exigences réglementaires dans le domaine de la sûreté. A cet effet, elle est complétée par la plaquette « l'essentiel sur l'organisation et la coordination de la sécurité maritime et portuaire » qui peut être consultée et téléchargée sur le site www.sgdsn.gouv.fr.

TITRE I

PRINCIPES RÉGISSANT LA SÛRETÉ MARITIME ET PORTUAIRE

CHAPITRE I : ENJEUX[5]

La France dispose d'un espace maritime considérable de près de 11 millions de km², dont 95 % bordent ses territoires ultramarins. L'importance de cet espace en fait la deuxième nation maritime et offre de nombreuses opportunités. La mer, à la fois motrice et vectrice de l'économie mondiale, génère des dépendances dans différents domaines tels que :

- les approvisionnements en énergie, issues de la mer ou provenant d'autres territoires ;
- l'exploitation et la gestion des ressources halieutiques et minérales ;
- les transports maritimes, qui représentent 90 % des échanges mondiaux en volume de marchandises transportées et 80 % en valeur[6] ;
- le transport de passagers, qui représente pour les ports français un flux proche de trente millions de personnes[7] ;
- les communications par câbles sous-marins, qui concentrent 99 % des transmissions intercontinentales.

Dans des contextes géopolitiques et économiques concurrentiels, marqués par de fortes incertitudes, la France doit faire face à de multiples enjeux liés plus particulièrement :

- à la liberté d'action de sa défense, dont sa dissuasion ;
- à la sécurisation des personnes et des biens, dont les infrastructures situées sur le littoral ;
- à la sécurisation des réseaux sous-marins de communication ;
- au maintien de la libre circulation des personnes et des biens, dont l'accès en toute sécurité aux ports et au littoral, condition indispensable pour son économie ;
- à la préservation et l'exploitation contrôlée des ressources naturelles des espaces maritimes.

5 - Cf. Stratégie nationale de sûreté des espaces maritimes, adoptée le 10 décembre 2019.
6 - 10,6 milliards de tonnes en 2017 (source ministère chargé des transports).
7 - Ministère chargé des transports, chiffres clés du transport, édition 2021, Commissariat général du développement durable.

CHAPITRE II : PÉRIMÈTRE

Ces enjeux induisent, pour les acteurs étatiques et privés, une exigence de sûreté :

- en mer[8], pour les navires :
  - sous pavillon français ;
  - sous pavillon étrangers, détenus en propriété ou affrétés par des armateurs français ;
  - sous pavillons étrangers, d'intérêt pour la France au regard des biens et des personnes transportées ou de la navigation réalisée (liaisons maritimes entre la France continentale et la Corse, transports de marchandises à destination ou provenant d'acteurs économiques français, etc.).
- en mer[9], pour les îles artificielles, installations et ouvrages réalisés et exploités conformément à la Convention des Nations Unies sur le droit de la mer, de 1982, dite de *Montego Bay ;*
- en mer ou dans les ports, sur les plans d'eau situés dans les limites portuaires de sûreté (LPS)[10] ;
- à terre, dans les ports comprenant au moins une installation portuaire fournissant des services à certaines catégories de navires[11] :
  - les installations portuaires et leurs éventuelles *zones à accès restreint* (ZAR), dédiées aux passagers ou aux marchandises, également situées dans les LPS ;
  - les points névralgiques situés dans les LPS, hors des installations portuaires (écluses, capitainerie, systèmes d'information, etc.) ;
  - les infrastructures désignées *points d'importance vitale* (PIV)[12] du secteur des transports, sous-secteur des transports maritime et fluvial.
- à terre, dans les ports autres que ceux précédemment visés tels que les ports de plaisance et les ports de pêche ;
- à terre, sur le littoral (liste non exhaustive) :
  - les infrastructures désignées PIV, quel que soit leur secteur d'activité d'importance vitale ;
  - les infrastructures des *opérateurs de services essentiels* (OSE), gestionnaires et exploitants portuaires ou exploitant de services de trafic maritime ;
  - les aéroports dotés d'une zone voisine aéronautique maritime ;
  - les chantiers de construction navale ;
  - les infrastructures, non PIV, du secteur de l'énergie (stockage et traitement de combustibles, réseaux de distribution, etc.) ;
  - les lieux à forte concentration de population, permanente ou temporaire (centres urbains, stations balnéaires, grands rassemblements, etc.).

Au regard de ce périmètre, la sûreté nécessite une articulation interministérielle robuste, car elle s'exerce dans de nombreux milieux, sur des zones maritimes et terrestres très vastes et avec des acteurs, publics et privés, aux activités et responsabilités diverses.

8 - En haute mer, ainsi que dans les eaux sous souveraineté et sous juridiction françaises.
9 - Dans les eaux sous souveraineté et sous juridiction françaises.
10 - Article L.5332-6 du code des transports, ces limites peuvent d'étendre au-delà des limites administratives du port.
11 - Navires à passagers, ou de charge de jauge égale ou supérieure à 500, qui effectuent des voyages internationaux, ainsi que les navires à passagers effectuant une navigation nationale de plus de 20 milles.
12 - Conformément au code de la défense (dans ses articles L.1332-1 à 1332-7 et R.1332-1 à 1332-42), qui constitue le cadre législatif et réglementaire du dispositif de sécurité des activités d'importance vitale (SAIV).

CHAPITRE III : MENACES

Les menaces pesant sur le domaine maritime au sens large et, plus particulièrement, sur le transport maritime et les opérations portuaires, sont définies, de façon complémentaire et cohérente, par plusieurs vecteurs :

- la stratégie nationale de sûreté des espaces maritimes qui présente les généralités sur les différentes menaces propres au monde maritime ;
- *la directive nationale de sécurité* (DNS) du secteur des transports (sous-secteur des transports maritime et fluvial), annexée à l'arrêté du Premier ministre du 23 mai 2016. Ce texte réglementaire porte notamment sur les menaces à caractère malveillant auxquelles sont exposés les *opérateurs d'importance vitale* (OIV) du secteur. Ces menaces font l'objet de scénarios détaillés dans l'annexe de cette DNS[13] ;
- l'évaluation de la menace terroriste dans le domaine maritime par la *coordination nationale du renseignement et de la lutte contre le terrorisme* (CNRLT) ;
- l'évaluation de la menace sur le trafic de stupéfiants dans les enceintes portuaires par la *cellule nationale de renseignement opérationnel dédiée au trafic de stupéfiants sur les plateformes portuaires* (CROSS portuaire), codirigée par l'OFAST et la DNRED, et associant la GMAR, le SCRT et la DCPAF ;
- le plan gouvernemental Pirate Mer n°10070/SGDSN/PSE/PSN/CD, édition juillet 2017, dont l'objet est la réponse de l'État à un acte de terrorisme, piraterie ou brigandage commis à quai, en mer ou depuis la mer, à l'encontre des navires et des intérêts français. Pour ce plan, les menaces sont caractérisées par plusieurs situations de référence.

Les menaces présentées dans ces documents, dont certains sont classifiés, ne sont données qu'à titre indicatif. Elles ont été retenues en fonction de leur probabilité de survenance, au regard des modes d'action observés, et des vulnérabilités propres aux activités maritimes, portuaires et sur le littoral. Il appartient aux ministères, à leurs services déconcentrés, aux collectivités territoriales et aux opérateurs d'analyser les menaces auxquelles les activités relevant de leur responsabilité sont plus particulièrement exposées.

En fonction de la localisation de la cible (en mer ou à terre), outre l'aspect humain, les vecteurs matériels utilisés pour la mise en œuvre de ces menaces peuvent être de nature maritime (navires de commerce, embarcations de servitude, mines, etc.), terrestre (véhicule, train, etc.), aérienne (aéronef piloté, drone, etc.) ou cyber.

Au regard de la numérisation croissante, des activités maritimes et portuaires, leur exposition aux menaces cyber est renforcée. En mer, les navires qui embarquent des équipes de plus en plus réduites recèlent désormais de nombreux systèmes d'information qui arment toutes les fonctions du navire et notamment les plus vitales (outils de navigation, communications, propulsion, systèmes de chargement et de stabilité, etc.). Pour des navires appelés à naviguer pendant plusieurs décennies, le risque d'obsolescence des systèmes numériques embarqués est avéré, ce qui les rend plus vulnérables à la croissance de la menace cyber et implique des efforts certains en matière de maintien en conditions opérationnelles. A terre, les infrastructures portuaires, pétrolières, d'énergies marines renouvelables, aujourd'hui toutes dépendantes d'outils numériques, peuvent être ciblées par des cyberattaques.

13 - Les menaces listées dans ce document, classifié et non publié au Journal officiel, ne s'adressent qu'aux OIV du secteur des transports, sous-secteurs des transports maritime et fluvial.

Le périmètre des menaces se veut le plus large possible car, dans les faits, elles sont souvent cumulatives (une organisation terroriste pourra, par exemple, utiliser l'argent de la drogue pour s'approvisionner en armes ou en explosifs).

Pour le présent document, les menaces retenues sont les suivantes:

- le terrorisme d'origine djihadiste, nationaliste, séparatiste, extrémiste[14] ;
- la piraterie et le brigandage ;
- la prolifération illicite :
  - d'armes de destruction massive, de leurs vecteurs et des matériels connexes ;
  - de produits chimiques ou biologiques à double usage.
- les trafics illicites de stupéfiants, d'armes, de produits contrefaits, etc ;
- l'immigration clandestine ;
- l'espionnage économique ;
- l'activisme, de toutes origines, impactant la sûreté par le détournement de navire, des actions sur des installations portuaires, etc. ;
- les stratégies hybrides[15] dont les menaces cyber.

14 - Se référer au rapport annuel d'EUROPOL sur la situation et la tendance du terrorisme en Europe. www.europol.europa.eu
15 - Objet d'un document de référence interministériel, transmis par la note 1008/SGDSN/AIST/AI/DR du 10 février 2021.

CHAPITRE IV : PRINCIPES DE SÛRETÉ

Renseignement

Les différentes menaces, souvent polymorphes, sont susceptibles de se manifester sur un vaste espace géographique, du littoral jusqu'à la haute-mer, et d'avoir notamment pour cible des passagers, des navires, des infrastructures, etc. Les mesures de sûreté à adopter, pour être efficaces face à ces menaces, à leur intensité et à leur probabilité de survenance, nécessitent en amont un système de veille, de recueil du renseignement, d'exploitation et de mise en alerte. Le renseignement est donc une fonction essentielle pour l'efficacité du dispositif de sûreté ; à défaut, celui-ci serait de fait inadapté par sa faiblesse, voire inacceptable par l'application de mesures contraignantes disproportionnées.

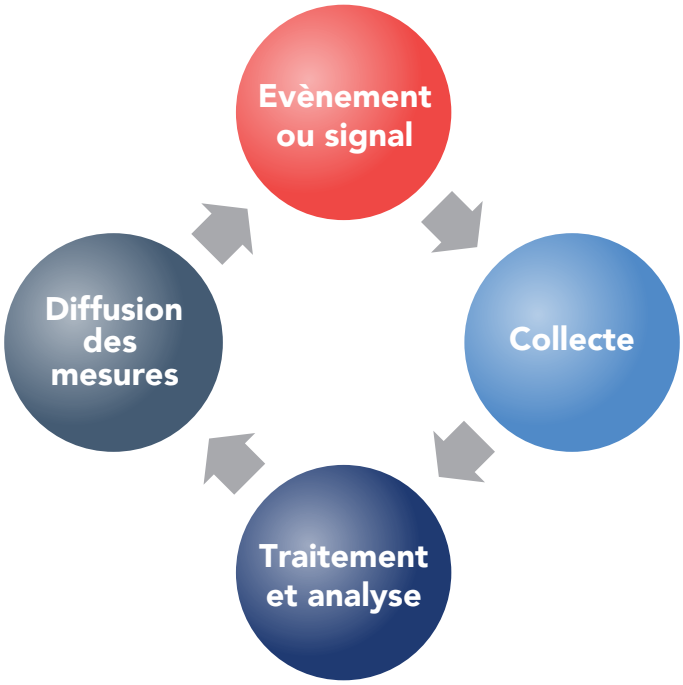


Figure I-IV-1 Cycle du renseignement

Le renseignement est la première des prescriptions fonctionnelles du code international pour la sûreté des navires et des installations portuaires[16] (*International Ship and Port Facility Security code – ISPS*), pour détecter les menaces et prendre des mesures de sauvegarde : « *Rassembler et évaluer les renseignements concernant les menaces contre la sûreté et échanger ces renseignements avec les Gouvernements contractants appropriés* ».

Les services et les directions de l'État organisent leur propre chaîne de recueil de renseignement. Les acteurs impliqués dans la remontée et le traitement des données observées et collectées par un acteur non étatique sont présentés dans le tableau en annexe 2.

16 - Article A-1.3.1.

En application du code de la défense[17], la *défense maritime du territoire* (DMT) a notamment pour objet de renseigner les autorités civiles et militaires sur les activités suspectes ou hostiles en mer et les menaces d'origine maritime qui concernent leurs domaines de responsabilités. Le dispositif mis en place s'appuie sur un réseau de capteurs (moyens des différentes administrations déployés en mer) puis, au niveau local, sur les *cellules de coordination de l'information maritime* (CCIM) placées auprès des préfets maritimes, au sein desquelles sont partagées les informations d'intérêt.

Afin de favoriser le partage des renseignements liés à la sûreté en mer et dans les ports à l'étranger, les armateurs français, comme les armements étrangers, peuvent par ailleurs participer à la *coopération navale volontaire* (CNV)[18]. Ils bénéficient en retour d'une évaluation de la menace dans les zones à risques au sein desquels naviguent et font escale leurs navires.

Au niveau central, la fusion des données recueillies et leur exploitation sont réalisées par la *coordination nationale du renseignement et de la lutte contre le terrorisme* (CNRLT). Sur la base des évaluations de la menace terroriste, le *secrétariat général de la défense et de la sécurité nationale* (SGDSN) réalise les notes de posture Vigipirate qui précisent les mesures de sûreté à adopter pour une période donnée.

Par ailleurs, la *cellule nationale de renseignement opérationnel dédiée au trafic de stupéfiants sur les plateformes portuaires* (CROSS portuaire) a vocation à centraliser et enrichir, au niveau national, les renseignements liés au trafic de stupéfiants.

Au niveau international, la communication de renseignements entre gouvernements contractants relève de la convention internationale de 1974 modifiée, pour la sauvegarde de la vie humaine en mer (*Safety Of Life At Sea – SOLAS*)[19]. Cette fonction est assurée par l'Adjoint Mer placé auprès du *haut fonctionnaire de défense et de sécurité* (HFDS) des ministères chargés des transports et de la mer.

Prévention

La prévention constitue le cœur de la politique de sûreté maritime et portuaire afin d'agir pour que les menaces ne se concrétisent pas et, le cas échéant, d'en limiter les effets possibles. La prévention, mise en œuvre par les services de l'État et les opérateurs, est continue.

A cet effet, de multiples dispositions ont été prises dans le domaine normatif avec des conséquences sur les organisations et les dispositifs déployés, en mer comme à terre.

Cadre international

Au niveau normatif, la convention SOLAS rend applicable le code international de gestion de la sécurité pour le transport maritime (*International Safety Management – ISM*), ainsi que le code *ISPS*[20]. Adopté par l'*organisation maritime internationale* (OMI) le 12 décembre 2002, le code ISPS, pierre angulaire de la prévention des domaines maritime et portuaire, a été repris, avec des compléments, dans le règlement européen n° 725/2004 du Parlement européen et du Conseil du 31 mars 2004. Son périmètre comprend la menace terroriste, le transport illicite de marchandises, l'immigration clandestine et les autres actes de malveillance de droit commun. Il porte sur :

- les navires à passagers ou de charge de jauge brute égale ou supérieure à 500 assurant des services maritimes internationaux ;

17 - Article D*1431-1.
18 - Instruction n° 165/SGDSN/PSE/PSN 2019 – n°100/SG Mer du 29 avril 2019 relative à la coopération navale volontaire.
19 - Règle 13 du chapitre XI-2.
20 - Annexé au chapitre XI-2 de la convention SOLAS.

- les navires à passagers assurant des services maritimes nationaux relevant de la classe A au sens de l'article 4 de la directive 2009/45/CE modifiée établissant des règles et normes de sécurité pour les navires à passagers[21] (article 3.2) ;
- le cas échéant, sur la base d'une évaluation du risque de sûreté, les navires effectuant une navigation intérieure (article 3.3) ;
- les unités de forage au large ;
- les installations portuaires, que les navires susmentionnés utilisent comme interface, où se déroulent les opérations commerciales entre ports et navires.

Ce code[22] repose sur trois niveaux de sûreté correspondant à un régime normal, à un risque accru et à une menace probable ou imminente[23].

Conformément à la convention *SOLAS*[24], le point de contact national est chargé d'apporter conseils et assistance aux navires, de signaler tout problème de sûreté que pourraient susciter d'autres navires, mouvements ou communications. Lorsqu'un risque d'attaque a été déterminé, les navires concernés et leur administration doivent être informés de toutes mesures de sûreté qui devraient être mises en place par le navire concerné pour se protéger contre l'attaque.

Sur la base des renseignements collectés sur l'état de la menace en mer, dans des ports français ou étrangers, l'Adjoint Mer placé auprès du SHFDS des ministères chargés des transports et de la mer propose aux services du Premier ministre (SGDSN et SGMer) de modifier le niveau de sûreté ISPS à bord des navires battant pavillon français ou dans les installations portuaires françaises pour les protéger contre un risque d'attaque. Le niveau de sûreté à appliquer est décidé par le Premier ministre.

Cadre national

Plan VIGIPIRATE

Face aux menaces d'actions terroristes, certaines mesures appelées par le code *ISPS* sont intégrées dans une organisation de sûreté nationale plus large, portée par le plan gouvernemental de vigilance, de prévention et de protection VIGIPIRATE. Sur le fondement de l'évaluation de la menace effectuée par la CNRLT avec les services de renseignement, le SGDSN diffuse des notes de postures VIGIPIRATE – qui déterminent les mesures devant être mises en œuvre par les services de l'État et les opérateurs. La corrélation entre les mesures *ISPS* et celles relevant du plan VIGIPIRATE est présentée en annexe 4 du présent document.

Application du code ISPS

La mise en œuvre du code ISPS, du règlement (CE) n°725/2004 et de la directive 2005/65/CE au niveau national est pilotée par la *direction générale des infrastructures et des mobilités* (DGITM) et plus particulièrement par sa *direction des transports ferroviaire et fluvial et des ports* (DTFFP), pour les ports et les installations portuaires, et par la *direction générale des affaires maritimes, des pêches et de l'aquaculture*[25] (DG AMPA) pour les compagnies maritimes et les navires. A l'exception de la permanence assurée par le *service du haut fonctionnaire de défense et de sécurité* (SHFDS) des ministères chargés des transports et de la mer, la fonction « point de contact national » vis-à-vis de la Commission européenne et des autres Etats membres, ainsi que vis-à-vis de l'*Organisation Maritime*

21 - Navires de plus de 24m effectuant des trajets à plus de 20 milles des côtes.
22 - Pour plus de précision, outre le code *ISPS*, il est possible de se reporter au programme national de sûreté des transports et des ports maritimes élaboré par le ministère chargé des transports.
23 - Cf. annexe 4.
24 - SOLAS XI-2 R13.2 à 6.
25 - Effective le 1er mars 2022.

Internationale (OMI), est assurée par la DGITM. Une représentation permanente de la France est assurée, par ailleurs, au sein de l'OMI.

En application des règles internationales, les mesures de prévention, prises dans les ports maritimes français pour application du code *ISPS* sont définies dans des plans de sûreté élaborés par les opérateurs, après l'évaluation par les services de l'Etat des menaces auxquelles ils sont susceptibles d'être exposés. Dans un processus d'amélioration continue, la DTFFP dispose d'auditeurs nationaux[26] qui contribuent également :

- à l'accompagnement des inspecteurs de la Commission européenne à l'occasion d'inspection en France ;
- à l'appui des autorités préfectorales sur les aspects réglementaires et les enjeux nationaux ;
- à l'accompagnement de la mise en œuvre effective des mesures de sûreté portuaire et maritime auprès des services déconcentrés, des collectivités territoriales et des opérateurs, notamment par la production de fascicules pédagogiques ;
- à la centralisation et au suivi des documents de sûreté des ports et des installations portuaires ;
- au recueil de la situation des ports et des installations portuaires de leur façade maritime vis-à-vis des obligations liées à la sûreté portuaire et maritime ;
- à l'élaboration de la doctrine, ainsi qu'à l'animation des réseaux locaux (autorités portuaires, forces de l'ordre, capitaineries, etc.) ;
- à différentes actions de sensibilisation, de formation et de prévention.

Plus particulièrement, pour les OIV du domaine portuaire, les dispositions de prévention face aux risques et aux menaces sont précisées par la directive nationale de sécurité (DNS) du secteur des transports, sous–secteur des transports maritime et fluvial[27].

La DGAMPA a la responsabilité de l'organisation et de l'animation de l'inspection des navires. L'approbation du plan de sûreté des navires (depuis la publication du décret n°2020-600), la délivrance, le renouvellement et le visa des certificats de sûreté des navires assujettis au code ISPS, relève de la responsabilité des chefs des centres de sécurité des navires, services des directions interrégionales de la mer (DIRM).

La DGAMPA assure le suivi et la supervision du processus de certification des navires et s'assure du respect des dispositions internationales et communautaires en la matière. Elle dispose pour ce faire au sein du Service des flottes et des marins (SFM) de la sous-direction de la sécurité et de la transition écologique des navires (STEN) d'un chargé de mission pour la sûreté et la cybersécurité des navires.

Le SHFDS des ministères chargés des transports et de la mer assure la permanence de la réception des communications émanant de gouvernements contractant à SOLAS[28] , la réception des déclarations[29] d'emploi d'équipes privées de protection des navires à bord des navires français et un suivi de l'état de la menace contre les navires français.

26 - Agents du bureau de la sûreté portuaire et fluviale de la DGITM accompagnés le cas échéant d'auditeurs volontaires issus d'autres services de l'Etat (DCPAF par exemple)

27 - Arrêté du 23 mai 2016 portant approbation de la directive nationale de sécurité applicable au secteur des transports (sous-secteur des transports maritime et fluvial).

28 - SOLAS XI-R13.1.4

29 - Les déclarations d'embarquement d'EPPN sont adressées au SHFDS du ministère des transports et au commandant de zone maritime compétent (art D5442-7 et D5442-8 du code des transports).

Cybersécurité

Le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information[30]. Le Premier ministre dispose à cette fin de l'*agence nationale de sécurité des systèmes d'information* (ANSSI), rattachée au *secrétaire général de la défense et de la sécurité nationale* (SGDSN). L'ANSSI assure ainsi le pilotage de la politique générale de cybersécurité et met en œuvre la stratégie nationale de cybersécurité et de cyberdéfense.

Le ministre de la transition écologique, chargé des transports, et le ministre de la mer conduisent conjointement la politique de cybersécurité maritime et portuaire par l'intermédiaire de la DTFFP, chargée de la cybersécurité des ports et des installations portuaires, et de la DGAMPA chargée de la cybersécurité des navires.

Par ailleurs, une structure dédiée consacrée à l'appréhension des menaces cyber, le *Conseil de cybersécurité du monde maritime* (C2M2), a été créé par décision du CIMER de novembre 2018 pour constituer la structure de gouvernance nationale de la cybersécurité maritime. Il est placé sous la présidence du SGMer, appuyé par l'ANSSI, et rassemble les représentants des opérateurs publics et privés du secteur maritime ainsi que les acteurs territoriaux.

Le SGMer pilote ce sujet au travers de la Commission interministérielle de sûreté maritime et portuaire (CISMAP) présidée par son cabinet et rassemblant l'ensemble des administrations concernées.

Enfin, la cybersécurité des infrastructures portuaires et maritimes fait l'objet de plusieurs dispositifs réglementaires :

- le code de la défense prévoit en effet que les opérateurs d'importance vitale du secteur doivent identifier leurs *systèmes d'information d'importance vitale* (SIIV) pour lesquels une atteinte en disponibilité, en intégrité ou en confidentialité aurait un impact significatif sur la réalisation de leurs missions vitales. Ils doivent appliquer à ces systèmes des règles de sécurité définies par le Premier ministre[31] et déclarer à l'ANSSI les incidents qui affectent ces systèmes ;
- les opérateurs de services essentiels, tels que définis par la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, doivent également identifier leurs systèmes d'informations essentiels pour lesquels une atteinte en disponibilité, en intégrité ou en confidentialité aurait un impact significatif sur la réalisation de leurs missions essentielles. Ils doivent appliquer à ces systèmes les règles de sécurité définies par le Premier ministre[32] et déclarer à l'ANSSI les incidents affectant ces systèmes ;
- la résolution MSC.428(98) adoptée le 16 juin 2017 préconise la prise en compte des risques cyber dans les systèmes de gestion de la sécurité issus du Code international de gestion de la sécurité. Elle s'applique donc à toutes les compagnies maritimes exploitant des navires relevant des dispositions de la Convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS 1974) ainsi que les navires relevant du Règlement (CE) 336/2006 du 15 février 2006.

30 - Loi n°2013-1168 du 18 décembre 2013.
31 - Arrêté sectoriel du 11 août 2016.
32 - Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

Texte de référence	Entité concernée	Évaluation	Plan	Approbation du plan
Code ISPS ***Règlement (CE) n°725/2004***	Navire	Évaluation de la sûreté du navire[33]	Plan de sûreté du navire[34]	Approbation par les chefs des centres de sécurité des navires (CSN)
	Installation portuaire	Évaluation de sûreté de l'installation portuaire (ESIP)[35]	Plan de sûreté de l'installation portuaire (PSIP)[36]	Approbation par la préfecture de département
Directive 2005/65/CE	Port	Évaluation de sûreté du port (ESP)[37]	Plan de sûreté portuaire (PSP)[38]	Approbation par la préfecture de département
DNS	OIV/PIV	Analyse des risques	PSO/PPP/PSSI	Approbation par arrêté du ministre coordinateur de la liste des PIV annexée au PSO Approbation du PPP par arrêté préfectoral

Tableau I-IV-2 Planification de prévention

Mesures de prévention particulières

L'initiative sur la sécurité des conteneurs *(Container Security Initiative – CSI),* lancée en janvier 2002 par le service des douanes et de la protection des frontières des États-Unis d'Amérique (USA), a pour objectif d'accroître la sûreté des conteneurs maritimes à destination du territoire américain. Pour la France, les ports du Havre et de Marseille sont parties prenantes de ce programme qui vise les cargaisons suspectes. Ce programme a fait l'objet de la décision du Conseil n° 2004/634/CE du 30 mars 2004, relative à la conclusion de l'accord entre la Communauté européenne et les USA, intensifiant et élargissant le champ d'application de l'accord de coopération douanière et d'assistance mutuelle en matière douanière pour y inclure la coopération relative à la sécurité des conteneurs. En sus, la réglementation communautaire a instauré un système de contrôle des importations appelé *Import Control System* (ICS), entré en vigueur le 1er janvier 2011. Ainsi, des obligations supplémentaires en matière de sûreté et de sécurité s'imposent aux opérateurs du commerce extérieur[39].

L'exploitation avant embarquement des données à caractère personnel détenues par les compagnies maritimes de transport doit permettre de prévenir la commission d'actes malveillants à bord des navires par des personnes présentant une menace potentielle ou avérée. La mise en place du

33 - *Ship Security Assessment – SSA.*
34 - *Ship Security Plan – SSP.*
35 - *Port Facility Security Assessment – PFSA.*
36 - *Port Facility Security Plan – PFSP.*
37 - *Port Security Assessment – PSA.*
38 - *Port Security Plan – PSP.*
39 - Règlement (CE) n° 648/2005 du parlement européen et du Conseil du 13 avril 2005 modifiant le règlement (CEE) n° 2913/92 du Conseil établissant le code des douanes communautaires.

système national de centralisation des données des dossiers passagers du transport maritime[40], plus communément appelé **PNR (pour *Passenger Name Record) maritime,*** est confié à l'*Agence nationale des données de voyage* (ANDV)[41] qui a fusionné le *service national des données de voyage* (SNDV) et l'*unité information passagers* (UIP)[42]. A terme, cette exploitation permettra non seulement le criblage automatique mais également le ciblage[43].

L'initiative de sécurité contre la prolifération *(Proliferation Security Initiative - PSI)* a pour objectif de lutter contre les transports illicites d'armes de destruction massive, de leurs vecteurs et des matériels connexes, dont la prolifération est qualifiée de menace à la paix et à la sécurité internationale par le Conseil de sécurité des Nations Unies (Résolution n° 2004/1540). Elle vise à renforcer la coopération opérationnelle entre les États participants pour interrompre les flux proliférant par les voies maritimes, aériennes et terrestres. Elle s'inscrit dans le respect des lois nationales et des règles de droit international, en particulier celles émanant du Conseil de sécurité de l'ONU ou de la Convention de Montego Bay. Au niveau national, la lutte contre la prolifération fait l'objet du plan gouvernemental d'intervention en vue d'une interception de biens contribuant à des activités de prolifération d'armes de destruction massive « interception prolifération »[44].

Outre les planifications susmentionnées et les dispositions prises en application de celles-ci, des **actions de sensibilisation et de prévention sont organisées localement par les services de l'État,** notamment par la gendarmerie maritime (GMar) et ses *pelotons de sûreté maritime et portuaire* (PSMP), par la police aux frontières, par les unités de gendarmerie départementale, par les services de sécurité publique et par la douane. Ces actions de sensibilisation, voire de contrôle, peuvent se dérouler à terre et en mer dans les eaux sous souveraineté française. Toutes ces actions sont réalisées de façon coordonnée, sous l'autorité des représentants de l'État[45]. Les référents des opérateurs, tels que les agents de sûreté des navires, des compagnies, des ports et des installations portuaires, mais plus largement les cadres des milieux maritime et portuaire, constituent des liens privilégiés pour relayer, au sein de leur organisation, les messages de prévention adaptés à leur exploitation, à leur environnement et au niveau de menace.

Enfin, la GMar dispose pour chaque port maritime d'un correspondant sûreté et, pour chaque façade maritime, d'un référent sûreté. La GMar assure notamment dans les principaux ports :

- l'analyse de sûreté des navires de commerce en escale dans les ports français ;
- un travail régulier de sensibilisation des cadres du milieu maritime et portuaire à la sûreté et à la détection des signes de radicalisation.

40 - Cf. article 14 de la loi n° 2017-1510 du 30 octobre 2017 sur la sécurité intérieure et la lutte contre le terrorisme, repris dans l'article L232-7-1 du code de la sécurité intérieure. S'il n'est pas à proprement parlé un système dédié à la sûreté, il participe à la sûreté des transports.
41 - Service à compétence nationale créé par le décret n° 2022-752 du 29 avril 2022. Il est rattaché au directeur général de la police nationale.
42 - Service interministériel à compétence nationale, assurant la gestion du système qui collecte et traite les données de réservation et d'enregistrement des passagers aériens.
43 - Le criblage permet le croisement des listes avec les fichiers de police choisis, tandis-que le ciblage permet une interrogation du système suivant des critères définis.
44 - Instruction n°11055/SGDSN/AIST/PST/S-SF du 18 octobre 2021.
45 - Préfets de département, préfets maritimes et, outre-mer, délégués du Gouvernement pour l'action de l'État en mer.

Protection

Cadre général

L'objectif principal de la protection est d'organiser la réponse de l'État pour agir efficacement lorsque la menace se concrétise. Dans le cadre de ce document, la protection, constituée d'un ensemble de dispositions permanentes et temporaires, a principalement pour objet de :

- **surveiller** la libre circulation des navires d'intérêt pour la France, les eaux sous juridiction française, les approches du territoire national sur ses façades maritimes, ainsi que le littoral, et plus particulièrement les ports ;
- **contrôler** les activités dans les eaux sous juridiction française et dans nos ports ;
- **réduire la vulnérabilité** intrinsèque de certaines activités maritimes et portuaires (concentration de passagers, importants volumes de matières dangereuses, navires en haute mer éloignés de la réponse de l'État, indispensable rapidité des échanges et des transferts de flux, etc.) ;
- **déceler et évaluer les menaces** visant le domaine maritime et portuaire ;
- **dissuader** de potentiels agresseurs par des mesures de protection, pour certaines de façon ostensible.

La protection s'étend de la haute mer au littoral et comprend *de facto* les ports et leurs installations, indispensables interfaces spécifiques entre les milieux maritime et terrestre. Au regard de l'importance de ces interfaces, l'Etat a renforcé leur protection en déployant dans certains ports des PSMP qui, outre leur capacité d'intervenir face à un acte de malveillance, sont à même de réaliser des missions spécifiques telles que la surveillance maritime et terrestre, la sécurisation des espaces portuaires (contrôles sous-marins de quais et de coques, de sécurisation des navires à passagers à l'embarquement et au débarquement, etc.), l'escorte de navires sensibles et le contrôle de navires (fouilles de sûreté, etc.). Les différents dispositifs de protection, privés et étatiques, pour être viables, se doivent d'être cohérents et adaptés aux contraintes organisationnelles et économiques des multiples acteurs.

Défense maritime du territoire - volet protection

Une importante partie de cette action de protection est réalisée à travers la *défense maritime du territoire* (DMT) qui, en application du code de la défense[46], concourt à assurer la sécurité du territoire, et notamment la protection des *installations prioritaires de défense* (IPD). Localement, mise en œuvre par le *commandant de zone maritime* (CZM) en métropole et par le *commandant supérieur* (COMSUP) des forces de souveraineté outre-mer, la DMT est permanente et a pour objet de :

- **surveiller** les approches du territoire national sur ses façades maritimes, de déceler et d'évaluer la menace qui peut s'y exercer sur ou dans la mer ;
- **renseigner** les autorités civiles et militaires sur les activités et les menaces, comme précédemment présentées dans le paragraphe relatif au renseignement ;
- **s'opposer** aux actions menées par voie de mer contre le territoire national et aux entreprises adverses contre les intérêts nationaux dans les approches de ce territoire, en particulier, contre les activités nationales dans toutes les zones, littorales et maritimes, où la France dispose de droits d'exploitation.

La mise en œuvre de la DMT consiste à disposer d'une capacité de surveillance et d'action d'autant plus dense et réactive que l'on se rapproche des côtes françaises et que le niveau de menace est important.

Pour cela, un zonage permet la convergence des efforts. Cette sectorisation géographique repose avant tout sur les « zones maritimes »[47], qui définissent la zone de responsabilité du CZM. Ce zonage, qui facilite par

46 - Articles D*1431-1 à D*1432-5.
47 - Cf. article D3223-51 du code de la défense.

ailleurs la concertation entre CZM, PREMAR et préfets de zone de défense et de sécurité, en collaboration étroite avec les préfets de département, permet d'aboutir à la création d'ensembles géographiques cohérents (rades et estuaires par exemple) dont la surveillance optique et radar est rendue possible par le regroupement de différents moyens fixes (sémaphores, vigies des ports, etc.) et mobiles (ensemble des moyens des différentes administrations déployés en mer et sur le littoral). De façon plus localisée, des *secteurs de protection rapprochée* (SPR) peuvent être établis à l'intérieur des grands ports de commerce, en fonction du niveau de menace ou de l'importance et de la vulnérabilité de certaines activités. Dans ce cadre, les missions de surveillance, notamment celles effectuées par les PSMP peuvent être renforcées et réorientées en coordination avec les mesures de sécurité portuaires terrestres. L'établissement d'un SPR est réalisé en cohérence avec la mise en œuvre locale des mesures, socles et additionnelles, du plan gouvernemental VIGIPIRATE (mesures MAR du domaine maritime) et celles du code *ISPS*.

La stratégie vise à protéger les eaux sous souveraineté, les navires, les zones réservées et les composants névralgiques des ports et des installations portuaires, et à maintenir un niveau de vigilance dans ces espaces et ces infrastructures.

La mission de DMT s'appuie de manière permanente sur l'ensemble des unités de la marine nationale et de la GMar, à terre et en mer, mais également sur les informations fournies par les *services départementaux du renseignement territorial* (SDRT), les groupements de gendarmerie départementaux et les services territoriaux de la *direction générale de la sécurité intérieure* (DGSI). Elle peut être renforcée par les capacités des autres forces armées et des administrations, notamment celles intervenant en mer.

Zones d'intervention	Moyens de la marine nationale et de la gendarmerie maritime	Renforts interarmées et étatiques
Approches maritimes (de la haute mer au littoral)	• Sous-marins nucléaire d'attaque • Aéronefs de surveillance ou de patrouille maritime • Bâtiments porte-hélicoptère avec le détachement embarqué et de possibles renforts en éléments spécialisés de commandos marine/fusiliers-marins • Patrouilleurs de haute mer et équivalents • Chasseurs de mines, groupes de plongeurs-démineurs et bâtiments supports et • Patrouilleurs et vedettes de la gendarmerie maritime • Commandos marine	• **Moyens des autres armées** ○ Dispositifs particuliers de sûreté (Ex. : DPSA/DPSM) • **Moyens des autres administrations** ○ Affaires Maritimes (patrouilleurs) ○ Douanes (patrouilleurs, vedettes et aéronefs)
Littoral	• 58 sémaphores équipés du système SPATIONAV de fusion de l'information • Fusiliers-marins • Groupements de gendarmerie maritime dont les pelotons de sûreté maritime et portuaire (PSMP) et les brigades de surveillance du littoral (BSL) • Drones (en cours d'expérimentation)	• **Moyens des autres armées** ○ Plots MASA, radars mobiles et fixes ○ renforts terrestres (Ex. : DRB) • **Moyens des autres administrations** ○ Affaires Maritimes (CROSS, ULAM) ○ Gendarmerie départementale (brigades nautiques côtières) et sections aériennes de gendarmerie

Figure I-IV-3 Moyens de la défense maritime du territoire[48]

48 - Source état-major des armées.

Équipes de protection des navires de commerce

Afin de protéger le trafic maritime contre les actes de piraterie, conformément au code des transports et en application des articles 224-6 à 224-8 du code pénal qui visent notamment la piraterie, sans préjudice de l'application d'accords internationaux, certains types de navires sous pavillon français[49] peuvent, en raison des menaces encourues, embarquer des équipes privées de protection au-delà de la mer territoriale des États, dans des zones fixées par arrêté du Premier ministre. Les agents dotés d'armes qui assurent ces missions prennent la dénomination d'***équipes privées de protection des navires*** (EPPN). Dans certains cas et par convention entre l'armateur et l'*état-major de la marine* (EMM) [50], ces missions de protection contre la piraterie peuvent également être assurées pa r des militaires de la marine nationale qui, ponctuellement, constituent à cet effet des ***équipes de défense et d'interdiction maritime*** (EDIM[51]).

Face à la menace terroriste, lorsqu'il existe un risque exceptionnel d'atteinte à la vie des personnes embarquées sur les navires, les EPPN peuvent exercer en haute mer et dans les eaux territoriales et les eaux intérieures maritimes françaises, après autorisation du préfet maritime ou du délégué du Gouvernement pour l'action de l'État en mer. Cette autorisation est délivrée sur demande de l'armateur, pour un trajet ou une ligne régulière défini[52]. Pour l'exercice de cette activité dans les eaux sous souveraineté étrangère, l'accord de l'État côtier doit être préalablement obtenu, et ce en particulier pour ce qui concerne l'emport et l'usage d'armes. Cet accord est recherché par le SGDSN, en lien avec le SGMer, le ministère chargé des affaires étrangères et les autres ministères concernés. Dans ce cadre, les EPPN ont pour mission, en cas d'attaque, d'alerter et renseigner les autorités, mettre les passagers à l'abri, intervenir afin de stopper l'agression en cours et de faciliter l'opération des unités d'intervention. Ces agents font l'objet d'une formation spécifique et d'une habilitation individuelle[53].

Pour le renforcement de la protection des navires à passagers sous pavillon français contre la menace terroriste, et plus particulièrement des ferries, la marine nationale met à la disposition des préfets maritimes une capacité de protection embarquée. Ainsi, ces autorités peuvent déployer, de manière aléatoire ou ciblée, des ***équipes de protection des navires à passagers*** (EPNAP), constituées de personnels de la GMar, ou d'équipes mixtes composées de gendarmes maritimes et de fusiliers marins. Ces militaires peuvent exercer leur mission de protection en haute mer, dans les eaux sous souveraineté française et, sous réserve d'un accord, dans les eaux sous souveraineté étrangère. Ce déploiement fait l'objet d'une convention entre l'armateur bénéficiaire et la marine nationale. Pour les eaux sous souveraineté étrangère, l'accord de l'État côtier est préalablement recherché selon les mêmes modalités que pour les EPPN.

49 - Cf. Décret n° 2014-1418 du 28 novembre 2014 modifié, pris pour l›application de l›article L. 5442-1 du code des transports.
50 - Ces conditions sont définies par l'état-major de la marine qui, au regard des éléments apportés par l'armateur et des contraintes opérationnelles et organiques, apprécie l'absolue nécessité de faire réaliser ces missions par son personnel.
51 - Également dénommées EPE (équipes de protection embarquées), en fonction du format de l'équipe embarquée.
52 - Cf. Articles R5442-1 à R5442-16 du code des transports pour les modalités pratiques de mise en œuvre des EPPN.
53 - Cf. Code des transports et le titre VI du code de la sécurité intérieure.

Équipes		Statut des agents	Objet de la protection	Observations
Appellations	Acronymes			
Équipes privées de protection des navires	EPPN	Agent privé habilité	Piraterie	Dans des zones définies et pour certains navires.
			Terrorisme	Pas de zones définies, mais nécessité accord des États côtiers tiers pour leurs eaux sous souveraineté. Pour les navires à passagers.
Équipes de défense et d'interdiction maritime	EDIM	Militaire (marine nationale)	Piraterie	Convention entre les armateurs et la marine nationale.
Équipes de protection des navires à passagers	EPNAP	Militaire (GMAR et fusiliers marins)	Terrorisme	Convention entre les armateurs de navire à passagers et la marine nationale. Nécessité accord des États côtiers tiers pour leurs eaux sous souveraineté.

Tableau I-IV-4 Equipes de protection embarquées

Mesures de protection dans les ports

Les mesures de protection, préalablement planifiées, sont mises en œuvre par les services de l'État et les opérateurs. Dans les ports et à terre sur le littoral, elles sont également définies au regard du plan gouvernemental VIGIPIRATE et, pour les ports qui y sont assujettis, du code *ISPS*, du règlement (CE) n° 725/2004 et de la directive 2005/65/CE. A noter que les plans d'intervention de la famille Pirate comprennent également des dispositions de protection afin de limiter la probabilité de survenance d'un nouvel événement terroriste.

Périmètre	Référentiel	Planification par les opérateurs	Planification étatique
***Navire à quai ou au mouillage soumis au code* ISPS**	*ISPS* *Règlement (CE) n°725/2004*	Plan de sûreté du navire (PSN)	Plan gouvernemental VIGIPIRATE et plans gouvernementaux de la famille PIRATE dont PIRATE MER (et leurs déclinaisons locales)
***Installation portuaire soumise au code* ISPS**		Plan de sûreté de l'installation portuaire (PSIP)	
Port	*Directive 2005/65/CE*	Plan de sûreté portuaire (PSP)	
PIV dont les infrastructures portuaires désignées	DNS	PSO, *plan particulier de protection* (PPP) et PSP pouvant avoir valeur, en tout ou partie, de PPP[54]	*Plan de protection externe* (PPE) Plan gouvernemental VIGIPIRATE et plans gouvernementaux de la famille PIRATE (et leurs déclinaisons locales)
Autres navires et installations à terre	Pas d'obligation réglementaire		Plan gouvernemental VIGIPIRATE et plans gouvernementaux de la famille PIRATE dont PIRATE MER[55] (et leurs déclinaisons locales)

Tableau I-IV-5 Planification de protection de la sûreté maritime et portuaire

Pour les installations terrestres, les ports et leurs installations portuaires, ces différents plans de protection, conformes aux dispositions réglementaires, doivent notamment :

- présenter les différents espaces délimités (LPS, ZAR, etc.) ;
- prendre en compte les interactions entre les acteurs privés et publics localement impliqués dans les missions de sûreté ;
- préciser les procédures à appliquer en fonction du niveau de sûreté appelé par le code *ISPS* et le plan VIGIPIRATE ;
- définir les mesures à appliquer en cas de survenance d'un événement de sûreté.

54 - Cf. article R. 5332-22 du code des transports, l'équivalence totale ou partielle entre le PPP et le PSP peut être décidée par le représentant de l'Etat dans le département.
55 - Plan PIRATE MER dédié aux navires en mer ou dans les ports.

Intervention

Lorsque la survenance d'une menace paraît imminente ou lorsqu'un acte malveillant est perpétré, il est alors nécessaire d'intervenir afin de :

- faire cesser l'acte ou la menace, si nécessaire par la neutralisation des auteurs ;
- secourir les éventuelles victimes et protéger les personnes impliquées ou susceptibles de l'être ;
- protéger les biens et l'environnement des conséquences, directes et indirectes, de l'événement ;
- prendre toutes les dispositions pour éviter la réitération d'un tel acte ;
- mettre en œuvre la phase d'enquête judiciaire sous la direction et le contrôle de l'autorité judiciaire.

Dans un souci d'efficience, l'intervention est proportionnelle à l'intensité et à la dangerosité, potentielle ou avérée, de la menace ou de l'acte malveillant. A terre et dans les eaux sous souveraineté française, la réponse peut aller de la simple interpellation citoyenne, telle que définie par l'article 73 du code de procédure pénale, à la mise en œuvre simultanée de capacités relevant de différents ministères.

DMT – volet intervention

L'opposition aux actions menées par voie de mer contre le territoire national et aux entreprises adverses contre les intérêts nationaux dans les approches de ce territoire, en particulier, contre les activités nationales dans toutes les zones littorales et maritimes où la France dispose de droits d'exploitation, est confiée aux armées dans le cadre de la DMT.

Dans son volet intervention, la DMT recouvre l'ensemble des actions et des opérations conduites dans les eaux territoriales ou dans les approches maritimes face à une menace ou une force d'opposition violentes nécessitant de mettre en œuvre des capacités et modes d'action militaires.

En haute mer, la réponse à une menace ou à un acte de malveillance est réalisée dans le respect du droit international. Selon le cas, elle peut relever de l'État du pavillon, du navire ou de la plateforme agressée, ou de l'État côtier ciblé[56].

En fonction de la nature des menaces et des modes d'action utilisés par les agresseurs, les différents services à alerter et intervenants sont présentés en annexe 3. Leur coordination se fait sous la direction des autorités préfectorales, maritimes et terrestres, compétentes (Cf. chapitre III du titre II).

Plans gouvernementaux

Face aux actions terroristes, la réponse de l'État s'appuie sur les plans gouvernementaux dédiés. Au regard du périmètre du présent document, il s'agit notamment des plans Vigipirate et Pirate-mer. En raison de la similitude des modes d'action des agresseurs et bien que leurs motivations soient de nature différente, le plan Pirate-mer est également dédié à la réponse de l'État aux actes de brigandage et de piraterie maritimes.

Les opérations de secours à personnes sont réalisées concomitamment et en coordination avec les forces spécialisées chargées de faire cesser la menace. Pour les interventions se déroulant en mer, l'Etat a développé à cet effet une capacité nationale de renfort pour l'intervention à bord des navires (CAPINAV) à même de mener des missions de sécurité civile dans le domaine maritime.

En cas d'évènement terroriste, la sous-direction antiterroriste (SDAT) est immédiatement mise en alerte en vue de coordonner le volet judiciaire entre les services de la police nationale, ceux des

56 - Cf. Convention des Nations unies sur le droit de la mer de 1982, dite de Montego Bay.

douanes et les unités de la gendarmerie nationale. La GMar, dispose notamment de capacités d'investigation adaptées au milieu maritime (échelon de contact des PSMP[57] notamment), déploie des brigades de recherche sur chaque façade maritime et dispose d'une section de recherches à compétence nationale. Enfin, s'agissant du domaine maritime par nature ouvert sur le monde, des accords d'entraide pénale internationale ainsi que le réseau de coopération policière internationale facilitent la conduite des investigations.

Domaine Cyber

Pour faire face aux attaques dans le domaine numérique, l'association France Cyber Maritime a pour mission de renforcer la résilience du secteur maritime et portuaire. Elle est plus particulièrement chargée de mettre en œuvre, à terme, le *Maritime Computer Emergency Response Team (M-CERT)*, centre de veille, d'analyse, d'alerte et de recueil des incidents cyber avec l'appui de l'ANSSI. France Cyber Maritime et la Marine nationale sont par ailleurs liés par une convention formalisant l'échange direct d'expérience et d'information entre l'association et ALCYBER, autorité de coordination cyber de la Marine nationale et associant étroitement le *Maritime Information Cooperation and Awareness Center* (MICA Center), centre d'expertise dédié à la sûreté maritime, qui assure déjà des fonctions de recueil d'incidents au profit du secteur maritime. Les compagnies signataires du protocole de coopération navale volontaire donnent ainsi l'alerte cyber *via* le MICA Center.

Résilience

Lorsqu'un événement survient, il est primordial que ses conséquences ne mettent pas en jeu la continuité et la disponibilité des activités des opérateurs, publics ou privés, touchés. Il est essentiel qu'ils se prémunissent de ce risque en renforçant leurs dispositifs de prévention et de réaction à incident. Les OIV, conformément au code de la défense[58], ont l'obligation légale de disposer d'un *plan de continuité d'activité* (PCA)[59], rédigé de manière préventive sur la base d'une analyse des risques et des menaces auxquels ils sont susceptibles d'être exposés. Pour les autres opérateurs, l'élaboration d'un PCA, sans être obligatoire, est fortement recommandée.

Les OIV et OSE doivent par ailleurs tenir à jour et mettre en œuvre une procédure de gestion de crises en cas d'incidents de cybersécurité ayant un impact majeur sur leurs activités vitales ou essentielles. Cette procédure prévoit l'application de mesures techniques décidées par le Premier ministre.

De plus, quand l'événement, par l'ampleur des conséquences sociales ou économiques de la crise qu'il génère, appelle une réponse nationale, le ministre chargé de l'économie, qui est représenté en *cellule interministérielle de crise* (CIC)[60], peut activer la *cellule de continuité économique* (CCE). La CCE a pour objectif de rassembler les informations nécessaires pour évaluer et anticiper les conséquences économiques de niveau national ou international de la crise sur les grands secteurs d'activité. Elle permet au ministre chargé de l'économie de prendre les mesures et décisions adaptées destinées à assurer la continuité économique de la nation. Elle traduit la mobilisation des pouvoirs publics afin de limiter les impacts économiques à court et moyen termes d'une crise, aussi bien pour la population que pour les entreprises. Enfin, elle travaille sur l'anticipation des mesures à prendre pour accélérer le retour à la normale.

La CCE réunit les représentants des ministères concernés, les OIV impactés, en particulier ceux relevant de la compétence du ministre chargé de l'économie et les fédérations professionnelles les

57 - Les PSMP sont déployés dans les ports de Marseille-Joliette, de Marseille-Fos, du Havre, de Dunkerque, de Toulon, de Brest et de Cherbourg, Nantes, Saint-Nazaire et Calais.
58 - Cf. Article L. 2151-4 du code de la défense.
59 - Cf. le « Guide pour réaliser un plan de continuité d'activité » du SGDSN, édition 2013.
60 - Cf. Circulaire n°6095/SG du 1er juillet 2019 relative à l'organisation gouvernementale pour la gestion des crises majeures.

plus représentatives des secteurs affectés par la crise majeure en cours. Elle s'appuie, entre autres, au niveau local, sur le réseau national des *chargés de mission de sécurité économique* (CMSE) en poste auprès des préfets de zone de défense et de sécurité.

Le secrétariat de la CCE est assuré par le *service du haut fonctionnaire de défense et de sécurité* (SHFDS) des ministères économiques et financiers. Elle n'est pas nécessairement liée ou synchronisée avec la CIC. La CCE peut se prolonger jusqu'au retour à une situation économique normale afin d'assurer le suivi des mesures prises.

TITRE II

GOUVERNANCE DE LA SÛRETÉ MARITIME ET PORTUAIRE

CHAPITRE I : NIVEAU INTERNATIONAL

Les Gouvernements contractants à la Convention *SOLAS* sont tenus de mettre en place des dispositifs communs dédiés au renforcement de la sûreté maritime et portuaire. L'OMI est l'instance privilégiée de coopération interétatique dans ce domaine. Son mandat lui confère la responsabilité de rendre plus sûrs les transports maritimes, pour les personnes comme pour les biens. La France dispose d'une représentation permanente au sein de cette organisation. Cette représentation est en relation directe avec le point de contact national (DGITM). Par ce réseau, la France est en mesure d'influer sur l'élaboration des règles et des recommandations diffusées, notamment par le biais du comité de la sécurité maritime (*Maritime Safety Committee - MSC*).

Pour la France, la DGITM assure la fonction de point de contact national vis-à-vis de l'OMI, avec l'appui de l'Adjoint mer du SHFDS des ministères chargés des transports, des ports et de la mer. A ce titre, cet adjoint est le correspondant des gouvernements contractants à la convention SOLAS, dont le code ISPS. Dans ce cadre, il est notamment amené à communiquer à l'État du pavillon d'un navire les décisions de refus ou d'entrée au port, voire son expulsion. Il en informe également les autorités des ports d'escale suivants, ainsi que les autorités des États côtiers intéressés au regard de l'activité du navire.

En complément des dispositifs, essentiellement préventifs, appelés par le code ISPS, la convention pour la répression d'actes illicites contre la sécurité de la navigation maritime, dite convention SUA (*Suppression of Unlawful Acts*), a été conclue à Rome le 10 mars 1988. Cette convention et ses protocoles additionnels ont pour objectif principal de garantir la prise de mesures appropriées à l'encontre des auteurs d'actes illicites (notamment de nature terroriste) commis contre des navires[61].

Enfin, l'OMI travaille en étroite coopération avec les États Parties, parraine des institutions des Nations-Unies, des organisations régionales, des partenaires du développement et le secteur des transports maritimes dans son ensemble. Ces échanges renforcent la sûreté maritime au niveau mondial, ainsi que la répression de la piraterie, des vols à main armée à l'encontre des navires, des cyberattaques, des passagers clandestins et de toute activité maritime illicite. A cet effet, l'OMI élabore notamment des recommandations et des codes de bonnes conduites. Cet effort multilatéral de coopération permet de s'assurer que les mesures prises face aux principales menaces sont appropriées et efficaces, aux niveaux international, régional et national[62].

61 - En cas d'arraisonnement d'un navire opéré dans le cadre de la convention SUA (arraisonnement « art.8 bis »), le ministère des affaires étrangères est le point de contact des gouvernements et des autorités étatiques étrangères pour les demandes passives ou actives (compétence de la Mission des Conventions et de l'Entraide Judiciaire - DFAE/SEAJ/CEJ ou du Centre de crise et de soutien (CDCS) pendant les permanences de nuit ou les jours non-ouvrables).

62 - www.imo.org

CHAPITRE II : NIVEAU EUROPÉEN

La politique maritime intégrée de l'*Union européenne* (UE) s'appuie sur de nombreux acteurs institutionnels au premier rang desquels le Parlement européen, la Commission européenne et différentes directions générales.

Soucieux dès 2004 de renforcer la sûreté des navires, des ports et des installations portuaires des États membres, le Parlement européen et le Conseil ont rendu obligatoires les dispositions prévues par le règlement (CE) n° 725/2004 du 31 mars 2004 et la directive n°2005/65/CE du 26 octobre 2005.

Face aux menaces telles que la piraterie et l'immigration illégale, une *stratégie de sûreté maritime de l'Union européenne* (SSMUE) a été diffusée en 2014[63]. Elle est déclinée en actions dans différents thèmes : surveillance maritime, échange d'informations, gestion des risques, protection des infrastructures maritimes critiques, recherche et innovation. Ces actions sont suivies par les ministères compétents sous la coordination du le SGMer et du SGDSN au regard de leurs prérogatives respectives.

Conformément au règlement (CE) n°324/2008 du 09 avril 2008, les États membres de l'UE sont inspectés par la Commission européenne (CE) en charge de vérifier notamment que le code ISPS, transposé et renforcé dans le droit de l'Union européenne par le règlement (CE) n°725/2004 du Parlement européen et du Conseil du 31 mars 2004 est bien mis en œuvre dans les installations portuaires et à bord des navires qui relèvent du code ISPS. Ce règlement a été complété par la directive n°2005/65/CE du Parlement européen et du Conseil, du 26 octobre 2005, relative à l'amélioration de la sûreté des ports.

La Commission européenne annonce, au moins six semaines à l'avance, au point de contact national (DGITM) son intention d'effectuer une inspection. Toutefois, en cas d'événements exceptionnels, l'inspection peut être annoncée à plus bref délai. En dehors des autorités concernées, l'annonce d'une inspection est gardée confidentielle afin de ne pas en compromettre le déroulement. Ces inspections, donnent lieu à des rapports, relevant les non-conformités et les écarts aux textes en vigueur, adressés au point de contact pour la sûreté maritime pour éléments de réponse préparés par la DGITM, autorité de sûreté maritime compétente. Si elles ne sont pas corrigées dans un délai imparti fixé par la Commission, ces non-conformités peuvent conduire à une procédure d'infraction avec amendes.

Par ailleurs, les services compétents des ministères chargés des transports et de la mer, notamment le point de contact national et l'Adjoint mer du SHFDS de ces deux ministères, représentent la France au comité de sûreté maritime (*Maritime Security Committee - MARSEC*) réuni par la commission au cours duquel divers sujets sont débattus (rapports d'inspections, bonnes pratiques des États membres, interprétations communes des textes, évolutions de la réglementation face aux risques, présentations d'études financées par la Commission relatives à l'amélioration de la sûreté maritime et portuaire, etc). La DGITM peut également être invitée sur des points spécifiques.

Enfin, en complément des dispositions appelées par les exigences internationales et de l'UE, des accords intergouvernementaux peuvent être conclus avec d'autres États afin de renforcer la sûreté du trafic maritime des deux parties. Ces accords sont conclus dans le respect du droit national et en conformité avec le droit de l'Union européenne et le droit international. Les obligations qui ressortent de ces accords et qui s'imposent aux services de l'État et aux opérateurs privés leurs sont communiquées par les ministères compétents et les autorités préfectorales.

63 - Son plan d'action a fait l'objet d'une révision en juin 2018.

CHAPITRE III : NIVEAU NATIONAL

Gouvernance stratégique

Instances présidées par les services du Premier ministre

Conformément au décret n°95-1232 du 22 novembre 1995, le *comité interministériel de la mer* (CIMer) fixe les orientations de l'action gouvernementale dans tous les domaines de l'activité maritime. Il est présidé par le Premier ministre et réunit les ministères concernés qui, à l'issue, mettent en œuvre les actions retenues. Son secrétariat est assuré par SGMer.

Pour ce qui relève de la sûreté maritime et portuaire, ces actions font plus particulièrement l'objet d'un suivi et d'une coordination par la *commission interministérielle de sûreté maritime et portuaire* (CISMaP). Cette commission, présidée par le cabinet du Premier ministre, réunit les ministères concernés. Son secrétariat est assuré par le SGMer, avec un ordre du jour proposé en coordination avec le SGDSN. Elle se réunit au moins une fois par an, selon un calendrier défini par le cabinet du Premier ministre.

En sus de la CISMaP, des comités et des groupes de travail spécifiques, dont des actions sont tout ou partie dédiées à la sûreté, sont pilotés au niveau interministériel :

- au regard de l'évolution de la piraterie, un comité réunissant notamment des représentants des armateurs, du ministre des armées, du ministre de la mer et du ministre des affaires étrangères peut, de sa propre initiative, recommander au Premier ministre de redéfinir les zones au sein desquelles la protection armée des navires de commerce sous pavillon français est nécessaire ;
- sous l'égide du SGMer, les administrations de la *fonction garde-côtes* (FGC) intervenant en mer (marine nationale y compris la GMar, gendarmerie nationale, police nationale, sécurité civile, affaires maritimes et douanes) sont régulièrement réunies dans le cadre du comité directeur de la fonction garde-côtes. Selon les sujets, des acteurs privés, telles que des associations, peuvent être sollicités par cette instance (la *société nationale de sauvetage en mer* (SNSM) par exemple) ;
- le SGDSN définit la réponse de l'État face aux menaces et aux crises majeures. A cet effet, en concertation avec les acteurs publics et privés, le SGDSN réalise la planification de sécurité nationale (plans VIGIPIRATE et PIRATE-MER, instructions interministérielles dédiées à la sûreté, etc.). Au regard du niveau de la menace terroriste, le SGDSN propose au Premier ministre le niveau de la posture VIGIPIRATE. L'adaptation du dispositif de vigilance, de prévention et de protection fait l'objet d'une posture VIGIPIRATE adressée aux ministères, qui déclinent à leur tour des instructions dans leur champ de compétence propre. Elle précise en particulier l'évaluation de la menace, le niveau d'alerte qui en découle, ainsi que l'éventuel renforcement des mesures socles et l'activation de mesures additionnelles. De plus, le SGDSN réalise le suivi du plan d'action interministériel pour le renforcement de la sécurité dans les transports dont les avancées sont régulièrement présentées au cabinet du Premier ministre. Les actions de ce plan sont cohérentes avec celles découlant de la SNSEM.

  Par ailleurs, en relation avec la *direction générale des entreprises* (DGE) du ministère chargé de l'économie, le SGDSN participe aux travaux du *comité stratégique de la filière* (CSF) « Industries de sécurité »[64]. Les industries de sécurité participent ainsi à une filière d'excellence française, animée par un tissu dense d'entreprises. Ce comité fédère les efforts des acteurs publics et

64 - En tant que membre du bureau, au titre des représentants de l'Etat avec le ministère chargé de l'économie et des finances et le ministère de l'intérieur.

privés (par exemple le *groupement des industries de construction et activités navale* - GICAN) pour promouvoir le développement de solutions de sécurité efficaces.

Enfin, par délégation du Premier ministre, le SGDSN assure également le pilotage et la coordination interministérielle du dispositif SAIV. Il préside à cet effet la *commission interministérielle de défense et de sécurité* (CIDS) qui rend un avis à différentes étapes du dispositif de SAIV, depuis l'établissement des DNS, la désignation ou le retrait de nouveaux opérateurs du dispositif, l'étude des *plans de sécurité opérateur*, jusqu'à la liste des PIV proposés par l'opérateur. L'ANSSI pilote pour sa part la partie cybersécurité et cyberdéfense du dispositif SAIV et accompagne les OIV dans la mise en œuvre des règles de cybersécurité. Par délégation du Premier ministre, l'ANSSI assure également le pilotage et la coordination interministérielle du dispositif de transposition de la directive européenne dite NIS65.

Instances de concertation présidées par des ministères (transport, mer, armées)

Les décisions prises par le Premier ministre (notamment dans le cadre du CIMER ou par son cabinet en CISMaP) et par les instances interministérielles, sont mises en œuvre par les ministères concernés.

Les ministères chargés des transports et de la mer assurent le pilotage de la politique de sûreté maritime et portuaire, le cas échéant conjointement s'agissant des ports maritimes. A cet effet, le premier dispose de la DGITM, « autorité de sûreté maritime compétente » au sens de la réglementation européenne. Le ministère de la mer s'appuie quant à lui sur la DG AMPA. Le SHFDS est par ailleurs commun aux ministères des transports et de la mer. La DGITM et la DGAMPA préparent les projets de textes législatifs et réglementaires relevant de leurs domaines respectifs. A cet effet, elles associent l'ensemble des acteurs publics et privés, dont des représentations professionnelles, au sein de deux instances de concertation :

- *le groupe interministériel de sûreté du transport maritime et des opérations portuaires*[66] (GISTMOP), présidé par le ministre des transports qui est représenté par le DTFFP. Le secrétariat de cette unité est assuré par le bureau de la sûreté portuaire et fluviale. Cette instance a pour mission :
  - de proposer aux ministres compétents les orientations générales de la politique nationale de sûreté du transport maritime et des opérations portuaires, ainsi que toutes dispositions législatives ou réglementaires et toutes actions permettant d'assurer et de renforcer la sûreté des navires et des ports maritimes ;
  - de formuler un avis sur toutes questions de sa compétence qui lui sont soumises par les ministres concernés ;
  - d'orienter l'action des comités locaux de sûreté portuaire (CLSP).
- *la commission centrale de sécurité* (CCS), mise en œuvre par la DG AMPA, a pour principal objet l'élaboration et l'application des règles de sécurité et de sûreté applicables aux navires de commerce[67]. Les opérateurs privés du secteur (armateurs, sociétés de classification, constructeurs, assureurs, etc.) et certaines associations professionnelles représentatives en sont membres à titre consultatif.

Dans le domaine SAIV et plus particulièrement les PIV situés dans les ports et sur le littoral[68], un ministère dit coordonnateur est chargé de rédiger une DNS pour chacun des 12 secteurs (et 22 sous-

65 - Directive sur la sécurité des réseaux et des systèmes d'information (UE - 2016/1148). Elle a pour objectif d'atteindre un niveau commun élevé de sécurité des réseaux et des systèmes d'informations dans toute l'Union Européenne.
66 - Cf. article R5332-3 du code des transports.
67 - Cf. Décret n° 84-810 du 30 août 1984 relatif à la sauvegarde de la vie humaine en mer, à la prévention de la pollution, à la sûreté et à la certification sociale des navires.
68 - A l'exception des PIV relevant du secteur Activités militaires de l'État.

secteurs) d'activité d'importance vitale. Au-delà du suivi des exigences réglementaires de planification, ces ministères coordonnateurs sont également les points de contact privilégiés des opérateurs relevant de leur(s) secteur(s) d'activité. Cette relation permet d'inscrire les OIV dans une démarche d'ensemble visant à adapter les conditions dans lesquelles la Nation se prémunit contre toute menace, et notamment la menace terroriste, en améliorant l'articulation des dispositions que mettent en œuvre respectivement les pouvoirs publics et les opérateurs, en particulier dans le cadre du plan VIGIPIRATE. Par ailleurs, outre son rôle de ministre coordonnateur du secteur d'activités civiles de l'Etat, le ministre de l'intérieur assure l'animation de la mise en œuvre territoriale du dispositif SAIV, afin de soutenir l'action des autorités préfectorales.

Ponctuellement, des groupes de travail peuvent être organisés par un ministère afin de traiter ou d'échanger sur un sujet particulier, de rechercher un avis ou d'informer différentes entités. A titre d'exemple, le ministère des armées et plus précisément l'*état-major de la marine* (EMM) organise annuellement un séminaire entre la marine nationale et les armateurs français. A cette occasion, les échanges et les collaborations relevant du domaine de la sûreté maritime sont abordés. De même, le ministère chargé des transports est en relation permanente avec les *agents de sûreté portuaire* (ASP) et les représentants des préfets afin d'échanger sur le cadre juridique et doctrinal.

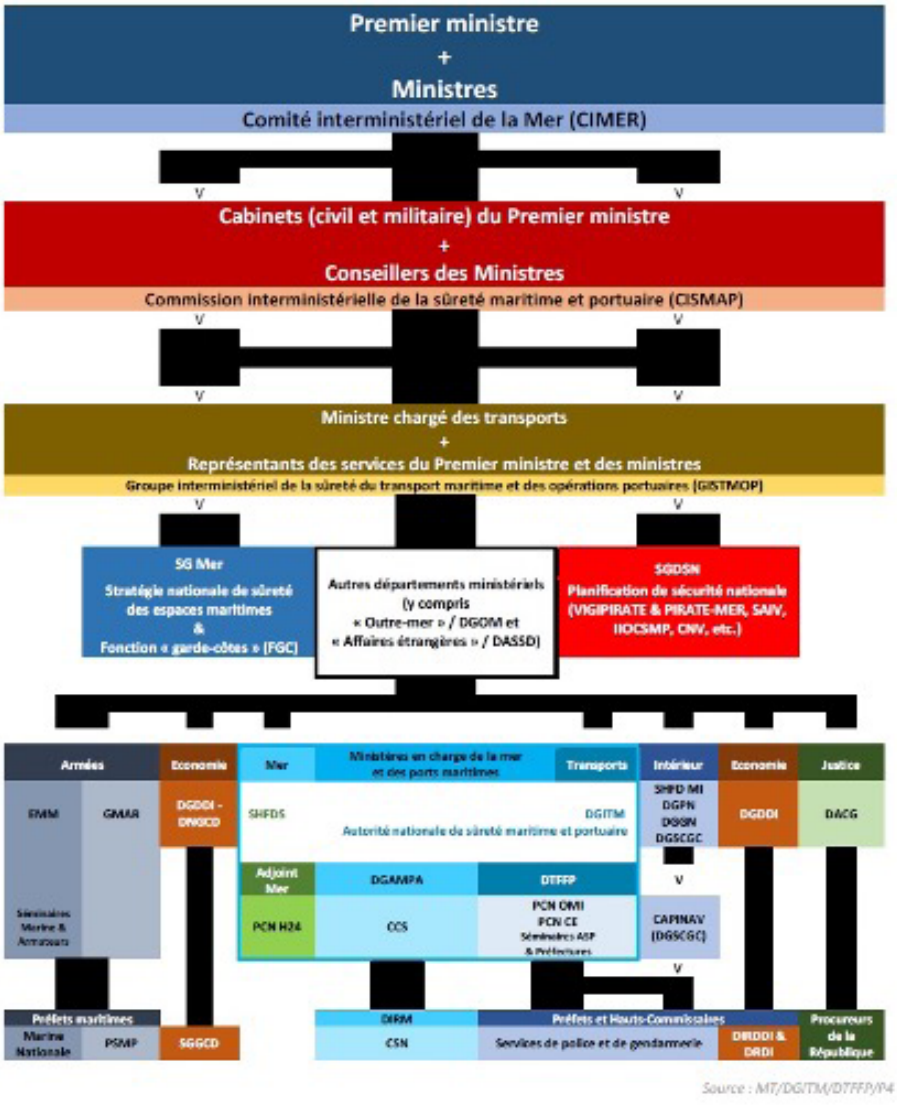


Schéma II-III-1 Gouvernance stratégique de la sûreté maritime et portuaire

Gouvernance locale

Au niveau local, la gouvernance de la sûreté maritime et portuaire est partagée par les différents représentants de l'État (les préfets de zone de défense et de sécurité, les préfets maritimes, les préfets de département et, outre-mer, les *délégués du Gouvernement pour l'action de l'Etat en mer* (DDG AEM). Dans le cadre de leurs prérogatives, ces autorités font appliquer les instructions et directives émanant du niveau stratégique et contrôlent leur parfaite exécution. Pour cela, ils s'appuient sur les *autorités investies du pouvoir de police portuaire* (AIPPP)[69] pour ce qui relève de la police des plans d'eau et des marchandises dangereuses, les autorités portuaires, les exploitants portuaires pour la sûreté, les différents services déconcentrés et les capacités des ministères présentes au sein de leur zone de compétence. La coordination entre les différentes autorités est plus précisément abordée au chapitre IV du titre II du présent document.

Le représentant de l'État dans le département

L'autorité du représentant de l'État dans le département s'exerce sur le territoire du département qui s'étend jusqu'aux limites administratives des ports. Vis-à-vis du domaine maritime, il est délimité par la limite des eaux du rivage et, dans les estuaires, par les limites transversales de la mer.

Le représentant de l'État dans le département[70] est chargé de la mise en œuvre locale de la sûreté portuaire au terme de l'article R. 5332-5-1 du code des transports. Veillant à la bonne mise en œuvre des dispositions nationales d'application du code *ISPS*, il conduit les évaluations de sûreté qui servent aux autorités et exploitants portuaires pour l'élaboration de leurs plans de sûreté qu'il approuve. Il recueille à ce titre les avis du CLSP et peut utilement s'appuyer sur les groupes d'experts associant d'autres services de l'État, ainsi que sur la GMAR et la police nationale qui disposent dans tous les ports majeurs d'un correspondant sûreté.

Conformément à l'article L. 122-1 du code de la sécurité intérieure, le représentant de l'État dans le département anime et coordonne l'ensemble du dispositif de sécurité intérieure. A cet effet, il fixe les missions autres que celles qui sont relatives à l'exercice de la police judiciaire et coordonne l'action des différents services et forces dont dispose l'État en matière de sécurité intérieure. Pour cela, il réunit régulièrement le directeur départemental de la sécurité publique, le commandant de groupement de la gendarmerie départementale, le chef du service départemental de renseignement territorial et, si le département est doté de ces forces, du directeur départemental de la police aux frontières, voire du commandant du PSMP[71].

De plus, pour les ports soumis à la directive n° 2005/65/CE et les installations portuaires soumises au code *ISPS*, pour l'ensemble des sujets relatifs à la sûreté, dont la recherche d'avis sur les évaluations et les plans dédiés, le préfet de département s'appuie sur les membres, permanents ou occasionnels, du CLSP. Le préfet peut également s'appuyer sur les correspondants sûreté de la GMAR et de la PAF.

Afin de prévenir tout acte malveillant ou de protéger les personnes, les biens et l'environnement face à une menace visant le milieu portuaire et le littoral, le préfet de département fait notamment appliquer les mesures, relevant de ses prérogatives, appelées par :

- le plan gouvernemental VIGIPIRATE ;
- la réglementation applicable au titre de la SAIV pour les PIV implantés dans les ports et, plus largement, sur le littoral. A noter que le préfet de département approuve, pour chaque PIV de

69 - Cf. article 5331-6 du code des transports.
70 - Pour la Polynésie française et la Nouvelle-Calédonie, les hauts commissaires de la République, et pour les îles de Wallis et Futuna, l'administrateur supérieur.
71 - En fonction de l'ordre du jour de la réunion.

son ressort territorial, le PPP rédigé par l'opérateur[72]. Il élabore également le PPE comportant les mesures de vigilance et d'intervention prévues en cas de menace ou d'actes malveillants visant ce PIV ;

- le règlement 725/2004 CE pour les installations portuaires et la directive n° 2005/65/CE pour les ports éligibles. A ce titre, ils sont respectivement dotés d'ESIP et d'ESP, ainsi que de PSIP et de PSP. Ces évaluations et ces plans sont approuvés par le préfet de département.

En cas d'acte de terrorisme survenant à bord d'un navire dans les limites administratives d'un port, conformément au plan gouvernemental Pirate-mer, le préfet de département assure la direction des opérations. Pour un acte de terrorisme survenant à terre dans un port, le préfet de département, met en œuvre les plans gouvernementaux « Pirate » adaptés à la nature et la situation de crise.

Le préfet maritime

Conformément au décret n° 2004-112 du 6 février 2004, le préfet maritime est le représentant de l'Etat en mer. Pour les missions de sûreté, comme pour les autres missions[73], son autorité s'exerce en mer, à partir de la limite des eaux. Elle ne s'exerce pas dans les limites administratives des ports. Dans les estuaires, elle s'exerce en aval des limites transversales de la mer. Pour remplir ses missions, le préfet maritime bénéficie du concours des services et administrations de l'Etat qui mettent à sa disposition les moyens et informations d'intérêt maritime dont ils disposent[74].

Les préfets maritimes disposent de *cellules de coordination de l'information maritime* (CCIM) qui assurent la centralisation et l'analyse du renseignement d'intérêt maritime, notamment pour ce qui relève des approches maritimes. Les administrations de la fonction garde-côtes y sont représentées.

Afin de prévenir tout acte malveillant ou de protéger les personnes et les biens face à une menace, le préfet maritime fait appliquer les mesures relevant de ses prérogatives appelées par le plan gouvernemental Vigipirate, et plus particulièrement les mesures MAR qu'il décline localement. Préalablement à son entrée dans un port, un navire peut faire l'objet d'un contrôle de sûreté s'il existe des raisons sérieuses de penser qu'il ne satisfait pas aux prescriptions prises en application du code *ISPS*. Dans les ports qui en sont dotés, cette mission est plus particulièrement confiée aux PSMP de la GMar.

Lorsqu'un acte de terrorisme maritime, de brigandage ou de piraterie, survient dans sa zone de responsabilité, le préfet maritime ou, outre-mer, le DDG AEM, propose au Premier ministre le déclenchement du plan gouvernemental Pirate-mer[75]. Dans ce cadre, il assure la direction des opérations en mer. A cet effet, il mobilise et met en œuvre les moyens nécessaires pour faire face à l'événement, dans le respect des dispositions portées par le plan cité ci-dessus, notamment pour ce qui relève de l'emploi de la force en mer.

Le commandant de zone maritime

En application des directives générales prises sur la base des décisions arrêtées en conseil de défense, la DMT, telle que présentée au titre I du présent document, est mise en œuvre sous l'autorité des *commandants de zone maritime* (CZM) en métropole, ou des COMSUP outre-mer. En métropole, les fonctions de CZM sont cumulées avec celles de préfet maritime.

Par ailleurs, les capacités militaires de la marine nationale engagées, en vertu d'une réquisition[76], au profit d'un préfet de département pour intervenir dans un port ou dans un estuaire, en amont de

72 - A l'exception des PIV relevant du secteur Activités militaires de l'État.
73 - Cf. arrêté du 22 mars 2007 et les arrêtés du 25 octobre 2016 établissant la liste des missions en mer incombant à l'État.
74 - Notamment les centres des opérations et de renseignement de la GMar et en leur sein les CEMAS.
75 - Plan gouvernemental n° 10070/SGDSN/PSE/PSN/– édition de juillet 2017.
76 - Instruction interministérielle n° 10100/SGDSN/PSE/PSN/NP du 14 novembre 2011 relative à l'engagement des armées sur le territoire national lorsqu'elles interviennent sur réquisition de l'autorité civile

la limite transversale de mer, agissent sous le contrôle opérationnel d'une autorité militaire désignée par le CEMA. Cette autorité militaire désignée est en liaison étroite avec l'autorité préfectorale requérante afin de réaliser l'effet final recherché préalablement défini. Pour les événements de terrorisme maritime, de piraterie et de brigandage, les modalités de coordination entre l'autorité, préfet maritime et CZM, et le préfet de département sont définies dans le plan gouvernemental PIRATE-MER.

Le préfet de zone de défense et de sécurité

Dans le domaine de la sûreté maritime et portuaire, le *préfet de zone de défense et de sécurité* (PZDS) est impliqué à deux titres :

Le préfet de zone[77] dirige l'action des préfets de département et des délégués de zone en ce qui concerne les mesures de défense non militaires. Il est à ce titre l'acteur territorial en charge de la coordination du dispositif SAIV. Il préside la *commission zonale de défense et de sécurité* (CZDS) et coordonne les inspections des PIV[78] situés dans sa zone de compétence. Sous son autorité, l'*état-major interministériel de la zone de défense et de sécurité* (EMIZDS) reçoit une mission générale d'animation, d'appui aux préfectures, et de relais d'information entre l'échelon central et les échelons départementaux.

Pour la coordination en cas de crise, si un événement survenant en mer ou à terre à des conséquences dans les deux milieux, le PZDS territorialement compétent s'assure de la cohérence des actions terrestres et maritimes.[79]

77 - Dans les cinq zones de défense et de sécurité d'outre-mer, cette mission est assurée par les hauts fonctionnaires de zone de défense et de sécurité d'outre-mer définis par l'article R. 1681-2 du code de la défense.
78 - A l'exception des PIV relevant du secteur Activités militaires de l'État.
79 - Cf. article L742-5 (V) du code de la sécurité intérieure.

CHAPITRE IV : TRIPLE *CONTINUUM*

Entre le niveau stratégique et les autorités du niveau local

Dans les collectivités territoriales de la République, le représentant de l'Etat, représentant de chacun des membres du Gouvernement, a la charge des intérêts nationaux, du contrôle administratif et du respect des lois[80].

En mer, les préfets maritimes et les DDG AEM sont les représentants directs du Premier ministre, et de chacun des membres du Gouvernement.

Les services déconcentrés de l'État à l'échelon départemental sont placés sous l'autorité du représentant de l'État dans le département. Le préfet maritime, ou le DDG AEM, anime et coordonne l'action des administrations intervenant en mer et la mise en œuvre de leurs moyens. Certaines politiques mises en œuvre localement, par leur aspect interministériel, relèvent directement des services du Premier ministre (par exemple le SGDSN pour les règles de cybersécurité ou encore le SGMER pour la transmission des alertes de sûreté des navires conformément à la convention *SOLAS*[81]).

Chaque ministre décline sa politique vers ses services à compétence nationale et ses services déconcentrés. A cet effet, il peut désigner localement des agents plus particulièrement chargés d'un sujet spécifique (le ministère de l'intérieur a ainsi mis en place des référents locaux à la sûreté portuaire). Ces politiques ministérielles sont réalisées de manière coordonnée, voire conjointe entre ministères concernés, comme le réalisent le ministère de l'intérieur et le ministère chargé des transports lors des sessions interministérielles régionales de sensibilisation à la sûreté portuaire.

En situation de crise, les relations entre le niveau stratégique et le niveau local sont notamment définies par la circulaire n°6095/SG du 1er juillet 2019 relative à l'organisation gouvernementale pour la gestion des crises majeures. Pour les actes de terrorisme maritime, de brigandage et de piraterie, le plan gouvernemental PIRATE-MER apporte des précisions complémentaires sur l'organisation *ad hoc*, notamment pour la décision de l'emploi de la force en mer qui relève du Premier ministre.

80 - Cf. article 72 de la Constitution du 4 octobre 1958.
81 - Instruction n° 46/SGMER/NP du 20 mai 2020.

Entre les acteurs, publics et privés, du niveau local

La multiplicité des acteurs, publics et privés, et leurs responsabilités respectives dans le domaine de la sûreté maritime et portuaire nécessite, pour répondre efficacement aux menaces, une étroite coordination. Pour cela, différentes instances d'échanges existent au niveau local.

Instances	Autorités présidant	Membres	Observations
Conférence maritime	Préfet maritime	Cf. article 4 du décret n° 2004-112 du 6 février 2004	Instance non spécifiquement dédiée à la sûreté. La présence des exploitants maritimes et portuaires n'est pas prévue.
Comité local de sûreté portuaire (CLSP)	Préfet de département	Cf. article R. 5332-4 du code des transports	Pour les ports et les installations portuaires soumis au code *ISPS*. La présence des agents de sûreté des compagnies maritimes n'est pas prévue. Toutefois, le préfet de département a la possibilité de faire participer toute personne qualifiée.
Réunion de sécurité publique	Préfet de département	DDSP, SDRT, CGGD, représentant DGSI et de la cellule départementale de renseignement opérationnel sur les stupéfiants (CROSS portuaire), représentants des directions et services dont la présence est requise par le préfet de département.	Réunion hebdomadaire non appelée par un texte réglementaire. Pour les sujets liés au domaine portuaire, la GMar, lorsqu'elle est implantée dans le département, est représentée à cette réunion. Pour les sujets à l'ordre du jour liés au domaine maritime susceptibles d'avoir des conséquences ou des liens avec le domaine terrestre, le Préfet maritime est associé. Si le sujet est inopinément abordé, le préfet maritime est en informé.
Réunion de l'état-major départemental de sécurité	Préfet de département et Procureur de la République	Idem ci-dessus, ainsi que les représentants des Douanes, de la PAF, de l'administration pénitentiaire, de l'éducation nationale	Réunion mensuelle. Pour les représentations de la GMAR et du préfet maritime, idem ci-dessus

Tableau II-IV-1 Instances de concertation locales

Au regard des périmètres de ces instances et de leurs représentations, les particularités locales impliquent que des réunions dédiées à la sûreté maritime et portuaire sont souvent, de manière connexe, réalisées par les autorités préfectorales, maritimes et terrestres. C'est le cas pour les planifications de protection des grands événements se déroulant sur le littoral, à terre comme en mer, et leur mise en œuvre, pour lesquels ces autorités, doivent mettre en place, de manière concertée, des dispositifs cohérents. A cet effet, des arrêtés préfectoraux conjoints peuvent être pris.

Plus généralement, les échanges sur la sûreté maritime et portuaire entre les préfets de département et les préfets maritimes sont réguliers. Afin d'avoir une approche plus large, ils ne se limitent pas aux grands événements, tels que susmentionnés, et aux réunions des CLSP qui concernent les seules installations soumises au code *ISPS*. A l'initiative des autorités locales, ces échanges peuvent prendre la forme d'une réunion comprenant deux temps, l'un dédié aux seuls acteurs étatiques et le second ouvert aux acteurs publics du monde maritime et portuaire. Ce type de réunion est une opportunité pour :

- présenter les tendances des menaces susceptibles de viser l'activité maritime et portuaire de la zone dans le respect de la protection du secret ;
- faire un point sur les dispositifs de sûreté maritime, privés et publics, déployés (failles régulièrement observées, bonnes pratiques à généraliser, etc.) ;
- rappeler les dernières évolutions réglementaires, présenter celles à venir avec, le cas échéant, leurs difficultés d'application ;
- apprécier les attentes des différents acteurs.

Ces échanges entre les acteurs publics et privés viennent en complément :

- des actions de sensibilisation à la sûreté réalisées *in situ* auprès des usagers de la mer et des opérateurs portuaires, notamment par la GMAR et, plus largement, par les forces de sécurité intérieure ;
- des audits et des contrôles réglementaires[82].

Pour ce qui relève plus particulièrement des audits, des inspections et des contrôles des installations portuaires et des ports qui, par leurs caractéristiques, sont simultanément soumis aux dispositions du code *ISPS* et aux obligations relevant du dispositif de *sécurité des activités d'importance vitale*, les autorités préfectorales s'attachent à :

- coordonner les contrôles de la commission zonale de défense et de sécurité, réalisés au titre de la SAIV, avec les contrôles *a priori* (tous les 5 ans) et de conformité (tous les ans) appelés par le code *ISPS*, réalisés par les agents de l'État désignés par le préfet de département. Le cas échéant, des contrôles conjoints peuvent être réalisés. Cette coordination est d'autant plus importante qu'en sus sont réalisés :
  - des audits par le ministère chargé des transports, associant le cas échéant des référents sûreté des douanes pour les installations portuaires les plus sensibles au regard des orientations prévues par l'instruction interministérielle du 7 juillet 2021 relative à la mise en œuvre de la stratégie nationale de sécurisation des ports maritimes contre le trafic de drogue ;
  - des inspections par la Commission européenne ;
  - des contrôles de la sécurité des systèmes d'information des OIV[83] à la demande du Premier ministre (ANSSI) ;
- partager, entre les niveaux zonal et départemental, les conclusions des contrôles susmentionnés ;
- prendre en compte les possibles équivalences, totales ou partielles, entre les PSP et les PSIP avec les PPP, telles qu'autorisées par le code des transports[84].

82 - Cf. Le programme national de sûreté du transport et des ports maritimes, diffusé par le ministère chargé des transports.
83 - Pas plus d'un contrôle par année civile, conformément à l'article R1332-41-12 du code de la défense.
84 - Cf. Articles R5332-22 et R5332-29 du code des transports. Ces équivalences restent du ressort du préfet de département.

Entre la mer et la terre

Nonobstant la comitologie dédiée à la sûreté maritime et portuaire précédemment évoquée, le *continuum* organisationnel entre les autorités terrestres et maritimes nécessite d'être formalisé à travers un document d'interface. Sa forme, rédigé comme un outil opérationnel, pratique et évolutif, n'est pas imposée aux autorités afin qu'elle puisse être adaptée aux particularités de leurs zones de compétence. Les éléments portés par ce document ne doivent pas être redondants avec ceux figurant dans les plans de sûreté portuaire.

Ce document, établi entre chaque préfet de département du littoral et le préfet maritime concerné, précise notamment :

- les limites géographiques entre leurs zones de compétences respectives, avec une attention particulière pour les ports ;
- les missions et les services dédiés, relevant de leurs prérogatives, intéressant la sûreté maritime et portuaire, dont les PSMP pour les ports qui en sont dotés ;
- les modalités d'échanges et de coordination de leurs services, dont le partage des menaces et des alertes ;
- le traitement des navires :
  - au mouillage avec débarquement de passagers à terre en dehors des ports ;
  - suspectés d'activité illicite (immigration illégale, trafic de stupéfiants, transport de matériels ou de produits prohibés dans le cadre de la non-prolifération, etc.).
- les principes organisationnels et relationnels à mettre en œuvre en cas de crise, comprenant la déclinaison locale du plan Pirate-mer, dont le transfert d'autorité de la direction « menante » d'une opération.

Les préfets de zone de défense et de sécurité sont destinataires de ces outils d'interface. Une attention particulière doit être apportée par les autorités à leur rédaction et à leur mise à jour, car au-delà des dispositions appelées par le plan Pirate-mer, ces documents contribuent plus largement à la continuité de l'action de l'État lors des crises de toute nature touchant simultanément la mer et la terre.

ANNEXES

ANNEXE 1

LISTE DES SIGLES ET DES ACRONYMES

AD	Attaché de défense
AEM	Action de l'État en mer
ANDV	Agence nationale des données de voyage
ANSSI	Agence nationale de la sécurité des systèmes d'information
ASI	Attaché de sécurité intérieure
ASP	Agents de sûreté portuaire
CapINav	Capacité nationale de renfort pour l'intervention à bord des navires
CCE	Cellule de continuité économique
CCIM	Cellule de coordination de l'information maritime
CEMAS	Cellule d'évaluation des menaces et d'analyse de sûreté
CGGD	Commandant de groupement de la gendarmerie départementale
CIC	Cellule interministérielle de crise
CIMer	Comité interministériel de la mer
CISMaP	Commission interministérielle de sûreté maritime et portuaire
CLSP	Comité local de sûreté portuaire
CMSE	Chargé de mission de sécurité économique
CNRLT	Coordination nationale du renseignement et de la lutte contre le terrorisme
COM	Centre des Opérations Maritimes
ComGendMar	Commandement de la gendarmerie maritime
COMIA	Commandant interarmées
COMSUP	Commandant supérieur
CORGMar	Centre d'opérations et de renseignement de la gendarmerie maritime (local)
CRGN	Commandant de région de la gendarmerie nationale
CRMar	Centre de renseignement de la Marine
CNO	Centre national des opérations (gendarmerie nationale)
CROGMar	Centre de renseignement et d'opérations de la gendarmerie maritime (national)
CROSS	Centre régional opérationnel de surveillance et de sauvetage
CROSS (portuaire)	Cellule départementale de renseignement opérationnel sur les stupéfiants
CSF	Comité stratégique de la filière

CSI	*Container Security Initiative*
CZGN	Commandant de zone de la gendarmerie nationale
CZM	Commandant de zone maritime
DACG	Direction des affaires criminelles et des grâces
DASSD	Direction des affaires stratégiques, de sécurité et du désarmement
DDG	Délégué du gouvernement
DDPAF	Directeur départemental de la police aux frontières
DDRT	Directeur départemental du renseignement territorial
DDSP	Directeur départemental de la sécurité publique
DGAMPA	Direction générale des affaires maritimes, des pêches et de l'aquaculture
DGGN	Direction générale de la gendarmerie nationale
DGITM	Direction générale des infrastructures, des transports et des mobilités
DGOM	Direction générale des outremers
DGSE	Direction générale de la sécurité extérieure
DGSI	Direction générale de la sécurité intérieure
DIRD	Directeur interrégional des douanes
DMT	Défense maritime du territoire
DNGCD	Direction nationale garde-côtes des douanes
DNS	Directive nationale de sécurité
DNRED	Direction nationale du renseignement et des enquêtes douanières
DRM	Direction du renseignement militaire
DRRI	Direction régionale du renseignement intérieur
DRSD	Direction du renseignement et de la sécurité de la défense
DTFFP	Direction des transport ferroviaire et fluviale et des ports
EDIM	Équipes de défense et d'interdiction maritime
EMA	État-major des armées
EMM	État-major de la marine
EPE	Équipe de protection embarquée
EPNAP	Équipes de protection des navires à passagers
EPPN	Équipe privée de protection des navires
ESIP	Évaluation de sûreté de l'installation portuaire
ESP	Évaluation de sûreté du port
FGC	Fonction garde-côtes
GISTMOP	Groupe interministériel de sûreté du transport maritime et des opérations portuaires
GMar	Gendarmerie maritime

GPD	Groupe de plongeurs démineurs
HFDS	Haut fonctionnaire de défense et de sécurité
IPD	Installation prioritaire de défense
ISM	*International Safety Management* (Code *ISM*)
ISPS	*International Ship and Port Facility Security* (Code *ISPS*)
ISSC	*International Ship Security Certificate*
LPS	Limites portuaires de sûreté
M-CERT	*Maritime Computer Emergency Response Team*
MICA Centre	*Maritime Information Cooperation and Awareness Centre*
MSC	*Maritime Safety Committee*
NEDEX	Neutralisation, enlèvement, destruction des explosifs
OIV	Opérateur d'importance vitale
OSE	Opérateur de service essentiel
OMI	Organisation maritime internationale
PCA	Plan de continuité d'activité
PIV	Point d'importance vitale
PNR	*Passager Name Record*
PPE	Plan de protection externe
PPP	Plan particulier de protection
PSO	Plan de sécurité d'opérateur
PSI	Proliferation Security Initiative
PSIP	Plan de sûreté de l'installation portuaire
PSMP	Peloton de sûreté maritime et portuaire
PSP	Plan de sûreté portuaire
PZDS	Préfet de zone de défense et de sécurité
SAIV	Sécurité des activités d'importance vitale
SCRT	Service central du renseignement territorial
SDRT	Service départemental du renseignement territorial
SGDSN	Secrétariat général de la défense et de la sécurité nationale
SGMer	Secrétariat général de la mer
SHFDS	Service du haut fonctionnaire de défense et de sécurité
SMC	Secteur maritime côtier
SNSEM	Stratégie nationale de sûreté des espaces maritimes
SNSM	Société nationale de sauvetage en mer
SOLAS	*Safety Of Life At Sea* (Convention *SOLAS*)

SPR	Secteur de protection rapprochée
SRGMar	Section de recherches de la gendarmerie maritime
SRRT	Service régional du renseignement territorial
SSMUE	Stratégie de sûreté maritime de l'Union européenne
SSP	*Ship Security Plan*
UCLAT	Unité de coordination de la lutte antiterroriste
UE	Union européenne
UIP	Unité information passagers
ZRP	Zone de responsabilité permanente

ANNEXE 2
TABLEAU DE LA CHAINE DE REMONTÉE DU RENSEIGNEMENT, D'ORIGINE NON ÉTATIQUE

Observation locale	Traitement local				Traitement central		
Entité témoin	**Personne signalant**	**Point de contact étatique**	**Exploitation locale**	**Fusion du renseignement**	**Exploitation nationale**	**Synthèse et exploitation par périmètre**	**Exploitation et orientations nationales**
Navire en mer ou en escale soumis au code ISPS et coopérants[85]	Agent de sûreté du navire	MICA Center Navire d'État à la mer GMAR Point de contact étatique Représentation diplomatique[86]	COM/CCIM CORGMAR[87]/ CEMAS AD et ASI	Représentant de l'État en mer (PREMAR et DDG outre-mer)	EMA/EMM (CRMAR et CROGMAR) CNO DRM	DRM DRSD DGSE SDAO DGSI DNRED TRACFIN	CNRLT SGDSN[88] HFDS Transports et Mer (Adjoint mer)
Autres navires en mer ou en escale à l'étranger	Agent de sûreté du navire[89] -- Capitaine du navire	MICA Center[90] -- Navire d'Etat à la mer GMAR Point de contact étatique Représentation diplomatique[91]		Ambassadeur	MEAE MININT/DCI MINARM/ DGRIS		
Navires à quai soumis au code ISPS	Agent de sûreté du navire	GMAR Point de contact étatique Gendarmerie nationale Police nationale Services des douanes	CORGMAR/ CEMAS CGGD Police nationale (PAF, SP, RT) Bureaux principaux de la douane	Préfet de département	CRGN/CZGN DZPAF DZSP SRRT DRRI DIRD	EMA/EMM/ CROGMAR et DRM DGGN DGPN DGSI DNRED	CNRLT SGDSN[92] HFDS Transports et Mer (Adjoint mer)
Autres navires à quai	Capitaine du navire						
Ports et installations portuaires soumis au code ISPS	Agent de sûreté portuaire/Agent de sûreté de l'installation portuaire						
Autres ports	Exploitant						
Autres infrastructures sur le littoral	Exploitant, élus, citoyens, etc.						

85 - Navires des armateurs parties prenantes pour la coopération navale volontaire ou le contrôle naval volontaire.
86 - Pour les navires en escale à l'étranger.
87 - Il existe un centre d'opérations et de renseignement de la gendarmerie maritime par façade maritime métropolitaine.
88 - Secrétariat de l'évaluation de la menace terroriste et élaboration de la note de posture Vigipirate.
89 - Pour les navires soumis au code *ISPS*.
90 - Pour les navires soumis au code *ISPS* et coopérant en escales à l'étranger.
91 - Pour les navires en escale à l'étranger non soumis au code ISPS.
92 - Secrétariat de l'évaluation de la menace terroriste et élaboration de la note de posture Vigipirate.

ANNEXE 3
TABLEAU DES ALERTES ET DES INTERVENANTS

Modes d'action au regard des menaces identifiées	Entités recevant l'alerte		Services primo-intervenants		Observations
	Domaine maritime	Domaine portuaire et littoral	Domaine maritime	Domaine portuaire et littoral	
Navire détourné	CROSS	Capitainerie Centres de traitement de l'alerte (17 et 112)	Marine nationale et administrations de la FGC	PSMP **(GMAR)** Gendarmerie nationale Police nationale	Si besoin, les moyens des armées peuvent être réquisitionnés par l'autorité préfectorale pour intervenir dans le domaine portuaire et sur le littoral.
Prise d'otage sur un navire ou une infrastructure	CROSS	Capitainerie Centres de traitement de l'alerte (17 et 112)	Marine nationale, PSMP **(GMAR)** et Gendarmerie nationale	PSMP **(GMAR)** Gendarmerie nationale Police nationale	
Attentat	CROSS	Capitainerie Centres de traitement de l'alerte (17 et 112)	Marine nationale, PSMP et Gendarmerie nationale	PSMP **(GMAR)** Gendarmerie nationale Police nationale	
Engin explosif ou colis suspect	CROSS	Capitainerie Centres de traitement de l'alerte (17 et 112)	Groupes de plongeurs démineurs de la marine nationale (GPD) PSMP **(GMAR)**	Gendarmes NEDEX des PSMP **(GMAR)** Service de déminage de la sécurité civile GPD Police nationale	Les démineurs de la sécurité civile interviennent à terre et dans les plans d'eau des ports civils. Les GPD interviennent en mer et sur le littoral jusqu'à la laisse de haute mer.
Attentat à caractère NRBC	CROSS	Capitainerie Centres de traitement de l'alerte (17 et 112)	Marine nationale, PSMP **(GMAR)** Sécurité civile dont la CAPINAV	PSMP **(GMAR)** Gendarmerie nationale Police nationale Sécurité civile	

Modes d'action au regard des menaces identifiées	Entités recevant l'alerte		Services primo-intervenants		Observations
	Domaine maritime	Domaine portuaire et littoral	Domaine maritime	Domaine portuaire et littoral	
Attaque cyber	ANSSI MICA Center	ANSSI	ANSSI pour OSE M-CERT (à terme) SR GMAR	ANSSI pour OIV	
Trouble à l'ordre public	CROSS	Capitainerie Centres de traitement de l'alerte (17 et 112)	Marine nationale dont la GMAR Gendarmerie nationale	PSMP (GMAR) Gendarmerie nationale Police nationale	
Découverte de personnes en situation irrégulière	CROSS	Capitainerie Centres de traitement de l'alerte (17 et 112)	Marine nationale dont la GMAR Gendarmerie nationale	Gendarmerie nationale Police nationale	
Infraction en lien avec l'intelligence économique	CROSS	Capitainerie Centres de traitement de l'alerte (17 et 112)	GMAR Douanes	PSMP (GMAR) Gendarmerie nationale Police nationale Douanes	
Infraction relative à un trafic illicite	CROSS	Capitainerie Centres de traitement de l'alerte (17 et 112)	Douanes, Marine nationale dont la GMAR	Douanes PSMP (GMAR) Gendarmerie nationale Police nationale	
Infraction en lien avec la prolifération illicite	CROSS	Capitainerie Centres de traitement de l'alerte (17 et 112)	Douanes, Marine nationale dont la GMAR	PSMP (GMAR) Gendarmerie nationale Police nationale	

ANNEXE 4
CORRÉLATION ENTRE LE PLAN VIGIPIRATE ET LE CODE *ISPS*

Les mesures du code *ISPS*, spécifiques aux domaines maritime et portuaire ouverts à l'international, et celles du plan gouvernemental Vigipirate, dédiées à de plus larges domaines, ont la même finalité : sur décision du Gouvernement, mettre en œuvre des mesures visant à renforcer les dispositifs de sûreté face à une menace. Le code *ISPS*, comme le plan gouvernemental Vigipirate, a 3 niveaux.

Niveau *ISPS* 1 : désigne le niveau auquel le navire ou l'installation portuaire est normalement exploité.

Niveau *ISPS* 2 : désigne le niveau, rehaussé, applicable tant qu'il existe un risque accru d'incident de sûreté.

Niveau *ISPS* 3 : désigne le niveau, exceptionnel, applicable pendant la période de temps où le risque de sûreté est probable ou imminent.

A contrario de ce qui prévalait *ante*, **il n'y a plus de symétrie entre les niveaux de sûreté du code *ISPS* et les niveaux du plan Vigipirate**. Cette suppression a été opérée afin d'apporter une réponse plus adaptable, plus ciblée et donc plus viable dans sa mise en œuvre par sa cohérence avec la menace.

Toutefois, il reste bien une corrélation entre certaines mesures MAR du plan Vigipirate et des mesures appelées par le code *ISPS*.

Cette corrélation est spécifiée dans le catalogue des fiches mesures du plan Vigipirate. Les mesures prises en application du code ISPS font explicitement référence à ce code dans leur intitulé, notamment par la mention « Opérateurs *ISPS* ». D'une manière générale, il y a une cohérence entre le niveau *ISPS* et le niveau de contrainte de la mesure Vigipirate.

Par leur spécificité et leur niveau de détail, les dispositions appelées par le code *ISPS* ne sont pas toutes reprises par les mesures de vigilance et de protection du plan Vigipirate.

Enfin, l'attention des opérateurs maritimes et portuaires doit être appelée sur la nécessité de planifier les modalités de mise en œuvre des mesures de sûreté imposées aux différents niveaux, telles que définies par le règlement (CE) n° 725/2004 portant le code *ISPS*, et la directive 2005/65/CE, et d'apprécier les conséquences sur leurs activités.

ANNEXE 5
PRINCIPALES RÉFÉRENCES LÉGISLATIVES ET RÉGLEMENTAIRES

Textes internationaux

- Convention internationale du 9 avril 1965 modifiée visant à faciliter le trafic maritime international (FAL) ;
- Convention internationale de 1974 modifiée pour la sauvegarde de la vie humaine en mer (*Safety Of Life At Sea – SOLAS*) ;
- Convention des Nations unies sur le droit de la mer de 1982, dite de Montego Bay ;
- Convention pour la répression d'actes illicites contre la sécurité de la navigation maritime, conclue à Rome le 10 mars 1988 et ses protocoles additionnels, dite convention SUA (*Suppression of Unlawful Acts*) ;
- Code international de gestion de la sécurité pour le transport maritime (*International Safety Management – ISM*) du 1er juillet 2002 ;
- Code international relatif à la sûreté des navires et des installations portuaires (Code *ISPS*) du 12 décembre 2002 ;
- Règlement (CE) n° 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 ;
- Règlement (CE) n° 648/2005 du parlement européen et du Conseil du 13 avril 2005 modifiant le règlement (CEE) n° 2913/92 du Conseil établissant le code des douanes communautaires ;
- Décision du Conseil n° 2004/634/CE du 30 mars 2004 relative à la conclusion de l'accord entre la Communauté européenne et les États-Unis d'Amérique intensifiant et élargissant le champ d'application de l'accord de coopération douanière et d'assistance mutuelle en matière douanière afin d'y inclure la coopération relative à la sécurité des conteneurs et aux questions connexes ;
- Règlement (CE) n°324/2008 du 9 avril 2008 (modifié) établissant les procédures pour la conduite des inspections effectuées par la Commission dans le domaine de la sûreté maritime ;
- Directive n° 2005/65/CE du Parlement et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports ;
- Directive n° 2008/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 ;
- Directive (UE) n° 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

Lois

- Loi n°94-589 du 15 juillet 1994 relative à l'exercice par l'Etat de ses pouvoirs de police en mer, modifiée par l'ordonnance n°2019-414 du 7 mai 2019 ;
- Loi n° 2016-816 du 20 juin 2016 pour l'économie bleue ;
- Loi n° 2017-258 du 28 février 2017 relative à la sécurité publique ;
- Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme ;
- Loi n°2018-133 du 26 février 2018, titre 1er relative à la transposition de la directive (UE) 2016/1148 du 6 juillet 2016 (« directive Network and Information Security »).

Codes

- Code de la défense ;
- Code pénal ;
- Code de procédure pénale ;
- Code de la sécurité intérieure ;
- Code des transports.

Décrets

- Décret n° 84-810 du 30 août 1984 (modifié) relatif à la sauvegarde de la vie humaine en mer, à la prévention de la pollution, à la sûreté et à la certification sociale des navires ;
- Décret n° 95-1232 du 22 novembre 1995 (modifié) relatif au comité interministériel de la mer et au secrétariat général de la mer ;
- Décret n° 2004-112 du 6 février 2004 (modifié) relatif à l'organisation de l'action de l'État en mer ;
- Décret n° 2004-374 du 29 avril 2004 (modifié) relatif aux pouvoirs des préfets, à l'organisation et à l'action des services de l'État dans les régions et départements ;
- Décret n° 2005-1514 du 6 décembre 2005 (modifié) relatif à l'organisation outre-mer de l'action de l'État en mer ;
- Décret n°2014-1418 du 28 novembre 2014 (modifié) pris pour l'application de l'article L. 5442-1 du code des transports ;
- Décret n° 2015-351 du 27 mars 2015 (modifié) relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale ;
- Décret n° 2016-1475 du 2 novembre 2016 (modifié) portant création de la capacité nationale de renfort pour l'intervention à bord des navires (CAPINAV) ;
- Décret n°2018-1270 du 26 décembre 2018 portant dispositions relatives aux conditions d'exercice des activités privées de sécurité ;
- Décret n°2022-752 du 29 avril 2022 portant création d'un service à compétence nationale dénommé « Agence nationale des données de voyage ».

Arrêtés

- Arrêté du 23 novembre 1987 modifié relatif à la sécurité des navires ;
- Arrêté du 22 mars 2007 établissant la liste des missions en mer incombant à l'État dans les zones maritimes de la Manche-mer du Nord, de l'Atlantique, de la Méditerranée, des Antilles, de Guyane, du sud de l'océan Indien et dans les eaux bordant les Terres australes et antarctiques françaises ;
- Arrêté du 22 Avril 2008 définissant les modalités d'établissement des évaluations et des plans de sûreté portuaires et des installations portuaires ;
- Arrêté du 2 juin 2008 fixant les conditions d'organisation des exercices et entraînements de sûreté dans les ports et installations portuaires ;
- Arrêté du 4 juin 2008 (modifié) relatif aux conditions d'accès et de circulation en zone d'accès restreint des ports et des installations portuaires et à la délivrance des titres de circulation ;
- Arrêté du 4 mars 2013 relatif à l'organisation et au service de la gendarmerie maritime ;
- Arrêté du 23 mai 2016 portant approbation de la directive nationale de sécurité (DNS) secteur des transports (sous-secteur des transports maritime et fluvial) ;
- Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Transports maritime et fluvial » ;
- Arrêtés du 25 octobre 2016 établissant la liste des missions en mer incombant à l'État dans la zone maritime de Polynésie française et dans la zone maritime de Nouvelle-Calédonie ;
- Arrêté du 11 août 2021 fixant la liste des ports prévues à l'article R. 5332-18 du code des transports.

Instructions et circulaires interministérielles

- Instruction n°165/SGDSN/PSE/PSN – n°100/SGMer du 29 avril 2019 relative à la coopération navale volontaire ;
- Instruction n° 46 SGMer du 20 mai 2020 relative à la transmission des alertes sur la sûreté des navires et aux échanges d'informations relatives à la sûreté entre les navires et les organismes à terre ;
- Circulaire n° 6095/SG du 1er juillet 2019 relative à l'organisation gouvernementale pour la gestion des crises majeures ;
- Instruction générale interministérielle n° 6600/SGDSN/PSE/PSN du 7 janvier 2014 relative à la sécurité des activités d'importance vitale ;
- Instruction interministérielle n° 10100/SGDSN/PSE/PSN/NP du 14 novembre 2017 relative à l'engagement des armées sur le territoire national lorsqu'elles interviennent sur réquisition de l'autorité civile ;
- Instruction du Premier ministre du 4 mai 2020 relative à la mise en œuvre de la capacité nationale de renfort pour les interventions à bord des navires.
- Instruction interministérielle du 7 juillet 2021 relative à la mise en œuvre de la stratégie nationale de sécurisation des ports maritimes contre le trafic de drogue

Plans gouvernementaux

- Plan d'intervention en vue d'une interception de biens contribuant à des activités de prolifération d'armes de destruction massive « interception prolifération » – n°11055/SGDSN/AIST/PST/S-SF du 18 octobre 2021 ;
- Plan gouvernemental d'intervention en vue d'une interception de biens ou matériels conventionnels à usage civil ou militaire « interception conventionnel » n° 11101/SGDSN/AIST/CD-SF du 25 juillet 2016 ;
- Plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes Vigipirate n° 10200/SGDSN/PSE/PSN/CD du 1er décembre 2016 ;
- Plan gouvernemental Pirate Mer n° 10070/SGDSN/PSE/PSN/CD, édition juillet 2017.

Autres documents

- Programme national de sûreté du transport et des ports maritimes, édition octobre 2005, du ministère chargé des transports ;
- Stratégie nationale de sûreté des espaces maritimes, révisée le 10 décembre 2019 ;
- Stratégie de cybersécurité des secteurs maritimes et portuaires du 19 juillet 2021 ;
- Dossier « L'essentiel en sûreté portuaire » du MTES/DGITM/DST/DSûT, version 01 du 23 janvier 2012 ;
- Dossier « La sûreté portuaire en 4 pages », du MTES/DGITM/DST/DSûT, version de mars 2016 ;
- Guide des bonnes pratiques de sécurité informatique à bord des navires ANSSI et MTES/DGITM/DAM, octobre 2016 ;
- Document de référence interministériel sur les stratégies hybrides n°1008/SGDSN/AIST/AI/DR du 10 février 2021 ;
- « Ports cybersécurisés », Guide de bonnes pratiques pour la cybersécurité dans le secteur portuaire, MTE/DGITM, janvier 2022.

INSTRUCTION INTERMINISTÉRIELLE

relative à l'organisation et à la coordination de la sûreté maritime et portuaire

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : DSAF/DPSG/BAEC/Section Édition. Juillet 2022.