

Centre de Droit Maritime & des Transports

Faculté de Droit et de Sciences Politiques Paul Cézanne

Aix-en-Provence



La mise en application ***du Code ISPS***

Par Angélique Morosi

Dirigé par Christian SCAPEL et Pierre Bonassies

Master II Droit Maritime & des Transports

Promotion 2005

Sommaire

<u>Glossaire</u>	p.3
<u>Introduction</u>	p.5
<u>I La menace actuelle</u>	p.7
1.1 Historique	p.7
1.2 La situation actuelle	p.14
1.3 Les objectifs principaux	p.25
<u>II La mise en application au quotidien</u>	p.26
2.1 Les textes complémentaires en matière de sûreté du transport maritime	p.26
2.2 L'organisation française	p.46
2.3 Les navires/les armateurs	p.51
2.4 Les ports	p.55
2.5 Les gouvernements	p.62
2.6 Les grandes lignes de l'application dans le reste du monde	p.62
2.7 Les taux de conformité aux mesures ISPS	p.71
<u>III Conséquences et solutions</u>	p.74
3.1 Les nouvelles clause des chartes parties	p.74
3.2 Les difficultés nées de l'application directe	p.76
3.3 Comment accroître la sûreté maritime ?	p.78
3.4 Les dérives à éviter	p.84
<u>Conclusion</u>	p.88
<u>Annexes</u>	p.91
<u>Table des annexes</u>	p.92
<u>Annexe I :</u> Le Code ISPS, partie A	p.93
<u>Annexe II :</u> Statistiques sur les actes de violence en mer	p.108
<u>Annexe III:</u> Les autorités impliquées dans le contrôle du navire au port	p.111
<u>Annexe IV:</u> Les équipements de sûreté	p.112
<u>Annexe V :</u> Les taux de conformité internationaux au Code ISPS	p.114
<u>Bibliographie</u>	p.118
<u>Tables des matières</u>	p.121

Glossaire

AFFMAR	: Affaires maritimes
AIS	: <i>Automatic Identification System</i> Système automatique d'identification
ASEAN	: <i>Association of South East Asian Nations</i> Association des nations du Sud-est asiatique
CGVMSL	: Corporation de gestion de la Voie maritime du Saint-Laurent
CSN	: Centre de sécurité des navires
CSO	: <i>Company Security Officer</i> Agent de sûreté de la compagnie (ASC)
CSR	: <i>Continuous Synopsis Record</i> Fiche synoptique continue (FSC)
DoS	: <i>Declaration of Security</i> Déclaration de sûreté
FCL	: <i>Full Container Load</i> Conteneur complet
IAGS	: <i>Institute for the Analysis of Global Security</i> Institut d'analyses sur la sûreté internationale
IIF	: <i>International Islamic Front</i> Front international islamique
ILO	: <i>International Labour Organization</i> Organisation Internationale du Travail (OIT)
IMB	: <i>International Maritime Bureau</i> Bureau Maritime International (BMI)
IMO	: <i>International Maritime Organization</i> Organisation Maritime Internationale (OMI)
ISM Code	: <i>International Safety Management Code</i> Code international de gestion de la sécurité des navires (Code ISM)
ISPS Code	: <i>International Ship and Port Facility Security Code</i> Code pour la sûreté des navires et des installations portuaires (Code ISPS)
ISEAS	: <i>Institute of South East Asian Studies</i> Institut d'études du Sud-est asiatique
ISSC	: <i>International Ship Security Certificate</i> Certificat international de sûreté du navire (CISN)
LCL	: <i>Less than Container Load</i> Conteneur de groupage
MSC	: <i>Maritime Safety Committee</i> Comité de la sécurité maritime
NATO	: <i>North Atlantic Treaty Organisation</i>

	Organisation du Traité de l'Atlantique Nord (OTAN)
PAM	: Port Autonome de Marseille
PFSA	: <i>Port Facility Security Assessment</i> Evaluation de sûreté des installations portuaires (ESIP)
PFSO	: <i>Port Facility Security Officer</i> Agent de sûreté de l'installation portuaire (ASIP)
PFSP	: <i>Port Facility Security Plan</i> Plan de sûreté de l'installation portuaire (PSIP)
RSO	: <i>Recognized Security Organization</i> Organisme de sûreté reconnu (OSR)
SAAG	: <i>South Asia Analysis Group</i> Groupe d'analyses d'Asie du Sud
SSA	: <i>Ship Security Assessment</i> Evaluation de sûreté des navires (ESN)
SSAS	: <i>Ship Security Alert System</i> Système d'alerte de sûreté du navire (SASN)
SSO	: <i>Ship Security Officer</i> Agent de sûreté du navire (ASN)
SSP	: <i>Ship Security Plan</i> Plan de sûreté du navire (PSN)
Soc	: <i>Statement of Compliance</i> Déclaration de conformité
SOLAS	: <i>Safety of Life at Sea Convention</i> Convention pour la sauvegarde de la vie humaine en mer
UNCITRAL	: <i>United Nations Commission on International Trade Law</i> Commission des Nations Unies pour le droit commercial international (CNUDCI)
UNCTAD	: <i>United Nations Conference on Trade and Development</i> Conférence des Nations Unies sur le commerce et le développement (CNUCED)
VMSL	: Voie maritime du Saint-Laurent
WCO	: <i>World Customs Organization</i> Organisation Mondiale des Douanes (OMD)

Introduction

L'activité maritime constitue le cœur du commerce international. Son poids est tel qu'après les attentats du 11 septembre 2001, il était inconcevable de ne pas l'intégrer dans la politique globale de sûreté alors mise en place. Dès novembre 2001, lors de sa 22^{ème} session, l'Organisation maritime internationale (OMI) demande à deux de ses comités¹ de s'atteler à la création de normes de sûreté visant les navires et les ports. Puis, suite à la Conférence diplomatique qui s'est tenue du 9 au 13 décembre 2002 au siège de l'OMI à Londres, un certain nombre d'amendements à l'annexe de la Convention internationale pour la sauvegarde de la vie humaine en mer telle que modifiée, dite Convention SOLAS de 1974², a été adopté en présence de 108 des gouvernements originellement contractants ainsi que d'observateurs de pays membres, de pays associés, d'agences spécialisées des Nations Unies, d'organisations intergouvernementales, et d'organisations non-gouvernementales³. Les mesures qui ont le plus révolutionné le secteur maritime concernent la mise en place du Code international pour la sûreté des navires et des installations portuaires, le Code ISPS⁴. Devant l'urgence de la situation, la procédure de l'amendement tacite a été utilisée. La règle d'adoption a été la suivante : plus d'un tiers des gouvernements contractants à la Convention, ou des gouvernements contractants dont les flottes marchandes représentaient au moins 50% du tonnage brut de la flotte mondiale des navires de commerce, devaient manifester leur opposition avant le 1^{er} janvier 2004.

Le Code ISPS est entré en vigueur le jeudi 1^{er} juillet 2004, soit à peine 18 mois après sa conception. Il relève de la sûreté maritime⁵ – à savoir la protection des navires contre les pratiques criminelles pouvant survenir en mer –, à ne pas confondre avec la sécurité maritime – à savoir la prévention des risques d'origine naturelle (tempêtes, typhons, cyclones) ou provoqués par la navigation maritime (échouements, incendies, explosions) –. Cette législation est toutefois très orientée vers le terrorisme maritime et n'aborde que peu ou pas les autres problématiques liées à la sûreté maritime telles que la piraterie, les passagers clandestins, le trafic de stupéfiants par mer, alors qu'elles sont pourtant nettement plus concrètes.

Ce Code est composé de deux parties, la partie A étant automatiquement obligatoire et la partie B n'étant pas directement exécutoire selon la volonté de l'OMI. Toutefois, au niveau national, nombreux sont les Etats qui ont rendu certaines recommandations de la partie B obligatoires. Il convient de noter que ce nouveau Code s'inspire, sur certains points, du Code international de gestion de la sécurité des navires, dit Code ISM, notamment au niveau de la structure. L'un de ses éléments novateurs réside en ce qu'il concerne également les installations portuaires, alors que toutes les législations précédentes ne se référaient qu'au navire, ce qui s'explique entre autre par le fait que le port est considéré comme l'un des maillons les plus

¹ Le comité de la sécurité maritime (*Maritime Safety Committee*, MSC) et le comité juridique.

² Publiée en France par le décret n° 80-369 du 14 mai 1980, cette Convention compte 155 gouvernements contractants représentant plus de 98% du tonnage mondial.

³ Site de l'OMI : http://www.imo.org/Newsroom/mainframe.asp?topic_id=583&doc_id=2689 et http://www.imo.org/includes/blastDataOnly.asp/data_id%3D10606/hesse_chara_sec.pdf.

⁴ Cf Annexe I : Le code ISPS, partie A, page 93.

⁵ Distinction établie par G. Gidel, *Le droit international de la mer*, Tome III, Paris, Sirey, 1934, page 455.

sensibles de la chaîne logistique et que les conséquences d'un acte terroriste dirigé contre un port dépasseraient physiquement les limites de l'enceinte portuaire. Le point 5 du préambule du Code ISPS ajoute qu' « il s'agissait du moyen le plus rapide de garantir que les mesures de sûreté nécessaires entrent en vigueur et prennent effet promptement. Il a toutefois été décidé que les dispositions concernant les installations portuaires se limiteraient à la seule interface navire/port ».

Le Code ISPS repose sur le principe de la gestion de risques qui doit prendre en compte deux facteurs fondamentaux : la vulnérabilité de la cible et les conséquences d'une attaque à cet endroit. Son but primordial est donc d'anticiper et d'atténuer au maximum les menaces pesant sur le transport maritime, sachant que le risque zéro est malheureusement utopique. Le point essentiel de ces nouvelles règles est que ce n'est que de la prévention alors qu'auparavant la lutte contre le terrorisme s'orientait plutôt vers la répression. Ici, l'objectif est d'agir en amont, notamment pour éviter qu'une interruption sérieuse du commerce mondial due à des actes de malveillance ne se produise. Cette nouvelle réglementation a concerné au 1^{er} juillet 2004 quelques 60 000 navires et 20 000 installations portuaires dans le monde entier et ces origines complexes sont diverses.

Dans une première partie, nous aborderons donc l'état de la menace actuelle afin d'évaluer pourquoi ces nouvelles mesures étaient nécessaires. Comme l'explique le préambule du Code ISPS, la menace s'intensifie ; la seule réponse sensée est donc une réduction de la vulnérabilité du monde maritime, ce qui correspond à l'apparition de ce Code.

Puis, nous nous pencherons sur l'application du Code ISPS au quotidien et sur les nombreuses réglementations qui l'accompagnent. Sous certains aspects, il s'agit essentiellement d'une procédurisation car nombre de mesures existaient déjà, sous une forme certes moins ordonnée et harmonisée. Enfin, nous terminerons par un bilan de l'année écoulée, pour définir quels ont été les avantages essentiels de cette réglementation, les imperfections qui ont été révélées ainsi que les améliorations à envisager.

I La menace actuelle

1.1. Historique

La violence en mer existe depuis que l'être humain a commencé à s'aventurer sur les océans et mers du monde, ce qui est d'autant plus problématique qu'il est difficile de protéger convenablement un navire une fois qu'il a quitté le port. Les périls auxquels il doit s'attendre de nos jours sont de deux ordres : le terrorisme maritime, qui émerge peu à peu, et la piraterie, qui sévit déjà depuis des millénaires.

1.1.1. Le terrorisme maritime

La première occurrence⁶ des mots *terrorisme*, *terroriste* et *terroriser* (du latin *terror*, *terroris* « terreur, effroi ») date de la fin du XVIII^e siècle, peu après la Révolution française. Ces termes sont directement liés au régime de la Terreur – 5 septembre 1793/27 juillet 1794 –. Cette période désigne les années au cours desquelles le Comité de Salut Public, dirigé par Robespierre, exécutait ou emprisonnait toutes les personnes qui étaient considérées comme contre-révolutionnaires.

Il est toutefois à noter que, même si les termes s'y rapportant sont récents, la pratique, elle, ne l'est pas. Il s'agit même d'un phénomène historiquement récurrent commun à toutes les sociétés et à toutes les cultures. Les méthodes utilisées par les terroristes existaient déjà sous l'empire romain, quand des groupements assassinaient les légionnaires occupants aux postes frontières. Le « terrorisme continu » est apparu, lui, simultanément à la propagation des idées démocratiques et nationalistes au XIX^e siècle. De manière plus générale, le mot terrorisme a ensuite servi à désigner l'opposition dans toutes les occupations⁷.

De nos jours, il est défini⁸ comme l'utilisation, par un groupe de personnes ou un État, d'actions violentes, ou illégales, réelles ou symboliques, avec la volonté délibérée de produire sur la cible un sentiment d'intimidation et de terreur. Le terrorisme vise la population civile en général ou une de ses composantes, mais il peut également concerner une institution ou un gouvernement car, en tant que moyen de pression extrêmement puissant, il peut contraindre leur action. L'objectif est d'imposer un système politique, d'obtenir la satisfaction de revendications, de causer des destructions à un ennemi mais ce n'est jamais à des fins personnelles. Il a généralement pour effet de déstabiliser une société et de troubler gravement l'ordre public et dans sa forme extrême, il peut aller jusqu'à la remise en question de l'ordre politique et social existant, voire jusqu'à la révolution. Il est à noter que les mouvements terroristes et le grand banditisme peuvent se rapprocher dans leurs modes d'actions et leurs objectifs. Sur le plan juridique, le terrorisme est un crime ou délit de droit commun visé notamment par l'article 421-1 du Code Pénal français⁹.

⁶ Site de l'encyclopédie libre Wikipédia : http://fr.wikipedia.org/wiki/Terrorisme#Etymologie_et_origines.

⁷ L'une des premières utilisations du terme dans ce sens remonte au gouvernement de Thiers avec l'envahisseur prussien, durant La Commune de 1871. La France de De Gaulle pendant la guerre d'Algérie, ou plus récemment, La Grande Bretagne en Irlande du Nord se sont appuyés sur le même concept.

⁸ Définition de l'encyclopédie Encarta.

⁹ Livre IV Des crimes et délits contre la nation, l'Etat et la paix publique, Titre II Du terrorisme.

Le terrorisme maritime est quant à lui un phénomène récent dans la mesure où il n'a commencé à se développer qu'à partir des années 60. Moins de 200 incidents terroristes ont eu lieu dans un environnement maritime et ceux qui se sont déroulés en mer sont encore moins nombreux¹⁰. Parmi les cas les plus tristement célèbres se trouve tout d'abord celui de la *Santa Maria*, navire de commerce battant pavillon portugais. Alors qu'il effectue la ligne Lisbonne – Floride, il est dérouté, le 22 janvier 1961, en pleine mer des Caraïbes par un commando constitué d'une vingtaine d'individus appartenant au Mouvement National pour l'Indépendance du Portugal, dont le capitaine Galvão, opposant à Salazar et partisan du général Delgado. Le but de l'opération est de dénoncer médiatiquement le régime autoritaire du président Salazar. Trois officiers de marine sont tués et un marin blessé. Les pirates se rendent au Brésil quelques jours plus tard, où ils demandent et obtiennent l'asile politique. Puis, le 15 février 1963, le navire vénézuélien *Anzoategui*, qui effectue la ligne La Guaira – Houston, est attaqué par un commando de terroristes qui exige la libération de prisonniers politiques détenus au Venezuela. Ils rejoignent alors l'île brésilienne de Maraca, où ils requièrent également l'asile politique mais ils y sont arrêtés pour acte de piraterie et extradés vers le Venezuela. Le 7 octobre 1985, un groupe de pirates palestiniens se réclamant du Front populaire de libération de la Palestine (FPLP) et composé notamment de Muhammad Abbas, Magid el-Molqi, Ibrahim Abdelatif, Yusuf Ahmed Saad et Mohamed Issa Abbas, intercepte le paquebot de croisière italien *Achille Lauro* qui effectue une croisière en Méditerranée, le long des côtes égyptiennes. Il prend en otage les 180 passagers et 331 membres d'équipage alors à bord et exigent la libération de 50 palestiniens détenus en Israël. Léon Kling-Hoffer, otage étasunien infirme, est assassiné et jeté par dessus bord. Le 9 octobre, le navire rejoint Port Saïd, en Egypte et les pirates acceptent d'interrompre leur action à condition d'être remis à l'Organisation de Libération de la Palestine (OLP). Le commando embarque donc le lendemain à bord d'un Boeing 737 d'Egyptair qui est intercepté en vol par des avions de chasse étasuniens qui le forcent à se poser sur la base OTAN de Sigonella, en Sicile. Les pirates sont arrêtés, remis à la police italienne et condamnés, à Rome, le 23 mai 1987. Enfin, le 11 juillet 1988, au large d'Athènes, le *City of Poros*, navire grec de plaisance, est attaqué par un commando de trois hommes du Conseil révolutionnaire du Fatah armés de pistolets-mitrailleurs et de grenades. Neuf personnes sont tuées et quatre-vingt-onze autres blessées. Le 24 mars 1992, une demande d'extradition à l'encontre du chef présumé du commando, Samir Mohamed Ahmed Khaidir, est formulée par le juge français Bruguière auprès des autorités libyennes.

Selon Philippe Boisson, docteur en droit¹¹, ces quatre attentats relèvent du même modus operandi, à savoir le détournement¹² d'un navire par un groupe armé et la prise d'otages. Le but est d'alerter l'opinion publique internationale en mettant en lumière un problème politique particulier. Il est à noter qu'un tel acte est puni de vingt ans de réclusion criminelle par l'article

¹⁰ Terrorisme.Net : http://www.terrorisme.net/p/article_136.shtml

¹¹ BOISSON Philippe, *La sûreté des navires et la prévention des actes de terrorisme dans le domaine maritime*, DMF n° 640, p. 723, septembre 2003.

¹² Fait de s'emparer ou de prendre le contrôle par la violence ou la menace de violence d'un aéronef, d'un navire ou de tout autre moyen de transport à bord desquels des personnes ont pris place, ainsi que d'une plateforme continentale fixe située sur un plateau continental afin de commettre un vol, de kidnapper des passagers, ou pour tenter d'obtenir la satisfaction d'une revendication nationaliste, religieuse ou politique, ce qui s'oppose strictement au déroutement, acte volontaire de l'équipage consistant à changer de cap pour des raisons techniques ou météorologiques.

224-6 du Code pénal, voire de la réclusion criminelle à perpétuité lorsque cette infraction est accompagnée de tortures, actes de barbarie ou s'il en est résulté la mort d'une ou plusieurs personnes par l'article 224-7.

Par contre, les attaques plus récentes témoignent d'une véritable mutation du terrorisme international qui devient un terrorisme global. L'objectif est désormais de causer des dommages massifs au bâtiment, à l'équipage et à l'environnement par le biais d'attentats suicides. Le premier exemple révélateur de cette nouvelle forme qu'a pris le terrorisme est celui du destroyer étatsunien *USS Cole* qui est percuté par une embarcation piégée d'explosifs alors qu'il est en cours d'escale dans le port d'Aden, au Yémen, le 12 octobre 2000. Attribué à Al Qaeda, l'attaque tue dix-sept marins étatsuniens et en blesse quarante deux autres. Le 9 novembre, deux suspects sont arrêtés par la police yéménite. Selon l'opinion exposée par M. Raman¹³ lors de la Conférence internationale sur la sûreté nationale dans une région en mutation, organisée à Singapour les 28 et 29 octobre 2004, il s'agit d'une frappe tactique¹⁴ – et ce comme la plupart des attaques terroristes qui ont eu lieu depuis 1985 – visant à donner libre cours à la colère ressentie dans cette région contre les Etats-Unis. Cette attaque correspondrait ainsi à une sorte de terrorisme punitif.

L'attentat contre le pétrolier double coque *Limburg* battant pavillon français le 6 octobre 2002 à 8h00 du matin au large du Yémen en est une autre illustration. D'une capacité de 300 000 tonnes, le VLCC¹⁵ *Limburg* n'est chargé qu'avec environ 55 000 tonnes ce jour-là. Abordé à tribord par une embarcation chargée d'explosifs lancée à pleine puissance contre le navire, le pétrolier est en pleine manœuvre d'approche, à trois kilomètres du terminal d'Ash Shihr, province de Hadramout, pour compléter sa cargaison. Egalement imputé à Al Qaeda, cette attaque fait une victime, un membre de l'équipage qui s'est noyé alors que l'équipage abandonnait le navire en feu, et blesse vingt quatre personnes. Par ailleurs, une pollution générée par les résidus de brûlage – environ 12 000 tonnes d'hydrocarbures d'Arabian Heavy ont brûlé – en a résulté en sus de la nappe de 200 à 300 tonnes de brut qui a atteint les plages yéménites. A l'opposé de l'*USS Cole*, cet attentat revêtirait pour M. Raman un aspect stratégique¹⁶ dont l'objectif était d'interrompre au moins momentanément mais sérieusement, le commerce pétrolier depuis le Yémen.

Autre élément témoignant de l'éventualité de la menace pour le transport maritime: en 2002, un complot fomenté par une cellule d'Al Qaeda et qui visait à attaquer des navires britanniques et étatsuniens traversant le détroit de Gibraltar et la mer Méditerranée aurait été découvert et déjoué. En effet, les autorités marocaines ont confirmé le 11 juin 2002 avoir arrêté en mai trois saoudiens. Ils se seraient entraînés en Afghanistan et auraient été envoyés pour préparer des attaques avec des zodiac par Abdul Rahim Mohammed Abda al-Nasheri, chef des

¹³ Ancien haut fonctionnaire du gouvernement de l'Inde, figure réputée de la communauté du renseignement, ainsi que membre d'honneur de l'*Observer Research Foundation* (ORF).

¹⁴ Le but est généralement de faciliter les actes de terrorisme terrestre par le biais de trafic d'armes ou de stupéfiants, en transportant clandestinement des terroristes.

¹⁵ *Very Large Crude Carrier*.

¹⁶ Tout comme les actes terroristes généralement perpétrés par les *Liberation Tigers of Tamil Eelam* ou Tigres de libération de l'Eelam tamoul (LTTE), organisation séparatiste du Sri Lanka dans le but d'affaiblir les capacités militaires et économique de l'Etat sri lankais et ce pour atteindre leur objectif final, à savoir l'avènement d'un Etat tamoul indépendant.

opérations navales d'Al Qaeda également arrêté en 2002. Surnommé le Prince de la Mer, il est suspecté d'être le cerveau de l'opération contre le *USS Cole*.

De même, en février 2004, une boîte contenant 3,6 kilos de TNT, déposée par un membre présumé du groupe Abbu Sayyaf¹⁷, explose à bord du SuperFerry 14 dans la baie de Manille, alors qu'il venait de quitter Mindanao une heure plus tôt. C'est le cas de terrorisme maritime le plus meurtrier à l'heure actuelle puisque 100 personnes ont trouvé la mort dans cet attentat.

Enfin, en mars 2004, dans le port israélien d'Ashdod, l'un des plus animés du pays, deux kamikazes palestiniens appartenant aux Brigades des martyres d'Al Aqsa ainsi qu'au Hamas, se sont faits explosés. Ils ont tués 10 israéliens et en ont blessé 18 autres. Il semblerait qu'ils soient entrés en fraude dans le port quatre heures auparavant en se cachant à l'intérieur d'un conteneur qui avait transité par un autre port avant d'arriver en Israël.

1.1.2. La piraterie

A l'inverse du terrorisme maritime, la piraterie se pratiquait déjà dans l'Antiquité dans le bassin méditerranéen. Elle est définie par l'article 101 de la Convention des Nations Unies sur le Droit de la Mer du 10 décembre 1982¹⁸ comme « l'un quelconque des actes suivants :

a) tout acte illicite de violence ou de détention ou toute déprédation commis par l'équipage ou des passagers d'un navire ou d'un aéronef privé, agissant à des fins privées, et dirigé : i) contre un autre navire ou aéronef, ou contre des personnes ou des biens à leur bord, en haute mer; ii) contre un navire ou aéronef, des personnes ou des biens, dans un lieu ne relevant de la juridiction d'aucun Etat;

b) tout acte de participation volontaire à l'utilisation d'un navire ou d'un aéronef, lorsque son auteur a connaissance de faits dont il découle que ce navire ou aéronef est un navire ou aéronef pirate;

c) tout acte ayant pour but d'inciter à commettre les actes définis aux lettres a) ou b), ou commis dans l'intention de les faciliter ».

La piraterie s'oppose aux actes des corsaires en ce qu'elle n'est pas mandatée par un gouvernement. Il est à noter que ce phénomène protéiforme est essentiellement régional et que, dans les eaux territoriales, il s'agit non plus de piraterie mais de vol en mer. Il convient également d'observer que le Bureau Maritime International (BMI)¹⁹ a créé, en 1999, un centre de surveillance de la piraterie²⁰, à Kuala Lumpur, en Malaisie. Il publie chaque année un rapport regroupant les actes de piraterie et autres attaques criminelles survenues en mer. Cette étude analyse les mutations de la piraterie et identifie les zones à risques afin que les équipages puissent prendre des mesures préventives. Au quotidien, ce centre répertorie tous les actes de violence en mer²¹. Il diffuse ainsi tous les jours des bulletins d'information à l'attention des navires via le système satellitaire Inmarsat C²² à partir desquels il publie un rapport hebdomadaire. Il fournit par

¹⁷ Groupe rebelle musulman du Sud des Philippines spécialisé dans le kidnapping d'étrangers. Site de Libération : <http://www.liberation.fr/page.php?Article=282361>.

¹⁸ Site des Nations Unies : <http://www.un.org/french/law/los/unclos/closindx.htm>.

¹⁹ Il s'agit d'un organisme dépendant de la Chambre Internationale de Commerce (CCI) créé en 1981.

²⁰ *Piracy Reporting Centre of the International Maritime Bureau*.

²¹ Cf Annexe II : Statistiques sur les actes de violence en mer, page 108.

²² Cf infra 2.1.3.1.2 Les textes du MSC, page 37.

ailleurs une assistance gratuite aux bâtiments ayant été attaqués. Enfin, cet organisme est financé par les donations de 25 organisations de l'industrie maritime, dont des P&I clubs, des armateurs et des assureurs.

En termes généraux, la piraterie²³ est en augmentation constante depuis 1991, époque à laquelle une centaine de cas seulement était relevée. L'abordage est la manœuvre la plus récurrente, puis viennent les tentatives d'abordage et les détournements. La pratique consistant à prendre en otage l'équipage n'est apparue massivement que vers 1995, c'est désormais la pratique la plus répandue. Enfin, les navires les plus fréquemment attaqués sont les pétroliers et les transports de marchandises diverses à l'aide de couteaux ou d'armes à feu et ce depuis 1997 car avant, les pirates n'étaient généralement pas armés.

De façon plus spécifique, la caractéristique principale de l'année 2002²⁴ a été une augmentation marquée du nombre d'abordages réussis contre des navires au mouillage – c'est le cas de la plupart des 370 incidents recensés, contre 335 en 2001 –, combinée à une baisse sensible des tentatives d'attaques de navires en mouvement. Cette constatation laisse supposer que la menace a été gravement sous estimée par de nombreux équipage. Le nombre de détournements est lui passé de 16 à 25. L'essentiel des événements rapportés²⁵ sont l'œuvre de petits bateaux, remorqueurs, barges ou bateaux de pêche dans les eaux indonésiennes – 103 incidents contre 91 en 2001 –, au Bangladesh – 32 attaques contre 25 l'année précédente – ou en Inde – 18 cas contre 27 en 2001 –. Le continent américain enregistre une hausse de 300% sur un an : le nombre d'incidents passe de 21 en 2001 à 65 en 2002²⁶. La région asiatique, quant à elle, reste stable avec 170 incidents recensés. Par contre, la Somalie devient un pays critique ; le risque est passé de possible à certain. Le BMI estime qu'un navire réalisant une escale non prévue dans un port somalien, qui ralentit ou s'arrête près des côtes sera presque inévitablement abordé par des milices armées qui extorquent ensuite des sommes substantielles aux propriétaires de navire pour leur rendre leur navire et/ou leur équipage. Il semblerait par ailleurs que les pirates aient plutôt tendance à viser des navires transportant des cargaisons de valeur, telles que l'huile de palme ou encore le gasoil. Enfin, le rapport mentionne à plusieurs reprises que les pirates jettent les membres d'équipage par-dessus bord et les laissent pour morts.

Pour ce qui est du premier semestre 2003 uniquement, la piraterie a connu une hausse de 37% en comparaison avec la même période sur l'année précédente, soit 234 attaques. Les eaux indonésiennes restent les plus dangereuses avec 64 incidents, suivies du détroit de Malacca – détroit qui côtoie l'Indonésie, la Thaïlande et la Malaisie et qui enregistre 15 attaques –, de la Malaisie, des Philippines et du Vietnam. Pour l'ensemble de l'année, 445 cas de piraterie ont été recensés – en mer, à l'ancrage ou dans un port, soit une augmentation de 120% sur un an – dont 332 avec abordage, 19 concernant des navires détournés et plus de 90 pour le seul détroit de Malacca.

²³ Cf Annexe II : Statistiques sur les actes de violence en mer, page 108.

²⁴ Site de la CCI : http://www.iccwbo.org/home/news_archives/2003/stories/piracy%20report_2002.asp.

²⁵ Page personnelle de Mark Bruyneel, expert néerlandais en piraterie : <http://home.wanadoo.nl/m.bruyneel/archive/modern/imb2002.htm>.

²⁶ Les pays de la zone qui enregistrent une hausse sensible sont la Guyane – qui passe de 0 à 12 actes recensés –, le Venezuela – de 1 à 8 –, la Colombie – de 1 à 7 –, le Pérou – de 1 à 6 –, l'Equateur – de 8 à 12 – ou encore le Brésil – de 3 à 6 –.

En 2004²⁷, les actes de piraterie sont tombés à 325 – soit une baisse de près de 27% – mais ils sont désormais plus violents : 30 membres d'équipage ont perdu la vie contre 21 en 2003. Les eaux indonésiennes restent les plus dangereuses, même si le nombre d'incidents passe de 121 en 2003 à 93, car elles représentent, à elles seules, plus d'un quart des actes criminels recensés en mer sur l'année. Par ailleurs, la baisse des actes recensés dans les eaux nigériennes – qui passent de 39 en 2003 à 28 en 2004 – n'est que peu rassurante puisque les attaques au large du pays le classent en troisième position des Etats à risques à l'échelle mondiale. Par contre, au niveau du seul continent africain, le Nigeria est considéré comme le pays le plus dangereux. Enfin, un des traits dominants de 2004 est que le détournement de remorqueurs et de barges ainsi que la prise en otage de l'équipage enregistre une hausse préoccupante, et ce particulièrement au Nord du détroit de Malacca et au Nord de l'île de Sumatra. Il semblerait désormais que ce soit plus l'œuvre des « syndicats du crime » que de rebelles séparatistes.

La tendance qui prédominait en 2004 se poursuit en 2005²⁸ puisque le nombre d'attaques a baissé d'environ 30% à l'échelle mondiale au premier semestre. En effet, « seuls » 127 actes de violence ont été recensés de janvier à juin 2005, contre 182 l'année précédente à la même période. En six mois, des pirates ont abordé 92 navires, six bâtiments ont été détournés et 176 membres d'équipage ont été pris en otages. L'Indonésie reste le pays le plus dangereux puisqu'elle compte 42 incidents, soit le tiers du total enregistré. Par contre, aucun acte de violence n'a été recensé dans le détroit de Malacca dans les mois qui ont suivi le terrible tsunami du 26 décembre 2004 et ce jusqu'à la fin du mois de février. Depuis, huit incidents violents ont été enregistrés. La Somalie, quant à elle, redevient risquée après deux ans de calme. Entre avril et juin 2005, huit attaques de pirates armés de fusils et de grenades ont été dénombrées au large de la côte Est du pays. Dans quatre cas au moins, des membres d'équipage ont été pris en otages en échange d'une rançon. Le Capitaine Pottengal Mukundan, directeur du BMI, est pessimiste à ce sujet. Il a en effet déclaré que « les pirates qui opèrent au large de la Somalie sont devenus de plus en plus audacieux. Ils s'emparent des navires une fois qu'ils sont à l'extérieur des limites territoriales et les forcent à naviguer vers la haute mer. Les demandes de rançon sont plus fortes que jamais et les négociations visant à faire relâcher les navires et les équipages sont âpres et interminables. Le manque total d'application de la loi dans cette zone laissent les navires et les marins sans aucune protection ». Enfin, plusieurs autres zones ont vu les actes de violence en mer augmentés, notamment le Nigeria – quatre incidents ont eu lieu dans la rivière Bonny depuis le 24 mai 2005 – et l'Irak – quatre incidents violents ont été rapportés au large du terminal pétrolier de Basra depuis le 22 avril 2005 alors que, au cours des dernières années, la piraterie semblait inexistante dans cette région –.

Il est un constat incontournable et inquiétant sur l'ensemble des quatre ans : les actes de piraterie n'ont enregistré aucune baisse significative, voire ont même augmenté dans certaines zones, ce qui est assez problématique depuis l'entrée en vigueur du Code ISPS. Cette observation souligne par là même que ces nouvelles mesures ont une portée assez limitée dans le sens où, bien souvent, les pays qui ne peuvent les mettre financièrement en application sont les plus

²⁷ Site de la Chambre de Commerce Internationale : <http://www.icc-ccs.org/main/news.php?newsid=40>.

²⁸ Site de la CCI : <http://www.icc-ccs.org.uk/>.

touchés. De plus, si des pirates peuvent contourner ces mesures, des terroristes, par définition mieux organisés et plus déterminés, le pourront aisément. Le Capitaine Pottengal Mukundan, estime que, dans certaines régions du monde, il est trop aisé d'aborder illégalement un navire marchand. D'autant que la piraterie est en pleine mutation depuis quelques années et intègre une dimension politique, ce qui devient « alarmant vu la dévastation qu'elle cause dans le reste du monde ». D'après un communiqué du BMI en date du 2 septembre 2003, des groupes de pirates lourdement armés²⁹ attaquent des petits pétroliers dans le détroit de Malacca à l'aide de vedettes rapides ou de bateaux de pêche. Ils semblent suivre le mode d'action des rebelles séparatistes membres du mouvement pour la libération de la région d'Aceh – appelé aussi Gerakin Aceh Merdeka, GAM – et sont prêts à prendre plus de risques pour servir leur cause. Un exemple frappant est celui de l'attaque du pétrolier *Penrider* à 12 milles marins de Port Kelang, en Malaisie – soit environ 22 km –. Le navire transporte alors 1 000 tonnes de fuel et fait route de Singapour à Penang quand un navire de pêche avec, à son bord, 14 pirates armés l'intercepte. Après avoir dépouillé l'équipage de ses biens et l'avoir forcé à naviguer dans les eaux indonésiennes, les pirates sont partis en emmenant le Capitaine, le chef mécanicien et un autre membre d'équipage en otages. Les négociations de rançon se sont éternisées avant qu'ils ne soient libérés sains et saufs. Les assaillants se seraient réclamés du GAM et bien que la police malaisienne ait conclu que le *modus operandi* correspondait effectivement, il n'y a pas de preuve tangible. Certaines agences de presse rapportent même que ce pourrait tout aussi bien être d'autres individus qui copieraient leur méthode. Ce qui est certain, c'est qu'il s'agissait bel et bien de la première attaque du genre par des pirates indonésiens si près des côtes malaisiennes et si loin au Sud d'Aceh. En de pareilles circonstances, le manque crucial d'informations fiables fait cruellement défaut.

Une remarque importante mérite pourtant d'être faite. Il n'existe, à l'heure actuelle, aucune certitude quant à ce que des organisations terroristes, notamment jihadistes appartenant au *International Islamic Front*³⁰, et des groupes de pirates opérant, notamment dans la région de l'Asie du Sud et du Sud-est, soient liés³¹. La principale raison est idéologique car leurs objectifs sont de fait très différents : le pirate attaque à des fins personnelles, il veut son butin mais ne veut que très rarement mourir pour sa cause, par opposition au terroriste. Par contre, il est presque certain que des groupes de terroristes ethniques ou rebelles opérant dans la région indonésienne commettent de plus en plus d'actes de piraterie pour pouvoir financer leur lutte contre le gouvernement indonésien. Le risque le plus sérieux n'est donc pas que les pirates et les terroristes s'associent mais bien que les terroristes recrutent parmi des pirates déjà expérimentés, ce qui augmenterait leur force d'attaque.

²⁹ Ils possèdent des armes très sophistiquées, principalement des armes automatiques, des AK 47, des fusils d'assaut M16 ainsi que des embarcations à grande vitesse et donc par déduction les terroristes potentiels aussi. La tendance s'est inversée car jusqu'en 1996, les pirates étaient le plus souvent désarmés. Cf Annexe II : Statistiques sur les actes de violence en mer, page 108.

³⁰ Front islamique international (IIF).

³¹ Site de Terrorisme.Net : http://www.terrorisme.net/p/article_136.shtml.

1.2. La situation actuelle

Graham Gerard Ong³² prédisait, dans un article datant de septembre 2003 : « Prochaine étape, le terrorisme maritime » mais qu'en est-il exactement ?

Il n'existe pas d'organisation terroriste spécialisée dans les attaques maritimes ; en revanche, plusieurs mouvements terroristes classiques ont ou sont en passe d'acquérir les moyens de commettre des actes terroristes non seulement à terre, dans les airs, dans les eaux territoriales mais également en haute mer. C'est pourquoi il est certain que la question que tout le monde se pose à l'heure actuelle est celle de la réalité de la menace d'actes terroristes contre le monde maritime en tant que vecteur fondamental du commerce mondial. En effet, selon la CNUCED, en termes de volume, plus de 46 000 navires avec, à leur bord, 1,25 millions de marins et desservant quelques 4 000 ports, ont acheminé 80% des quelques six milliards de tonnes de marchandises échangées en 2001 dans le monde.

Il faut observer de plus que, contrairement aux autres modes de transport, et ce dans une certaine mesure aux vues des attaques évoquées antérieurement, le secteur maritime a été relativement épargné par des attentats massifs, ce qui est un facteur d'autant plus préoccupant. Comparé aux actes de terrorisme aérien qui sont en augmentation depuis 1967, les attaques terroristes dirigées contre l'industrie maritime, que ce soit dans les eaux territoriales ou en mer, sont assez rares. Il y a essentiellement deux raisons à cela. La première est d'ordre technique : à l'exception des attentats-suicides dont le but n'est pas la fuite, il est particulièrement difficile de s'enfuir après une attaque en haute mer. La seconde est plutôt idéologique : les terroristes veulent que le théâtre même de leur action soit suffisamment évocateur, afin que le retentissement soit maximal et que la force d'intimidation sur l'Etat attaqué et sur l'opinion publique soit à son comble, ce que la mer ne peut fournir que dans une moindre mesure par rapport à la terre ou à l'air. Tout est question d'orchestration et d'opérations spectaculaires dont tout un chacun se souviendra.

Toutefois, étant donné que le terrorisme se concentre plutôt désormais sur des actes de terrorisme économique car ils ont des conséquences plus impressionnantes, il est évident que le milieu maritime fournit un cadre nettement plus vaste que l'aérien ou le terrestre puisque l'essentiel du commerce mondial se fait par navire. Nombreux sont ceux qui voient donc le maritime comme la prochaine cible après l'attentat aérien new-yorkais du 11 septembre 2001, l'attentat ferroviaire madrilène du 11 mars 2004 et l'attentat dans le métro londonien du 7 juillet 2005. Enfin, du fait de la multiplication des attaques, les lieux à terre qui auraient pu servir de cibles potentielles sont nettement mieux protégés si bien que les groupuscules terroristes vont se recentrer sur ce qui leur semble être relativement plus accessible, à savoir les infrastructures maritimes.

Il est par ailleurs à noter que les navires sont un des moyens de transport les plus vulnérables – et tout particulièrement les pétroliers qui sont une proie relativement facile et d'une grande portée symbolique –, étant donné qu'il est possible de les atteindre sous l'eau, depuis la

³² Chercheur à l'*Institute of South East Asian Studies*, ISEAS, il est l'auteur d'une étude intitulée : *Pre-empting Maritime Terrorism in Southeast Asia*, ISEAS Viewpoints, Nov. 29, 2002. Site consacré à la mer de Chine du Sud : <http://community.middlebury.edu/~scs/docs/Ong-Preempting%20Terrorism%20and%20Piracy,%20ISEAS.pdf>.

terre, par les airs, de les aborder depuis la mer ou de les attaquer de l'intérieur. Cette dernière éventualité est la plus à craindre selon Laurent Galy, professeur à l'Ecole nationale de la marine marchande (ENMM) de Nantes. Il estime qu'il existe une carence au niveau de la surveillance du recrutement des équipages si bien que des terroristes pourraient plus ou moins aisément s'infiltrer et se faire passer en toute impunité pour des marins. Ceci corrobore le fait qu'un grand nombre de certificats détenus par des marins sont obtenus de façon frauduleuse ; en réalité, jusqu'à 80% des certificats décernés par certains pays se sont avérés être des faux³³. Lors d'une étude menée par l'OMI en 2001³⁴, 13 000 faux certificats ont été signalés, dont 90% en provenance des Philippines, sachant que seulement 56% des administrations maritimes contactées pour cette enquête ont répondu. L'OMI relève également que, dans 10 pays contrôlés sur 13, la fraude officielle est un fait avéré.

En outre, le fait que la main d'œuvre du secteur maritime soit d'origines extrêmement variées devient un facteur de risque supplémentaire alors que l'inter-culturalité est généralement un facteur incontestable d'évolution. Certains y voient également une gêne dans le sens où en cas d'attaque, un marin qui n'a pas la nationalité du pavillon ne s'engagera pas avec la même énergie pour lutter et défendre les intérêts du pays dans lequel le navire est immatriculé. Tout est relatif mais le corollaire est bien évidemment qu'un navire livré aux mains d'individus malfaisants en devient logiquement d'autant plus dangereux.

Les cargaisons sont également un élément à prendre en compte dans l'analyse de la menace, et notamment du fait de la conteneurisation qui, en réalité, s'avère problématique. Représentant un progrès indiscutable pour le transport maritime, il n'en reste pas moins qu'il est techniquement impossible qu'un armateur ou un affréteur ouvre tous les conteneurs qui vont charger sur un navire pour en vérifier le contenu, sinon les escales seraient absolument ingérables, les coûts engendrés faramineux, les délais de livraison intenable. D'autant plus que certains conteneurs arrivent déjà plombés – c'est le cas notamment des FCL³⁵ –. Sans compter le fait que le transporteur maritime n'a matériellement pas le temps d'en vérifier le contenu, il ne faut pas perdre de vue que si le chargeur livre un conteneur plombé, c'est pour éviter de faire subir une nouvelle manutention à la marchandise, sachant qu'il s'agit du premier risque de dommages. De plus, le risque de vol s'en trouve accru, ce type de contrôle coûte relativement cher – il faut, entre autre, la présence de manutentionnaires et de pointeurs – et la concurrence est particulièrement rude dans le secteur maritime³⁶. Ceci constitue une difficulté à part entière car presque la moitié du commerce mondial en valeur et 90% des marchandises transportées de nos jours le sont par conteneur, elles sont des plus diversifiées, leur description reste souvent volontairement floue et leur provenance n'est pas toujours clairement établie. S'ajoute à cela le fait que les propriétaires de navires dissimulent leur identité, ce système étant facilité par l'existence de nombreux intermédiaires. Il s'agit donc incontestablement d'un point sensible

³³ Site d'information militaire suisse du nom de CheckPoint:

<http://www.checkpoint-online.ch/Checkpoint/Monde/Mon0072-TerrorismeMaritime.html>.

³⁴ Site de la BBC : <http://news.bbc.co.uk/1/hi/world/asia-pacific/1804146.stm>.

³⁵ *Full Container Load*, empoté par le chargeur, par opposition au *Less than Container Load*, qui sert dans le cadre du groupage, si bien que dans cette optique, il peut parfaitement être empoté par le transporteur qui sera alors au fait de son contenu.

³⁶ Le transporteur maritime peut ouvrir un conteneur plombé, il lui suffira alors de remplacer un plomb et de préciser sur le connaissement que le conteneur a été déplombé et replombé avec le conteneur n°X.

puisque les conteneurs peuvent contenir clandestinement des personnes – ce qui est somme toute assez fréquent au vu du nombre de clandestins découverts chaque année dans des conteneurs – ou des armes conventionnelles, nucléaires, chimiques, voire biologiques. Le conteneur est d'ailleurs considéré comme le moyen le plus à même de transporter une bombe nucléaire ou radiologique.

Les menaces les plus sérieuses à l'heure actuelle³⁷ sont l'infiltration de l'équipage par des terroristes pour commettre un des actes suivants : le détournement et la mise à feu d'un chimiquier, d'un super pétrolier, d'un gazier ou de n'importe quel navire transportant des marchandises dangereuses, explosives, toxiques ou inflammables et qui serait utilisé comme bombe flottante dans un port, dans un détroit, dans une zone côtière très peuplée ou dans une zone économique sensible. L'attaque d'un navire pour provoquer des pertes massives en vies humaines ou une prise d'otages géante sur un ferry ou un bateau de croisière dans les eaux internationales sont pareillement à redouter. Le détournement d'un navire pour faire de la contrebande d'armes, d'explosifs et de stupéfiants ou encore pour transporter des clandestins³⁸ suscite une crainte tout aussi sérieuse. Ce type d'actions peut également avoir pour dessein la piraterie basique visant à utiliser les recettes des transports maritimes pour financer des activités terroristes autres. Dans le même état d'esprit, un navire « fantôme » repeint et renommé – ce qui est une pratique courante pour les pirates asiatiques depuis les années 80 – pour transporter des armes et des hommes sur le lieu terrestre de l'attentat ou pour blanchir des fonds illicites destinés à des organisations terroristes, est à envisager. Il ne faut pas non plus négliger l'utilisation de petites embarcations pour attaquer des cibles sur la côte ou au mouillage, telles que des installations portuaires, des navires de guerre, des bateaux de croisière en escale dans un port, des ferrys, des installations pétrolières offshore, des raffineries, des établissements spécialisés dans la recherche nucléaire, etc. D'autant plus que les terroristes se sont déjà illustrés au cours de ce genre d'opérations, notamment lors de l'attentat du terminal offshore de Bassora, dans le Sud de l'Irak, le samedi 24 avril 2004³⁹. Des kamikazes ont de fait essayé d'attaquer des tankers exportant du brut irakien à l'aide de petites embarcations piégées mais ont été interceptés par la marine étatsunienne. Il n'en demeure pas moins que deux soldats étatsuniens ont péri dans l'explosion de l'un des canots. Peter Swift, directeur général d'Intertanko⁴⁰, estime que les ports accueillant le trafic international restent le point faible de la lutte antiterroriste. Deux jours plus tard, le lundi matin, le terminal de Bassora, par lequel transitent 80% des quelques 1,9 millions de barils quotidiennement exportés d'Irak, était de nouveau officiellement opérationnel. D'après la Lloyd's, grande compagnie d'assurances britannique, le terminal aurait été complètement détruit si la tanker visé avait été totalement chargé. Enfin, les voies maritimes peuvent servir à aider des terroristes à s'échapper, des armes de destruction massive peuvent être

³⁷ Site de l'Institut d'études internationales de Montréal : <http://www.er.uqam.ca/nobel/cepes/pdf/BULL71.pdf>.

³⁸ Le trafic d'êtres humains est un phénomène qui est malheureusement en augmentation constante, et ce principalement en provenance du Moyen-Orient, d'Afrique ou d'Asie vers l'Europe occidentale qui attire chaque année des dizaines de milliers d'immigrants clandestins. Les trafiquants ont longtemps utilisé la Turquie mais, maintenant, ils passent plutôt par la Libye ou la Tunisie car le gouvernement turc a déployé des efforts significatifs en la matière. Le souci majeur est que ce sont désormais souvent des groupes du crime organisé qui sont impliqués, le corollaire étant nécessairement des abus innombrables des droits de l'homme.

³⁹ Site du Monde : http://www.lemonde.fr/web/recherche_breve/1,13-0,37-851377,0.html.

⁴⁰ *International Association of Independent Tanker Owners* – Association internationale des propriétaires indépendants de pétroliers.

dissimulées dans des conteneurs ou des aéronefs peuvent être utilisés pour commettre des attentats-suicides contre des cibles sur l'eau. En 1992, après s'être fait arrêté par la police hindoue, un terroriste pakistanais appartenant à l'organisation Babbar Khalsa aurait déclaré lors de son interrogatoire qu'au cours de son entraînement, il lui avait été suggéré de prendre des leçons de pilotages à l'aéroclub de Bombay dans le but de s'écraser sur une plateforme pétrolière offshore.

Sachant que les terroristes peuvent soit utiliser des armes nucléaires, biologiques, chimiques ou radiologiques qui dispersent des substances radioactives, soit procéder via des plongeurs équipés de mines pour parvenir à leurs fins et que les experts évoquent souvent les risques que représenterait un engrais, comme le nitrate d'ammonium qui peut être transformé en explosif puissant⁴¹, il faut également être capable de prévoir les conséquences dramatiques de tels actes pour être prêt à faire face. Le plus plausible seraient non seulement des pertes en vies humaines catastrophiques mais aussi des dommages conséquents à l'environnement ainsi qu'une paralysie quasi instantanée de l'économie mondiale. L'interruption dépendrait essentiellement du temps que pendant lequel durerait le blocage et des coûts qui seraient impliqués pour relancer la machine économique ; hautement préjudiciable notamment pour les pays en voie de développement, elle serait inévitablement suivie d'une dégradation des échanges mondiaux car les gouvernements engageraient des frais colossaux en toute hâte pour garantir une sûreté post-attaque à leur population et à leurs villes. D'après des estimations étatsuniennes⁴², le coût d'une fermeture de port comprise entre sept et dix jours, suite à une attaque terroriste majeure, serait d'environ 58 milliards de dollars américains. La suppression des escales vers le pays en cause, mais également vers tous ceux à risques serait inéluctable. Suite à l'opération contre le *Limburg*, le déroutement sur les pays voisins a coûté près d'1% du PIB au Yémen. Une attaque terroriste dans un port ruinerait des années d'efforts passées à gagner en compétitivité puisque sa réputation du port en serait définitivement entachée.

De même, les taux d'affrètement enregistreraient une hausse marquée, comme cela a été le cas à la suite de l'attentat contre le *USS Cole*, le *Limburg* ou encore le terminal de Bassora. Les armateurs se sont montrés plutôt alarmistes dans la dernière hypothèse car ils estimaient que si d'autres navires marchands se faisaient attaqués, la surprime d'assurance imposée pendant la guerre du Golfe devrait être rétablie dans l'ensemble du Golfe arabo-persique. En cas d'attaque spécifique contre un élément de l'industrie pétrolière, le prix du baril de pétrole flamberait, ce qui ne ferait qu'aggraver les conditions de la reprise économique. Enfin une montée en flèche des primes d'assurances en découlerait, comme cela a été le cas après l'attentat contre le *Limburg* ou contre le terminal de Bassora. En effet, les assureurs avaient triplé le montant des primes pour les navires escalant au Yémen suite à la première attaque et dans le second cas, la hausse a

⁴¹ Il a déjà été utilisé à plusieurs reprises dans des attentats au camion piégé – à Nairobi, à Mombasa, à Oklahoma City en 1995 – ou pour plusieurs attentats en Indonésie – Bali en octobre 2002 et Jakarta en août 2003 –. Il aurait même déjà causé des accidents dans le contexte maritime – Texas City et à Brest en 1947 – et terrestre – 300 tonnes de cet engrais était impliquées lors de l'explosion de l'usine AZF à Toulouse le 21 septembre 2001 –. Il est à noter à ce propos que les USA et d'autres pays membres de l'OCDE ont importé plus de 1,6 millions de tonnes de nitrate d'ammonium en 2000, et ce principalement par mer. Site d'information militaire suisse du nom de Check Point: <http://www.checkpoint-online.ch/CheckPoint/Monde/Mon0072-TerrorismeMaritime.html>.

⁴² D'après les estimations du *Conference Board* et du Cabinet de conseil Booz Allen Hamilton Inc, site de l'OCDE : http://www.oecd.org/document/45/0,2340,en_2649_34487_4395885_119690_1_1_37407,00.html

concerné les super pétroliers chargeant des cargaisons dans le port d'al-Basra – ex port de Mina al-Bakr –. Selon Michael Richardson⁴³, en cas d'attaque par une bombe nucléaire ou radiologique, les primes d'assurance atteindraient très certainement des niveaux prohibitifs. Plus l'attaque sera désastreuse, plus l'envolée des primes sera exorbitante. Il n'existe pas, à l'heure actuelle, d'assurance pour une attaque terroriste maritime utilisant une bombe nucléaire ; le coût de la reprise serait absolument inimaginable et il estime même qu'il n'est pas du tout certain que la solvabilité d'une compagnie d'assurance privée soit suffisante.

Par ailleurs, en 2003, l'Unité éconómico-analytique de l'équivalent du ministère des affaires étrangères australien a conduit une étude sur l'impact qu'aurait un attentat terroriste majeur pour les pays en voie de développement (PVD), en intégrant une dimension maritime⁴⁴. Les coûts seraient disproportionnellement plus élevés pour eux, notamment du fait de leurs besoins en investissements étrangers directs qui sont subordonnés à un environnement économique sûr et stable. Il ressort, de plus, que les primes d'assurance le seraient également, et ce aussi bien pour les marchandises que pour les navires en provenance des PVD du fait de l'incertitude pesant sur la fiabilité de leurs procédures locales de sûreté.

1.2.1 La situation en France

La France⁴⁵ dispose de plus de 10 000 km de littoral et 72% des échanges commerciaux français s'effectuent par mer. Quant à la flotte nationale, elle est composée d'environ 200 navires. Au niveau portuaire, la France⁴⁶ compte au total sept ports autonomes⁴⁷, qui sont en premier lieu des ports de commerce. Représentant plus de 80% du trafic maritime français de marchandises, ce sont, de plus, des établissements publics de l'Etat depuis la loi n° 65-491 du 29 juin 1965. Puis elle dispose de 23 ports d'intérêt national qui sont également des ports de commerce et de pêche mais qui font partie, eux, des attributions de l'Etat. En termes de marchandises, à peu près 20% du tonnage est couvert par les ports d'intérêt national qui réalisent presque 50% du trafic de marchandises diverses non conteneurisées et plus de 80% du trafic passagers. Enfin, la France dénombre 532 ports décentralisés, dont 304 ports de commerce et de pêche qui dépendent des Conseils Généraux de départements et qui disposent la plupart du temps d'une zone réservée à la plaisance, ainsi que 228 ports de plaisance placés sous la responsabilité directe des communes.

La situation politique du pays est telle que le gouvernement a une position assez neutre au niveau des conflits internationaux actuels, notamment en Irak, donc la perspective de représailles est a priori moindre. Par contre, la Méditerranée peut représenter un danger potentiel pour la France dans la mesure où il s'agit d'une mer fermée par laquelle transitent de nombreuses matières dangereuses. Les actes de piraterie y sont totalement inexistants mais la contrebande

⁴³ Ancien éditeur en Asie de l'*International Herald Tribune* et chercheur pour l'ISEAS. Site du journal *Asia Times*: http://www.atimes.com/atimes/Front_Page/FF16Aa02.html.

⁴⁴ Site de l'Institut australien de politique stratégique : http://www.aspi.org.au/pdf/Maritime_terrorism%20India_AB.pdf

⁴⁵ Site du Sénat : http://www.senat.fr/rap/a04-076-20/a04-076-20_mono.html#toc0.

⁴⁶ Site du ministère des transports, de l'équipement, du tourisme et de la mer : http://www.mer.equipement.gouv.fr/commerce/01_ports_francais/01_organisation_portuaire/index.htm.

⁴⁷ Six en métropole : Marseille-Fos, Le Havre, Dunkerque, Nantes Saint-Nazaire, Rouen, Bordeaux et un dans les Antilles, en Guadeloupe : Pointe-à-Pitre Jarry.

d'armes et de stupéfiants⁴⁸ se révèle être l'une des principales préoccupations. En juin 2003⁴⁹, les autorités grecques ont arrêté en Méditerranée un navire suspect, le *Baltic Sky*, qui a fait escale en Turquie avant de revenir en Méditerranée alors qu'il effectuait un voyage Tunis – Soudan, ce qui les a alerté. A son bord, se trouvaient 8 000 détonateurs et quelques 700 tonnes d'explosifs – de l'Anfo⁵⁰ essentiellement –. Selon Georges Anomeritis, ministre grec de la navigation, le manifeste du bateau indiquait qu'il était affrété par une compagnie établie au Soudan mais le code postal de l'adresse à Khartoum ne correspondait à rien. Il a estimé que la puissance explosive potentielle du chargement était comparable à celle d'une bombe atomique, sachant que la plus petite ogive nucléaire de l'arsenal étatsunien a une charge équivalente à 300 tonnes de TNT, mais il dramatise à l'excès la situation selon Michael Richardson⁵¹. De même, en avril 2004, la police italienne a souhaité inspecter au port de Gioia Tauro un conteneur embarqué sur un navire turc à destination de New York. Certaines divergences apparaissaient au niveau des déclarations en douane et il contenait en réalité 8 000 fusils AK 47, 11 mitraillettes ainsi que d'autres marchandises, le tout pour une valeur de plus de sept millions de dollars américains. Le même mois, la douane turque a découvert à Istanbul 500 fusils AK 47 dans un conteneur qui venait juste d'être débarqué d'un navire en provenance de Bulgarie et à destination du Paraguay, d'après les informations portées sur le manifeste.

Mise à part la contrebande, la nature des marchandises qui transitent en Méditerranée représente un péril. Du seul point de vue énergétique, plus de 65 % du pétrole et du gaz naturel consommés en Europe occidentale passent chaque année par la Méditerranée. De plus, la zone compte de nombreux pipelines, les principaux reliant la Libye à l'Italie et le Maroc à l'Espagne. Le Port autonome de Marseille (PAM) est directement concerné de par les trafics qu'il enregistre⁵² et ce d'autant plus qu'il est entouré de raffineries et d'entreprises pétrochimiques. Un incident impliquant un super pétrolier plein et de telles installations raserait la région de la carte.

1.2.2. La situation dans le reste du monde

1.2.2.1. La situation en Asie

1.2.2.1.1. La situation en Asie du Sud-est

Le Sud-est asiatique est a priori la zone la plus sensible à l'heure actuelle, et notamment l'Indonésie. Que ce soit en termes de piraterie ou de terrorisme maritime, ce pays est considéré comme le plus risqué depuis au moins quatre années consécutives. Cette concentration de pirates sur la zone peut s'expliquer par le fort taux de chômage qui affecte l'Indonésie depuis la grave crise financière de 1997 ainsi que par le nombre élevé de groupes « mafieux » sévissant dans les alentours.

⁴⁸ Il est à noter à ce sujet qu'en France, les seules personnes habilitées à procéder à la recherche et à la constatation des infractions dans le domaine du trafic de stupéfiants en mer sont définies à l'article 1 du décret n° 97-545 du 28 mai 1997 modifiant les articles 12 et 16 de la loi n° 94-589 du 15 juillet 1994 relative aux modalités de l'exercice par l'Etat de ses pouvoirs de contrôle en mer.

⁴⁹ Site d'information militaire suisse du nom de CheckPoint:

<http://www.checkpoint-online.ch/CheckPoint/Monde/Mon0072-TerrorismeMaritime.html>

⁵⁰ Explosif à base de nitrate d'ammonium fabriqué dans le commerce et utilisé principalement pour l'exploitation minière.

⁵¹ Site d'information militaire suisse du nom de CheckPoint:

<http://www.checkpoint-online.ch/CheckPoint/Monde/Mon0072-TerrorismeMaritime.html>

⁵² Cf infra 2.4.1 L'exemple du Port Autonome de Marseille, page 60.

Selon les experts de la région⁵³, les LTTE représentent, à l'échelle mondiale, le risque le plus sérieux. Leur chef politique est S.P. Tamilchelvan. Ils auraient, semble-t-il, les moyens humains et matériels d'orchestrer des attaques maritimes. D'une part, ils disposeraient d'au moins deux ou trois navires de commerce battant pavillon de complaisance. Ils les utiliseraient, en dehors des cargaisons légitimes, pour le transport d'armes et d'équipements militaires vers le Pakistan, la Thaïlande ou encore l'Ukraine. D'autre part, les LTTE seraient capables d'organiser des actions militaires aussi bien classiques que non conventionnelles et disposeraient de commandos suicides, les Sea Tigers. Le 10 octobre 2001⁵⁴, quatre embarcations suicides pilotées par des Tigres tamouls percute un petit pétrolier caboteur, le *Silk Pride*, chargé de 160 tonnes de kérosène et de 275 tonnes de diesel dans la péninsule de Jaffna, au Sri Lanka. Sept personnes ont été tuées au total mais, « par chance », les cuves de chargement n'ont pas été endommagées, l'incendie qui a pris à l'arrière a été rapidement maîtrisé et le navire a été escorté par des militaires à destination. Il s'agit là de leur stratégie favorite. L'utilisation principale qui est faite de leur capacité maritime vise des objectifs logistiques de transport d'hommes, armes, explosifs, stupéfiants pour faciliter les opérations terroristes à terre. Ils mettent aussi leurs compétences au service d'autres organisations terroristes ; de fait, en 1995, les LTTE ont permis au groupe Abbu Sayyaf et au Front maure de libération islamique (MILF⁵⁵) de transporter une cargaison d'armes et de munition depuis le Pakistan jusqu'au Sud des Philippines. Une autre de leur caractéristique est de recruter des enfants orphelins pour servir dans leurs rangs ; or, depuis le désastre causé par le tsunami, les enfants qui se retrouvent complètement seuls au monde sont nombreux. La situation est donc préoccupante, ne serait-ce que d'un point de vue humanitaire. Autre élément notable, ils ne semblent visiblement pas prêts à démanteler leur organisation ni à engager un processus de paix avec l'autorité sri lankaise.

Les spécialistes estiment ensuite que des formations terroristes du Moyen-Orient, telle que le Hezbollah, sont également opérationnellement capables de perpétrer des attaques maritimes de grande envergure. Ils envisagent parallèlement que les groupuscules d'origine égyptienne Gama'at Al-Islamiyah⁵⁶ et le Djihad Islamique seraient intéressés par l'acquisition d'une capacité d'attaque maritime. Certains supposent que ces trois formations se préparent ou se soient préparés dans les camps d'entraînement des LTTE. Ils considèrent de même que le *Popular Front for the Liberation of Palestine – General Front*⁵⁷ puisse mettre à la disposition d'autres groupes ses « compétences » maritimes. D'autre part, même si les commandos du Jemaah Islamiya⁵⁸ ont été diminués par les arrestations de leurs têtes pensantes, dont Abu Bakar Bashir et Riduan Isamuddin, ils restent une menace conséquente. Enfin, il existe d'autres formations terroristes actives dans la région, comme Lashkar Jihad, Laskar Jundullah ou encore Rabitatu'l Mujahideen.

⁵³ Site du SAAG : <http://www.saag.org/papers12/paper1154.html>.

⁵⁴ Site du Cèdre (Centre de documentation, de recherche et d'expérimentations sur les pollutions accidentelles des eaux) : <http://www.le-cedre.fr/>.

⁵⁵ Mouvement séparatiste islamiste originaire du Sud des Philippines.

⁵⁶ Ils sont considérés comme les cerveaux des attentats à la bombe perpétrés contre le World Trade Center en 1993.

⁵⁷ Front de Libération de la Palestine.

⁵⁸ Considérés comme la filière régionale en Asie du Sud-est d'Al Qaeda et originaires de Thaïlande, ils sont notamment responsables des attentats à la bombe de Bali, en octobre 2002.

A l'heure actuelle, le problème tangible de l'Asie du Sud-est est la piraterie qui est en augmentation constante⁵⁹. En outre, dans le quatrième rapport du BMI, remis en octobre 2003, il est également suggéré que les rebelles séparatistes du GAM sont à l'origine de la plupart des actes de piraterie aux visées terroristes perpétrées dans le détroit de Malacca ou dans les eaux indonésiennes.

Pour ce qui est du terrorisme pur, l'ISEAS évalue la menace dans la région en deux temps. Du fait de la combinaison entre pirates traditionnels et mouvements extrémistes indigènes sur la zone, il envisage en premier lieu l'éventualité d'attaques suicides dans le détroit de Malacca contre des navires de commerce ou de guerre qui seraient coulés dans l'un des endroits les plus étroits. En effet, il s'agit du détroit le plus fréquenté au monde, constituant ainsi une voie d'eau particulièrement à risques. Il relie le commerce mondial et les principales raffineries de pétrole du Moyen-Orient, d'Asie et d'Europe. Il est le point de passage obligé pour sortir du port de Singapour, deuxième port au monde en termes de trafic, et une route vitale pour l'approvisionnement pétrolier de la Chine – environ 60% des navires qui l'empruntent battent pavillon chinois –. S'étalant sur 500 milles marins en longueur – soit environ 926 km –, le détroit de Malacca est extrêmement étroit, notamment dans la partie Sud-est où la largeur maximum est de 20 milles marins – soit un peu plus de 37 km – pour un minimum de 1,3 milles marins – soit 2,4 km – près de Singapour. Chaque année, c'est plus d'un tiers du commerce mondial qui transite par ce détroit, et notamment la moitié des cargaisons transportées par mer, les deux tiers des échanges mondiaux de gaz naturel liquéfié ainsi que la moitié du ravitaillement mondial en pétrole – soit 10 millions de barils par jour, ce qui équivaut à 13% du ravitaillement planétaire –, ce qui représente entre 50 000 et 330 000 navires⁶⁰. L'interruption des artères commerciales et énergétique du monde serait instantanée en cas d'attaque. L'impact qu'elle causerait ainsi que la dévastation qui s'ensuivrait sont inimaginables.

En second lieu, l'ISEAS considère les détournements comme un risque potentiel du fait que la zone est infestée de pirates. Tony Tan⁶¹ estime, pour sa part, que les terroristes recherchent de tels impacts. Il observe par ailleurs la précision quasi militaire des attaques récemment menées contre des navires de commerce, qui s'enhardissent et deviennent de plus en plus violentes, ce qui lui fait craindre que les pirates ne s'associent ou ne se soient déjà associés avec des terroristes. Ceci résume assez bien l'attaque le 16 janvier 1999 du *Le Chaumont*, pétrolier battant pavillon français d'une capacité de 131 654 tonnes de port en lourd. Alors que, les cales pleines, il traverse le canal Philipp, au large de Singapour dans les eaux indonésiennes, il est assailli par des pirates qui menacent l'officier de quart avec une machette. Ils le font alors naviguer à pleine vitesse durant 70 minutes sans personne à la barre avant de s'enfuir. De même, le détournement, au large de Sumatra, du chimiquier *Dewi Madrim*⁶², en mars 2003, par dix

⁵⁹ Cf supra 1.1.2 La piraterie, page 10.

⁶⁰ Site de Libération : <http://www.liberation.fr/page.php?Article=282361> et de Terrorisme.Net : http://www.terrorisme.net/p/article_136.shtml.

⁶¹ Vice-premier ministre et ministre de la coordination des politiques de défense et de sûreté de Singapour. Site d'information militaire suisse du nom de CheckPoint: <http://www.checkpoint-online.ch/CheckPoint/Monde/Mon0072-TerrorismeMaritime.html>

⁶² Site d'information militaire suisse du nom de CheckPoint: <http://www.checkpoint-online.ch/CheckPoint/Monde/Mon0072-TerrorismeMaritime.html>.

pirates armés de mitraillettes et de machettes, utilisant des radios VHF⁶³ ainsi qu'une vedette pour l'intercepter est une autre illustration parfaite de la situation. Les pirates ne se sont guère préoccupés de rapporter un butin, ils ont détruit la radio de bord, pris la barre et dérouté le navire pendant environ une heure. Ils ont également pris en otage le Capitaine et un officier dans le but supposé d'acquérir le savoir-faire nécessaire à la conduite d'une attaque maritime. En effet, d'après le rapport de la société de conseil en sécurité Aegis Defence Services, basée à Londres, il semblerait qu'ils voulaient apprendre à diriger un navire. Le quotidien *The Economist* a pour sa part vu dans le détournement du *Dewi Madrim* « l'équivalent des pirates de l'air Al Qaeda ayant mené les attaques du 11 septembre après avoir suivi les cours de pilotage en Floride ».

Poursuivant dans cette même optique, l'étude de Aegis Defence Services révèle que le groupe Abbu Sayyaf est soupçonné d'avoir kidnappé un ingénieur de maintenance dans une station balnéaire de Sabah aux Philippines en 2002. Quand il a été relâché en juin 2004, il aurait déclaré que ces ravisseurs savaient qu'il était instructeur de plongée sous-marine et que c'est pour cette raison qu'ils l'auraient enlevé car ils voulaient être formés. Enfin, toujours en 2004, le propriétaire d'une école de plongée de Kuala Lumpur aurait observé qu'un certain nombre de malaisiens de souche voulait se faire enseigner la plongée mais n'était par contre pas du tout intéressé par le fait d'apprendre à décompresser.

Il est un autre aspect à prendre en compte : le manque de ressources financières de certains pays de la zone qui n'ont pas les moyens de se mettre en conformité avec le Code ISPS, ce qui rend la tâche plus aisée pour les pirates ou les terroristes puisque les points sensibles de la navigation internationale restent dépourvus de protection ou, en tout état de cause, moins bien protégés que ce qu'ils ne devraient l'être. L'Indonésie, qui est la nation la plus concernée, est aussi celle qui a subi le plus de critiques pour ne pas donner les moyens suffisants à sa marine et à ses garde-côtes de surveiller convenablement sa partie du détroit de Malacca et d'y faire régner l'ordre. Tant et si bien qu'en juin 2004, le commandant en chef de la marine indonésienne envisageait de donner l'ordre de tirer à vue pour tuer les pirates et terroristes présents dans ses eaux.

1.2.2.1.2. La situation en Inde

Un incident majeur est survenu en Inde le 2 avril 2004 quand une cargaison de 150 lance-rockets accompagnés de 840 rockets, de près d'un million de munitions en tout genre, de 2 000 lance-grenades, de 25 000 grenades et de plus de 1 700 fusils d'assaut a été interceptée par les autorités locales après avoir été transportée clandestinement par mer au Bangladesh. Selon les experts mandatés sur place, cette découverte aurait pu servir à armer deux bataillons d'infanterie. Toutefois, il a été impossible pour la communauté internationale de découvrir les expéditeurs de ce chargement. M. Raman⁶⁴ estime que les difficultés majeures du pays viennent du fait que le Bangladesh se montre réticent pour agir contre le terrorisme maritime, voire qu'il permettrait à certains individus malfaisants de s'échapper du Pakistan par la mer pour rejoindre des camps terroristes.

⁶³ Bande de fréquences comprises entre 156 et 174 MHz. Informations obtenues lors d'un stage au CROSS La Garde en avril 2005.

⁶⁴ Site du SAAG : <http://www.saag.org/papers12/paper1154.html>.

La seconde source d'inquiétude concerne Dawood Ibrahim et son organisation. De par leurs diverses actions terroristes, actes de désobéissance civile et incitation aux émeutes, ils sont une menace constante pour le gouvernement hindou. Ils sont par ailleurs officiellement recherchés par les USA depuis le 16 octobre 2003 ; en effet, l'équivalent étatsunien du ministère de l'économie et des finances a émis l'ordre 13224 et a demandé aux Nations Unies de considérer Dawood Ibrahim comme un terroriste international afin de geler ses actifs aux USA et d'empêcher toute transaction avec des ressortissants étatsuniens grâce à la résolution n°1373. Son but est d'identifier et d'anéantir les ressources financières qui relient l'économie souterraine et le terrorisme.

1.2.2.2. La situation en Australie⁶⁵

L'ampleur de la menace dans ce pays dépend en partie des déploiements militaires australiens au niveau mondial – notamment en Irak – qui font craindre des représailles. D'autre part, le voisinage immédiat de l'Australie avec l'Asie du Sud-est rend la menace plus tangible du fait de l'augmentation de la piraterie dans les eaux du Sud-est asiatique mais également de par les échanges privilégiés qu'à l'Australie avec cette zone. Le commerce avec le Sud-est asiatique excédait, en 2004, les 40 milliards de dollars australiens par an, soit quelques 31 milliards de dollars américains. Par ailleurs, Singapour, l'Indonésie, la Thaïlande et la Malaisie figuraient parmi les 15 premières destinations des exportations australiennes. Une attaque terroriste économique dans la région affecterait inmanquablement ces deux zones.

Enfin, il ne faut pas oublier la particularité de la géographie australienne elle-même. En tant qu'île, elle est cernée par les eaux et compte 37 000 km de côtes, soit un littoral parmi les plus étendus de la planète et donc particulièrement difficile à protéger. Lors du séminaire sur le contre-terrorisme maritime organisé à New Delhi, en Inde les 29 et 30 novembre 2004, Aldo Borgu⁶⁶, a fait état des éléments qui rendent le secteur maritime primordial pour l'économie australienne. Le pays compte 70 ports commerciaux majeurs, 300 installations portuaires distinctes et sa Zone Economique Exclusive (ZEE) s'étend sur 16 millions de km². Environ 3 000 navires impliqués dans le commerce international et côtier escalent dans les ports australiens chaque année, soit plus de 21 000 touchés au total. Pour l'année 2000/2001, la part des exportations australiennes transportées par mer, en valeur, a représenté 83% du volume total des exportations nationales. Par ailleurs, la part du total des échanges réalisés par mer était de 77%. Le port de Melbourne génère chaque année 70 milliards de dollars australiens de par son activité commerciale, soit environ 54 milliards de dollars américains, et 20 000 emplois ; le port de Sydney, quant à lui, représente 45,5 milliards de dollars australiens, soit près de 35 milliards de dollars américains, et 17 000 emplois.

Enfin, d'après une étude conduite par les services de renseignement australiens, il est plus probable que les navires soient la cible de l'attaque plutôt que le moyen d'attaquer, ce qui explique pourquoi les mesures de sûreté à bord ont été renforcées. Par ailleurs, les autorités

⁶⁵ Site de l'Institut australien de politique stratégique (ASPI), qui est un organisme indépendant créé par le gouvernement australien: http://www.aspi.org.au/pdf/Maritime_terrorism%20India_AB.pdf.

⁶⁶ Au sein de l'ASPI, Aldo Borgu est responsable du développement et de la gestion des programmes de recherche en matière d'opérations militaires, de moyens de défense, de terrorisme et d'antiterrorisme.

australien estiment que les infrastructures pétrolières offshore seraient une cible privilégiée sur leur territoire de par le symbolisme politique qu'elles renferment.

1.2.2.3. La situation au Canada⁶⁷

Le secteur maritime est primordial au Canada. En effet, le pays compte environ 200 000 km de littoral. Son système maritime s'étend sur 200 milles marins au large du littoral, soit plus de 370 km, et s'avance sur plus de 3 700 km à l'intérieur du continent grâce au réseau des Grands Lacs et de la Voie Maritime du Saint-Laurent (VMSL). Chaque année plus de 1,5 millions de croisiéristes – essentiellement en provenance des USA – et près de 3,5 millions de conteneurs à destination de toute l'Amérique du Nord transitent par les 250 ports canadiens. Le pays dispose, en plus, de 10 terminaux internationaux, 19 interprovinciaux et près de 300 intraprovinciaux dédiés aux traversiers, sorte de ferrys. En 2001, les traversiers canadiens ont notamment transporté quelques 40 millions de passagers et 17 millions de véhicules.

En 2000, la valeur des échanges commerciaux maritimes du Canada, au niveau mondial, atteignait environ 100 milliards de dollars canadiens, soit quelques 82 millions de dollars américains, pour un volume total de 740 milliards de dollars canadiens, soit plus de 608 millions de dollars américains. L'industrie maritime emploie directement plus de 30 000 personnes et génère des revenus annuels moyens de 2,6 milliards de dollars canadien, soit environ 2,1 milliards de dollars américains. Enfin, en sus de la position stratégique qu'occupe l'industrie du transport maritime au Canada, la menace pour ce pays vient de sa proximité immédiate avec les USA.

1.2.2.4. La situation en Turquie⁶⁸

Le détroit du Bosphore, dans la Mer Noire, qui s'étale sur 17 milles marins en longueur – soit presque 32 km – est un point sensible pour le commerce maritime. Plusieurs milliers de pétroliers et autres navires le traversent chaque année avec à leur bord du pétrole brut, du gaz naturel liquéfié ainsi que d'autres produits industriels chimiques, sans compter les 20 000 tonnes de déchets radioactifs qui doivent transiter par le détroit sur 10 ans d'après une loi votée par la Douma russe en 2001. De plus, d'ici 2010, le nombre de navires empruntant cette route maritime devrait augmenter de 50%. Il est à noter que le détroit du Bosphore a un ratio de six accidents pour un million de milles marins parcourus, soit 9,5 accidents par kilomètre ; ce taux d'accident correspond au double de celui du canal de Suez. La situation est d'autant plus préoccupante que le Bosphore traverse Istanbul, à savoir une métropole de plus de 16 millions d'habitants. C'est la raison pour laquelle la Turquie a introduit de nouveaux contrôles, en particulier sur les pétroliers, consistant entre autre en un système électronique d'information et de gestion quant au trafic maritime⁶⁹.

L'autre problème de la Turquie est la contrebande d'armes et de stupéfiants ainsi que le trafic d'êtres humains par mer. Ce pays a été et reste historiquement un point de transbordement

⁶⁷ Site du ministère des transports canadien, Transports Canada : <http://www.tc.gc.ca/vigilance/spu/maritime/rehaussement/systeme.htm>.

⁶⁸ Site de l'*Institute for the Analysis of Global Security* (IAGS, Institut d'analyses sur la sûreté internationale) : <http://www.iags.org/n0124051.htm>

⁶⁹ *Vessel Traffic Management and Information System* (VTMIS).

clé du fait de sa position géographique qui lui permet de relier l'Europe et l'Asie. Depuis le milieu des années 80, une nouvelle tendance est apparue : des organisations terroristes ayant des revendications plutôt politiques ont commencé à s'associer au trafic de stupéfiants pour financer leurs achats d'armes, en tout cas au départ, c'est ce qui s'appelle le narco-terrorisme.

1.3. Les objectifs principaux

Comme évoqué précédemment, le but premier, à l'heure actuelle, est de commettre des actes de terrorisme maritime économique afin de perturber le bon fonctionnement du commerce mondial. Ceci est l'apanage de tout terroriste, qu'il appartienne à une organisation terroriste de type idéologique, ethnique, religieux, ou sectaire et les exemples terrestres ne manquent pas⁷⁰. La motivation essentielle est d'ébranler l'économie internationale en faisant souffler un vent de panique sur le marché boursier. Sur le plan maritime, seule une attaque menée contre un des centre nerveux du trafic maritime pourrait avoir un tel écho, à savoir, les ports, le détroit de Malacca, le détroit d'Hormuz – aux alentours de l'Iran et d'Oman –, Bab el-Mandab – au large du Yémen et de la corne de l'Afrique –, le détroit du Bosphore en Turquie, le détroit de Gibraltar – entre le Maroc et l'Espagne –, le Canal de Suez et le Canal de Panama car la densité de navires dans ces points d'étranglement principaux est très élevée.

Pour ce qui est d'une frappe en pleine mer, l'effet serait moindre et de toute façon, l'opération serait quasiment impossible à réaliser selon l'Amiral Sir Alan West. Cependant, l'intérêt d'un tel acte serait l'impact psychologique qu'il ne manquerait pas de produire au sein du secteur industriel ou parmi les Etats du monde entier et pas seulement ceux qui ont été visés, ainsi que la réaction en chaîne qu'il ne manquerait pas de provoquer.

Olivier Halloui, responsable du département sûreté maritime de Secopex⁷¹, estime que « le ratio faisabilité/dommages infligés est nettement en faveur d'une opération terroriste ». En effet, « en engageant de faibles moyens, (...) [les] résultats [peuvent être] effroyables » ; par le biais d'une vulgaire petite vedette, un super pétrolier peut en effet être gravement endommagé et sa cargaison exploser. Il convient de noter que la menace pèse aussi bien sur les navires de commerce ou à passagers que sur les bâtiments de guerre puisque le but est de faire un maximum de dégâts. En 2003, 22% des navires attaqués étaient des pétroliers.

Les terroristes recherchent des pertes en vie humaines monstrueuses, des dégâts massifs au niveau matériel et environnemental ; leur but est que leur action soit le plus spectaculaire possible. Ils se livrent à une véritable bataille psychologique et entretiennent un climat de peur permanent. Il s'agit de terrorisme global, qui, pour Jürgen Habermas⁷², « porte les traits anarchistes d'une révolte impuissante en ce qu'il est dirigé contre un ennemi qui, dans les termes

⁷⁰ Prise d'otage de représentants de l'Organisation des pays exportateurs de pétrole (OPEP) en 1975 par un groupe terroriste dirigé par Ilich Ramírez Sánchez, dit Carlos, un terroriste international ; explosions dans le quartier financier de Londres dues à l'Armée républicaine irlandaise (IRA) dans les années 80 ; attentats à l'explosifs au World Trade Center à New York le 26 février 1993 ; explosions simultanées à Bombay contre des cibles économiques, dont la Bourse, en mars 1993 ; explosions à Bali et Mombasa en 2002 ; attaques contre des experts étrangers travaillant pour l'industrie pétrolière en Arabie Saoudite en 2004 ; explosions dans la région du Sinaï, en Egypte, contre des touristes israéliens en 2004 également et contre l'industrie touristique globale le 23 juillet 2005. La liste n'est malheureusement pas exhaustive.

⁷¹ Société de sûreté maritime reconnue organisme de sûreté maritime depuis février 2005.

⁷² Philosophe et sociologue allemand, lors d'un entretien avec la journaliste Giovanna Borradori paru dans le Monde Diplomatique de février 2004, page 17 : <http://www.monde-diplomatique.fr/2004/02/HABERMAS/11007>.

pragmatiques d'une action obéissant à une finalité, ne peut absolument pas être vaincu. Le seul effet possible est d'instaurer dans la population et auprès des gouvernements un sentiment de choc et d'inquiétude ».

II La mise en application au quotidien

Le Code ISPS s'applique aux navires effectuant des voyages internationaux et qui rentrent dans les catégories suivantes: navires à passagers, dont les engins à grande vitesse à passagers, navires de charge, dont les engins à grande vitesse à cargaisons, d'une jauge brute égale ou supérieure à 500 tonneaux, unités de forage mobiles au large. Il s'applique de même aux installations portuaires desservant ces types de navires (section A/3.1 du Code ISPS). Par contre, il ne s'applique ni aux navires de guerre, ni aux navires de guerre auxiliaires, ni aux navires appartenant ou exploités par un gouvernement contractant et affectés exclusivement à un service public non commercial (section A/3.3 du code ISPS).

Ce Code établit le cadre d'une coopération internationale par le biais de mesures qui ne sont que des prescriptions techniques dont le but est de prévenir des actes de malveillance et non pas d'agir. En effet, l'action est un domaine totalement distinct en termes de responsabilité, de compétence, d'organisation administrative, de procédures opérationnelles et de techniques⁷³. Il existe bien évidemment des liens entre les deux domaines mais il faut établir une distinction nette et précise. De même, l'ISPS ne doit pas être confondue avec la surveillance en mer dans sa globalité puisque celle-ci dépend, en France par exemple, de la marine nationale⁷⁴ et de la douane.

Il est un autre point à noter : le Code parle d'installations portuaires⁷⁵ et non pas de ports, c'est-à-dire de terminaux, si bien que la charge de travail en a été considérablement augmenté. Enfin, le Code ISPS est directement inspiré de la législation étatsunienne et notamment du *Maritime Transportation Security Act (MTSA)*⁷⁶ du 25 novembre 2002 qui impose des règles encore plus strictes.

2.1 Les textes complémentaires en matière de sûreté du transport maritime

Il est à noter que la législation maritime en matière d'actes criminels est très ancienne puisque des ordonnances et textes de loi traitant du sujet remontent notamment à 1584, 1650, 1691, 1718, 1799 et 1825. Plus récemment, la Convention internationale sur la haute mer, conçue à Genève le 29 avril 1958 et celle sur le droit de la mer de Montego Bay de 1982,

⁷³ La question a été discutée avec Bruno Célérier, administrateur en chef de 1^{ère} classe, chef de la division de l'action de l'Etat en mer, lors d'un entretien à la Préfecture maritime de Toulon le mercredi 22 juin 2005.

⁷⁴ Il est à noter que l'organisation générale de la marine nationale a été fixée par le décret n° 91-671 du 14 juillet 1991.

⁷⁵ « (...) emplacement (...) où a lieu une interface navire/port. Elle comprend les zones telles que les zones de mouillage, les postes d'attente et leurs abords à partir de la mer » (règle XI-2/1.1.9 de la Convention SOLAS). Pour la France, la limite a été établie à 25m du côté mer et idem du côté terre.

⁷⁶ Loi sur la sûreté du transport maritime aux Etats-Unis.

harmonisent les règles nationales et coordonne l'action des Etats signataires, dont la France, en matière de lutte contre la piraterie (respectivement articles 14 et 100⁷⁷).

La lutte contre le terrorisme est devenue depuis quelques années une préoccupation majeure au niveau international. L'Union européenne s'est penchée sur la question à plusieurs reprises⁷⁸ car⁷⁹ plus de 90% de ses échanges extérieurs transitent par mer pour 40% de l'ensemble de ses échanges économiques, plus d'un milliard de tonnes de marchandises touchent ses ports, un tiers de la flotte mondiale appartient à des compagnies maritimes européennes et le secteur maritime emploie plus de 2,5 millions de personnes. Quant aux Nations Unies, elles ont déjà réalisé un nombre considérable de conventions internationales spécifiquement dédiées à ce fléau⁸⁰. Même s'il est vrai que beaucoup sont dédiées au secteur aérien, il n'en reste pas moins que certaines règles peuvent en être reprises, ou au moins servir de base de réflexion. Il existe par ailleurs des conventions internationales qui ne concernent que l'environnement maritime, notamment la Convention pour la répression des actes illicites contre la sécurité de la navigation maritime conclue à Rome le 10 mars 1988, dite Convention SUA⁸¹.

Par ailleurs, la résolution A.584 de l'Assemblée du 20 novembre 1985 a permis au MSC d'établir des mesures techniques pratiques et détaillées de sûreté pour les passagers et les équipages en s'inspirant des travaux de l'OACI⁸². Puis la circulaire MSC/Circ. 443 du 26 septembre 1986 a introduit, pour la première fois, l'élaboration de plans de sûreté pour les navires et les installations portuaires ainsi que la désignation d'officiers de sûreté. Enfin, la circulaire MSC/Circ. 754 du 5 juillet 1996 a étendu le champ d'application du texte précédent aux transbordeurs à passagers.

2.1.1. La législation française

Au niveau purement national, il existait déjà des dispositions légales en matière de sûreté maritime et portuaire bien avant le Code ISPS. Elles sont notamment présentes dans le Livre III du Code des ports maritimes (articles L. 323-5 et R. 324-1 à R. 324.5), ou encore dans le décret n° 97-1162 du 17 décembre 1997, relatif à la sûreté des transports maritimes et des opérations portuaires qui s'y rattachent. De même, la directive relative à la vigilance maritime du 12 février 1998 et l'arrêté du 14 mai 1999, qui institue le comité national de sûreté du transport et des

⁷⁷ Les deux articles sont quasiment identiques : « Tous les Etats doivent coopérer dans toute la mesure du possible à la répression de la piraterie en haute mer ou en tout autre endroit ne relevant de la juridiction d'aucun Etat » (article 14). « Tous les Etats coopèrent dans toute la mesure du possible à la répression de la piraterie en haute mer ou en tout autre lieu ne relevant de la juridiction d'aucun Etat » (article 100).

⁷⁸ L'antiterrorisme, en Europe, passe par la Convention européenne pour la répression du terrorisme, signée à Strasbourg le 27 janvier 1977 et par la déclaration JAI sur la lutte antiterroriste du Conseil Justice et affaires Intérieures. Adoptée lors du Conseil européen du 25 mars 2004, elle prône, entre autre, la solidarité, l'assistance aux victimes, la coopération et le renforcement des contrôles. Site du gouvernement luxembourgeois : http://www.gouvernement.lu/salle_presse/actualite/2004/03/25somet/.

⁷⁹ Site de l'Institut d'études internationales de Montréal : <http://www.er.uqam.ca/nobel/cepes/pdf/BULL71.pdf>.

⁸⁰ Convention contre la prise d'otages de New York du 17 décembre 1979 ; Convention internationale pour la répression des attentats terroristes à l'explosif du 12 janvier 1998.

⁸¹ *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*. Ce texte donne à l'Etat du pavillon une compétence exclusive pour intervenir en haute mer afin de poursuivre des terroristes, des pirates ou des criminels maritimes. Il est entré en vigueur le 1^{er} mars 1992, le même jour qu'un protocole de l'ONU applicable, lui, aux plates-formes fixes localisées sur un plateau continental. BOISSON Philippe, *La sûreté des navires et la prévention des actes de terrorisme dan le domaine maritime*, DMF n° 640, p. 723, septembre 2003.

⁸² Organisation Internationale de l'Aviation Civile.

ports maritimes⁸³ et les comités locaux de sûreté portuaire⁸⁴, traitent de la question. Puis les autorités françaises ont rédigés des textes suite à l'avènement du Code ISPS.

2.1.1.1. Les arrêtés

Le premier arrêté ⁸⁵, du 5 décembre 2003, fixe les conditions de délivrance de l'attestation de formation d'agent de sûreté de navire (SSO) en France pour former du personnel répondant aux exigences de la section A/12.2 du Code ISPS. Il convient, entre autre, d'avoir suivi une formation dans un centre de formation agréé⁸⁶ dispensant le programme détaillé en annexe du présent arrêté et d'avoir réussi le contrôle des connaissances attendant. Les cours, répartis sur 21 heures minimum, incluent trois modules de prévention des actes illicites, un module de sûreté portuaire, un module sur les responsabilités des parties impliquées dans l'ISPS, un module SOLAS/ISPS, un module sûreté du navire, un module sur le plan de sûreté du navire, un module sur la gestion de foule, un module sur le matériel de sûreté ainsi qu'un module sur la formation de l'équipage pour les exercices et pour s'assurer que chacun comprend ses responsabilités à bord.

Le deuxième arrêté ⁸⁷, qui date du même jour, fixe les conditions de délivrance de l'attestation de formation d'agent de sûreté de la compagnie (CSO) en France pour former du personnel répondant aux exigences de la section A/11.2 du Code ISPS. Les conditions d'obtention sont les mêmes sauf que la durée de la formation est de 32 heures. Le contenu des cours reste sensiblement le même si ce n'est les techniques de formation du personnel à terre.

Le troisième arrêté ⁸⁸, en date du 17 juin 2004, fixe les conditions de délivrance de l'attestation de formation d'agent de sûreté de l'installation portuaire (PFSO) en France pour former du personnel répondant aux exigences de la section A/17.2 du Code ISPS. Les conditions d'obtention sont de nouveau les mêmes, le volume horaire de la formation est de 32 heures, comme pour les CSO, seul le contenu des cours varie. La formation contient un module sur les objectifs de la sûreté et la réglementation, un module de méthodologie de l'évaluation de la menace et de sensibilisation aux risques, un module de prévention des actes illicites, un module consacré aux navires, un module sur les PFSP et un module de gestion de crise.

Le quatrième arrêté⁸⁹, du 25 juin 2004, porte sur la reconnaissance des organismes de sûreté maritime (RSO) et crée une commission consultative de reconnaissance. Il est à noter que c'est le « ministère chargé de la mer » qui accorde les reconnaissances pour deux ans aux organismes qui en ont fait la demande – en précisant dans quel domaine ils veulent exercer leur

⁸³ Il a en charge l'application des conventions et accords internationaux ainsi que des mesures législatives et réglementaires, coordonne et oriente l'action des comités locaux et peut proposer toute mesure de sûreté (article 3).

⁸⁴ Ils ont un rôle consultatif auprès du préfet de département, ils peuvent proposer exceptionnellement des mesures spécifiques temporaires et ils examinent les tâches entre les organismes qui ont des responsabilités en matière de sûreté (article 5).

⁸⁵ Publié au JO n° 9 du 11 janvier 2004, page 918, texte n°10. Site de Legifrance : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=635985&indice=10&table=JORF&ligneDeb=1>.

⁸⁶ Dans la pratique, il s'agit des ENMM ou de sociétés privées.

⁸⁷ Publié au JO n° 9 du 11 janvier 2004, page 920, texte n° 11. Site de Legifrance : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=635986&indice=11&table=JORF&ligneDeb=1>.

⁸⁸ Publié au JO n° 183 du 8 août 2004, page 14155 texte n°8. Site de l'ancien ministère des transports : <http://www2.equipement.gouv.fr/bulletinofficiel/fiches/BO200415/A0150008.htm>.

⁸⁹ Publié au JO n° 179 du 4 août 2004 page 13879 texte n°22. <http://www2.equipement.gouv.fr/bulletinofficiel/fiches/BO200415/A0150011.htm>.

compétence (terminaux à passagers, à conteneurs, à produit pétroliers, etc – (article 4) et qui répondent aux critères de base – en termes de formation, d'expérience et de compétences en matière de sûreté – (annexe I de l'arrêté, article 2.3). Chaque RSO doit ensuite émettre un rapport d'activité annuel.

Enfin, le cinquième arrêté ⁹⁰, en date du 16 décembre 2004, établit la liste des sept premiers RSO reconnus par le ministère des transports, de l'équipement, du tourisme et de la mer, et ce en application de l'arrêté précédent.

2.1.1.2. Les circulaires conjointes de la DTMPL⁹¹ et du HFD

Mer⁹²

La circulaire n° 922⁹³ du 19 décembre 2003 met en œuvre des mesures de renforcement de la sûreté des installations portuaires. Elle vise en premier lieu la corrélation nécessaire entre les prescriptions du Code ISPS et les mesures nationales déjà en vigueur, telle que le plan Vigipirate⁹⁴ ou les autres plans de sûreté déjà en vigueur dans les ports depuis les instructions n°3800⁹⁵ et n°4600⁹⁶ du Secrétariat Général de la Défense Nationale (SGDN) ainsi que la directive ministérielle de vigilance maritime DTMPL/PM-DN-FC/DM du 12 février 1998. En second lieu, la circulaire n° 922 est consacrée à la première phase de mise en œuvre des mesures ISPS en identifiant les installations portuaires concernées⁹⁷, en désignant les PFSO puis en engageant des PFSA.

La circulaire n° 323⁹⁸, en date du 29 mars 2004, fait suite à la précédente en précisant certaines modalités d'exécution. Elle donne, en plus, des instructions pour « permettre la pleine application » des mesures de sûreté ISPS au niveau des installations portuaires, pour ce qui est de l'élaboration et de l'approbation des PFSP qui sont établis par les PFSO. La circulaire n°323 fournit donc un plan type – il s'agit d'un document protégé –, donne des conseils quant aux équipements à mettre en place, explicite la formation que doit recevoir le personnel de l'installation et précise le statut de confidentialité ou non des documents de sûreté portuaire, une fois arrêté par le préfet. Les documents en question sont notamment le PFSA, le PFSP, les déclarations de sûreté (DoS)⁹⁹ ainsi que le registre de sûreté de l'installation portuaire, qui sont à

⁹⁰ Publié au JO n° 2 du 4 janvier 2005 page 194 texte n°28. Site de Legifrance :

<http://www.legifrance.gouv.fr/WAspad/Visu?cid=716578&indice=23&table=JORF&ligneDeb=1>.

⁹¹ Direction du Transport Maritime, des Ports et du Littoral.

⁹² Haut Fonctionnaire de Défense Mer ; depuis le décret n° 2005-471 du 16 mai 2005 qui fixe l'organisation de l'administration centrale du ministère de l'équipement, des transports, de l'aménagement du territoire, du tourisme et de la mer, il s'agit du Haut Fonctionnaire de Défense du ministère des transports et il a un adjoint mer.

⁹³ Site de Secopex : http://www.isps.fr/regle_france/922DTMPL.doc.

⁹⁴ Plan gouvernemental créé en 1978 sous la présidence de Valéry Giscard d'Estaing suite à une vague d'attentats en Europe. Ce dispositif de sécurité visant à prévenir les menaces ou à réagir en cas d'actions terroristes a été remanié à trois reprises : en juin 1995, en juin 2000 et en mars 2003. Il est à noter que le 7 juillet 2005 à 13h00, la France est passée en niveau d'alerte Vigipirate rouge suite aux attentats du métro londonien. Site Wikipédia : <http://fr.wikipedia.org/wiki/Vigipirate>.

⁹⁵ Instruction du 15 mars 1984 sur la sûreté et la sécurité des ports maritimes de commerce.

⁹⁶ Instruction du 8 février 1993 sur la sécurité des points et réseaux sensibles.

⁹⁷ Il faut ensuite remplir la fiche OMI de renseignements, pour informer l'organisation sur les installations portuaires concernées par les mesures de sûreté ISPS.

⁹⁸ Site de Secopex : http://www.isps.fr/regle_france/323DTMPL.doc.

⁹⁹ La DoS est définie comme un « accord conclu entre un navire et soit une installation portuaire soit un autre navire avec laquelle ou lequel une interface se produit et spécifiant les mesures de sûreté que chacun appliquera » par la règle 1.1.15 du chapitre XI-2 de la Convention SOLAS (soit règle XI-2/1.1.15) et est explicitée par la section A/5 du Code ISPS.

protéger soigneusement. Il est à noter que le Code ISPS ne rend que le registre à bord du navire obligatoire (section A/10) mais n'aborde pas la question pour les installations portuaires. Par contre, la circulaire n° 323 subordonne l'approbation du PFSP à ce document et le calque sur celui du navire¹⁰⁰.

2.1.1.3. Le décret 2004-290 du 26 mars 2004¹⁰¹

Ce décret ratifie et publie les amendements à l'annexe à la Convention SOLAS de 1974 et le un code international pour la sûreté des navires et des installations portuaires, dit code ISPS.

2.1.1.4. L'instruction n° 412

Ce texte, provenant du SG Mer¹⁰² sur demande du Premier ministre, est daté du 28 juin 2004. Il concerne les « échanges d'informations avec les navires ayant l'intention d'entrer dans un port, ou avec les navires exploités dans les eaux territoriales ou y entrant [ainsi que le] contrôle des navires dans un port ou dans les eaux territoriales ¹⁰³ ». Parallèlement à cela, il définit la responsabilité de chacun des intervenants.

Le système explicité dans cette instruction est basé sur la détermination préalable à l'entrée dans le port du « degré de dangerosité du navire attendu ». Les premiers en contact physique avec le navire sont les pilotes maritimes qui doivent être sensibilisés à « la détection d'anomalies » de façon à en avertir immédiatement les autorités de police portuaire¹⁰⁴. Il est à noter que cette instruction précise clairement que, à moins que l'autorité de police portuaire n'ait la certitude que le navire « présente un danger immédiat dans le port », elle devra l'accueillir dans le port « même s'il n'est pas parfaitement conforme aux normes ISPS ». Dans ce cas, elle pourra lui délivrer un avertissement et demander une DoS et/ou faire inspecter le navire à quai. Ce n'est qu'après trois avertissements que le refus d'accès au port peut être envisagé.

2.1.1.5. L'instruction n° 413

Cette instruction émane du SG Mer et du Premier ministre. En date du 20 juin 2004, elle a été corrigée une première fois le 4 avril 2005. Elle explicite l'organisation de l'administration française en cas d'alerte de sûreté émise par un navire. En effet, elle traite de la « transmission des alertes sur la sûreté des navires et [des] échanges d'informations relatives à la sûreté entre les navires et les organismes à terre ». Cette instruction se réfère donc à la règle XI-2/6 de la Convention SOLAS relative au système d'alerte du navire (SSAS). Cette règle définit un schéma spécifique de transmission dans lequel ce sont les autorités du pavillon du navire concerné qui sont directement prévenues. Par contre, dans le cadre du signalement d'une détresse maritime, la règle veut que ce soit l'organisme compétent le plus proche de la zone où a eu lieu l'incident qui

¹⁰⁰ Il doit, entre autre, répertorier les incidents ou infractions aux mesures de sûreté ainsi que les changements de niveau de sûreté et des détails sur les exercices, la formation, l'entretien du matériel de sûreté, les audits internes ou externes, les modifications apportées au PFSP.

¹⁰¹ Publié au JO n°75 du 28 mars 2004, pages 5955 texte n°5. Site de Legifrance : <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=MAEJ0430019D>.

¹⁰² Secrétariat général de la mer. Cf infra 2.2.2 Au niveau local, page 49.

¹⁰³ Cf Annexe III : Les autorités impliquées dans le contrôle du navire au port.

¹⁰⁴ Autorité en charge de l'exercice de la police portuaire dans le port, dans les conditions prévues par le livre III du Code des ports maritimes. En pratique, il s'agit de la Capitainerie.

soit informé. Il convient d'observer que l'instruction n° 413 admet, dans l'urgence, de transmettre des informations relatives aux alertes de sûreté par téléphone mais il est impératif de « doubl[er ces communications téléphoniques] de messages écrits, dans les meilleurs délais ».

Ce texte prévoit également d'effectuer deux exercices par an pour mettre en pratique cette instruction, dont un qui doit être jumelé avec l'exercice de mise en oeuvre de Pirate-mer¹⁰⁵. Enfin, l'instruction n° 413 s'accompagne de 11 fiches définissant les autorités compétentes dans la transmission de l'alerte ainsi que leur éventuelle responsabilité en fonction du type de navire source. La fiche n°1 concerne l'alerte émanant d'un navire français en mer par le SSAS. La fiche n°2 traite de l'alerte émanant d'un navire français à la mer, par un moyen autre que le SSAS, et reçue par un CROSS¹⁰⁶ ou par un centre équivalent outre-mer. La fiche n°3 s'intéresse à l'alerte émanant d'un navire français en mer, par un moyen autre que le SSAS, et reçue par un centre étranger. La fiche n°4 correspond à un navire étranger, en mer, ayant émis une alerte par le SSAS. La fiche n°5 explicite le cas d'un navire étranger, en mer, ayant lancé une alerte émise par un moyen autre que le SSAS et reçue par un CROSS ou par un centre équivalent outre-mer. La fiche n°6 s'applique pour les navires français se trouvant dans un port français, en amont des limites de la responsabilité du REMAR¹⁰⁷ ou du DG/COMAR¹⁰⁸ outre-mer. La fiche n°7 se rapporte au navire étranger se trouvant dans un port français, en amont des limites de la zone de responsabilité du REMAR ou du DG/COMAR outre-mer. La fiche n°8 vise le navire français situé dans un port étranger ayant émis une alerte par le SSAS. Le navire français, situé dans un port étranger, ayant émis une alerte par un moyen autre que le SSAS dépend de la fiche n°9. La fiche n°10 porte sur le navire battant pavillon français ou étranger, non directement agressé, mais qui pressent un risque de menace alors qu'il se trouve en mer territoriale française, et ce en application de la convention SOLAS, règle XI-2/7.2 relative aux menaces contre les navires. Enfin, la fiche n° 11 considère l'information des navires français et étrangers, présents en mer territoriale française ou ayant fait part de leur intention d'y entrer, sur les menaces contre les navires et le niveau de sûreté adopté, d'après la règle XI-2/7 de la Convention SOLAS. Au niveau de sûreté 1¹⁰⁹, il n'est pas nécessaire de diffuser l'information vers les navires. Les préfets de département renseignent les capitaineries au sujet des niveaux de sûreté du port et celles-ci en

¹⁰⁵ Il s'agit d'une déclinaison du plan Vigipirate. Ce plan gouvernemental d'intervention spécialisé sert à réagir en cas d'actes de terrorisme maritime avérés et identifie notamment les autorités chargées de l'intervention.

¹⁰⁶ Centre Régional Opérationnel de Surveillance et de Sauvetage. Il est à noter qu'il en existe sept au total : le CROSS Corsen, le CROSS Etel, le CROSS Fort-de-France, le CROSS Gris Nez, le CROSS Jobourg, le CROSS La Garde et le CROSS La Réunion. Les CROSS ont une copie des SSP de tous les ferries réguliers de leur zone et ils utilisent quotidiennement TRAFIC 2000. Ce système, mis au point par la direction des AFFMAR (affaires maritimes), permet un suivi des navires de commerce au large des côtes françaises. Il fournit, entre autre, le n°OMI du navire, son n° d'immatriculation, son nom, son pavillon, le nom de son propriétaire et/ou de son gérant, des détails sur sa cargaison et sur ses caractéristiques propres, son n°MMSI (*Maritime Mobile Service Identity* ou Identité du service mobile maritime), le nom de sa société de classification, le nom de son P&I club, les visites relatives au Memorandum (MOU), etc. Les informations collectées sont primordiales pour les CROSS et les capitaineries de ports qui en seront très prochainement équipés si ce n'est déjà fait (informations obtenues lors du stage au CROSSMED en avril 2005). TRAFIC 2000, qui s'intègre dans le programme de la marine nationale SPATIONAV, fait suite à la directive 2002/59/CE du 27 juin 2002 sur la mise en place d'un système communautaire de suivi du trafic maritime et d'information. Site du ministère des transports, de l'équipement, du tourisme et de la mer : http://www.mer.equipement.gouv.fr/securite/03_navigation/02_cross/trafic2000.pdf.

¹⁰⁷ Préfet maritime. Cf infra 2.2.2 Au niveau local, page 49.

¹⁰⁸ Binôme constitué, outre-mer, par le Délégué du Gouvernement pour l'action de l'Etat en mer – institué par le décret n° 79-413 du 25 mai 1979 modifié par le décret n° 91-1249 du 11 décembre 1991 –, assisté du Commandant de la Marine.

¹⁰⁹ Il est à noter que, en France, il faut faire concorder les trois niveaux de sûreté avec les quatre niveaux du plan Vigipirate : jaune, orange, rouge et écarlate.

informent les navires à destination de leur port. Pour les navires restant en mer territoriale, le SG Mer et le SGDN communiquent aux préfets maritimes les niveaux de sûreté applicables et ce sont les coordonnateurs nationaux délégués (CND) qui diffusent l'information via « l'information nautique¹¹⁰ [émise] sous forme d'AVURNAV¹¹¹ ou de NAVAREA¹¹² ».

Il est à noter de façon générale que la transmission de l'alerte implique, à peu de choses près, toujours les mêmes intervenants¹¹³, si ce n'est pour les navires étrangers, auquel cas les autorités du pavillon concerné sont impliquées en plus des autorités françaises.

2.1.1.6. Les ordonnances

L'ordonnance n° 2004-691 du 12 juillet 2004¹¹⁴ établit des dispositions d'adaptation au droit communautaire dans le domaine des transports maritime, aérien et ferroviaire. Elle modifie le Code des ports maritimes, le Code du travail maritime, le Code de l'aviation civile et, entre autre, la loi n°82-1153 du 30 décembre 1982 modifiée, loi d'orientation sur les transports intérieurs (LOTI). Elle dispose notamment que l'autorité portuaire doit pourvoir fournir en permanence des informations et des statistiques quant aux mouvements des navires, au trafic maritime de passagers et de marchandises, au nombre de personnes à bord et aux caractéristiques des marchandises (nouvel article L. 153-1). Elle renforce les pouvoirs de police portuaire vis-à-vis des navires en prévoyant que l'accès d'un navire au port puisse être subordonné à un contrôle préalable et que le dépôt d'une caution puisse être exigé (nouvel article L. 323-5 transféré du chapitre IV au chapitre III du titre II du Livre III). Enfin, dans l'ordre interne uniquement, la zone portuaire de sûreté s'étend au-delà des limites administratives du port – définies par le préfet de département – puisqu'elle englobe également les « zones terrestres contiguës au port intéressant la sûreté de opérations portuaires » (nouveau chapitre IV du Titre II du Livre III, article L. 324-1). Il est à noter à ce sujet qu'il existe un plan de sûreté du port dans son ensemble et que chaque plan de sûreté d'installation portuaire doit être compatible avec le plan général de sûreté du port (nouvel article L. 324-4). Par ailleurs, les bagages et les personnes peuvent être contrôlés par des officiers de police judiciaire (OPJ), des agent de police judiciaire ou leurs adjoints, et même par des « agents de nationalité française ou ressortissant d'un Etat membre de la Communauté européenne » placés sous l'autorité des OPJ. Quant aux navires, la même règle est applicable hormis pour ce qui est des « parties à usage exclusif d'habitation et des locaux syndicaux » (nouvel article L. 324-5).

¹¹⁰ Elle est définie par l'instruction du Premier ministre du 3 mai 2002 comme étant « un renseignement de sécurité maritime (RSM), nécessaire ou simplement utile aux navigateurs pour leur permettre d'assurer leur sécurité et celle des autres usagers de la mer, qu'il s'agisse de choisir leur route, de signaler des situations ou des dangers particuliers, de faciliter les secours en cas de besoin, de déterminer leur position, de permettre la meilleure présentation dans les ports et mouillages et de connaître les ressources qu'ils pourront y trouver. L'information nautique désigne également l'action d'informer ».

¹¹¹ Avertissement urgent de navigation, tel que défini dans l'instruction du Premier ministre du 3 mai 2002. Les messages AVURNAV sont valable 10 jours mais en cas de changement de niveau de sûreté, un nouvel AVURNAV serait émis.

¹¹² Avertissement urgent de navigation de zone, tel que défini dans l'instruction du Premier ministre du 3 mai 2002, sachant que les mers et océans du globe sont divisés en 16 zones NAVAREA. Ces messages sont diffusés en télex sur les fréquences HF (bande de fréquences comprises entre 4 000 et 27 500 kHz).

¹¹³ Cf infra 2.2.1 Au niveau national, page 46.

¹¹⁴ Publiée au JO n° 162 du 14 juillet 2004, page 12717 texte n°19. Site de Legifrance : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=710285&indice=19&table=JORF&ligneDeb=1>.

L'ordonnance n° 2005-898¹¹⁵ du 2 août 2005 remet à jour les livres III et IV du Code des ports maritimes. Une zone maritime et fluviale de navigation¹¹⁶ est instaurée par l'article L 301.1. La police du plan d'eau, qui intègre « l'organisation des entrées, sorties et mouvements de navires, bateaux ou engins flottants » (article L. 302-6), est également applicable dans cette nouvelle zone. Cette ordonnance se justifie par la crainte d'attaques contre des navires dans un port car ils constituent des proies faciles dans ce contexte du fait de leur vitesse réduite et d'une capacité de manœuvre particulièrement limitée. Ce texte précise par ailleurs que les officiers de ports et officiers de port adjoints ont toute latitude pour monter à bord des navires « en cas de péril grave et imminent et lorsque leurs ordres n'ont pas été exécutés »¹¹⁷. Ils peuvent ainsi tout mettre en œuvre pour mettre un terme à la situation dangereuse (article L. 303-2). Un autre point intéressant est que ce texte dispose clairement que seule l'autorité portuaire peut autoriser l'entrée d'un navire dans le port (article L. 311-1). Enfin, l'article 321-8 précise que « le fait de s'introduire ou de tenter de s'introduire sans autorisation dans une zone d'accès restreint est puni d'une amende de 3 750 euros ».

2.1.2. La législation européenne

2.1.2.1. Le règlement (CE) n° 724/2004¹¹⁸

L'Agence européenne de sécurité maritime a été créée par le règlement (CE) n° 1406/2002 du 25 août 2002 pour la sécurité maritime et la prévention des pollutions. Le présent règlement, en date du 31 mars 2004, modifie pour la seconde fois le règlement (CE) n° 1406/2002. Il ajoute, entre autre, comme objectif principal de l'Agence, le fait d'« assurer un niveau élevé, uniforme et efficace de (...) sûreté maritime » (article 1.1). Son rôle est d'assister techniquement et scientifiquement les Etats membres à mettre en œuvre la sûreté maritime (articles 1.2 et 2.g) et de secondar la Commission européenne au niveau de l'application de la législation en question (article 2-b). Enfin, les membres de l'Agence doivent désormais avoir des compétences et une expérience en matières de sûreté maritime (article 10.4 et 16.1).

2.1.2.2. Le règlement (CE) n° 725/2004¹¹⁹

Règlement européen émis par le Conseil et le Parlement le 31 mars 2004 également, ce texte vise à servir de « base pour l'interprétation et la mise en œuvre harmonisées » (article 2) des prescriptions de l'OMI en matière de sûreté maritime. Il étend ainsi l'application du chapitre XI-2 de la Convention SOLAS et de la partie A du Code ISPS aux navires à passagers relevant de la

¹¹⁵ Information communiquée par Marie-José Heurte, Chargée de mission au SG Mer, suite à un entretien téléphonique le 1^{er} août 2005. Publiée au JO n° 179 du 3 août 2005, page 12 702, texte n° 44. Site de Legifrance : <http://www.legifrance.gouv.fr/WAspad/Visu?cid=744453&indice=44&table=JORF&ligneDeb=1>.

¹¹⁶ Elle est définie comme « comprenant, en dehors des limites administratives du port, les espaces nécessaires à l'approche et au départ du port. Ces espaces sont constitués des chenaux d'accès au port et des zones d'attente et de mouillage ».

¹¹⁷ La loi n° 94-589 du 15 juillet 1994 – qui est en passe d'être modifiée pour insister sur la sûreté – et le décret n° 95-411 du 19 avril 1995 traitent également du refus d'obtempérer de la part d'un navire. Ils prévoient la possibilité d'exercer des mesures de contrôle et de coercition en mer ainsi que des amendes.

¹¹⁸ Publié au JO de l'Union européenne (UE) n° L 129 du 29 avril 2004 pages 0001-0005. Site de l'UE : <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004R0724:FR:HTML>.

¹¹⁹ Publié au JO de l'UE n° L 129 du 29 avril 2004 pages 0006-0091. Site de l'UE : <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004R0725:FR:HTML>.

classe A¹²⁰, à leurs compagnies ainsi qu'aux installations portuaires les desservant à compter du 1^{er} juillet 2005 (article 3.2), ce qui n'équivaut pas pour autant à l'ensemble du port. Les navires de classe A sont des navires engagés dans le trafic national, avec à leur bord plus de 12 passagers et s'éloignant de plus de 20 milles marins des côtes – soit environ 37 km –. Le règlement (CE) n° 725/2004 laisse ensuite le choix aux Etats membres d'appliquer cette réglementation à tous les navires opérant des services intérieurs, aux compagnies ainsi qu'aux installations portuaires les desservant à partir du 1^{er} juillet 2007 (article 3.3). Ils doivent alors en informer la Commission européenne et procéder à des révisions périodiques quinquennales. Par ailleurs, ce règlement rend obligatoire un certain nombre de dispositions de la partie B du Code, qui n'étaient jusque là que de simples recommandations, pour aider à mettre en place la partie A (article 3.5). Les sections concernées sont :

- * B/1.12 sur la révision des plans de sûreté des navires,
- * B/1.16 sur l'évaluation de sûreté des installations portuaires,
- * B/4.1 sur la protection de la confidentialité des plans et des évaluations de sûreté,
- * B/4.4 sur les organismes de sûreté reconnus,
- * B/4.5 sur les compétences minimales des organismes de sûreté reconnus,
- * B/4.8 sur l'établissement du niveau de sûreté,
- * B/4.14, B/4.15, B/4.16 sur les points de contact et renseignements concernant les plans de sûreté des installations portuaires,
- * B/4.18 sur les documents d'identification,
- * B/4.24 sur l'application par les navires des mesures de sûreté préconisées par l'État dans les eaux territoriales duquel ils naviguent,
- * B/4.28 sur les effectifs des navires,
- * B/4.41 sur la communication de renseignements en cas d'expulsion d'un port ou de refus d'y entrer,
- * B/4.45 sur les navires d'un État non-partie à la convention,
- * B/6.1 sur les obligations pour la compagnie de fournir au capitaine des informations concernant les opérateurs du navire,
- * B/8.3 à B/8.10 sur les standards minimums concernant l'évaluation de sûreté du navire,
- * B/9.2 sur les standards minimums concernant le plan de sûreté du navire,
- * B/9.4 sur l'indépendance des organismes de sûreté reconnus,
- * B/13.6 et B/13.7 sur la périodicité des exercices et des entraînements de sûreté pour les équipages des navires, et pour les agents de sûreté des compagnies et des navires,
- * B/15.3 et B/15.4 sur les standards minimums concernant l'évaluation de la sûreté de l'installation portuaire,
- * B/16.3 et B/16.8 sur les standards minimums concernant le plan de sûreté de l'installation portuaire,
- * B/18.5 et B/18.6 sur la périodicité des exercices et des entraînements de sûreté au sein des installations portuaires, et pour les agents de sûreté des installations portuaires.

¹²⁰ Au sens de l'article 4 de la directive 98/18/CE du Conseil du 17 mars 1998 établissant des règles et normes de sécurité pour les navires à passagers.

Il est à noter un point essentiel à ce sujet : la section B/1.5 précise clairement qu'aucune recommandation de la partie B du Code « ne saurait contrevenir ou être interprétée de façon à modifier l'objectif du chapitre XI-2 de la convention SOLAS et de la partie A du Code ». En cas, de conflit, ce n'est jamais la partie B qui prime. Le règlement (CE) n° 725/2004 prévoit également un processus d'inspections supervisées par la Commission européenne. Le but est qu'elle vérifie l'efficacité du contrôle de l'application effective des règles de sûreté mis en œuvre par les Etats membres. Abordé au considérant 14, ce « contrôle communautaire des mesures de sûreté » (article 2) est explicité à l'article 9.4. et 9.5 du présent règlement.

Enfin, ce texte, entré en vigueur le 19 mai 2004 – la transposition au niveau de Etats membres étant prévue le 1^{er} juillet 2004 – permet aux Etats membres (article 5) de conclure des arrangements bilatéraux ou multilatéraux entre eux, tels que prévu à la règle XI-2/11 de la convention SOLAS. Applicables au trafic régulier sur des routes fixes, ces accords visent à promouvoir le transport maritime intracommunautaire à courte distance.

2.1.2.3. La proposition de directive du 11 juin 2004¹²¹

Cette proposition de directive du Parlement européen et du Conseil est relative à l'amélioration de la sûreté des ports. Elle tend à coordonner, au niveau communautaire, les mesures de sûreté portuaires existantes pour un système de sûreté uniformisé applicable à l'enceinte portuaire dans sa globalité. En effet, le port, jonction entre la mer et la terre, s'étend bien au-delà des seules installations portuaires visées par le Code ISPS et sa vulnérabilité concerne malheureusement « l'ensemble de ses éléments constitutifs ». Selon Loyola de Palacio¹²², « avec cette proposition, [le Parlement et le Conseil ont] l'intention de construire un nouvel élément important des défenses de la Communauté contre les actions illicites intentionnelles. (...) Il faut que les ports deviennent aussi peu vulnérables que possible aux actes illégaux, y compris les attaques terroristes. Ils ne doivent pas être des cibles faciles (...) car l'enjeu est trop important ».

Cette proposition de directive complète ainsi les mesures présentées par la Commission en mai 2003 visant un renforcement de la sûreté des navires et des installations portuaires¹²³. Le but est de fournir le cadre communautaire nécessaire à la protection de toute la chaîne logistique du transport maritime en évitant toute distorsion de la concurrence entre Etats membres. La directive s'appliquerait « aux personnes, aux infrastructures et au matériel, y compris les moyens de transport, [présents] dans les ports ainsi que dans les zones adjacentes » (article 2.1). Les Etats membres doivent contrôler les plans de sûreté portuaire qui seraient rendus obligatoires par le présent texte et leur application effective. Parallèlement à cela, des sanctions « efficaces, proportionnées et dissuasives » en cas de non-respect doivent être fixées (article 18). La directive instaurerait également la désignation obligatoire d'un agent de sûreté portuaire dans chaque port pour servir de point de contact avec la Commission (article 9) ainsi que la création d'un « comité de la sûreté portuaire » (article 10) pour conseiller l'autorité responsable et superviser les mesures de sûreté, en tout cas pour les Etats membres n'en ayant pas encore et en ressentant la nécessité.

¹²¹ Site de l'UE : <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52004PC0076:FR:HTML>.

¹²² Vice-présidente de la Commission européenne et commissaire chargée des transports et de l'énergie de l'époque.

¹²³ COM (2003) 229 final.

2.1.2.4 Le règlement (CE) n° 884/2005¹²⁴

En date du 10 juin 2005, ce règlement de la Commission européenne fait suite au règlement (CE) n° 725/2004 et est entré en application le 1^{er} juillet 2005. Il établit les procédures pour « contrôler l'application du règlement (CE) n° 725/2004 au niveau de chaque Etat membre ainsi que des installations portuaires et compagnies concernées. Les inspections (...) [sont effectuées par les agents de la Commission,] d'une manière transparente, efficace, harmonisée et cohérente (article 1).

Ce règlement réitère le principe du règlement (CE) n° 724/2004 selon lequel l'Agence européenne pour la sécurité maritime doit fournir une assistance technique pour les contrôles (article 6), mettant ainsi en relation les trois textes. Il définit ensuite les critères de qualification et de formation des inspecteurs de la Commission (article 7) ainsi que, entre autre, la procédure d'annonce de l'inspection, via le HFD du ministère des transports en France, (article 8) et les critères d'établissement du rapport d'inspection (article 11).

2.1.3. La législation internationale

2.1.3.1 La législation de l'OMI

2.1.3.1.1 La Résolution 1¹²⁵

Le 12 décembre 2002, la Conférence diplomatique des gouvernements contractants à la Convention SOLAS amendée a adopté toute une série d'amendements connexes à la Convention, en plus du code ISPS. Le chapitre V de la Convention inclut désormais le système AIS¹²⁶ (règle V/19). Par ailleurs, le chapitre XI a été subdivisé en XI-1, Mesures spéciales pour renforcer la sécurité maritime, et XI-2, Mesures spéciales pour renforcer la sûreté maritime.

La nouvelle règle XI-1/3 établit que tout navire doit avoir son numéro d'identification marqué de façon définitive et lisible à deux endroits. Il doit apparaître sur la superstructure ou, pour les navires à passagers, sur une surface visible depuis les airs, ainsi qu'à la machine et ce dès le 1^{er} juillet 2004 pour les navires neufs, ou au plus tard à la première mise en cale sèche qui suit cette date pour les navires construits avant le 1^{er} juillet 2004. La fiche synoptique continue (CSR) relève du même chapitre, règle XI-1/5. Elle doit relater au minimum les 10 derniers ports d'escale et doit obligatoirement être conservée à bord.

Le chapitre XI-2 reprend les grandes lignes du Code ISPS qui constitue la résolution 2. Il reprend les définitions principales, le champ d'application des mesures de sûreté, les obligations des gouvernements contractants en matière de sûreté, les prescriptions relatives aux compagnies ainsi que leurs responsabilités spécifiques. Il traite par ailleurs du système d'alerte de sûreté des navires, des menaces contre les navires, du pouvoir discrétionnaires du Capitaine en matière de sécurité et de sûreté du navire ainsi que des mesures liées au contrôle et au respect des dispositions.

¹²⁴ Publié au JO de l'UE n° L 148 du 11 juin 2005 pages 0025-0029. Site de l'UE : <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32005R0884:FR:HTML>.

¹²⁵ Site de Secopex : http://www.isps.fr/regle_OMI/solasconf532.pdf.

¹²⁶ *Automatic Identification System*.

2.1.3.1.2 Les textes du MSC

Les textes émis par le MSC visent généralement à apporter des précisions pour permettre une application optimale des nouvelles mesures afin de renforcer la sûreté maritime.

Le premier texte qui traite de la question est la circulaire MSC/Circ. 1067¹²⁷ qui date du 28 février 2003. Elle rappelle brièvement aux Etats membres les diverses obligations nées de l'adoption du nouveau chapitre XI-2 de la Convention SOLAS ainsi que du Code ISPS et notamment la date d'entrée en vigueur de ces nouvelles mesures. A ce sujet, elle précise qu'il ne sera accordé aucun délai (résolution 6, paragraphe 1) et que les Etats membres doivent s'efforcer d'assister techniquement ceux qui auraient des difficultés (résolution 5, paragraphe 1) à se conformer aux nouvelles règles dans les temps. Dans le même ordre d'idées, la circulaire MSC/Circ. 1097¹²⁸, en date du 6 juin 2003, dispense des conseils généraux sur l'application globale du chapitre XI-2 de la Convention SOLAS et du Code ISPS tout en faisant référence à la résolution précédente. Puis la circulaire MSC/Circ. 1104¹²⁹ du 14 janvier 2004 rappelle aux gouvernements contractants leurs engagements six mois avant l'entrée en vigueur des nouvelles mesures car les statistiques alors disponibles à ce moment-là rapportaient des taux de conformité loin d'être satisfaisants.

La circulaire MSC/Circ.1072¹³⁰, en date du 26 juin 2003, est basée sur les directives élaborées par le Sous-comité des radiocommunications et de la recherche et du sauvetage, dit Sous-comité COMSAR. Elle traite de la conception du SSAS, rendu obligatoire par la règle XI-2/6 de la Convention SOLAS amendée. Le but est d'envoyer un signal ou un message à l'autorité compétente tel qu'il ne soit pas audible à bord du navire ni pour les bâtiments environnants. Trois systèmes sont admissibles au titre de cette circulaire mais ils ne sont pas exhaustifs. Le premier est un « équipement de suivi exclusif » fourni par des prestataires de services de trafic. Il envoie un compte rendu de position par intervalles de six heures via satellite et, en cas d'activation soit d'un bouton soit d'un capteur ou autre, le compte rendu de position aura un format différent signalant une anomalie à bord. Les prestataires de services, qui assurent le suivi des transmissions, en informent alors immédiatement la compagnie maritime concernée. Le deuxième système possible repose sur l'équipement SMDSM¹³¹. Il convient toutefois de procéder à un réglage manuel des fréquences pour signifier la différence entre une alerte de sûreté et un message de détresse ou de sécurité classique. Le SSAS peut utiliser des radiocommunications spatiales de type Inmarsat¹³² C¹³³, mini-C¹³⁴ ou Inmarsat D¹³⁵. Enfin, la troisième possibilité consiste à établir, au préalable, un code qui permet d'envoyer des messages vocaux ou des

¹²⁷ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D6909/1067.pdf.

¹²⁸ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D7624/1097.pdf.

¹²⁹ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D8598/1104.pdf.

¹³⁰ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D7496/1072.pdf.

¹³¹ Système Mondial de Détresse et de Sécurité en Mer. Il s'agit d'une réglementation internationale définissant les moyens de radiocommunication et de repérage exigibles sur les navires pour assurer la sécurité de la vie humaine en mer. Document communiqué par le CROSS La Garde lors d'un stage en avril 2005.

¹³² *International maritime satellite organization*. Cette organisation a été établie par la Convention du même nom en date du 3 septembre 1978. Elle dispose d'un système de télécommunications utilisant des satellites et des stations terriennes côtières. Document communiqué par le CROSS La Garde lors d'un stage en avril 2005.

¹³³ Le standard C, miniaturisé, traite uniquement les communications télex sous forme digitale.

¹³⁴ Il a les mêmes fonctionnalités que le précédent mais de plus faible puissance.

¹³⁵ Muni d'un système GPS, il est utile pour la surveillance à distance et la diffusion brève d'informations.

transmission de données contenant des mots-clés. L'échange se fait généralement entre le navire et la compagnie maritime. Le SSAS doit avoir au moins deux points d'activation à bord, dont un obligatoirement à la passerelle (règle XI-2/6.2.3.1). La circulaire précise qu'il s'agit généralement de combinés de téléphone, de claviers ou encore de boutons fixes ou portatifs.

La circulaire MSC/Circ. 1073 du 10 juin 2003¹³⁶ regroupe des directives adressées aux MRCC¹³⁷ en cas d'actes de violence à l'encontre des navires. Elle modifie la circulaire MSC/Circ. 967 qui ne concernait que les actes de piraterie et d'attaques à main armée pour y inclure tout incident de sûreté tel que défini dans la règle XI-2/1.2.13 de la Convention SOLAS ¹³⁸. Le but est que les MRCC sachent exactement qui contacter, à quel moment, et ce en fonction de la situation à laquelle ils sont confrontés.

La circulaire MCS/Circ. 1074¹³⁹ a été réalisée le même jour que la précédente mais celle-ci sert de guide pour le processus de reconnaissance des RSO dans le respect des sections A/4.3 et B/4.3 à B/4.7 ainsi que de la règle XI-2/1.16. Globalement, ils peuvent agir au nom de l'administration ou de l'autorité désignée du gouvernement contractant pour approuver des SSP, procéder aux contrôles des navires, émettre et approuver des ISSC et organiser des PFSA.

La résolution MSC. 159 (78) du 21 mai 2004 comporte des recommandations intérimaires sur les mesures de sûreté liées au contrôle et au respect des dispositions renforçant la sûreté maritime. Elle explicite ainsi la règle XI-2/9 de la Convention SOLAS qui doit être mis en relation avec les sections B/4.29 et B/4.40 du Code ISPS. Il est à noter que ce contrôle doit être fondé soit sur une évaluation approfondie des risques, soit sur des renseignements fournis au préalable, généralement de façon anonyme, mais dans ce dernier cas, ils doivent être formellement authentifiés.

Dans le même état d'esprit, la circulaire MSC/Circ. 1111¹⁴⁰ du 7 juin 2004 émet des recommandations sur l'application du chapitre XI-2 de la Convention SOLAS et du Code ISPS. Elle rappelle ainsi, dans la section B/9.51, que le SSP doit prévoir des mesures et des procédures de sûreté à mettre en œuvre quand, lors de l'interface navire/installation portuaire, l'un ou l'autre ne satisfait pas aux nouvelles prescriptions. Si ce n'est pas le cas, il faut établir une DoS. De même, en cas de doute sur la sûreté de l'installation portuaire, il convient en premier lieu de contacter le PFSP, voire, en second lieu, d'établir une DoS. La circulaire revient également sur le fait que le PFSP doit envisager des mesures à appliquer vis-à-vis d'un navire qui n'applique pas correctement l'ISPS ou qui n'y est pas tenu (section B/16.56). Par ailleurs, dès que le PFSP sait qu'un tel navire est en approche, il devrait demander l'avis des « autorités chargées de l'exécution des mesures liées au contrôle et au respect des dispositions » (règle XI-2/9) ainsi que celui des autorités qui ont approuvé le PFSP. Le texte précise qu'un chantier naval peut être désigné comme installation portuaire tant qu'il se plie aux mêmes règles qu'une installation portuaire « classique », la question étant du ressort du gouvernement et dépend de sa position au moment

¹³⁶ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D7430/1073.pdf.

¹³⁷ *Maritime Rescue Co-ordination Center*, équivalents étrangers des CROSS français institués en 1979 par la Convention de Hambourg.

¹³⁸ « Tout acte suspect ou toute circonstance suspecte qui menace la sûreté du navire, y compris une unité mobile de forage au large et un engin à grande vitesse, ou d'une installation portuaire ou d'une interface navire/port ou d'une activité de navire à navire ».

¹³⁹ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D7501/1074.pdf.

¹⁴⁰ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D9980/msccirc1111french.pdf.

où elle se pose. C'est également le cas pour les navires effectuant des essais en mer ou pour la suspension ou l'annulation du ISSC pour un navire en cours de transformation ou de réparation. Pour ce qui est des navires en construction, tant qu'ils n'ont pas un ISSC en règle, ils ne sont pas considérés comme des navires au sens du chapitre XI-2 de la Convention SOLAS et de la partie A du code ISPS et leur sûreté dépend du chantier naval. Enfin, cette circulaire estime que les unités flottantes de production, de stockage et de déchargement (FPSO) et les unités de stockage flottantes (FSU) – servant à la production d'hydrocarbures au large et qui ne sont pas des navires au sens du chapitre XI-2 de la Convention SOLAS et de la partie A du Code ISPS – doivent appliquer certaines mesures de sûreté, sans toutefois les définir, afin de ne pas « contaminer » les navires soumis à l'ISPS lors d'une interface.

La circulaire MSC/Circ. 1112¹⁴¹ du 7 juin 2004 traite, elle, du congé à terre des gens de mer et de l'accès au navire. Cette circulaire rappelle qu'il faut rechercher le bon équilibre entre la nécessité d'accroître la sûreté, le respect des droits fondamentaux des gens de mer et des travailleurs portuaires et l'efficacité de l'exploitation des navires, qui passe par les services d'approvisionnement, de réparation et d'entretien à terre. De même, elle souligne que la règle A/16.3.15 du Code ISPS oblige les plans de sûreté à prévoir les congés à terre des gens de mer ainsi que l'accès « des visiteurs au navire, y compris les représentants des services sociaux et des syndicats des gens de mer ». Les exploitants des installations portuaires doivent également tenir compte de ces besoins. Enfin, ce texte précise que ce n'est pas parce que les mesures de sûreté sont centrées principalement sur l'interface navire/installations portuaires que les gens de mer ou les navires doivent être considérés comme une menace potentielle supérieure. D'ailleurs, il dispose que toute mesure ayant un effet négatif sur « l'élément humain » doit être signalé à l'OMI. Il est à noter qu'aux USA, les formalités pour descendre à terre sont désormais d'une telle complexité que bien souvent, les marins n'essaient même plus de descendre pendant les escales.

La circulaire MSC/Circ. 1130¹⁴² du 14 décembre 2004 propose un guide sur les renseignements de sûreté à fournir avant l'entrée au port. Elle s'adresse aux Capitaines, aux compagnies maritimes ainsi qu'aux « fonctionnaires concernés et autorisés » et fait suite à une préoccupation quant à « la prolifération de demandes de renseignements (...) [de] sûreté » qui affecte le trafic commercial. Ainsi, ce texte fournit une liste normalisée de renseignements que doit fournir tout navire avant d'entrer au port mais qui n'est pas exhaustive¹⁴³. Il est à noter que cette liste reprend les informations demandées par la règle XI-2/9.2.1 et qu'en cas de contestation, le navire peut se voir refuser l'accès au port. La Capitaine est la personne qui doit transmettre ces renseignements, à moins qu'il ne demande au SSO ou au CSO de le faire en son nom. Avec son autorisation expresse, l'agent du navire au port sera également en mesure de communiquer ces renseignements à l'autorité nationale désignée par le gouvernement contractant. Il est à noter que

¹⁴¹ Site Secopex :

http://www.isps.fr/regle_OMI/1112CONGE_A_TERRE_DES_GENS_DE_MER_ET_ACCES_AUX_NAVIRES.pdf.

¹⁴² Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D10885/1130.pdf.

¹⁴³ L'Etat du port peut également demander au Capitaine des informations sur la personne chargée du recrutement de l'équipage, sur celle qui décide de l'emploi du navire ainsi que sur les différentes parties impliquées dans la ou les chartes parties sous lesquelles opère le navire. Il peut aussi demander les coordonnées des points de contact de ces parties en cas d'affrètement coque nue ou à temps (règle XI-2/5 de la Convention SOLAS et section B/6.1 du Code ISPS).

le délai minimal requis pour soumettre ces informations est de 24 heures avant l'arrivée, à moins que l'Etat du port n'ait pris d'autres dispositions qu'il doit immédiatement faire connaître à l'OMI.

La circulaire MSC/Circ. 1131¹⁴⁴ du 14 décembre 2004 a élaboré des recommandations intérimaires pour que les gouvernements contractants et les installations portuaires puissent procéder à des auto-évaluations facultatives. Le but est de les aider à mettre en place les nouvelles mesures imposées par l'OMI mais aussi à conserver le niveau de sûreté ainsi atteint. Cette circulaire propose donc une méthodologie d'analyse basée sur des questionnaires reprenant les points essentiels de la nouvelle réglementation afin de vérifier qu'ils sont effectivement appliqués.

La circulaire MSC/Circ.1132¹⁴⁵ du 14 décembre 2004 renferme un guide répondant aux diverses questions qui se sont posées au 1^{er} juillet 2004 lors de la mise en application des nouvelles mesures de sûreté. Pour ce qui est des niveaux de sûreté, il est rappelé que seul un gouvernement contractant peut les établir pour les navires battant son pavillon (règle XI-2/3.1), et qu'il doit en informer les installations portuaires sur son territoire et les navires avant ou pendant leur séjour dans un de ses port (règle XI-2/3.2). De plus, le niveau de sûreté n'est pas nécessairement homogène. Un gouvernement contractant ne peut obliger un navire ou une installation portuaire à réduire son niveau de sûreté ; en cas d'incompatibilité, une DoS doit être établie. Il est à noter qu'un navire a l'obligation de remplir une DoS sur demande de l'installation portuaire mais la réciproque n'est pas vraie, l'installation portuaire devant juste accuser réception de la demande de DoS (section A/5.3). La DoS ne doit être utilisée que dans des cas exceptionnels liés à des risques élevés si bien qu'en opérant au niveau 1, il ne devrait théoriquement pas y avoir de DoS. Les inspecteurs procédant au contrôle par l'Etat du port ne devraient pas s'attendre à ce qu'un navire ait systématiquement des DoS couvrant ses dix dernières escales ou ses activités de navire à navire. Par ailleurs, en cas d'incident de sûreté, le navire ou l'installation portuaire ne doivent pas attendre que leur gouvernement contractant rehausse leur niveau de sûreté mais, au contraire, ils doivent immédiatement appliquer les mesures de sûreté prévues dans leur plan pour faire face à une telle situation. Enfin, cette circulaire revient sur l'importance du dialogue entre les différents acteurs de la sûreté maritime en soulignant que le caractère confidentiel des informations échangées fait qu'elles ne devraient pas être transmises par le biais de simples « ondes métriques ». L'intérêt de ce dialogue est de s'accorder sur les procédures à appliquer quand le navire est au port, ce qui facilite grandement, entre autre, l'intervention des pilotes, l'identification des arrimeurs, les inspections de sécurité, la conduite des exercices d'évacuation et d'entraînement ainsi que l'accès au navire par du personnel à terre qui doit être nécessairement soumis à la présentation d'un document d'identité.

La circulaire MSC/Circ. 1133¹⁴⁶ du 14 décembre 2004 sert à rappeler aux Etats membres que si l'Etat du port impose des mesures de contrôle répondant à la règle XI-2/9 de la Convention SOLAS, ce dernier a l'obligation d'en informer le point de contact national de l'Etat du pavillon ainsi que l'OMI et le RSO ayant délivré le certificat international de sûreté si besoin est (règle XI-2/9.3.1).

¹⁴⁴ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D10840/1131.pdf.

¹⁴⁵ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D10984/1132.pdf.

¹⁴⁶ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D10886/1133.pdf.

Enfin, la circulaire MSC/Circ. 1109/Rev.1¹⁴⁷ du 14 décembre 2004 s'attaque au problème des fausses alertes générées par le SSAS ainsi qu'à celui des « doubles alertes », de détresse plus de sûreté. Le MSC avait proposé dès juin 2004 aux gouvernements contractants de procéder à une évaluation du SSAS pour voir quels étaient les dysfonctionnements les plus récurrents mais le fait est, que pour les navires construits avant le 1^{er} juillet 2004, la pose du SSAS peut se faire au plus tard lors de la première visite de l'installation radioélectrique après le 1^{er} juillet 2004 (règle XI-2/6.1). Si bien que de nombreux navires n'en étaient pas pourvus à la date de réunion du MSC. Toutefois, il est possible d'établir que les fausses alertes sont généralement dues à une défaillance technique du SSAS lui-même ou à une activation malencontreuse. L'exemple du Japon est révélateur¹⁴⁸ : sur 10 fausses alertes de sûreté émises entre le 23 juillet 2004 et le 13 octobre 2004, trois sont dues à un défaut d'un instrument de bord et les sept autres relèvent d'une manipulation incorrecte. Pour ce qui est de la double alerte, elle peut venir du fait qu'une situation de détresse peut être immédiatement suivie d'un incident de sûreté et qu'un incident de sûreté peut ensuite conduire à une situation de détresse. Les alertes seraient donc actionnées en même temps. Dans pareil cas, il revient au gouvernement contractant concerné d'établir un ordre de priorité d'action. Enfin, les résultats obtenus n'étant que limités, le MSC invite donc les gouvernements contractants à poursuivre cette enquête pour les réunions suivantes.

2.1.3.1.3 Proposition d'amendement

Formulée par les USA, elle a été présentée dans la Lettre circulaire n° 2595 du 10 novembre 2004¹⁴⁹. Elle vise l'insertion d'une règle XI-2/14 sur l'identification et le suivi automatique des navires à grande distance qui devraient communiquer des renseignements sur leur identité, leur position au large des côtes ainsi que l'heure et la date de leur position. Si le navire est à 300 milles marins ou plus – soit plus de 555 km –, les informations doivent avoir été réactualisées au moins une fois au cours des quatre dernières heures ; s'il est à moins de 300 milles marins, les informations doivent dater de moins d'une heure.

2.1.3.2 La législation de l'OIT¹⁵⁰

Le 19 juin 2003, lors de sa 91^{ème} conférence annuelle, l'OIT a adopté une nouvelle convention sur les pièces d'identité des gens de mer, la convention n° 185¹⁵¹, afin de remplacer la Convention n° 108 de 1958¹⁵². Ce texte, entré en vigueur le 9 février 2005, fait suite à la résolution 8 adoptée le même jour que le Code ISPS sur le renforcement de la coopération entre l'OMI et l'OIT¹⁵³. Il établit, article 3, un système d'identification des marins plus rigoureux. La

¹⁴⁷ Site de l'OMI : http://www.imo.org/includes/blastDataOnly.asp/data_id%3D10887/1109-Rev-1.pdf.

¹⁴⁸ Site de Secopex : http://www.isps.fr/Actualité/tableau_code_ISPS.pdf.

¹⁴⁹ Site de Secopex : http://www.isps.fr/Actualité/proposition_règle_14_solas.pdf.

¹⁵⁰ Organisation Internationale du Travail.

¹⁵¹ La France l'a ratifiée le 16 février 2004 par la loi 2004-146.

¹⁵² BOISSON Philippe, *La sûreté des navires et la prévention des actes de terrorisme dans le domaine maritime*, DMF n° 640, p. 723, septembre 2003.

¹⁵³ Il est à noter à ce sujet qu'un comité de travail mixte OIT/OMI sur la sécurité des ports a été mis en place par le MSC en juin 2003 et par le Conseil d'administration du Bureau international du travail en mars 2003 et qu'il s'intéresse à la sûreté des navires dans le cadre de l'interface navire/port.

méthode retenue¹⁵⁴ scanne les empreintes digitales qui figurent au dos de la carte sous forme de code barre en deux dimensions. Une base de données électronique par Etat signataire est également prévue par l'article 4 pour lutter contre la falsification. Il est à noter que cette carte d'identité biométrique¹⁵⁵ permettra de faciliter les procédures d'obtention des visas mais il ne faut pas perdre de vue qu'il ne s'agit pas de passeport.

Enfin, l'OIT devrait étendre ces mesures à l'ensemble des personnes travaillant dans l'enceinte portuaire puisqu'elle prépare un projet sur une pièce d'identité uniformisée.

2.1.3.3 La législation de l'OMD¹⁵⁶

En juin 2002, l'OMD a adopté une résolution relative à la sûreté et à la facilitation de échanges de la chaîne logistique. L'objectif est d'empêcher le transport frauduleux d'armes de destruction massive dans le but de commettre des actes terroristes. Il est à noter que la douane est assez stricte quant aux scellés apposés sur les conteneurs : ils doivent répondre à la norme ISO/PAS 17712 qui vise des « scelllements mécaniques de haute sécurité¹⁵⁷ » dont l'OMD rappelle l'utilité dans son « Cadre de normes visant à sécuriser et à faciliter le commerce mondial », en date de juin 2005. Cependant, la problématique généralement liée aux scellés demeure, à savoir qu'ils ne sont pas inviolables ; un expert de la question, M. Fortin, l'a d'ailleurs confirmé au groupe de travail du Conseil Economique et Social des Nations Unies¹⁵⁸, réuni lors d'une session portant sur les problèmes douaniers intéressant les transports, et ce notamment à propos des dispositions techniques de la Convention TIR¹⁵⁹. Il observe qu'il suffit d'ôter la tête du scellement – même pour un plomb certifié par cette norme ISO – avec une perceuse pour le retirer complètement. Ensuite, il ne reste plus qu'à replacer le plomb original en le fermant avec une nouvelle tête, ce qui ne laisse selon lui aucune trace d'effraction. Les solutions proposées sont donc d'entourer les deux poignées de la porte par un câble de scellement ou de positionner un « mécanisme antirotation » entre le scellement et sa tête, qui auraient tout deux le même numéro d'identification et de protéger ce numéro en le plastifiant.

Enfin, il est à noter¹⁶⁰ que la Commission de politique générale de l'organisme a élaboré le « Cadre de normes » en décembre 2004 pour sécuriser l'ensemble de la chaîne logistique. Ces nouvelles normes visent l'agrément des intervenants du transport, ainsi qu'une déclaration électronique préalable des marchandises. Ce nouveau système s'inspire largement du C-TPAT. Il est à noter enfin que cette méthode de la déclaration systématique se retrouve dans le règlement (CE) n° 648/2005 qui modifie le code des douanes communautaire.

¹⁵⁴ Communiqué de presse de Steria, entreprise choisie comme l'un des trois fournisseurs exclusifs, en date du 17 août 2005 : http://www.euronext.com/file/view/0,4245,1626_53424_637231306,00.pdf.

¹⁵⁵ La biométrie permet l'identification d'une personne sur la base de caractères physiologiques ou de traits comportementaux automatiquement vérifiables et identifiables. Il existe deux catégories de technologies biométriques : les techniques d'analyse comportementales (dynamique de la signature et autres) et les techniques d'analyse de la morphologie humaine (empreintes digitales, traits du visages, voix, dessin du réseau veineux de l'œil, etc). Site Biométrie On Line : http://biometrie.online.fr/Faq_index.htm.

¹⁵⁶ Organisation Mondiale des Douanes.

¹⁵⁷ Site de l'OMD :

<http://www.wcoomd.org/ie/Fr/Presse/OMD%20-%20CADRE%20DE%20NORMES%20juin%2021%20final.pdf>.

¹⁵⁸ Site de la commission économique pour l'Europe de l'ONU :

<http://www.unece.org/trans/bcf/wp30/documents/TRANS-WP30-218f.pdf>.

¹⁵⁹ Convention douanière relative au transport international de marchandises sous le couvert de carnets TIR, 1975.

¹⁶⁰ Site de Secopex : <http://www.isps.fr/supply-chain-security.htm>.

2.1.3.4 La législation étatsunienne

Les USA ont adopté toute une série de lois nationales et accords bilatéraux avant même l'entrée en vigueur du Code ISPS et qui, depuis, viennent en complément car ils estiment que les mesures prises en matière de sûreté du transport maritime sont insuffisantes. A titre d'exemple, le 21 octobre 2002, les garde-côtes étatsuniens avaient déjà émis une circulaire¹⁶¹ contenant des recommandations explicites quant aux mesures à prendre à bord des navires pour les protéger.

D'après les notes de synthèse d'une étude réalisée en avril 2003 par Sophia Clément Noguier¹⁶², intitulée « Stratégies régionales américaines : révolution stratégique après le 11 septembre ? »¹⁶³, cette « politique bilatérale asymétrique », basée sur une série d'impératifs étatsuniens, est caractéristique des stratégies régionales adoptées par les USA depuis les attentats du 11 septembre 2001. De même que les sanctions assez lourdes prévues en cas d'inexécution. Un autre principe de base de cette nouvelle stratégie est le « retour à l'ordre inter-étatique en tant que cadre de la politique internationale ». Il s'accompagne d'une prétention de contrôle plutôt que d'influence qui s'illustre parfaitement dans leur désir d'être présents dans plusieurs régions du globe ou par le biais du contrôle des flux d'information. Par ailleurs, ils mettent la pression auprès des instances internationales pour un libéralisme toujours plus grand et des voies maritimes ouvertes alors que tous les autres pays pensent uniquement en termes de sûreté du transport maritime.

Enfin, les USA envisagent de ne plus délivrer de visas aux marins servant à bord de navires étrangers et souhaitant pénétrer dans un port étatsunien en ne se référant qu'aux listes d'équipage.

2.1.3.4.1 La *Container Security Initiative*, ou CSI¹⁶⁴

Cette série de mesures a été annoncée pour la première fois en janvier 2002. Conçue par la douane étatsunienne, son but est d'« améliorer de façon significative le mode de fonctionnement du commerce maritime ». Il s'agit d'un programme de ciblage des marchandises à risques qui permet de filtrer les conteneurs au départ du port étranger, avant même qu'ils ne soient chargés pour les USA, les marchandises devant être déclarées 24H à l'avance. Or, il s'avère que l'un des éléments critiques de cette théorie est justement la capacité à obtenir des informations fiables en amont.

En juin 2004, la Grèce est devenue le 18^{ème} port à adhérer à la CSI du fait des Jeux Olympiques d'été sur son territoire. Le corollaire est que des agents de sûreté étatsuniens se sont donc déployés au Pirée, principal port grec, pour aider à l'identification et à la vérification des conteneurs suspects. La CSI était déjà opérationnelle à ce moment-là dans 16 ports majeurs d'Europe, d'Asie et du Canada. Dressée par la douane étatsunienne, cette liste de ports se base

¹⁶¹ *Navigation and Vessel Inspection Circular n°1002*.

¹⁶² Docteur en Sciences Politiques et Maître de conférence à l'IEP Paris, elle a travaillé au Centre d'Etudes et de Recherches Internationales (CERI), a été Chargée de recherche à l'Institut d'Etudes de sécurité de l'UE (O) ainsi que Chef du bureau Amérique du Nord et relations transatlantiques à la Délégation aux affaires stratégiques du ministère de la défense. Site du centre de géostratégie de l'Ecole normale supérieure : <http://www.geostrategie.ens.fr/membres.php>.

¹⁶³ Site du ministère de la défense :

http://www.defense.gouv.fr/sites/das/dossiers/strategies_regionales_americaines_apres_le_11_septembre825.

¹⁶⁴ Site de l'Institut d'études internationales de Montréal : <http://www.er.uqam.ca/nobel/cepes/pdf/BULL71.pdf>.

sur les 214 000 navires qui ont transporté 5,7 millions de conteneurs en 2001 vers les USA, soit les deux tiers du trafic de conteneurs entrants, et qui comptent parmi les 20 plus gros ports du monde. La CSI permet d'identifier et de scanner un nombre de conteneurs relativement faible aux vues du volume total embarqué. Le but est de trouver d'éventuelles armes de destruction massive ou des substances radioactives dangereuses que des terroristes auraient pu placer à l'intérieur. Les autorités étatsuniennes considèrent qu'il s'agit de « défense en profondeur ». Ce dispositif complémentaire de l'ISPS s'explique par le fait qu'il existe à l'heure actuelle plus de 15 millions de conteneurs en circulation qui réalisent environ 232 millions de voyage chaque année. Parallèlement à cela, quelques sept millions de conteneurs arrivent annuellement dans les seuls ports étatsuniens. La vérification de conteneurs arrivant aux USA par mer a augmenté jusqu'à concerner 5.2% des arrivées totales en septembre 2003, contre 2% l'année précédente. En 2004 et à l'échelle mondiale, moins de 1% des conteneurs embarqués à bord d'un navire était scanné à l'aide de rayons X ou de rayons gamma. La CSI permet également de vérifier, à l'origine, l'identité des chargeurs et des réceptionnaires.

2.1.3.4.2 La Proliferation Security Initiative¹⁶⁵, ou PSI.

Annoncée par Georges W Bush, cette initiative informelle date du 31 mai 2003 et a été présentée devant l'Assemblée Générale des Nations Unies le 24 septembre de la même année. La PSI énonce une série d'interdictions présentées comme compatibles avec l'ordre juridique actuel. De fait, le droit international permet d'interdire des navires suspects ou de monter à bord en haute mer uniquement en ayant la permission de l'Etat du pavillon du bâtiment, à moins qu'il ne batte aucun pavillon, qu'il s'agisse d'un bateau pirate transportant des esclaves ou des stupéfiants ou qu'il soit utilisé pour transporter des marchandises illicites. Si ces conditions ne sont pas respectées, c'est illégal ; c'est pourquoi les USA essaient parallèlement de faire pression sur les Etats qui n'ont pas encore ratifié la Convention SUA pour qu'ils le fassent mais également pour y ajouter de nouvelles infractions, à savoir celles visées par la PSI.

L'objectif premier de la PSI est d'interrompre et de dissuader le commerce illicite d'« armes de destruction massive [– armes nucléaire, chimique ou biologique –], ainsi que leurs vecteurs et les matériaux connexes », au départ ou vers des pays en faveur de la prolifération. Les nations qui y ont adhéré acceptent ainsi de rechercher tout aéronef, navire, camion, train transportant une cargaison suspecte ainsi qu'à confisquer les chargements d'armes ou de missiles qui aggravent la propagation des armes. Les 11 premiers pays signataires ont été les USA, la Grande-Bretagne, la France, l'Allemagne, l'Australie, le Japon, le Portugal, l'Espagne, l'Italie, les Pays-Bas et la Pologne. Selon les autorités étatsuniennes, plus de 60 Etats y participaient en juin 2005, le but étant de concerner le maximum d'acteurs.

Le premier exercice PSI a été réalisé en Australie, au large du Queensland, en septembre 2003. Ce pays a également abrité la première réunion du groupe de travail des experts PSI le 30 novembre 2004. Puis deux exemples concrets d'application de la PSI se sont produits en deux ans. En octobre 2003, les autorités allemandes et italiennes ont intercepté le *BBC China*, navire

¹⁶⁵ Initiative de sécurité contre la prolifération (traduction employée par le Sénat français) : <http://www.senat.fr/rap/r03-388/r03-3882.html>. Site de *The Jamestown Foundation*, organisme d'information politique : http://www.jamestown.org/publications_details.php?volume_id=391&issue_id=2872&article_id=23400.

appartenant à une société allemande, alors qu'il traversait le canal de Suez. Il transportait à son bord de l'équipement permettant d'obtenir de l'uranium enrichi à destination de la Libye. Puis, en juillet 2003, ce sont les autorités espagnoles qui ont cette fois saisi un navire acheminant des armes vers le Sénégal.

Il est à noter que cette initiative n'est pas sans soulever une certaine controverse, et ce justement au sujet de sa conformité avec le droit international mais également sur deux autres points. Le premier se réfère à la nécessité absolue de se baser sur des renseignements fiables, sinon le risque d'incidents diplomatiques va se multiplier. L'interdiction d'un navire chinois qui était supposé transporter des précurseurs chimiques¹⁶⁶ ou l'interception de missiles Scud¹⁶⁷ commandés par le gouvernement yéménite à la Corée du Nord transportés à bord du *So San* et relâchés deux jours plus tard, soulignent le risque de médiatiser des événements de « peu d'importance » qui affectent la crédibilité du projet d'ensemble. Ceci est d'autant plus préjudiciable que la Chine, par exemple, est assez critique vis-à-vis de la PSI. Le second point concerne la coopération des Etats ne participant pas à la PSI et qui peuvent s'opposer catégoriquement à une inspection à bord, c'est un risque certain avec des dispositions qui ne proviennent pas d'instances internationales.

2.1.3.4.3 Le *Custom-Trade Partnership against Terrorism*, ou C-TPAT

Il s'agit d'un accord entre exportateurs vendant aux USA et la douane étatsunienne. Le but est de garantir la fiabilité de l'ensemble de la chaîne logistique utilisée par les exportateurs. Le fait d'y participer constitue un véritable avantage concurrentiel puisque les contrôles à l'entrée sur les terminaux sont moindres et les procédures administratives de dédouanement accélérées. Le corollaire est très logiquement que les délais de livraison sont nettement plus rapides. Il s'agit là d'un atout incomparable sur un marché mondial caractérisé par le principe du 0 stock et de l'approvisionnement « juste à temps ». La première entreprise française à avoir été certifiée C-TPAT a été Michelin pour garantir que l'empotage, le transport et la manutention sont réalisés par des entreprises sûres. Désormais, c'est une vérification des procédures qui s'opère plutôt qu'un contrôle des conteneurs. Ce système répond au fait que de nombreux contrôles sont initiés sur la base de clients douteux et pas nécessairement à cause de la marchandise elle-même.

2.1.3.4.4 La règle des préavis

Il s'agit d'une règle imposant l'envoi à la douane étatsunienne des manifestes de chargement de toutes les marchandises à destination des USA 24 heures avant le chargement du navire. Cette mesure existe depuis le 2 février 2003. Les douaniers étatsuniens sont d'ailleurs présent dans un certain nombre de ports à l'étranger et peuvent faire qu'une marchandise suspecte n'embarque pas en émettant un « *Do not load order* ». Il est à noter que le port de New

¹⁶⁶ « Substances chimiques légales destinées à l'industrie chimique que les fabricants se procurent illégalement pour produire des drogues illicites. Elles peuvent être extrêmement dangereuses : l'anhydride acétique, par exemple, qui est utilisé en production d'acétate de cellulose, colorations, arômes ou médicaments (aspirine), est également une substance chimique clé pour produire de l'héroïne. Principalement légal, le commerce des précurseurs de drogues fait l'objet d'un contrôle et d'un suivi très attentif selon le règlement n° 3677/90 du Conseil de l'UE et le règlement n° 3769/92 de la Commission, mais il n'est pas interdit ». Site de l'UE :

http://europa.eu.int/comm/taxation_customs/customs/customs_controls/drugs_precursors/index_fr.htm.

¹⁶⁷ Missile balistique à courte portée développé par l'Union Soviétique dans les années 50.

York a adopté des mesures encore plus strictes et notamment le fait qu'un navire souhaitant entrer dans le port doit prévenir les autorités de son arrivée 96 heures à l'avance. A San Francisco, les garde-côtes montent à bord deux jours avant que le navire ne pénètre dans le port.

2.1.3.4.5 Le *Public Health Security and Bioterrorism Preparedness and Response Act*¹⁶⁸, dit *Bioterrorism Act*, ou BTA

Adoptée le 12 juin 2002, cette loi est entrée en vigueur le 12 décembre 2003. La BTA oblige à envoyer un préavis pour tous les produits alimentaires importés ou offerts aux fins d'importation aux USA. Ce préavis doit être envoyé à la *Food and Drug Administration (FDA)*¹⁶⁹. De plus, tous les établissements, qu'ils soient étrangers ou nationaux doivent être enregistrés auprès de cette fédération dès lors qu'ils « fabriquent, transforment, emballent ou entreposent des aliments destinés à la consommation humaine ou animale sur le sol étatsunien ». En cas de non respect du préavis, le produit alimentaire importé en question pourrait être entreposé au port d'arrivée ou dans un établissement sécuritaire jusqu'à ce qu'il soit conforme à la BTA, ou qu'il soit réexporté, voire détruit. Parallèlement à cela, la FDA a publié en 2004 un guide traitant des amendes civiles qui sont infligées dans ce cas. Il est à noter que l'application complète de la BTA a débuté à compter du 13 août 2004.

2.2 L'organisation française

2.2.1. Au niveau national

La première personne concernée à l'échelon national est le Premier ministre. Il s'appuie ensuite sur deux organismes dont il a la tutelle, à savoir le SG Mer et le SGDN, qui travaillent en étroite collaboration, d'autres ministères pouvant également être impliqués. Le SG Mer a été créé par le décret n° 95-1232 du 22 novembre 1995. Il coordonne les décisions gouvernementales émises par une quinzaine de départements ministériels. Par ailleurs, il contrôle et évalue la politique maritime du gouvernement qui résulte d'une concertation avec les élus et l'ensemble des professionnels concernés. Enfin, il anime et coordonne l'action des préfets maritimes.

Le SGDN a été institué par le décret n° 62-808 du 18 juillet 1962 relatif à l'organisation de la défense nationale et ses attributions ont été fixées par le n° 78-78 du 25 janvier 1978. Ses missions principales sont liées aux questions de sécurité intérieure et de défense. Il est donc directement impliqué dans la lutte antiterroriste.

Ces deux organismes sont consultés par le gouvernement dans le but de l'aider à définir la politique à suivre en matière de sûreté maritime, notamment pour ce qui est des niveaux de sûreté qui sont calqués sur les mesures du plan Vigipirate. Néanmoins, en cas de conflit entre une mesure ISPS et une mesure Vigipirate, il est à noter que la seconde doit nécessairement primer. Le SG Mer et le SGDN évaluent la menace en fonction des informations qui leur sont fournies par les services spécialisés du renseignement.

¹⁶⁸ Loi sur la réactivité et les capacités militaires pour lutter contre le bioterrorisme et garantir la sûreté de la santé publique.

¹⁶⁹ Fédération américaine des aliments et drogues. Elle exerce un contrôle rigoureux sur les industries alimentaires, pharmaceutiques et cosmétiques.

Vient ensuite l'Autorité Nationale de Sûreté avec le HFD du ministère des transports. L'instruction n°412 le définit comme étant le point de contact national permanent pour les questions de sûreté maritime, et ce vis-à-vis des autres gouvernements contractants, de la Commission européenne ou de l'OMI. Au niveau national, il a pour mission de « faciliter, suivre et informer sur l'application des mesures de sûreté maritime [ainsi que de] fournir des renseignements concernant les plans de sûreté des installations portuaires [dont les coordonnées des PFSO] ou des conseils aux agents de sûreté¹⁷⁰ ». De plus, en tant que point de contact national, il peut éventuellement être informé par ses homologues étrangers qu'un de leur navire, se trouvant dans une zone sous contrôle français, a émis une alerte de sûreté, et ce au titre de la Convention SOLAS, règle XI-2/13.1.4. Il transmet alors l'information à qui de droit, à savoir le CROSS Gris Nez. Le HFD du ministère des transports doit pareillement relayer les informations relatives à une alerte de sûreté d'un navire battant pavillon étranger mais naviguant en zone de compétence française aux autorités désignées de ce pavillon. Dans le cas d'un navire français émettant une alerte de sûreté à l'étranger, il doit prévenir les autorités riveraines de la zone.

Le CROSS Gris Nez, qui a notamment participé au groupe de travail ayant aidé à l'élaboration de l'instruction n° 413, est l'organisme français qui reçoit la notification des alertes de sûreté, et ce en application de la règle XI-2/6.2.1 de la Convention SOLAS, pour les navires français naviguant partout dans le monde. Les alertes sont généralement émises directement par les navires par le biais du SSAS. Mais il est également possible que le CROSS Gris Nez les reçoivent indirectement, trois cas sont alors possibles. Tout d'abord, ce peut être la compagnie maritime qui notifie l'alerte au CROSS si elle lui est parvenue en premier¹⁷¹. Ensuite, il est à noter que des alertes de sûreté peuvent également être émises « en clair », c'est-à-dire sans passer par le SSAS mais en utilisant les voies habituelles servant à envoyer un message de détresse – VHF – ou par tout autre moyen, notamment le téléphone portable par souci de discrétion. Elles peuvent ainsi être réceptionnées par l'organisme compétent avoisinant la zone de menace qui retransmettra immédiatement l'information au CROSS Gris Nez. Enfin, les autorités du pavillon d'un navire étranger informent le CROSS Gris Nez si leur navire est en haute mer, mais dans une zone relativement proche des territoires français, ou s'il est en mer territoriale française ou encore s'il est dans un port français. Ces autorités peuvent également contacter le CROSS ou centre équivalent outre-mer compétent pour la zone où est situé le navire menacé. L'alerte doit être traitée de la même façon que si elle était reçue via le SSAS.

Dès réception de l'alerte d'un navire en mer, le CROSS Gris Nez informe¹⁷², au niveau central, le HFD du ministère des transports et le SG Mer, ou à défaut le CICADMER¹⁷³. Le SG Mer doit répercuter l'alerte vers le SGDN, ainsi que vers le cabinet du Premier ministre. Parallèlement à cela, il doit demander au CICADMER de rédiger un message pour en informer les ministères concernés. Le HFD du ministère des transports, pour sa part, doit informer officiellement la compagnie maritime. Il est à noter qu'une fois l'alerte émise, une procédure de levée de doute est engagée via le CSO contractuel du navire. Celui-ci tente de contacter le navire sous prétexte d'un

¹⁷⁰ Sur ces deux derniers éléments, la définition fait référence aux points B/4.14 à B/4.16 du Code ISPS.

¹⁷¹ Cf supra 2.1.1.5 L'instruction n° 413, page 30.

¹⁷² Cf supra 2.1.1.5 L'instruction n° 413, page 30.

¹⁷³ Centre interministériel de coordination d'aide à la décision MER. Il dépend de l'Etat Major de la marine nationale.

message de routine, en utilisant, par exemple, un code établi entre eux au préalable. En l'absence de réponse, il faut considérer que l'acte de violence est en train d'être perpétré (paragraphe 4.2.2, MSC/Circ. 1073). Si la compagnie confirme au HFD du ministère des transports qu'il s'agit d'une fausse alerte, ce dernier doit en informer le CROSS Gris Nez qui, à son tour, doit immédiatement prévenir tous ceux qu'il a déjà contactés. Si l'alerte s'avère fondée, le HFD du ministère des transports doit en informer le Commandant de la zone maritime Atlantique au titre du contrôle naval ainsi que le représentant permanent français auprès de l'Etat riverain, si le navire est en mer territoriale étrangère. Il doit également donner l'ordre au CROSS Gris Nez d'informer le MRCC étranger compétent pour la zone où se trouve le navire.

Au niveau territorial et si le navire est en zone SAR¹⁷⁴ française, le CROSS doit prévenir le PREMAR ou le DG/COMAR outre-mer ainsi que le CROSS ou le centre équivalent outre-mer le plus proche de l'incident. Si la situation du navire peut avoir des répercussions terrestres – s'il est proche des côtes françaises –, le PREMAR ou le DG/COMAR avertit à son tour le préfet de zone de défense, ou l'autorité équivalente outre-mer. Ce dernier prévient ensuite le préfet de département susceptible d'être désigné comme autorité locale chargée de la direction des opérations à terre. Quant au CROSS ou au centre équivalent d'outre-mer proche de l'incident, il fournit au PREMAR, ou au DG/COMAR, les informations nécessaires à la gestion de la menace et qui sont contenues dans la circulaire MSC/Circ. 1073, paragraphes 4.2.1 et 4.2.2. Il peut également solliciter les unités de sauvetages qualifiées pour cette opération, sachant que leur intervention dépend uniquement de la décision de l'« autorité responsable de l'opération » (paragraphe 4.3.3, MSC/Circ. 1073).

Si le navire n'est pas dans une zone SAR française, il convient de prévenir au niveau territorial, le commandant de zone maritime et le MRCC étranger compétent à cet endroit. Enfin, conformément à la règle XI-2/6.6 de la Convention SOLAS, l'Etat du pavillon doit immédiatement informer l'Etat ou les Etats étranger(s) riverain(s) de la zone d'alerte, qui est/sont dès lors impliqué(s) dans la crise. L'initiative de cette décision politique dépend du cabinet du Premier ministre car elle ne peut être que gouvernementale.

Si l'alerte provient d'un navire dans un port français¹⁷⁵, la procédure reste sensiblement la même si ce n'est que le CROSS Gris Nez doit prévenir, dès réception de l'alerte, et ce au même titre que le SG Mer et le HFD du ministère des transports, la Capitainerie du port concerné ou, à défaut, la permanence mise en place par « l'autorité investie du pouvoir de police portuaire », à moins qu'elle n'en soit déjà informée. La Capitainerie, ou la permanence, prévient à son tour le préfet de département ou le représentant de l'Etat dans la collectivité d'outre-mer. Il incarne l'autorité compétente pour mettre en œuvre les mesures d'intervention et commande les forces de sûreté, ces fonctions étant définies dans le paragraphe 4.1.1, MSC/Circ. 1073. La Capitainerie, ou la permanence, informera pareillement le service de police ou de gendarmerie compétent dans le port, le PREMAR, ou le DG/COMAR d'outre-mer, le CROSS ou le centre équivalent outre-mer le plus proche du lieu de l'alerte, la compagnie ou son représentant local, le PFSO, voire l'agent de

¹⁷⁴ *Search And Rescue* ; au niveau international, l'appellation la plus employée est *Sea Rescue Region* (SSR).

¹⁷⁵ Cf supra 2.1.1.5 L'instruction n° 413, page 30, fiches n°6 et n°7.

sûreté portuaire, ainsi que toute autorité ou personne prévue par le plan de sûreté de l'installation portuaire et/ou par le plan de sûreté portuaire.

L'action concrète qui suit une alerte avérée ne dépend plus des prescriptions ISPS mais de Pirate-mer en France. Ce plan gouvernemental relève de la compétence du PREMAR en mer. Toutefois, si le navire concerné est situé dans un port français, le préfet de département, ou le représentant de l'Etat dans la collectivité d'outre-mer, est compétent au niveau portuaire et est placé à son tour sous l'autorité de la cellule interministérielle de crise. Dans ce cas, le PREMAR, ou le DG/COMAR outre-mer, peuvent s'appuyer sur le CROSS, ou le centre équivalent outre-mer, géographiquement compétent. Ce dernier peut, si besoin est, organiser l'action des unités de sauvetage. Sinon, pour ce qui est de la lutte antiterroriste « active », ce sont les unités d'intervention qui agissent, à savoir notamment le GIGN¹⁷⁶ et les commandos marine¹⁷⁷. Enfin, d'un point de vue plus global, il convient d'observer que la marine nationale, dans son ensemble, joue un rôle significatif dans la protection du littoral français à travers le concept de « sauvegarde maritime » qu'elle développe depuis trois ans¹⁷⁸. Elle a notamment travaillé à la mise au point du système de surveillance SPATIONAV¹⁷⁹ en relation avec la douane et les AFFMAR.

Les inspecteurs des centres de sécurité des navires (CSN)¹⁸⁰ sont également impliqués au niveau des contrôles des mesures ISPS alors qu'à l'origine, ils ne faisaient appliquer que la convention SOLAS sur la sécurité maritime. Ils ont du suivre une formation pour être habilité ISPS et peuvent, lors de leur visite de contrôle, consulter l'intégralité du SSP, même les parties confidentielles. Toutefois, le Capitaine ne doit les leur montrer qu'après avoir obtenu l'approbation écrite de l'Etat du pavillon. Les inspecteurs des CSN procèdent de la même façon que pour un

¹⁷⁶ Groupe d'Intervention de la Gendarmerie Nationale créé en 1975.

¹⁷⁷ Au nombre de cinq – Commandos Hubert (action sous-marine), Jaubert (assaut), Trepel (assaut), Penfentenyo (reconnaissance) et De Montfort (appui et destruction à distance) –, ils sont également dénommés les « Bérêts verts ». Ils interviennent pour le COS – Commandement des opérations spéciales créé en 1992 et regroupant 2 000 militaires. Le COS est leur employeur majoritaire (environ 80% des interventions) mais l'Etat major de la marine fait aussi appel à eux pour des missions de service public (arraisonnement de bâtiments en mer, contrôle du trafic maritime, sauvetage en mer). Site du GIGN : <http://www.gign.org/unites-francaises/cos.php> –. Seuls deux commandos marine sont particulièrement spécialisés dans la lutte antiterroriste maritime. Le premier est le commando d'action sous-marine (CASM) Hubert. Basé dans le port du Canier sur la presqu'île de Saint Mandrier, dans le Var, il date du 30 mars 1953. Site de l'association Net Marine qui développe l'information militaire maritime française : <http://www.netmarine.net/forces/commando/hubert/>. Composé d'une cinquantaine de nageurs de combat brevetés, le CASM Hubert dispose d'une compagnie de soutien et d'une compagnie opérationnelle subdivisée en quatre sections, dont la section B, spécialisée dans le contre terrorisme maritime. La section B travaille en étroite collaboration avec l'escouade de contre-terrorisme et de libération d'otages (ECTLO) du commando Jaubert. Basé à Lorient, l'ECTLO Jaubert est issue de la scission du Groupe de combat en milieu clos (GCMC) suite à la réforme Commando 2001, l'autre partie ayant intégré le groupe B du commando Hubert. Elle compte 17 éléments et chacun a une spécialité bien déterminée, allant de l'armement et des munitions à la démolition et à la ciblerie, en passant entre autre par les renseignements, la progression individuelle et les effets spéciaux. Avec le GIGN, ces unités d'élite procèdent à des exercices antiterroristes en mer : dans l'Océan Atlantique, il s'agit de l'exercice Armor et en Méditerranée, de l'exercice Estérel.

¹⁷⁸ L'origine de ce concept date de l'échouement, dans la nuit du 17 février 2001, du navire *East Sea*, avec à son bord 900 réfugiés kurdes sur la plage de Boulouris, près de Saint-Raphaël.

¹⁷⁹ Système de surveillance des espaces sous juridiction nationale et des approches maritimes. Ce programme de surveillance radar a une portée théorique de 24 milles marins, soit plus de 44 km. Il permet le suivi et le positionnement des navires sur la zone de surveillance en temps réel. Les informations (nom et type du navire, son n° OMI, la route suivie, le type et le poids des marchandises, etc) sont fournies par le réseau de sémaphores en place le long des côtes et il ne concerne que la Méditerranée actuellement. Les navires sont obligés de répondre et les autres sémaphores ne redemandent ces détails qu'en cas de discontinuité au niveau de la réception de l'écho (informations obtenues lors du stage au CROSSMED en avril 2005).

¹⁸⁰ Ils interviennent dans le cadre de la directive du Conseil européen n° 95/21/CE du 19 juin 1995 concernant l'application aux navires faisant escale dans la Communauté européenne ou dans les eaux relevant de la juridiction des Etats membres, des normes internationales relatives à la sécurité maritime, à la prévention de la pollution et aux conditions de vie à bord des navires. Informations obtenues lors d'un entretien au CSN de Marseille le lundi 4 juillet 2005 avec Serge Heyraud, inspecteur habilité ISPS.

contrôle Paris MOU¹⁸¹ : s'il trouve un dysfonctionnement au niveau de la sûreté, ils incluront dans leur rapport une déficience, sachant qu'une seule annotation de la sorte peut entraîner l'immobilisation du navire. Ils doivent demander quel type d'exercice ont été effectués, quel en a été le résultat – positif ou si des problèmes sont apparus –, qui a participé – le but étant de s'assurer que ce ne sont pas toujours les mêmes qui s'entraînent sinon les exercices perdent de leur intérêt –. En cas de doute à propos d'un navire, le Commandant d'un port peut leur demander de monter à bord pour vérifier la capacité de l'équipage à gérer l'ISPS puis de faire un rapport sur leur visite.

Il est à noter enfin que l'administration française a procédé à des recrutements consécutifs aux nouvelles mesures de sûreté en vigueur¹⁸². Au cours du Conseil interministériel de la mer qui s'est tenu en avril 2004, il a été décidé que 40 postes supplémentaires d'officiers de port et d'officiers de ports adjoints¹⁸³ devaient être créés. En application de cette décision, 15 postes ont été pourvus en 2004 et 15 autres inscrits dans le projet de loi de finances pour 2005.

Par ailleurs, l'inspection générale de l'administration, de la police nationale et des finances, et le conseil général des ponts et chaussées, ont émis en 2004 une première estimation sur les coûts de mise en œuvre de l'ISPS dans les ports qui s'élevait à 111 millions d'euros en investissement et à 60 millions d'euros en fonctionnement. Ces chiffres se sont révélés assez proches de ceux inclus dans le rapport d'expertise de juin 2004, à savoir 100 millions d'euros en investissement et 63,3 millions pour le fonctionnement. La question du financement n'est pas encore définitivement établie car il est impératif de ne pas établir de distorsion de concurrence entre les ports européens comme le souligne le point 15 du règlement (CE) n°725/2004. Toutefois, la répartition devrait être telle qu'annoncée dans le projet de loi de finances 2005 : une partie devrait être financée par la Commission européenne ; l'Etat devrait ensuite prendre en charge les dépenses relevant strictement des engagements internationaux pris par lui ¹⁸⁴ « à titre permanent et dans l'intérêt général » dans la mesure où la sûreté est une mission régalienne de l'Etat, ce qui est estimé à 29 millions d'euros en investissement et 25 millions d'euros en fonctionnement; enfin, le financement des mesures de contrôle des sites¹⁸⁵, qui sont également profitables d'un point de vue sécuritaire, resteront à la charge des opérateurs privés. Ces coûts sont évalués à 60% des investissements et 64% du fonctionnement.

Le projet de loi prévoit également l'instauration d'une taxe portuaire sur les passagers des ferries et les croisiéristes. Provisoire, sa durée de vie est estimée à trois ans, le temps de rassembler les fonds nécessaires. La proposition table sur 2 euros par passager ferry piéton et 5 euros pour les véhicules. Cette taxe serait reversée à l'Etat qui l'injecterait en retour dans le financement de la sûreté portuaire.

¹⁸¹ Mémorandum de Paris.

¹⁸² Site du Sénat : <http://www.senat.fr/rap/a04-076-20/a04-076-2016.html>.

¹⁸³ Il est à noter qu'ils n'ont pas la qualité d'officier ou d'agent de police judiciaire.

¹⁸⁴ Celles-ci englobent les dépenses relatives aux PFSA et aux PFSP, à la formation et à la rémunération des PFSO, aux équipements de contrôle des conteneurs utilisés essentiellement par la douane, à savoir les scanners et aux contrôles sûreté des passagers.

¹⁸⁵ Il s'agit entre autre de la pose des clôtures, de l'organisation et de la gestion du gardiennage, de l'accroissement du rôle des officiers de port.

2.2.2. Au niveau local

Le préfet de département a une compétence en matière de sûreté portuaire – sur les activités portuaires et les plans d'eau dans les limites administratives du port – du fait que le Code ISPS s'applique également aux installations portuaires. Pour les Bouches du Rhône, il s'agit actuellement de Christian Frémont. Il est également préfet de la région Provence Alpes Côte d'Azur (PACA) et préfet de la zone de défense Sud¹⁸⁶. Il a notamment diligenté un exercice ISPS au PAM en novembre 2004¹⁸⁷, soit à peine quelques mois après sa prise de fonction. Cette initiative a regroupé les forces de police, la douane, les affaires maritimes et les services de sécurité du PAM, rassemblant ainsi quelques 130 personnes. Il s'agissait de la première coordination d'une telle envergure. Le *Tariq Ibn Ziyad*, en provenance d'Alger, a fait l'objet d'une inspection approfondie à son arrivée au port et avant de repartir. Au total, 520 personnes et 211 véhicules ont ainsi été contrôlés. Le résultat de l'opération a été une saisie de cigarettes et l'interpellation de trois passagers sans papier d'identité.

Le préfet maritime, quant à lui, est le représentant de l'Etat en mer, du Premier ministre et de chacun des ministres (article 1^{er} du décret n° 2004-112 du 6 février 2004)¹⁸⁸. Cet article précise également que son autorité s'exerce « à partir de la laisse de basse mer, sauf dans les ports à l'intérieur de leurs limites administratives et dans les estuaires en deçà des limites transversales de la mer ». Il a en charge les approches maritimes des ports et coordonne des administrations de l'Etat en mer. Officier général de marine (article 5) et commandant de zone maritime (article 6)¹⁸⁹, il a vu ses compétences s'élargir grâce à ce texte. Dans la mesure où il dispose d'une double casquette militaire et civile, il a une perception globale de la défense des intérêts nationaux en mer. Dans l'optique de l'action de l'Etat en mer¹⁹⁰, il peut faire appel aussi bien à la douane qu'à la gendarmerie maritime ou nationale, aux affaires maritimes ou encore à la marine nationale. Il dirige par ailleurs des « cellules de coordination de l'information maritime » regroupant les mêmes intervenants. Il a un rôle de soutien et d'appui quant aux mesures techniques et interviendra si le port refuse l'accès à un navire ou s'il l'expulse pour lui trouver, en liaison avec les autorités portuaires, une zone de mouillage. Enfin, il organise la visite en mer des inspecteurs habilités ISPS vu précédemment ainsi que la protection de cette équipe et de l'environnement immédiat du bateau.

2.3 Les navires/les armateurs

Pour se conformer aux exigences du Code ISPS, les armateurs ont du prendre un certain nombre de mesures, dont la nomination d'un agent de sûreté de la compagnie maritime (CSO) pour chaque navire ainsi que celle d'un agent chargé de la sûreté à bord (SSO) et leur formation.

¹⁸⁶ La zone de défense Sud comprend la région PACA, le Languedoc-Roussillon et la Corse.

¹⁸⁷ Article paru dans *Metro*, *Opération de contrôle au port*, novembre 2004.

¹⁸⁸ Publié au JO n° 32 du 7 février 2004, page 2616 texte n°4. Site de Legifrance : <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=PRMX0300220D>.

¹⁸⁹ Les fonctions d'un commandant de zone maritime sont notamment définies à l'article 3 du décret n° 74-968 du 22 novembre 1974 qui fixe l'organisation des commandements de zone maritime. Il est chargé, entre autre, du contrôle naval déterminé par le décret n° 73-247 du 11 mars 1973.

¹⁹⁰ Il est à noter que l'action de l'Etat en mer regroupe la lutte contre le terrorisme, contre le trafic de stupéfiants, contre les pollutions, contre l'immigration illégale ainsi que le contrôle des pêches.

Le premier doit s'assurer que l'évaluation de sûreté du navire (SSA)¹⁹¹ a été menée à bien et que le navire a, à son bord, un plan de sûreté (SSP)¹⁹² approuvé par l'administration chargée de cette tâche. Il est à noter que l'évaluation aussi bien que le plan doivent être remis à jour régulièrement. Le SSO doit s'assurer pour sa part que le plan de sûreté est correctement appliqué à bord en procédant à des exercices et en sensibilisant l'équipage aux nouvelles mesures de sûreté.

Le SSP doit notamment empêcher que des marchandises interdites¹⁹³ ne soient introduites à bord, l'équipage devant veiller à ce que la cargaison chargée soit conforme au manifeste. Mais il doit également inspecter le contenu des approvisionnements et s'assurer pareillement qu'il est bien analogue à la commande avant que de l'accepter à bord. Parallèlement à cela, les conditions d'accès à bord doivent être renforcées avec un premier contrôle à la coupée, qui peut être elle-même sécurisée par une porte en acier gardée¹⁹⁴. L'une des méthodes les plus pratiquées consiste à y poster un matelot qui doit demander à toute personne voulant monter à bord d'inscrire son identité, son heure d'arrivée et de départ sur un registre et il doit s'assurer qu'elle a une autorisation. Si la personne en question n'est pas prévue sur la liste des visiteurs attendus, le Capitaine en est immédiatement informé et donne des instructions. Ce système permet de savoir en permanence qui est à bord et rassure les Capitaines qui se déclarent heureux désormais de pouvoir identifier la personne qu'ils viennent de croiser dans une coursière.

De plus, un panneau d'avertissement est apposé en haut de l'échelle d'accès au navire et indique clairement les nouvelles mesures de sûreté ; comme vu au port autonome de Marseille lors d'une visite des installations le 1^{er} août 2005 avec un inspecteur du centre de sécurité des navires, il peut par exemple indiquer : « *Only authorized visitors shall be allowed on board* » ou « *Prohibited Access : Any person who wants to board will have to decline identity for ship's security.* » ou encore « *The watchman has the right to make body and luggage searches at any time to keep the ship's security. The Master* ». En effet, l'équipage peut et doit vérifier le contenu des bagages de toute personne désireuse de monter à bord. Il peut également procéder à des fouilles corporelles, soit à l'aide d'un détecteur de métaux portatif, soit par le biais d'une fouille tactile. Certains navires, notamment ceux à passagers, sont équipés d'un portique de détection semblable à ceux des aéroports. Il est installé soit avant l'échelle d'accès, à même le quai, soit à l'intérieur du bateau, juste après le premier sas d'entrée.

Une fois tous les contrôles effectués, un badge d'accès temporaire est remis au visiteur et son numéro est reporté dans le registre à côté des autres renseignements déjà inscrits pour cette personne. L'essentiel est ici de toujours pouvoir relier un badge à une personne physique. Le registre doit être tenu de la même façon que ceux gardés sur le pont ou à la machine, à savoir que les informations doivent être écrites à l'encre et doivent être lisibles. Les officiers de l'Etat du

¹⁹¹ Prescrite par la section A/8 du Code ISPS, il s'agit d'une étude méthodique des risques qui est fonction des mesures de sûreté existantes, de la menace potentielle, des points faibles à bord.

¹⁹² Le plan de sûreté de chaque bâtiment doit être fonction des spécificités d'un navire en particulier pour être efficace. Il doit permettre de protéger les personnes à bord, la cargaison, les provisions de bord et le navire lui-même (section A/9 du Code ISPS). Il doit établir les différentes mesures à prendre en fonction du niveau de sûreté.

¹⁹³ Armes, substances dangereuses et engins destinés à être utilisés contre des personnes, des navires ou des ports et dont la présence à bord n'est pas autorisée (section A/9.4.1 du code ISPS).

¹⁹⁴ Cf Annexe IV: Les équipements de sûreté. Il est à noter que la plupart des équipements de sûreté auxquels il est fait référence ont été consultés sur le site de Secopex :

<http://www.isps.fr/ISPS-materiel-equipement-securite-protection.htm>.

pavillon ou des membres de l'autorité portuaire peuvent demander à consulter ce registre. Les équipages sont également souvent munis d'un badge d'identité, de préférence avec leur photo, en attendant la pièce d'identité uniformisée au niveau international sur laquelle travaille l'OIT. Sur les navires à passagers, il existe même parfois un système avec une carte électronique que les membres d'équipage doivent passer dans une borne de contrôle.

Il est à noter que, dans la mesure où la surveillance et la vigilance sont parmi les meilleurs moyens pour diminuer la vulnérabilité des navires, les rondes sur le pont doivent être intensifiées et l'usage généralisé des talkies-walkies recommandé. Le réseau de caméras de surveillance participe de fait aux nouvelles mesures de sûreté et peut s'avérer très utile en cas d'alerte pour savoir immédiatement qui est en cause. Sur les navires de commerce, il s'agit d'un élément nouveau. L'installation s'est avérée quelque peu problématique au niveau technique dans la mesure où les navires marchands naviguent dans des zones qui sont sujettes à de fortes perturbations météorologiques. Il a donc fallu les équiper avec du matériel particulièrement résistant et donc onéreux. A priori, seules les zones sensibles ou celles d'accès restreint sont surveillées. Pour ce qui est des navires à passagers, ils en sont déjà équipés depuis un certain temps, même s'il est vrai que le nombre de caméras – désormais multidirectionnelles et équipée d'un zoom puissant – a été augmenté, si bien qu'à l'heure actuelle, aucun centimètre carré du bâtiment n'échappe à la vidéosurveillance. Toutefois, ce système n'est pertinent que si une personne est devant les écrans de contrôle pour vérifier en temps réel ce qui se passe sur le navire ; sinon, il ne s'agit que de mesures de contrôle postérieur, voire d'éléments de preuve en cas d'enquête, qui n'ont en réalité pas grand intérêt – dans le cadre de l'ISPS bien sûr – une fois la menace à exécution puisque le propre de ce Code est la prévention des actes malveillants et non pas l'action ou les sanctions a posteriori. Un autre élément s'intégrant dans le dispositif de surveillance est l'éclairage. Quand le navire est à quai ou en approche, toutes les zones sensibles doivent être correctement éclairées à bord et le plan d'eau attenant au bâtiment aussi, de façon à repérer les éventuels intrus.

Le plan rend également obligatoire la sécurisation des zones d'accès restreint ou des quartiers de l'équipage. L'interdiction d'accès doit être clairement matérialisée, soit par un panneau d'interdiction, soit en peignant la porte d'une couleur différente, soit par une combinaison des deux. Les dispositifs employés peuvent être, en plus des portes fermées à clé ou par un cadenas, l'existence d'un premier sas. Il barre ainsi l'entrée ou l'accès aux escaliers extérieurs permettant entre autre d'accéder au château à l'aide d'une grille ou d'une sorte de « pré-porte » en acier, la porte étant ensuite elle-même munie d'un verrou intérieur. Des digicodes ou des lecteurs de cartes magnétiques sont alors souvent installés pour permettre d'ouvrir ces portes sécurisées mais le problème a été le même que pour la vidéosurveillance. Pour le réseau extérieur, il a fallu trouver un système suffisamment résistant aux intempéries pour durer plus d'une traversée intercontinentale, ce qui a demandé pour certains armateurs près de six mois de recherche. Certains équipages utilisent à la place des verrous ou cadenas, des plombs en plastique destinés en temps normal à fermer les écoutilles ou aux conteneurs. Bien que moins résistants, ils ont toutefois l'avantage, par une simple vérification visuelle, de savoir immédiatement s'il y a eu effraction car ils sont à usage unique. Les hublots extérieurs des zones

réglementées peuvent également être sécurisés par l'apposition de grilles, tout comme les écubiers¹⁹⁵ qui sont parfois considérés comme des zones sensibles. Certains plans de sûreté ont même été jusqu'à énumérer les garde-rats¹⁹⁶ en tant que mesures de sûreté effectives. Enfin, la mesure ultime de protection du navire est le barrage électrique ¹⁹⁷ de 9 000 volts non mortels, pour l'entourer. Cette clôture électrifiée sert de dernier rempart de défense à la fois contre les pirates et le terrorisme maritime, et une alarme peut également être ajoutée au dispositif.

Le SSP doit également permettre de répondre à une menace de sûreté ou à une infraction aux mesures de sûreté¹⁹⁸. Dans cette optique, il doit expliciter les tâches du personnel du navire ayant des responsabilités en matière de sûreté, tout comme les rôles des autres membres de l'équipage dans ce domaine. La sûreté est une question de coopération et de travail d'équipe, c'est pourquoi tout l'équipage doit être correctement informé de ses devoirs et chacun doit y participer activement. La sensibilisation est primordiale c'est pourquoi il n'est pas rare de trouver à bord des panneaux d'information sur les divers aspects du Code ISPS, les dernières mises à jour, ainsi que les obligations mais également les avantages qu'il comporte.

Un autre point essentiel est la maîtrise des diverses mesures et équipements de sûreté¹⁹⁹ qui s'acquière via une formation spécifique et les exercices obligatoires de sûreté²⁰⁰. Ces nouvelles règles se doivent d'être de véritables automatismes pour être utiles. Il est tout aussi capital que les équipages soient bien conscients que, à tout moment, tout peut arriver et soient donc, dans toute la mesure du possible, préparés à l'inattendu.

Enfin, il est à noter que le plan doit donner au Capitaine le pouvoir et la responsabilité absolus de prendre des décisions concernant la sécurité et la sûreté du navire et de solliciter l'assistance, si besoin est (règle XI-2/8 de la Convention SOLAS). Mais les obligations d'un navire ne s'arrête pas à l'évaluation et au plan : il doit toujours conserver à bord des registres.

Les registres portent sur les activités visées par le plan de sûreté²⁰¹. Par ailleurs, une fois doté d'un plan approuvé, les navires font l'objet d'inspection et de contrôle²⁰² pour s'assurer que les mesures de sûreté requises sont concrètement et correctement appliquées (règle XI-2/9 de la Convention SOLAS). Si les navires sont effectivement en règle, un Certificat international de

¹⁹⁵ Ouverture ronde, percée à l'avant du navire, à droite et à gauche de l'étrave, pour le passage du câble relié à l'ancre.

¹⁹⁶ Petites planchettes en bois. Il en existe de deux sortes : des circulaires qui sont plus efficaces contre les rats ou des planchettes dont la partie inférieure comporte une encoche pour être à cheval sur la corde reliée à l'ancre.

¹⁹⁷ Cf Annexe IV: Les équipements de sûreté, page 112.

¹⁹⁸ Il s'agit entre autre des procédures d'évacuation des personnes à bord ou des dispositions pour maintenir les activités essentielles du navire ou de l'interface navire/port (section A/9.4.4 du Code ISPS).

¹⁹⁹ L'équipement le plus sensible du point de vue de l'utilisation au quotidien est le système d'alerte du navire.

²⁰⁰ L'un des exercices les plus communs est la recherche d'une bombe à bord entre deux piles de conteneurs. Il faut donc procéder à une fouille complète du navire, délimiter un périmètre de sécurité autour de la bombe qui va finir par exploser. Un incendie se déclare car la bombe était à proximité d'une marchandise dangereuse, il faut donc éteindre le feu en prenant toutes les précautions nécessaires dues à la classe IMO de la marchandise puis le bord doit appeler le siège de la compagnie pour l'informer des mesures prises. Tout l'intérêt de l'exercice est qu'il associe sûreté et sécurité. Informations obtenues lors d'un entretien avec le département sûreté d'un armateur.

²⁰¹ Il s'agit de la formation, des exercices pratiques, des menaces à la sûreté et incidents de sûreté survenus, des infractions aux mesures de sûreté, des changements des niveaux de sûreté, des communications liées directement à la sûreté du navire – et ce a fortiori en cas de menace spécifique à l'encontre du navire ou de l'installation portuaire –, des audits internes et examens des activités liées à la sûreté, des examens périodiques de l'évaluation et du plan de sûreté du navire, des modifications apportées au plan ainsi que de l'entretien, l'étalonnage et la mise à l'essai de tout matériel de sûreté à bord, y compris le SSAS (section A/10 du Code ISPS).

²⁰² Une vérification initiale complète est prévue, ainsi qu'une vérification de renouvellement tous les cinq ans, auxquelles s'ajoute au moins un contrôle intermédiaire, de préférence deux ans et demi après la vérification initiale et enfin tout contrôle supplémentaire décidé par l'Etat du pavillon est possible (section A/19.1.1).

sûreté (ISSC) attestant qu'ils sont en conformité avec le chapitre XI-2 de la Convention SOLAS et la partie A du Code ISPS leur est délivré (section A/19.3 du code ISPS). D'une durée maximale de cinq ans, il doit rester à bord pour pouvoir systématiquement être présenté sur demande, notamment lors des contrôles par l'Etat du port. Il est à noter que son temps de vie peut légalement être prorogé dans trois cas bien spécifiques²⁰³. A l'inverse, le certificat peut également perdre définitivement sa validité²⁰⁴.

Au début de la mise en place, des certificats provisoires d'une durée maximale de six mois étaient admissibles. Un an après, tous les navires, même les neufs, doivent impérativement avoir des certificats définitifs. D'ailleurs, un navire sortant d'un chantier naval et n'étant pas certifié n'aura pas l'autorisation de naviguer. Il subsiste uniquement deux cas dans lesquels un navire d'un Etat contractant peut être en possession d'un certificat international provisoire de sûreté : s'il change de propriétaire ou s'il change de pavillon. Dans ces deux seules éventualités, un temps de battement sera toléré.

Enfin, d'après une étude du comité de Transport Maritime de l'OCDE intitulée « La suppression de l'assurance de la navigation sous norme » rendue publique en juin 2004²⁰⁵, « la garantie d'un P&I club sera automatiquement suspendue – sous réserve du pouvoir d'appréciation dont disposent les administrateurs du club pour en décider autrement – si le niveau de classification n'est pas maintenu ou si l'assuré/le membre manque aux obligations réglementaires de la société de classification ou de l'Etat du pavillon ou à celles prescrites à la fois par le Code ISM et par le Code ISPS. La garantie est aussi systématiquement suspendue si le navire change de gérant ». La sanction d'un P&I a une force de dissuasion incomparable par rapport à celle d'un simple assureur commercial car une compagnie maritime radiée d'un P&I de renom ne sera plus acceptée ensuite chez d'autres tout aussi réputés, le corollaire étant qu'elle devra avoir recours à un P&I moins renommé, donc, dans l'imaginaire collectif, moins sérieux, et pourrait ainsi se voir refuser l'entrée de certains ports pointilleux, ou en tout cas subir des contrôles plus approfondis.

2.4 Les ports

Il est un fait certain, c'est que, désormais, la politique d'ouverture du port sur la ville, qui prévalait voilà à peine quelques années, n'est malheureusement plus de mise. De plus, du fait de l'élargissement de la Communauté européenne et du Traité de Schengen, les contrôles d'accès aux frontières, et notamment dans les ports maritimes, étaient devenus dans un premier temps plus souples avant que d'être renforcés en 1996, suite à la recrudescence des mouvements terroristes en France²⁰⁶. Il est à noter par ailleurs que des comités locaux de sûreté portuaire existaient déjà en France depuis l'arrêté interministériel du 14 mai 1999. Pour ce qui est du Code ISPS lui-même, il impose, en premier lieu, de procéder à une évaluation de la sûreté de l'installation

²⁰³ Si, après la visite de renouvellement, le nouveau certificat ne peut être délivré avant la date d'expiration du précédent, le délai sera de cinq mois ; si le certificat arrive à échéance mais que le navire n'est pas dans un port apte à le contrôler, le délai sera de trois mois mais uniquement pour rallier le port de contrôle ; enfin, si le navire n'effectue que des voyages courts et que son certificat n'a jamais été prorogé, le délai sera de un mois maximum.

²⁰⁴ Les quatre possibilités que cela survienne sont si les contrôles pertinents ne sont pas achevés dans les délais spécifiés, si les visas prescrits suite à la vérification intermédiaire n'ont pas été apposés sur le certificat, si le navire change de propriétaire, enfin si le navire change de pavillon.

²⁰⁵ Site de l'OCDE : <http://www.oecd.org/dataoecd/39/4/34029659.pdf>.

²⁰⁶ Lamy manutention, n°11 octobre 2004, étude 360 : Sûreté des installations portuaires pages 360-2 à 360-60.

portuaire (PFSA)²⁰⁷ pour définir concrètement les risques auxquels elle est exposée. Cette évaluation doit ensuite permettre d'établir un plan de sûreté (PFSP) en complète adéquation avec l'installation portuaire. Il est à noter qu'en France, les deux doivent être approuvés par le Préfet de département et que le PFSP doit également être examiné par le Comité local de sûreté portuaire. Une fois approuvé, le plan doit être transmis à la DTMPL ainsi qu'au HFD du ministère des transports. Selon Christian Paris²⁰⁸, PFSO du port de Rouen, le PFSP est un excellent « moyen de donner l'alerte pour réagir [aux] menace [de sûreté] ». Il a les mêmes fonctionnalités que le SSP²⁰⁹ et la particularité de devoir établir des procédures pour faciliter les congés à terre du personnel du navire ou les changements de personnel, de même que l'accès des visiteurs au navire, y compris les représentants des services sociaux et des syndicats des gens de mer.

Il convient d'observer que, tout comme pour le navire, le PFSA et le PFSP ne sont pas figés et doivent être réactualisés en fonction des fluctuations de la menace et/ou des modernisations apportées à la structure même de l'installation portuaire, de façon à rester pertinents. Toutefois, l'Etat dans lequel se situe l'installation portuaire doit établir une liste des modifications qui ne doivent pas être décidées sans son approbation préalable (section A/16.6 du code ISPS).

Pour être conforme aux normes ISPS, l'installation portuaire doit également avoir un agent de sûreté de l'installation portuaire (PFSO) ayant reçu une formation adéquate (section A/18.1 du Code ISPS). Il est entre autre responsable de l'élaboration et du suivi du PFSP et ce même s'il ne l'établit pas directement. L'installation portuaire doit aussi se munir d'un certain nombre d'équipements de sûreté²¹⁰ qui sont fonction de son plan. Parmi les moyens les plus sophistiqués figure le système de vidéo détection. Il devrait progressivement remplacer la vidéosurveillance. Installé sur l'ensemble de la zone portuaire, il a un effet dissuasif en plus du contrôle des flux de personnes pénétrant dans l'enceinte du port, ce qui permet d'améliorer en parallèle la sécurité du site en réduisant les vols. Les caméras sont équipées de détecteurs de mouvement qui déclenchent une alarme sonore et visuelle au centre de surveillance et y affichent immédiatement l'image suspecte pour l'analyser en temps réel. Tout l'intérêt de ce dispositif réside en ce que les informations puissent être ensuite retravaillées à l'aide d'un ordinateur. Certains logiciels d'analyse d'images peuvent même s'adapter aux dernières technologies en matière de reconnaissance d'images, telles que la reconnaissance biométrique, l'identification des plaques d'immatriculation ou encore le numéro ISO d'un conteneur, ce qui permet une gestion des flux logistiques et une traçabilité des boîtes sur terminal.

Pour ce qui est ensuite de la transmission des données, il existe un dispositif de dernière génération tout aussi perfectionnée que le précédent, le Réseau Radio Maillé, RRM. Il s'agit d'un

²⁰⁷ Il s'agit d'identifier les infrastructures potentiellement à risques, les menaces plausibles et les faiblesses de l'installation portuaire (section A/15 du Code ISPS). Le plan doit donc décrire l'installation dans son ensemble, sa structure, son réseau électrique, son réseau d'eau ainsi que les mesures de sûreté à prendre spécifiquement aux trois niveaux de sûreté pour ce qui est du gardiennage, du pourcentage de contrôle à effectuer, de l'éventuel renfort de l'Etat au niveau 3, de l'échéancier des moyens à mettre en œuvre, etc.

²⁰⁸ Site de la CCI de Rouen : http://www.rouen.cci.fr/club_risques/cr_mai_2005.pdf.

²⁰⁹ Empêcher d'introduire dans l'installation portuaire ou à bord des navires amarrés des marchandises interdites, établir les procédures pour réagir face à une menace ou à incident de sûreté, expliciter les tâches du personnel (section A/16 du Code ISPS).

²¹⁰ Site de Secopex : <http://www.isps.fr/ISPS-materiel-equipement-securite-protection.htm>.

réseau sans fil basé sur la technologie Wi-Fi²¹¹, mais amélioré, pour la transmission numérique de données, de voies ou de vidéos. Sécurisé, ce système est modifiable à souhait et peut donc être étendu pour agrandir une installation de vidéo détection. Le premier intérêt de ce système est qu'il évite la pose de câbles, sachant qu'avec le génie civil, elle représente environ 40% du prix total d'un système de vidéosurveillance. Le second est qu'il rend possibles les connexions mobiles : de fait, les inspecteurs du contrôle par l'Etat du port et la douane peut accéder instantanément aux données des serveurs centraux, les agents de sécurité effectuant des rondes peuvent se connecter rapidement au fichier des empreintes digitales. Il est à noter que cette technologie, en pleine expansion, est largement employée aux USA et qu'elle permet de créer des réseaux à l'échelle d'une ville.

Puis viennent les équipements de sûreté plus classiques, le premier étant la clôture. D'après l'annexe 5 de la circulaire n° 323 de la DT MPL et du HFD Mer²¹², pour être efficace, une clôture doit mesurer au minimum 2,50 mètres de hauteur, et ce depuis l'instruction n° 3800 du SGDN. L'annexe ajoute qu'une clôture « devrait être dimensionnée – fondations et structure – pour résister à la pression d'un groupe de 25 ou 30 personnes (...). Des bavolets en partie haute, d'une longueur minimum de 50 cm, garnis de 3 fils ronce, inclinés de 45° vers l'extérieur, renforcent la protection quand le site s'y prête. Dans les zones exigeant une protection renforcée, la mise en place de concertina²¹³ peut être envisagée. Des clôtures doubles peuvent également être installées, l'intervalle étant éventuellement garni de concertinas [, mais] elles ne sont efficaces que si l'établissement d'un pont entre les clôtures est rendu impossible par leur écartement – 2 mètres au minimum – ou si les deux clôtures sont établies à des hauteurs différentes ».

L'inconvénient est que les clôtures ne font en réalité que délimiter le périmètre d'une propriété, c'est pourquoi, pour accroître leur efficacité, il vaut mieux les associer à un système de détection. Ceux-ci sont nombreux²¹⁴.

²¹¹ Contraction de *Wireless Fidelity* ou Accès Sans Fil à l'Internet (ASFI) en français. Un réseau Wi-Fi est un réseau conforme à la norme IEEE 802.11, standard international décrivant les caractéristiques d'un réseau local sans fil à haut débit (11 Mbps – Millions de bit par seconde – ou supérieur). Le Wi-Fi est basé sur une liaison utilisant des ondes radio-électriques (radio et infrarouges) en lieu et place des câbles habituels. Site de l'encyclopédie informatique libre CommentCaMarche.net : <http://www.commentcamarche.net/wifi/wifiintro.php3>. L'IEEE est l'Institut des ingénieurs en électromécanique et en électronique (*Institute of Electrical and Electronics Engineers*) et il a émis cette norme en 1997.

²¹² Cf infra 2.1.1.2 Les circulaires conjointes de la DT MPL et du HFD Mer, page 29.

²¹³ Rouleaux de fil de fer barbelés.

²¹⁴ Une première solution consiste à électrifier le grillage avec des impulsions non mortelles de 9000 volts qui déclenchent, parallèlement au choc électrique, une alarme, exactement comme pour le navire. Il existe ensuite plusieurs systèmes reposant sur l'utilisation de câbles : les nappes de fils tendus, d'un poids de 30 kilogrammes, sont fixées sur des têtes de détection et toute tentative de coupure ou d'écartement déclenche une alarme ; le maillage détecteur est composé d'un câble coaxial noué et bloqué par des coquilles en acier inox. Ce matériel ressemble à un grillage qui serait superposé sur la clôture et réagit dès que quelqu'un essaie de le couper ; un câble, électrique cette fois, peut aussi être dissimulé dans le réseau de concertina pour un taux de défaillance proche de zéro ; enfin, un câble en fibre optique fixé sur une clôture va analyser les vibrations causées par toute tentative d'escalade ou de coupure. L'avantage est que ce système ne se déclenche pas inutilement à cause de la pluie, du vent ou de la grêle et son périmètre de détection peut atteindre 400 m. Autre exemple, les barrières hyperfréquences, composées d'un émetteur et un récepteur. Le premier génère un faisceau d'énergie invisible vers le second, qui est implanté à une distance maximale de 200 m et qui traite le signal reçu en continu. Toute modification du signal est analysée et une alarme se déclenche si l'amplitude du signal est suffisante. Enfin, le dernier dispositif est celui dit de la détection enterrée, par le biais de tubes à pression enterrés à 25 cm dans le sol. Le principe de base est celui de la pression différentielle : les tuyaux sont remplis par un mélange d'eau et de glycol – composé chimique qui possède au moins deux fonctions alcool – et un capteur analyse toute variation de pression générée entre autre par le poids d'un corps. Ce système est couplé avec une alarme. Ce système a une couverture de détection de 200 m maximum.

L'éclairage a également un rôle important à jouer dans la sûreté en tant que deuxième méthode de sûreté le plus couramment utilisé. Il doit être suffisamment puissant et bien disposé pour permettre une surveillance effective des plans d'eau, des installations portuaires et de leurs abords immédiats.

La protection des accès, autre élément essentiel du plan de sûreté de l'installation portuaire, se décompose en deux temps. Il faut considérer en premier lieu les dispositifs matériels qui empêchent physiquement l'accès à la zone. Les grilles aux entrées et aux sorties des ports et les « dispositifs anti-bélier de régulation de trafic »²¹⁵ rentrent dans cette catégorie. Le contrôle des accès constitue le second élément. Il est particulièrement problématique au niveau de l'installation portuaire du fait du nombre d'individus qui circulent dans un port. Il peut être assuré par le biais de plusieurs moyens, dont le traditionnel système des badges et autres cartes à présenter aux barrières et tourniquets d'entrée et de sorties. Toutefois, comme pour le navire, il faut toujours être capable de les associer à un propriétaire physique. C'est pourquoi il vaut mieux privilégier les systèmes d'identification par empreinte digitale, avec mémorisation de celles du personnel, plutôt que les dispositifs de pass électroniques. Il est à noter que le contrôle aux accès doit être le plus rapide possible tout en restant impérativement fiable, de façon à ne générer aucun engorgement. Dans cette optique, le ministère français de l'intérieur travaille actuellement sur un projet de documents d'identité biométriques. Les informations recueillies sont retraitées par un système informatique qui permet de localiser n'importe quel individu présent sur site – visiteurs ou employés – ainsi que de conserver un historique des différents mouvements d'entrée et de sorties.

En ce qui concerne les visiteurs, il convient de demander à chaque personne souhaitant entrant dans le port son identité, le motif de sa venue, la durée de sa visite et des informations sur son véhicule s'il en a un. Il existe alors trois hypothèses : la première est celle du visiteur attendu et connu dont les empreintes sont déjà mémorisées et reconnues par les divers systèmes d'accès des endroits où il est autorisé à se rendre. La deuxième est celle du visiteur attendu mais inconnu, ses empreintes seront mémorisées après les contrôles d'entrée. Enfin, la troisième hypothèse est celle du visiteur non attendu et inconnu. Les renseignements recueillis à l'entrée de la zone portuaire sont transmis au PFSO dans les trois cas mais dans la dernière éventualité envisagée, le PFSO est immédiatement informé et décide de la conduite à tenir.

Du point de vue des salariés²¹⁶, il est à noter que l'introduction d'un système de contrôle aux accès ne peut se faire qu'en accord avec le Code du Travail, et ce dans la mesure où ce dispositif génère des changements au niveau des conditions de travail. La direction qui veut s'engager dans cette voie doit donc demander aux représentants des salariés, et notamment au Comité de l'hygiène, de sécurité et des conditions de travail, son avis sur la question. Parallèlement à cela, en France, il faudra par ailleurs suivre scrupuleusement les prescriptions de la Commission Nationale Informatique et Libertés (CNIL) en matière de fichiers informatiques nominatifs.

²¹⁵ Cf Annexe IV : Les équipements de sûreté, page 112.

²¹⁶ Informations recueillies sur le site de Secopex.

Enfin, au niveau technique, il convient d'observer qu'il existe des règles imposant, entre autre, de privilégier la sécurité des personnes. Il est par ailleurs requis de pouvoir procéder au déverrouillage à distance ou en local, en cas d'incendie, des dispositifs de sûreté. En outre, il est à noter que les compagnies d'assurances demandent, quant à elles, des « preuves d'intrusion intentionnelles », surtout en cas d'incident sans effraction.

Quant aux marchandises, elles peuvent être inspectées à l'aide de scanner mobile à rayons X montés sur des véhicules de type fourgon. Ce système, dit d'inspection non intrusive, permet de longer le véhicule à inspecter en roulant à vitesse réduite pour rechercher des clandestins, de la drogue, des matières explosives ou encore de matières radioactives. Il est à noter que les scanners représentent l'élément le plus onéreux du budget sûreté, si bien que, avant de s'engager dans une telle acquisition, il faut prendre en considération l'activité du port ainsi que ses prétentions commerciales – à savoir si le port compte, entre autre, participer à la CSI, au C-TPAT ou non –.

Il convient d'observer, en dernier lieu, que certains ports, notamment en Allemagne, ne laisse plus les véhicules pénétrer sur les terminaux. Les personnes souhaitant rentrer dans le port doivent laisser leurs véhicules personnels en dehors de l'enceinte portuaire et utiliser les navettes mises à leur disposition. Par ailleurs, le Conseil constitutionnel²¹⁷ s'est prononcé sur les conditions de fouille des navires et des véhicules. Les personnels de sécurité privés « ne peuvent procéder, sans le consentement de l'intéressé, qu'à l'inspection visuelle des bagages à main ; (...) l'opération dans le cadre de laquelle ils peuvent pratiquer, sauf refus des personnes concernées, des palpations de sécurité ou des fouilles de bagages à main ne peut être ordonnée que par le préfet, en raison de menaces graves pour la sécurité publique et de circonstances particulières, pour un temps et dans des lieux déterminés ; (...) les modalités ainsi prévues ne portent pas atteinte à la liberté individuelle ». Il en est de même pour les officiers de port et les officiers de port adjoints. Il apparaît donc que²¹⁸, si le préfet n'ordonne pas les contrôles comme vu ci-dessus, les opérations de contrôle prévues à l'article L. 324-4 du Code des ports maritimes sont susceptibles de porter atteinte aux libertés individuelles.

Deux remarques restent encore à faire en ce qui concerne la sûreté des installations portuaires. La première est que, en vertu de l'article L. 324-5, alinéa 4 du Code des ports maritimes, les agents de la douane « peuvent (...) procéder au contrôle des personnes, des bagages, des colis, des marchandises, des véhicules et des navires, à l'exception des parties à usage exclusif d'habitation et des locaux syndicaux ». La seconde concerne l'opposabilité aux tiers des PFSP. La section A/16.8 du code ISPS précisant qu'il « doit être protégé contre tout accès ou toute divulgation non autorisée », il apparaît que seules les dispositions communiquées ou rendues publiques peuvent être opposables aux tiers.

²¹⁷ Cons. const., 13 mars 2003, n°2003-467 DC, JO 19 mars 2003.

²¹⁸ Lamy manutention, n°11 octobre 2004, étude 360 : Sûreté des installations portuaires pages 360-2 à 360-60.

2.4.1 L'exemple du Port Autonome de Marseille²¹⁹

Le PAM s'étend sur 300 hectares à Marseille même – bassins ouest – et sur 10 000 hectares à Fos – bassins est –. Sa délimitation a été consacrée par un arrêté du 21 février 1994. Il compte 24 installations portuaires publiques utilisées pour une multitude de trafics – pétrolier²²⁰, chimique, gazier²²¹, vracs solides, vracs liquides, fruitier mais surtout passager et conteneurisé –. Tous les PFSP du PAM ont été approuvés, si bien que ses installations portuaires sont reconnues par l'OMI et répertoriées dans sa base de données²²². En échange, le port dispose d'une lettre d'approbation pour chaque PFSP, émise par les autorités françaises et qui correspond à une déclaration de conformité de l'installation portuaire, non obligatoire pour l'heure (section B/16.62 du Code ISPS). Elle peut être demandée par les navires car elle atteste que le PFSP est bien appliqué et que les mesures préconisées sont adaptées à l'installation portuaire concernée.

La sûreté au PAM dépend d'une organisation bien spécifique : elle concerne en premier lieu le directeur général du port, puis le Commandant du port qui relève de la Capitainerie, donc plutôt de l'aspect sécuritaire, et qui dispose de l'autorité de police portuaire. Viennent ensuite Pierre Deroi, qui est son adjoint direct en la matière, et Laurent Bauer, responsable de l'ensemble du département sûreté, tous deux se situant au même niveau hiérarchique, puis une soixantaine de personnes, y compris les administratifs, qui se dédie exclusivement à la sûreté, une dizaine d'entre elles assurant une permanence 24h/24h.

Le PAM doit traiter entre 27 et 30 navires par jour, ce qui représente un problème de sûreté minime à résoudre chaque semaine mais il n'y a jamais eu jusqu'à présent d'incident sérieux et les diverses procédures sont rentrées dans les habitudes pour Pierre Deroi. En cas d'alerte de sûreté dans l'enceinte portuaire, le port doit informer les autorités compétentes et laisser la main à la douane ainsi qu'à la gendarmerie maritime. Il est à noter que le contrôle des accès maritimes est à la charge de l'Etat, le port ne faisant que de la prévention à ce niveau-là à l'aide de radar, de caméras ou de vedettes pour investiguer si besoin est, mais un officier de port n'a pas à intervenir. Par contre, le contrôle des accès terrestres dépend logiquement du port : des sociétés de gardiennage privées vérifient l'identité des chauffeurs de camions qui viennent livrer ainsi que les badges d'accès de chaque individu souhaitant pénétrer dans le port²²³. Il existe actuellement 15 000 cartes portuaires permanentes pour les personnes travaillant dans l'enceinte du PAM, à savoir les agents portuaires, les agents maritimes, les représentants maritimes, les dockers et autres, sachant qu'au total, environ 40 000 personnes sont amenées à venir y travailler. Si bien que le PAM procède à des contrôles inopinés à l'intérieur du port ; il s'agit aussi

²¹⁹ Informations obtenues lors d'un entretien au PAM le vendredi 1^{er} juillet 2005 avec Pierre Deroi, responsable du bureau défense (il est en liaison avec la Préfecture et fait partie de sa cellule de crise), des plans de secours (antipollution, sauvetage, port refuge, de sécurité des terminaux et de sûreté) et agent de sûreté des installations portuaires du PAM, et au cours d'une conversation téléphonique avec Laurent Bauer, directeur du département sûreté du PAM, le mardi 9 août 2005.

²²⁰ Le PAM occupe le 3^{ème} rang mondial en tant que port pétrolier avec quelques 60 millions de tonnes de pétrole par an, Fos assurant 40% des besoins en pétrole brut de la France et alimentant aussi l'Allemagne et la Suisse.

²²¹ Le terminal GDF 1 fournit à lui seul 11% des besoins énergétiques français en méthane.

²²² Cette base permet de trouver les contacts ISPS par pays, d'avoir des détails sur les installations portuaires (n° ID du port, sa latitude, sa longitude, le point de contact sur place, la date d'approbation du PFSP et s'il a déjà été remplacé) et de savoir si un pays ou une installation portuaire ont mis en place des procédures sûreté alternatives (comme les USA par exemple). Site de l'OMI : <http://www2.imo.org/ISPSCode/ISPSInformation.aspx>.

²²³ J'en ai eu la preuve concrète lors de la visite du PAM le 1^{er} août : il est nécessaire de présenter ces papiers d'identité et/ou professionnels à chaque poste de contrôle.

bien d'une tactique d'intimidation que de dissuasion. Toutefois, pour ce qui est des marchandises ordinaires, les autorités portuaires n'ont pas à avoir connaissance de ce qui circule sur le port, cela relève de la douane. C'est le cas d'un transitaire qui va chercher sa marchandise, il l'amène sur le port, le plomb est apposé par la douane et il a une autorisation pour se rendre jusqu'au terminal. Le contrat passe du chauffeur du transitaire au manutentionnaire, qui stocke et surveille le conteneur, puis du manutentionnaire au navire. Le port n'intervient que pour les marchandises dangereuses qui dépendent du pouvoir régalien de la Capitainerie.

Comme le prévoit le Code ISPS, le PAM procède à des exercices de sûreté. L'un des scénarios envisageables est une tentative de pénétration dans l'enceinte portuaire pour évaluer la capacité de réaction des différents intervenants. Les exercices majeurs impliquent la cellule de crise de la préfecture de département, le parquet de Paris, la division nationales antiterroriste (DNAT), la brigade antiterroriste de Paris, la préfecture de police, le procureur de la République, la police, la douane, les pompiers, les AFFMAR voire les armateurs s'ils le souhaitent. Ce type d'opérations permet également de vérifier la pertinence des mesures nouvellement instituées, sachant que le PAM s'était penché bien avant sur la question et ce d'ores et déjà dans l'objectif de se prémunir contre d'éventuels actes terroristes – suite à la recrudescence de la menace en France au milieu des années 90 – mais aussi pour lutter contre la petite délinquance – notamment pour ce qui était des vols de conteneurs entiers –. Désormais, la gestion des conteneurs est informatisée et aucune boîte ne peut quitter l'enceinte portuaire sans vérification. Quant au contrôle du contenu, il est assuré par la douane à l'aide d'un scanner mobile²²⁴ qui a coûté près de cinq millions d'euros au PAM pour être accrédité CSI. Il peut traiter de 20 à 30 conteneur par heure, ce qui peut paraître assez lent mais reste suffisamment dissuasif. Pour ce qui est des autres mesures de sûreté, il est à noter que les moyens humains ont été renforcés – une soixantaine de personnes effectuent des rondes sur l'ensemble du domaine portuaire avec des voitures équipées de GPS pour une localisation plus facile si elle se font attaquées et sur 105 personnes employées par la Capitainerie, 55 sont affectées à la sûreté –. Par ailleurs, plus de 200 caméras sont déjà en place – l'objectif étant d'atteindre les 300 d'ici peu – et sont reliées à des PC sûreté qui retraitent l'information, sachant que chaque bassin compte deux PC sûreté, un pour les accès terrestres et l'autre pour les accès maritimes qui sont surveillés par les officiers de la Vigie. Enfin, l'enceinte portuaire est équipée d'un double système de clôtures, la première pour définir les limites extérieures du port et la seconde entoure les terminaux. Il convient finalement d'observer qu'en cas d'alerte, la configuration du PAM est telle que si les différents ponts qui le composent sont ouverts, le port est alors divisé en plusieurs zones infranchissables, de façon à isoler la menace.

Pour terminer, il est à noter que l'ensemble des coûts engagés s'élève à près de 28 millions d'euros, ce qui est considérable mais il ne faut pas perdre de vue le fait que la facture aurait pu être nettement plus élevée du fait que ces mesures viennent en complément de ce qui existait déjà. Par ailleurs, le port n'impose à l'heure actuelle aucune taxe, ni aux navires, ni aux entreprises de transports routiers ni aux passagers.

²²⁴ Cf Annexe IV : Les équipements de sûreté, page 112.

2.5 Les gouvernements

Les gouvernements contractants doivent fixer les niveaux de sûreté²²⁵ appropriés en fonction de la menace au moment T et ils ne peuvent déléguer cette tâche (section A/4.3 du code ISPS) car ils sont un élément prédominant du dispositif de sûreté. En effet, les niveaux de sûreté établissent un lien entre le navire et l'installation portuaire car ils déclenchent l'application de mesures de sûreté adaptées à la situation du navire et de l'installation portuaire.

De plus, les gouvernements contractants doivent communiquer tous les renseignements relatifs à ces niveaux de sûreté aux navires battant leur pavillon, aux ports situés sur leur territoire ainsi qu'à tous les navires souhaitant entrer dans un de leur port ou y séjournant (règle XI-2/3 de la Convention SOLAS). Parallèlement à cela, les gouvernements ont une véritable obligation d'information envers l'OMI, notamment quant aux coordonnées du point de contact national – ce qui est totalement compatible, en France, avec l'article 6²²⁶ de la loi n°78-753 du 17 juillet 1978 (JO du 18 juillet) sur la communication des documents administratifs –. En outre, conformément à la règle XI-2/13.4, les Etats contractants doivent aussi fournir à l'OMI, tous les cinq ans, une liste indiquant tous les PFSP approuvés ainsi que le ou les lieu(x) concerné(s) par les PFSP et la date d'approbation.

Enfin, l'Etat a en charge de délivrer les ISSC et doit contrôler l'application des prescriptions de sûreté en procédant à des inspections à bord des navires (règle XI-2/9 de la Convention SOLAS).

2.6 Les grandes lignes de l'application dans le reste du monde

2.6.1. Aux USA

Le Congrès étatsunien a adopté une loi le 14 novembre 2002 fixant un certain nombre d'exigences en matière de sûreté, dont le fait de conduire des évaluations de vulnérabilité, d'avoir des cartes de sûreté portuaire et de mettre en place le système AIS tout en imposant de lourdes sanctions pénales en cas de non respect. Le 1^{er} mars de l'année suivante, le *Department of Homeland Security*²²⁷ était créé.

Puis, dès le 1^{er} juillet 2004, les garde-côtes étatsuniens ont clairement fait savoir qu'ils comptaient monter à bord de tout navire ne respectant pas les nouvelles règles de sûreté maritime lors de sa première venue post-ISPS dans un port étatsunien²²⁸. Dans le même ordre d'idées, le secrétaire à la défense Donald Rumsfeld a immédiatement déclaré que les USA ne ménageraient en aucun cas leurs efforts en matière maritime chaque fois que les bénéfices seraient supérieurs aux coûts. La forte implication étatsunienne dans l'ISPS s'explique bien évidemment en premier

²²⁵ Le premier niveau correspond à des mesures minimales applicables en continu, le deuxième à des mesures additionnelles renforcées et le troisième à des mesures exceptionnelles pour un laps de temps déterminé.

²²⁶ Il interdit de communiquer des documents administratifs qui porteraient atteinte à la sûreté de l'Etat, à la sécurité publique ou à la sécurité des personnes. Lamy manutention, n°11 octobre 2004, étude 360 : Sûreté des installations portuaires pages 360-2 à 360-60.

²²⁷ Equivalent à un ministère de la sûreté intérieure qui regroupe quelques 22 agences fédérales.

²²⁸ Site de *The Economist* : http://www.economist.com/agenda/displayStory.cfm?story_id=2804108.

lieu par l'obsession sécuritaire qui est la leur suite aux attentats du 11 septembre 2001 mais en second lieu, elle vient également de l'importance du secteur maritime pour ce pays. Il est à noter²²⁹ que ce pays a un littoral de 142 641 km, 60 000 navires au long cours touchent les 361 ports étatsuniens chaque année et que la moitié des importations étatsuniennes arrivent par voie maritime, dont 90% par conteneur. Le Commandant des garde-côtes étatsuniennes a chiffré les dépenses totales pour l'industrie entraînées par les diverses mesures de sûreté à quelques sept milliards de dollars américains pour les années à venir²³⁰.

Les marines étatsunienne et australienne ont débuté leurs exercices dès octobre 2003, lors d'une application conjointe basé sur une interception. Le nom de code était « *Pacific Protector* » et il s'agissait de la première des 10 opérations prévues par ces deux nations.

De même, le 5 octobre 2003, les USA et l'Inde ont réalisé un exercice basé sur cinq jours. Ils l'ont dénommé « *Malabar-2003* » et il a impliqué plus de 2 000 individus évoluant dans le milieu naval. Selon le commandant hindou Manobar Nambiar, l'intérêt était d'accroître les capacités communes des deux corps de marine. Le scénario consistait à rechercher le navire suspect, avant de l'aborder et enfin à s'en emparer.

Il convient de noter en dernier lieu que, depuis le 23 mai 2005²³¹, les garde-côtes étatsuniens imposent des conditions d'entrée supplémentaires dans leurs ports aux navires qui, au cours de leurs cinq dernières escales, ont touché des Etats dans lesquels des mesures antiterroristes efficaces ne sont pas maintenues selon les USA. Les nations concernées sont la République démocratique du Congo, la Guinée-Bissau, le Libéria, la Mauritanie et Nauru. Les navires visés doivent impérativement opérer au niveau de sûreté 2. Par ailleurs, ils doivent avoir placé des membres d'équipage à chaque point d'accès du bâtiment lorsqu'ils séjournent dans un port d'un des Etats cités ci-dessus, de façon à avoir une « visibilité totale (...) sur les installations à quai et sur le plan d'eau ». Ils doivent également avoir consigné toutes les actions de sûreté entreprises par le navire dans le registre prévu à cet effet et doivent les indiquer sur la notice d'arrivée à remettre à la douane étatsunienne. Ils doivent se tenir prêt à remplir une DoS aux USA et à poster des gardes armés employés par une société privée à tous les points d'accès du navire quand ils seront dans un port étatsunien.

2.6.2. Au Canada²³²

L'amélioration de la sûreté du transport maritime n'est pas une nouveauté pour le Canada. Immédiatement après les attentats du 11 septembre 2001, les autorités canadiennes ont établi cinq priorités pour orienter la stratégie du gouvernement fédéral en matière de sécurité publique et de lutte antiterroriste. Le but est de dissuader et de détecter les terroristes avant de les

²²⁹ Site de l'Institut d'études internationales de Montréal : <http://www.er.uqam.ca/nobel/cepes/pdf/BULL71.pdf>.

²³⁰ Site de Salvamos, association européenne pour la recherche, la formation et le sauvetage en milieu aquatique : <http://www.salvanos.org/modules.php?op=modload&name=News&file=article&sid=523&mode=thread&order=0&hold=0>.

²³¹ Notice USCG – 2005 – 21093 du 2 mai 2005. Les garde-côtes se sont basés sur la section 70110 du MTSA qui permet au *Secretary of Homeland Security* d'imposer de nouvelles conditions d'entrée vis-à-vis de ports qui ne respectent pas les mesures ISPS. Site du *Department of Homeland Security* : http://www.dhs.gov/interweb/assetlibrary/HSSTAC_MtgNotice_2005May18-19.pdf.

²³² Site de la marine canadienne : http://www.marine.forces.gc.ca/mspa_news/news_issues_f.asp?category=4&title=30.

poursuivre ou de les expulser du territoire, d'améliorer les plans d'urgence visant la protection des infrastructures ainsi que de favoriser les initiatives internationales et les relations avec les USA pour que les navires immatriculés au Canada et respectant les normes de sûreté canadiennes puissent entrer dans les ports étatsuniens et vice versa. Puis les autorités canadiennes ont aussitôt pris toute une série de mesures préventives. Pour l'essentiel, il s'agissait pour les navires intercontinentaux de donner un préavis 96H avant de pénétrer dans les eaux canadiennes – contre 24H auparavant – ainsi que de se soumettre à un contrôle préalable à l'entrée dans le système des Grands Lacs et de la VMSL. Les protocoles d'arraisonnement ont été améliorés pour accélérer le temps d'intervention en cas de menace et le contrôle des conteneurs a été perfectionné par l'établissement d'équipes conjointes de la douane dans les principaux ports. Enfin, la présence policière a été accrue plus spécifiquement dans les installations dédiées aux croisières.

Dans cette optique, le gouvernement canadien a engagé 7,7 milliards de dollars canadiens, soit plus de 6 milliards de dollars américains, dans la lutte antiterroriste globale et la protection de la sécurité publique. Sur la totalité de la somme, 172,5 millions de dollars canadiens, soit près de 142 millions de dollars américains, ont été spécifiquement alloués à la sûreté maritime – dont 60 millions dès le budget de décembre 2001, soit 49 millions de dollars américains –, entre autre pour la surveillance aérienne des plans d'eau et la mise en place de l'AIS. Le versement de la somme a été échelonné sur six ans. Quatre groupes de travail incluant des représentants du gouvernement et de l'industrie maritime ont par ailleurs formé : un pour les navires, un pour les installations maritimes, un pour les unités mobiles de forage en mer et un pour le Programme d'accès aux zones réglementées des infrastructures maritimes. Leur tâche consistait à faciliter l'élaboration de la réglementation dans ces quatre secteurs clé.

Enfin, le Canada a satisfait aux exigences du Code ISPS par le biais de l'article 5²³³ de la Loi sur la Sûreté des Transports Maritime (LSTM). Il a en effet permis l'élaboration du Règlement sur la sûreté du transport maritime (RSTM) du 21 mai 2004²³⁴. Ce règlement met en œuvre l'intégralité de la partie A du code ISPS ainsi que certaines dispositions de la partie B. Il est à noter que le pays recense environ 100 navires immatriculés au Canada d'une jauge brute supérieure à 500 tonneaux et effectuant des voyages internationaux pour quelques 4 000 navires battant pavillon étranger d'une jauge brute supérieure à 500 tonneaux et faisant escale dans les ports canadiens. Le RSTM dépasse les exigences de l'OMI pour être plus en adéquation avec les particularités maritimes du Canada. Il s'applique en effet à tout « navire ayant une jauge brute supérieure à 100 tonneaux autres que les bâtiments remorqueurs », aux « bâtiments remorqueurs remorquant un chaland à l'arrière ou le long de son bord ou poussant un chaland, si le chaland transporte certaines cargaisons dangereuses » ainsi qu'aux installations portuaires les desservant

²³³ « Le gouverneur en conseil peut, par règlement, régir la sûreté du transport maritime et notamment : **a)** viser à prévenir les atteintes illicites au transport maritime et, lorsque de telles atteintes surviennent ou risquent de survenir, faire en sorte que des mesures efficaces soient prises pour y parer; **b)** exiger ou autoriser un contrôle pour la sécurité des personnes, des biens, des bâtiments et des installations maritimes; **c)** régir l'établissement de zones réglementées; **d)** régir la tenue et la conservation de dossiers et d'autres documents relatifs à la sûreté des opérations maritimes, notamment des copies de règlements, de mesures et de règles de sûreté; **e)** prévoir l'exigence du dépôt auprès du ministre de ces documents ou leur fourniture sur demande; **f)** régir la préservation et la restitution de tout élément de preuve saisi sans mandat ou de tout bâtiment retenu en application de la présente loi ».

²³⁴ Publié le 2 juin 2004 dans la partie II de la Gazette du Canada (Journal Officiel du gouvernement du canadien depuis 1841), Vol. 138, n° 11.

(article 401). Il est à noter que les navires soumis au Code ISPS et déjà présents dans les eaux canadiennes au 1^{er} juillet 2004 ont du faire état de leur Certificat international de sûreté avant de pouvoir ressortir du territoire canadien.

Au niveau procédural, Transports Canada a demandé à tous les acteurs concernés par les nouvelles exigences introduites par l'ISPS et par le RSTM de soumettre aux autorités leurs plans de sûreté au plus tard le 31 janvier 2004²³⁵, l'approbation de ces plans devant être terminée fin mai-début juin 2004. Les plans de sûreté des 13 écluses de la VMSL – considérées comme des zones contrôlées ; les postes de contrôle, les salles des machines, ainsi que le périmètre immédiat des navires étant des zones à accès réglementé – ont été approuvés dès le 4 juin 2004. Des attestations de conformité leur ont donc été délivrées²³⁶ car les équipements de sûreté – clôtures, barrières, serrures, caméras, etc – ont été renforcés ; de plus, suite au RSTM, les contrôles d'accès se sont durcis – ils reposent sur la présentation de pièces d'identité infalsifiables et plastifiées ²³⁷ – pour les sociétés d'approvisionnement et de services aux navires, pour les embarquements ou débarquements – d'un équipage océanique ou international, de membres de la famille, de pilotes ou pour les navires canadiens et étatsuniens –, pour l'accès des véhicules, pour les navires de croisière, les visiteurs inattendus ou les membres d'équipage voulant accéder au navire.

Il convient d'observer que dès le 1^{er} juillet 2004, des inspecteurs de la sûreté maritime de Transports Canada, de la VMSL et de la Garde côtière étatsunienne sont montés à bord de tous les navires étrangers qui sont entrés dans cette voie navigable par Montréal. Tous ceux n'ayant pas subi cette vérification initiale avant le 1^{er} juillet ont du la repasser, sauf ceux ayant subi un examen de conformité par les gardes-côtes étatsuniens et ayant reçu une lettre de conformité entre avril 2004 et le 30 juin 2004. Par ailleurs, la Corporation de gestion de la Voie maritime du Saint Laurent (CGVMSL) exige des déclarations de sûreté dans certains cas précis²³⁸.

Pour ce qui est du financement des nouvelles mesures de sûreté au niveau gouvernemental, les autorités canadiennes ont annoncé, le 7 mai 2004, le Programme de contribution pour la sûreté des installations portuaires. Ils y ont alloué 115 millions de dollars canadiens, soit près de 95 millions de dollars américains, dans le but de soutenir les 19 administrations portuaires canadiennes membres de l'association des administrations portuaires canadiennes (AAPC). Ce financement – à hauteur de 25% par les ports et de 75% par le gouvernement fédéral – permettra, selon les propos de Al Soppitt²³⁹, président de l'AAPC, « la mise en œuvre complète et efficace [des] plans [de sûreté] » par le biais de l'acquisition des équipements

²³⁵ Site du Groupe Canada Newswire :

<http://www.newswire.ca/fgov/fr/releases/archive/May2004/21/c6623.html>.

²³⁶ Site de la CGVMSL : http://www.greatlakes-seaway.com/fr/navigation/isps_bg.html.

²³⁷ Sont acceptables les permis de conduire, cartes d'identité avec une photo émise par une agence gouvernementale, passeports, cartes d'identité d'employé, cartes d'identité syndicale ou cartes d'identité de marin.

²³⁸ Pour les navires océaniques, la CGVMSL attendra l'avis de Transports Canada qui se basera sur les informations du préavis de 96H ou sur un changement de niveau de sûreté. Deuxièmement, les bateaux de navigation intérieure n'ont théoriquement pas à fournir une DoS. Troisièmement, une DoS sera exigée lorsque l'interface concernera un navire transportant des marchandises dangereuses en vertu de la réglementation étatsunienne 33CFR160.204. Quatrièmement, il en sera de même pour les navires dont le pays d'immatriculation n'est pas un Etat contractant. Enfin cinquièmement, une DoS est obligatoire quand l'interface concerne un navire de croisière. Les intervenants au niveau d'une DoS sont l'agent régional de la sécurité, le coordonnateur des services maritimes ou le superviseur de quart au moment où la demande est présentée et le CSO.

Site de la CGVMSL : http://www.greatlakes-seaway.com/fr/navigation/isps_adv.html.

²³⁹ Site de l'Association of Canadian Port Authorities :

http://www.acpa-ports.net/pr/releases/release_07052004-funding-f.html.

nécessaires. Le budget sûreté 2004 du port d'Halifax²⁴⁰ a lui dépassé les 1,5 millions de dollars canadiens, soit 1,2 millions de dollars américains et ce pour procéder à l'évaluation de la sûreté, pour acheter un nouveau navire patrouilleur pour le port, pour moderniser le système de vidéosurveillance ainsi que le système d'éclairage sur l'ensemble du domaine portuaire et enfin pour mettre en place des clôtures supplémentaires.

2.6.3. A Singapour

La sûreté portuaire de Singapour est une des plus serrées au monde. Basée sur des patrouilles intensifiées par les garde-côtes et la marine, elle possède parallèlement un réseau intégré de surveillance et d'information pour traquer et contrôler les activités suspectes. Afin d'éviter, dans toute la mesure du possible, que de petites embarcations croisent des navires de commerce à hauts risques, les routes de navigation ont été spécialement réorganisées. La République de Singapour a de plus mis en place un système d'escortes ponctuelles pour certains navires marchands qui empruntent le détroit de Singapour ou les eaux adjacentes.

2.6.4. En Chine²⁴¹

La Chine, grande nation maritime par définition, compte, au total, quelques 130 ports impliqués dans le commerce international, soit plus de 10 000 installations portuaires, ainsi que près de 2 000 navires battant pavillon chinois et effectuant des voyages internationaux, ce qui représentait un défi énorme selon les propos d'un représentant des communications de la République populaire de Chine. Pour se mettre en conformité avec l'ISPS, le gouvernement chinois a notamment créé deux textes qui reprennent les prescriptions de la réglementation internationale : le Code pour la sûreté des installations et le Code pour la sûreté des navires, qui sont entrés en vigueur respectivement en novembre 2003 et en mars 2004. Le but est de « garantir une application exhaustive » des nouvelles prescriptions de l'OMI.

Pour ce qui est de la sûreté portuaire, les autorités chinoises ont émis, au préalable, un « recueil de recommandations pour la pratique de la sûreté des installations portuaires ». Puis elles ont mis en place un groupe de travail dont la mission était de conseiller les industries portuaires, de coordonner leurs actions, d'évaluer la sûreté des installations portuaires ainsi que d'approuver les plans de sûreté. Fin octobre 2004, 590 installations portuaires avaient été certifiées, soit 95% du total estimé et plus de 1 700 personnes avaient été formées à la sûreté des installations portuaires.

Pour ce qui est ensuite de la sûreté des navires, la Société de Classification de Chine a été désignée comme organisme de sûreté reconnu et a été chargée de vérifier et de certifier les bateaux. Fin octobre 2004, 638 Certificats internationaux de sûreté avaient été décernés aux navires chinois au long cours, soit 93% du total estimé. La formation des personnels impliqués dans la sûreté des navires a également été mise en œuvre et un guide pour former les gardes de sûreté des navires ainsi que des compagnies maritimes a été édité.

²⁴⁰ Site du port d'Halifax : <http://www.portofhalifax.ca/AbsPage.aspx?id=1152&siteid=1&lang=2>.

²⁴¹ Séminaire de l'OCDE sur le transport maritime, organisé à Paris les 4 et 5 novembre 2004. Site de l'OCDE : <http://www.oecd.org/dataoecd/19/61/33949707.pdf>.

Pour s'assurer de la mise en place effective des nouvelles mesures de sûreté, le gouvernement chinois a organisé un exercice pratique de sûreté impliquant des navires et des installations portuaires le 30 juin 2004. Le résultat, positif, a confirmé que les systèmes de sûreté étaient effectifs dès le premier jour de l'entrée en vigueur des normes internationales. Toutefois, les autorités chinoises soulignent l'importance de réitérer ses exercices comme le prévoit expressément le Code afin d'éviter que l'habitude ne réduise leurs efforts à néant.

2.6.5. En Australie²⁴²

Le Premier ministre australien et son cabinet fixe la politique antiterroriste au niveau national et l'*Attorney General*²⁴³ ainsi que son équipe sont responsables de son exécution. Pour ce qui est de la composante maritime, l'équivalent du ministère des transports est responsable du développement de la politique de sûreté maritime et le service de la douane australienne a en charge la surveillance maritime. Les *Coastwatch*²⁴⁴ australiens sont une subdivision de la douane et ont à leur disposition tous les moyens dont dispose l'Unité maritime nationale de la douane, à savoir des aéronefs et des navires pour remplir cette mission.

Dès juillet 2004, le gouvernement australien a annoncé une série de mesures de sûreté maritime dont le coût a été estimé à 102 millions de dollars australiens, soit près de 79 millions de dollars américains, sur quatre ans. Il s'agit, entre autre, de fournir à l'Unité maritime nationale de la douane des équipements supplémentaires pour doubler sur l'année les sorties quotidiennes en mer, ainsi que de passer de 80 000 conteneurs examinés chaque année à 100 000. Des scanners à neutron, permettant de détecter des explosifs et d'autres substances illicites, ainsi que des chiens spécialement entraînés pour l'environnement maritime devraient être mis sur zone.

Les nouvelles dispositions doivent également permettre aux douaniers de monter à bord de la plupart des navires escalant pour la première fois dans le pays. A la fin de l'année 2004, ils accédaient à environ 80% des navires, contre à peine 40% en 2000. Parallèlement à cela, le réseau de vidéosurveillance de la douane devrait être étendu à 31 nouveaux ports pour compléter les 32 déjà équipés. Un nouveau système réglementaire demandant aux compagnies maritimes de fournir aux autorités des informations sur les passagers et l'équipage à bord avant l'arrivée du navire devrait être établi. Une carte d'identification de sûreté devrait également être introduite pour tous les employés de l'industrie maritime australienne et un certain nombre de pouvoirs limités supplémentaires devraient être accordés aux agents de sûreté maritime privés. Enfin, ces nouveaux engagements doivent renforcer la collecte de renseignements. Ils sont focalisés sur la « redistribution de l'information au moment opportun vers les ports clé du pays et l'industrie maritime en général ». Ils doivent aussi permettre une révision de la politique globale de sûreté du gouvernement australien pour ce qui est des équipements pétroliers offshore ainsi que des

²⁴² Site de l'Institut australien de politique stratégique :

http://www.aspi.org.au/pdf/Maritime_terrorism%20India_AB.pdf

²⁴³ En Australie, procureur général, ministre de la justice, ministre responsable de la police et des services de renseignements (*Australian Security Intelligence Organisation*, ASIO).

²⁴⁴ Les *Coastwatch* ne sont pas des garde-côtes dans le sens entendu aux USA ou encore au Royaume-Uni. Ils fournissent une assistance maritime civile, assistent un certain nombre d'agences gouvernementales, identifient et agissent contre la pêche illégale, assurent la protection de l'environnement maritime et contribuent à la protection des espèces du milieu marin (site de la douane australienne : <http://www.customs.gov.au/site/page.cfm?u=4238>)

installations de gaz. Quant aux forces de défense australiennes, elles ont recentré leurs efforts sur l'amélioration des tactiques d'assaut des navires en mouvement et sur des exercices amphibies de lutte antiterroriste. Des dragueurs de mines et des navires de reconnaissances de la marine australienne accompagnent désormais les patrouilles de surveillance renforcées, ce qui n'a pas manqué de créer un débat épineux dans le pays. Beaucoup y ont vu un moyen d'accentuer la sûreté aux frontières en général et pas seulement du fait du terrorisme, notamment pour intercepter les immigrants en situation irrégulière, ce qui est apparu disproportionné.

Pour se mettre en conformité avec le Code ISPS, 248 plans de sûreté, navires et installations portuaires confondus, ont été approuvés avant la date limite imposée par l'OMI. La plupart des coûts engendrés par la mise en application des nouvelles exigences de sûreté ont été supportés par le secteur maritime. Le gouvernement australien les a chiffrés à plus de 313 millions de dollars australiens en investissement initial la première année, soit quelques 241 millions de dollars américains, et à 96 millions de dollars australiens en investissement, soit environ 74 millions de dollars américains.

Il est à noter que l'amélioration de la sûreté maritime est une telle priorité en Australie que la question est devenue un élément de différenciation lors des élections fédérales du 9 octobre 2004. Le programme de campagne du gouvernement de John Howard, réélu pour la troisième fois, reprend certains points évoqués dans le programme de juillet 2004 et y ajoute de nouveaux éléments. Les plus marquants sont, entre autre, l'augmentation du nombre d'exercices antiterroristes avec comme premiers thèmes la prise en otage d'un ferry dans la baie de Sydney ou encore une attaque contre une plateforme pétrolière offshore, ainsi que l'accroissement de la flotte de navires de surveillance. Il envisage par ailleurs « d'identifier, de vérifier et de valider » les données récoltées par un système radar à haute fréquence²⁴⁵, à l'aide de nouveaux aéronefs sans pilote. Enfin, il souhaite rendre l'accord de défense entre les cinq puissances²⁴⁶ que sont Singapour, la Malaisie, le Royaume-Uni, la Nouvelle-Zélande et l'Australie plus percutant en matière d'antiterrorisme afin de pouvoir réagir face aux menaces contemporaines de type non conventionnel qui pèsent sur la région. Aldo Borgu voit deux raisons essentielles à cette dernière décision. Tout d'abord, le premier exercice pratique du FPDA a eu lieu en octobre 2004 et était essentiellement basé sur le terrorisme maritime. Il l'a ressenti comme une tentative visant à asseoir le FPDA dans le contexte de la sûreté contemporaine plutôt que comme une expérience sérieuse de lutte antiterroriste. La seconde explication est que, en juin 2004, lors d'une conférence de presse relative au FPDA, le ministre malaisien de la défense a clairement déclaré que, en cas d'activités terroristes quelles qu'elles soient sur le sol malaisien ou singapourien, ce serait la Malaisie et Singapour qui s'en occuperaient spécifiquement. De cette façon, Aldo Borgu estime qu'il relaye le FPDA a un rôle de simple coordinateur des exercices et des échanges d'information tout en lui refusant une quelconque « implication opérationnelle » dans la lutte antiterroriste à proprement parler. Il est donc évident que des efforts restent à faire en la matière.

²⁴⁵ *High Frequency Surface Wave Radar System*. Récemment installé, il est localisé dans le détroit de Torres, entre l'Australie et la Nouvelle Guinée.

²⁴⁶ *Five Power Defence Arrangements* (FPDA). Cet engagement réciproque de défense, signé en 1971, oblige les cinq nations participantes à se consulter en cas d'agression extérieure ou de menace d'attaque contre la Malaisie ou Singapour. Il s'inscrit dans le prolongement des garanties de défense que donnait le Royaume-Uni à la Malaisie et à Singapour mais qui ont cessé en 1967 suite au retrait des forces britanniques stationnées à l'Est du Canal de Suez.

2.6.6. L'OTAN²⁴⁷

Au niveau intergouvernemental²⁴⁸, L'OTAN souhaite restaurer une crédibilité quelque peu affectée par les positions diamétralement opposées de ses membres sur le conflit irakien et par ses difficultés à envoyer des troupes adéquates pour pacifier l'Afghanistan. Elle aspire à jouer un rôle marquant dans le XXI^e siècle et voit la sûreté maritime comme le maillon faible de la stratégie européenne en matière de lutte contre le terrorisme, c'est pourquoi elle veut y apporter sa contribution.

Ses objectifs sont « détecter, dissuader et se protéger des activités terroristes » grâce à une opération navale de lutte antiterroriste, mise en œuvre en coopération avec l'OMI. L'opération *Active Endeavour*²⁴⁹ a d'abord été lancée en Méditerranée orientale, le 6 octobre 2001, avec le déploiement des Forces navales permanentes de la Méditerranée²⁵⁰, celles-ci alternant tous les trois mois avec les Forces navales permanentes de l'Atlantique²⁵¹. Dirigée par les Forces navales alliées d'Europe du Sud²⁵² depuis Naples en Italie, *Active Endeavour* a été établie en signe de solidarité avec les USA. Cette opération représente « la concrétisation de l'engagement de l'OTAN envers les USA suite aux attentats du 11 septembre 2001 [mais] c'est aussi une importante contribution à la préservation de la paix, de la stabilité et de la sécurité de tous les pays membres de l'Alliance » selon le Vice Amiral italien Ferdinando Sanfelice di Monteforte, Commandant en chef des NAVSOUTH et de *Active Endeavour*. La base légale de cette opération est l'article 5²⁵³ du traité instituant l'OTAN. Il est à noter que c'est la première fois de l'histoire de l'alliance militaire que cette clause de défense collective est ainsi utilisée.

Les Etats présents dans l'OTAN ont mis en place des patrouilles communes dès 2003 ainsi que des « reconnaissances préparatoires systématiques » des routes maritimes aux points d'étranglement du trafic, dans les couloirs maritimes et dans les ports importants de toute la Méditerranée. Parallèlement à cela, ils ont décidé, le 4 février de la même année, d'intégrer le détroit de Gibraltar dans leur périmètre d'intervention car il est considéré comme une zone à

²⁴⁷ Alliance regroupant 26 pays d'Amérique du Nord et d'Europe qui se sont engagés à respecter les objectifs du Traité de l'Atlantique Nord, signé le 4 avril 1949. Son but est la sauvegarde de la liberté et de la sécurité de tous ses membres par des moyens politiques et/ou militaires.

²⁴⁸ Site de *The Economist* : http://www.economist.com/agenda/displayStory.cfm?story_id=2804108.

²⁴⁹ Le nom d'*Active Endeavour* n'a été officialisé que le 26 octobre 2001.

²⁵⁰ *Standing Naval Forces Mediterranean* (STANAVFORMED). Composées de plusieurs frégates, ainsi que de destroyers selon un système de rotation, ces forces de réaction immédiate doivent être capables de se déployer rapidement sur une zone de crise ou de tensions.

²⁵¹ *Standing Naval Forces Atlantic* (STANAVFORLANT). Elles fonctionnent sur le même mode que les précédentes.

²⁵² Allied Naval Forces Southern Europe (NAVSOUTH).

²⁵³ **Article 5 :** Les parties conviennent qu'une attaque armée contre l'une ou plusieurs d'entre elles survenant en Europe ou en Amérique du Nord sera considérée comme une attaque dirigée contre toutes les parties, et en conséquence elles conviennent que, si une telle attaque se produit, chacune d'elles, dans l'exercice du droit de légitime défense, individuelle ou collective, reconnu par **l'article 51 de la Charte des Nations Unies**, assistera la partie ou les parties ainsi attaquées en prenant aussitôt, individuellement et d'accord avec les autres parties, telle action qu'elle jugera nécessaire, y compris l'emploi de la force armée, pour rétablir et assurer la sécurité dans la région de l'Atlantique Nord. Toute attaque armée de cette nature et toute mesure prise en conséquence seront immédiatement portées à la connaissance du Conseil de Sécurité. Ces mesures prendront fin quand le Conseil de Sécurité aura pris les mesures nécessaires pour rétablir et maintenir la paix et la sécurité internationales.

Article 51 de la Charte des Nations Unies : Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales. Les mesures prises par des Membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité et n'affectent en rien le pouvoir et le devoir qu'a le Conseil, en vertu de la présente Charte, d'agir à tout moment de la manière qu'il juge nécessaire pour maintenir ou rétablir la paix et la sécurité internationales.

risques du fait des quelques 3 000 navires marchands qui l'empruntent quotidiennement. Ainsi, depuis le 10 mars 2003, ils peuvent escorter, sur demande, les navires civils le traversant, et ce à l'aide de frégates, de sous-marins, d'hélicoptères et d'avions de surveillance espagnols, portugais, allemands, norvégiens, danois et étatsuniens. Ce système a ensuite été suspendu à compter du 29 mai 2004. Puis, le 16 mars 2004, *Active Endeavour* a été étendue à l'ensemble du pourtour méditerranéen pour officialiser l'appui dont bénéficiait déjà l'opération de la part des pays membres du Conseil de partenariat euro-atlantique²⁵⁴, de ceux du Partenariat pour la paix²⁵⁵ ou encore des Etats participant au programme Dialogue méditerranéen²⁵⁶. Ceux-ci fournissaient, entre autre, des informations sur des navires a priori suspects transitant dans leurs eaux.

Parallèlement à cela, sur décision du Conseil de l'Atlantique Nord, organe de décision souverain de l'OTAN, ils ont commencé, dès le 29 avril 2003, à arraisonner tout bateau suspect, avec accord du Commandant de bord et de l'Etat du pavillon. Le navire doit alors décliner son identité et son activité ; les informations sont transmises aux NAVSOUTH à Naples ainsi qu'au Centre OTAN pour la navigation commerciale à Northwood, Grande Bretagne. En cas de doute, une équipe de 15 à 20 soldats peut monter à bord et procéder aux vérifications sur les documents et la cargaison. Le premier navire à avoir été arraisonné a été le *Nino Star*, battant pavillon des Comores au large de Chypre le 29 avril et sa cargaison s'est finalement avérée être en totale conformité avec son manifeste.

Le résultat concret d'*Active Endeavour*, est que, depuis son lancement, et ce jusqu'aux statistiques du 18 janvier 2005, plus de 67 000 navires ont été arraisonnés, les membres de l'alliance sont montés à bord de 95 navires et plus de 488 navires de commerce ont été escortés avec succès à travers le détroit de Gibraltar²⁵⁷. Cette opération a ainsi permis d'identifier clairement le trafic en Méditerranée, ce qui, en rendant la zone incontestablement plus stable et sécurisée, a été d'autant plus avantageux pour l'économie et le commerce. Toutefois, il n'en reste pas moins que des progrès restent à faire. C'est pourquoi, lors du sommet d'Istanbul, en Turquie, le lundi 28 juin 2004, les dirigeants de l'OTAN ont décidé d'accentuer l'opération *Active Endeavour*, notamment en y intégrant de nouveaux pays, comme la Russie et l'Ukraine qui ont été conviées à participer aux patrouilles de surveillance. Ils envisagent de fait d'étendre leur action à la Mer Noire car le risque d'attaques par des groupes du Caucase ou d'Asie Centrale y est potentiel due à l'attrait de certains chargements et à l'instabilité de la zone. L'incident qui s'est déroulé le 5 mai 2004 en est tout à fait caractéristique. Lors d'une crise politique majeure entre la République géorgienne autonome d'Adjarie et le pouvoir central à Tbilissi, le port géorgien de Batumi, donnant sur la Mer Noire et acheminant 60% des exportations pétrolières en provenance de la Mer Caspienne, a été miné sur un ordre attribué à Aslan Abashidze²⁵⁸.

²⁵⁴ *Euro-Atlantic Partnership Council* (EAPC). En plus des 26 pays membres de l'OTAN, les 20 autres Etats qui y participent sont essentiellement des nations d'Europe de l'Est.

²⁵⁵ *Partnership for Peace* (PfP). Ce regroupement compte 27 pays également présents au sein de l'EAPC.

²⁵⁶ *Mediterranean Dialogue*. Mis en place depuis une décennie, ce forum vise des questions politiques ainsi qu'une coopération pratique entre l'OTAN, l'Algérie, l'Egypte, Israël, la Jordanie, la Mauritanie, le Maroc et la Tunisie.

²⁵⁷ Il ne faut pas non plus manquer de signaler qu'*Active Endeavour* a eu des avantages inattendus : l'opération a sauvé la vie à des civils, notamment des ouvriers de plateformes pétrolières et a permis de secourir des navires sur le point de sombrer. Cette opération a également été profitable dans le sens où elle a substantiellement réduit la contrebande et l'immigration clandestine – la diminution est estimée à 50% –.

²⁵⁸ A la tête de l'Adjarie depuis son indépendance en 1991 à la suite de la chute de l'ex-URSS, il a démissionné le 5 mai 2004 avant de s'enfuir en Russie.

Depuis le sommet, l'Unité de renseignement sur les menaces terroristes est devenue un élément permanent au sein des quartiers généraux de l'OTAN établis à Bruxelles. Sa mission est d'accentuer le partage des informations et elle se réunit, dans cette optique, avec des experts du renseignement. Parallèlement à cela, les chefs d'Etat et de gouvernements présents ont opté pour le développement d'une série de mesures antiterroristes complémentaires. Il s'agit, entre autre, de nouvelles stratégies de défense utilisant des équipements de haute technologie pour réagir face à des armes de destruction massive, à des attaques au lance-roquettes ou à n'importe quel type de bombes artisanales après les avoir détectées. Il est à noter que, pendant le sommet, et ce pour se prémunir contre ce type de menaces, aucune marchandise dangereuse n'a été autorisée à emprunter le détroit du Bosphore.

Le problème essentiel qui subsiste, d'après *The Economist*, est que les équipements dont disposent l'OTAN sont inadaptés dans le sens où ils datent pour l'essentiel de la Guerre Froide qui s'est achevée voilà presque 15 ans. L'OTAN dispose effectivement d'une capacité de surveillance maritime conçue à l'origine pour repérer des bâtiments de guerre soviétiques massifs. Or, à l'heure actuelle, les terroristes utilisent plutôt des canots pneumatiques ou des petites vedettes ultra rapides, si bien que l'équipement n'est pas en adéquation avec les besoins. C'est pourquoi, ces derniers temps, l'OTAN recentre ses efforts sur le perfectionnement du réseau de renseignements pour suivre de près les principales voies navigables et compte sur le support logistique de ses Etats membres.

2.7. Les taux de conformité aux mesures ISPS

2.7.1 Au niveau français

La flotte française concernée par les nouvelles prescriptions de sûreté comptait 168 navires au 1^{er} juillet 2004. Au 30 juin 2004²⁵⁹, 162 navires avaient reçu leur certificat international de sûreté, soit 96,4% du total. A la fin 2004, le nombre de bâtiments français concernés par l'ISPS était estimé à 190 du fait, entre autre, des entrées et des sorties en flotte ainsi que des réarmements. Le processus d'approbation des plans de sûreté n'est pas du ressort des RSO en France mais de la DAMGM. Du fait de l'échéancier assez court de l'ISPS, un groupe de travail interministériel (GTI) regroupant le HFD du ministère des transports – ancien HFD Mer –, des experts étatiques spécialisés dans la navigation maritime et la sûreté, des représentants des ministères de la défense, de l'intérieur et des finances a été créé le 24 octobre 2003. Quant à la procédure même d'approbation, les inspecteurs de sécurité des navires et le HFD du ministère des transports ont en charge l'analyse des SSA et SSP²⁶⁰ puis la conduite d'une vérification initiale à bord²⁶¹ avant que de remettre un rapport d'audit au GTI. Le SSP doit ensuite être approuvé par l'administration et l'ISSC délivré. Cette dernière fonction relève du chef du centre de sécurité de rattachement du navire qui signe également l'ISSC. Il est à noter qu'à la fin 2004, 23 navires bénéficiaient de certificats provisoires.

²⁵⁹ *Le dispositif d'approbation des plans de sûreté des navires de commerce*, Amarres, 4^{ème} trimestre 2004, pages 3 à 5.

²⁶⁰ Pour les premiers plans, des représentants des directions générales de la police nationale, de la gendarmerie nationale et de la marine nationale les ont assistés.

²⁶¹ 18 navires ont été contrôlés par des sociétés de classification car ils étaient trop loin du territoire français.

Sur le plan pratique, octobre 2003 a été marqué par l'arrivée des premiers SSP. Le 15 mars 2004, les premières visites d'inspection ont eu lieu. Le 22 mars, les premiers rapports de visite ont été rendus au GTI. A la fin mars, 600 cadres de la marine marchande ont achevé la formation dispensée par l'ENMM de Nantes pour devenir inspecteurs de sécurité habilités ISPS. Le mois d'avril 2004 a vu l'arrivée massive des SSP. Enfin, les premiers ISSC ont été remis le 1^{er} mai.

Pour ce qui est des installations portuaires, et ce sur l'ensemble des ports français²⁶², 343 installations portuaires étaient concernées par les nouvelles mesures imposées par le Code ISPS au 1^{er} juillet 2004. Elles étaient réparties sur un total de 28 ports, dont les sept ports autonomes, 20 ports d'intérêt national et un port départemental. Au 30 juin 2004, 284 installations portuaires étaient conformes aux prescriptions de l'OMI en matière de sûreté maritime, soit 82,7%.

2.6.7.2 Au niveau international²⁶³

Le MSC a réalisé une étude sur différents aspects de la mise en application au 1^{er} septembre 2004 et au 30 novembre 2004. Le nombre d'Etats contractants s'élève à 153, dont 13 sans littoral, ce qui représente environ 9 541 installations portuaires déclarées. Au 30 novembre, 98,46% des PFSA avaient été approuvées – contre 95,23% au 1^{er} septembre 2004 – et 98,40% de PFSP avaient été soumis pour 97,07% approuvés – contre 94,28% de PFSP présentés et 92,37% d'approuvés deux mois plus tôt –.

L'étude permet ensuite une comparaison par zone géographique. Par ordre décroissant de conformité, au 30 novembre 2004, la première région géographique était l'Amérique du Nord, soit 2 nations, 467 installations portuaires déclarées et 100% de PFSP approuvés – contre 8 installations portuaires de moins et le même pourcentage d'approbation au 1^{er} septembre –. En deuxième position vient le Nord-ouest de l'Europe qui comprend 19 Etats, 3 868 installations portuaires déclarées et 99,95% de PFSP approuvés – contre 95,78% de PFSP approuvés pour les 3 819 installations portuaires déclarées au 1^{er} septembre 2004 –. L'Amérique latine et les Caraïbes, soit 30 gouvernements contractants, sont troisième avec 861 installations portuaires déclarées et un taux de PFSP approuvés de 98,72% - contre 813 installations portuaires déclarées et 82,90% de PFSP approuvés deux mois plus tôt, ce qui leur valait la sixième place –. Les 19 pays de la CEI²⁶⁴ et d'Europe orientale dénombrent 608 installations portuaires déclarées et le pourcentage d'approbation des PFSP atteint les 95,39% – contre 90,26% de PFSP approuvés pour les 493 installations portuaires déclarées, soit la cinquième place au 1^{er} septembre –. L'Asie et le Pacifique arrivent en cinquième position au 30 novembre 2004 avec 94,91% de PFSP approuvés pour les 3 084 installations portuaires déclarées dans 31 Etats – contre une quatrième place au 1^{er} septembre due aux 91,54% de PFSP approuvés pour 2 931 installations portuaires –. La sixième position est occupée par l'Afrique, 30 nations, 239 installations portuaires déclarées et 94,14% de PFSP approuvés – contre 177 installations portuaires déclarées, 93,22% de PFSP approuvés et la troisième place deux mois auparavant –. Enfin, les 22 Etats arabes et méditerranéens sont septième avec 414 installations portuaires déclarées et 83,57% de PFSP

²⁶² Cf supra 1.2.1 La situation en France, page 18.

²⁶³ Annexe V: Les taux de conformité internationaux au Code ISPS, page 114.

²⁶⁴ Communauté des Etats Indépendants issue de l'éclatement de l'ex-URSS.

approuvés – contre 11 installations portuaires déclarées de plus au 1^{er} septembre (soit 425) et seulement 79,53% de PFSP approuvés, ce qui les classait à la même position –.

La première observation est que, quatre mois après la date limite d'application de l'ISPS, et même si la plupart des taux de conformité sont proches des 100%, les prescriptions de la nouvelle réglementation internationale ne sont pas entièrement respectées. Ce constat témoigne de la difficulté de mise en oeuvre de ces nouvelles mesures. Le délai accordé, 18 mois, n'étant pas suffisant face à la masse de travail à accomplir, explique les chiffres vus ci-dessus. D'autant plus qu'il faut également tenir compte de la somme de travail tout aussi considérable pour les navires. Il est à noter ensuite que les Etats arabes et méditerranéens sont la seule zone à avoir perdu des installations portuaires sur les deux mois, toutes les autres régions géographiques ayant étendu l'application de l'ISPS à d'autres installations portuaires.

Cette étude du MSC permet également de savoir combien de gouvernements contractants se sont pliés à la règle de désignation de responsables sûreté. Au 1^{er} septembre, 84,31% d'entre eux avaient notifié un point de contact unique, pour 87,58% au 30 novembre. De même, quatre mois après l'entrée en vigueur du Code ISPS, 81,70% des Etats contractants avaient fourni le nom et les coordonnées des responsables de la sûreté des navires et 74,51% ceux des responsables de la sûreté des installations portuaires. Enfin, 62,75% des gouvernements contractants utilisent des RSO, sachant que 205 RSO existaient au 30 novembre 2004.

Pour ce qui est des navires²⁶⁵, l'analyse la plus récente date du mercredi 30 juin 2004, à 9h00. Elle relève directement de l'OMI cette fois et est basée sur les réponses de 46 gouvernements contractants représentant à eux seuls plus de 84% du tonnage mondial et 68% du nombre de navires concernés par les nouvelles mesures de sûreté. Il ressort qu'à la veille de la date limite d'application, 19 377 SSP avaient été soumis pour les quelques 22 539 navires astreints au Code ISPS et 11 996 certificats internationaux de sûreté remis, soit un taux de conformité de 53,2% – contre à peine 41,3% le 25 juin 2004. A titre de comparaison, à la même période, le taux de conformité des 7 974 installations portuaires concernées était de 53,4% – contre 31,9% cinq jours plus tôt –, soit 4 688 PFSP soumis pour 4 260 PFSP approuvés. La progression des chiffres en cinq jours de temps a rassuré Efthimios E. Mitropoulos, Secrétaire général de l'OMI, qui se dit confiant car les taux de conformité des navires et des installations portuaires sont assez proches et parce que « les niveaux effectifs de préparation, de vigilance et de sensibilisation sur le terrain [sont nettement] plus élevés que ce qui était prévu [à peine une semaine auparavant] ». Enfin, il convient d'observer que cette étude regroupait non seulement les chiffres fournis par les gouvernements contractants mais également ceux d'organismes du secteur maritime ayant un statut de consultants auprès de l'OMI. Il s'agit notamment de l'IACS²⁶⁶, d'Intercargo²⁶⁷, d'Intertanko, de l'IPTA²⁶⁸, d'ICCL²⁶⁹ et de BIMCO²⁷⁰. L'ICCL est le seul organisme à avoir délivré les ISSC à 100% des navires qu'il suivait au 30 juin 2004 – contre 88,9% le 25 juin –,

²⁶⁵ Site de l'OMI : http://www.imo.org/Newsroom/mainframe.asp?topic_id=892&doc_id=3687. Cf Annexe V : Les taux de conformité internationaux au Code ISPS, page 114.

²⁶⁶ *International Association of Classification Societies* – Association internationale des sociétés de classification.

²⁶⁷ *International Association of Dry Cargo Shipowners* – Association internationale des propriétaires de fret dry.

²⁶⁸ *International Parcel Tankers Association* – Association internationale de parcel tankers (transporteurs parcellaires).

²⁶⁹ *International Council of Cruise Lines* – Conseil international des compagnies de croisières.

²⁷⁰ Association internationale de navigation.

le plus faible taux de conformité étant celui de BIMCO, avec 18,6% de ces navires certifiés, soit le même pourcentage que cinq jours plus tôt.

Enfin, les derniers chiffres en la matière ont été rapportés dans des articles de l'OMI. Le premier, en date du 6 août 2004²⁷¹, souligne que plus de 90% de certificats internationaux de sûreté pour les navires ont été émis. Dans le second, daté du 17 février 2005²⁷², il apparaît que 94% des gouvernements contractants ont approuvé les PFSP de 97% des installations portuaires déclarées, sachant qu'il en existe plus de 9 600 dans le monde entier.

III Conséquences et solutions

3.1 Les nouvelles clauses des chartes parties²⁷³

Un certain nombre de clauses types a dû être créé pour faire face à la nouvelle réglementation. Dès novembre 2003, BIMCO disposait d'une clause type pour les affrètements à temps et, en mars 2004, pour les chartes parties au voyage ainsi que des clauses spécifiques pour les USA du fait de leurs lois supplémentaires, notamment la MTSA. Pour sa part, Intertanko travaille avec une seule clause pour les chartes parties au voyage. Enfin, les compagnies pétrolières ont également publié des clauses sûreté²⁷⁴ mais Philippe Boisson estime qu'elles sont nettement plus « pénalisantes » dans la mesure où le partage des coûts et des responsabilités n'est possible que si les mesures requises à l'encontre du navire concernent aussi l'ensemble des navires dans le port.

3.1.1 Les obligations des parties

Les obligations de l'armateur sont d'avoir un SSP en règle, de l'appliquer, de procurer une copie de l'ISSC à l'affrèteur s'il le lui demande, de lui donner les coordonnées du CSO et de supporter les coûts liés à la mise aux normes de sûreté de son navire, sinon sa responsabilité peut être engagée.

L'affrèteur, quant à lui, a une obligation classique d'information pour permettre à l'armateur d'appliquer correctement les mesures de sûreté de son SSP. La clause BIMCO requiert en outre qu'il fournisse ses coordonnées au CSO et au SSO ainsi que celles de tous les sous-affrèteurs en cas de charte partie au voyage. La clause Intertanko veut qu'il donne « l'identité et les coordonnées de toutes les parties aux contrats relatifs au navire et à son utilisation, lorsque de tels contrats ont été signés par l'affrèteur, le sous-affrèteur et par ses agents » ainsi que de « toutes les parties concernées par ces contrats ». Il doit enfin fournir « toute information pertinente relative à la cargaison du navire ou à l'utilisation exigée par l'armateur ». Les pertes, dommages ou dépenses entraînés par un non respect des obligations ci-dessus seraient à la charge de l'affrèteur. La clause BIMCO exclut la responsabilité pour dommages consécutifs afin

²⁷¹ Site de l'OMI : http://www.imo.org/Newsroom/mainframe.asp?topic_id=892&doc_id=3760.

²⁷² Site de l'OMI : http://www.imo.org/Newsroom/mainframe.asp?topic_id=892&doc_id=4714.

²⁷³ Site de la Chambre Arbitrale Maritime de Paris, CAMP, gazette n°6 : <http://www.arbitrage-maritime.org/fr/gazette.htm>.

²⁷⁴ Il existe, entre autre, la *STB's Security Regulation clause* révisée le 10 juin 2004, la *Vitol ISPS clause* pour les affrètements au voyage, la *ISPS clause* de Chevron du 28 avril 2004, la *SHELLVOYS-ISPS clause* du 19 mai 2004 et la *BPVOY 4*.

d'éviter des indemnités exorbitantes et indique par ailleurs que les retards survenant par sa faute seront indemnisés à hauteur des surestaries. De même, pour les affrètements au voyage et en ce qui concerne les dépenses relatives aux mesures de sûreté imposées par le port ²⁷⁵, BIMCO et Intertanko s'accordent : elles sont à la charge de l'affréteur, l'armateur assumant les frais découlant de l'application du SSP en fonction du niveau de sûreté en vigueur. Enfin, il est à noter que, d'après la clause BIMCO, l'armateur qui a rempli toutes ses obligations ne sera pas pénalisé en cas de retard du aux affrètements antérieurs, ceux-ci étant reportés dans la fiche synoptique continue. La règle veut qu'il en soit de la responsabilité de l'affréteur qui se doit d'être le plus attentif possible afin de juger des risques éventuels avant de choisir un navire, notamment s'il doit escaler aux USA.

3.1.2 Le refus d'accès au port

Sur cette question, Intertanko établit que si le navire ne peut entrer dans le port ou procéder aux opérations commerciales pendant plus de cinq jours, l'armateur peut demander à l'affréteur de désigner un port de substitution. Au bout de 48H, l'armateur, s'il n'a pas reçu de réponse, peut soit décharger la marchandise dans un port de son choix et ce à la charge de l'affréteur, soit mettre instantanément un terme à la charte partie si le navire est léger. Philippe Boisson précise, à ce sujet, qu'Intertanko ne propose cette clause qu'à titre optionnel parce qu'elle est susceptible de mettre les parties dans une « situation inconfortable » évidente.

3.1.3 La NOR²⁷⁶

Pour ce qui est de l'affrètement au voyage, la clause BIMCO permet à l'armateur d'envoyer la NOR avant même d'avoir reçu l'autorisation de sûreté des autorités de contrôle. Elle subordonne toutefois cette action au fait que le navire ait par ailleurs rempli toutes les autres obligations découlant de la charte partie. Philippe Boisson observe que les retards consécutifs aux mesures de sûreté sont assimilés à des staries ou à des surestaries en fonction de la situation.

3.1.4 La notion de port sûr

Cette notion fait généralement référence à la sécurité de la navigation et il est du devoir de l'affréteur de désigner un port sûr²⁷⁷. Philippe Boisson estime que ce concept peut être étendu à la sûreté maritime si des pirates ont envahi un port, si bien que la conduite des opérations commerciales en est nécessairement affectée. Par contre, une mauvaise mise en œuvre du PFSP par le chargeur ou le réceptionnaire ne suffit pas. Il insiste sur l'idée que la notion de port sûr ne peut être remise en question que par le danger qu'un navire rencontrerait dans un port. Enfin, si les armateurs veulent accroître leur protection, ils peuvent demander dans la charte partie à ce que l'affréteur ne se rende que dans des installations portuaires répondant aux normes ISPS.

²⁷⁵ Ses mesures sont relatives aux inspections, aux taxes et droit de port relatifs à la sûreté, à la présence de gardes à bord, aux remorqueurs d'escorte.

²⁷⁶ *Notice of Readiness* ou notice du navire prêt : envoyée par le Capitaine, elle atteste que le navire est apte à commencer les opérations commerciales.

²⁷⁷ Tout navire doit pouvoir entrer dans un port, procéder à des opérations commerciales et en repartir.

3.2. Les difficultés nées de l'application directe

Le principal problème évoqué, aussi bien du côté portuaire que du côté armateurs est le conflit entre règles de sécurité et mesures de sûreté. En effet, de nombreuses normes de sûreté présentes dans des SSP conduisent à des aberrations du point de vue de la sécurité, notamment au niveau de l'évacuation des passagers qui est rendue impossible par des portes cadenassées ou par des grilles aux points stratégiques. Dans pareil cas, la sécurité doit toujours primer et il est du devoir du Capitaine de faire respecter cette primauté²⁷⁸. Ce premier point explique pour l'essentiel la révision des plans de sûreté après le premier exercice pratique. Les autres raisons sont, entre autre, le fait que certaines mesures de sûreté étaient trop vagues ou trop générales pour être efficaces. Il est à noter que toute modification doit être envoyée à l'administration qui doit l'approuver avant qu'il ne soit procédé au changement.

L'autre difficulté majeure est celle des fausses alertes avec le SSAS. La question a d'ailleurs une telle incidence que le MSC a adopté une circulaire à ce sujet qui a déjà fait l'objet d'une révision²⁷⁹. Le seul moyen de remédier à cela est la connaissance approfondie de ce système, et ce aussi bien d'un point de vue théorique que pratique. Le deuxième point sensible au niveau du SSAS est que les sections A/9.4.17 et A/9.4.18 du Code ISPS disposent que le plan de sûreté du navire doit mentionner l'endroit où sont installées les commandes du SSAS ainsi que la façon de le déclencher, de le neutraliser et de le réenclencher, ce qui semble assez imprudent sachant que le SSP doit nécessairement rester à bord. Bien qu'il soit strictement confidentiel et qu'il doive être conservé dans un lieu protégé, il n'empêche que tout terroriste peut savoir que le plan doit contenir de telles informations puisque le Code ISPS est consultable sur Internet. Il est également vrai qu'un terroriste souhaitant monter à bord d'un navire dans l'optique de commettre un attentat ne se préoccupera pas du SSP. Il n'empêche que la question est actuellement en discussion, notamment au niveau armatorial, sans rien de formel pour l'instant. Il serait peut-être plus judicieux, par exemple, que seules deux personnes à bord sachent comment désamorcer le SSAS sans procédure écrite et que, par contre, la copie du SSP en possession de l'armateur soit la seule à le préciser.

Le cas des pilotes, qui sont aussi concernés par le Code ISPS, est également problématique. Ils subissent comme toutes personnes souhaitant monter à bord d'un navire des contrôles d'identité pour garantir qu'il s'agit bien de pilotes et pas de terroristes. Mais parfois les vérifications sont telles qu'il est arrivé que des pilotes soient bloqués à la coupée alors que le bâtiment continuait à faire route pour rejoindre son poste à quai dans des eaux dont l'équipage ne connaissait pas les spécificités, ce qui peut être très dangereux. La question est telle que les pilotes travaillent actuellement en collaboration avec un comité de l'OMI sur une adaptation du contrôle ISPS à leur rencontre²⁸⁰. Les français ont d'ailleurs proposé la mise en place généralisée d'un « fichier d'accompagnement » comprenant une photo et des renseignements sur le pilote qui est déjà utilisé au sein du PAM.

²⁷⁸ Cf supra 2.3 Les navires / les armateurs, page 51, règle XI-2/8 de la Convention SOLAS.

²⁷⁹ Cf supra 2.1.3.1.2 Les textes du MSC, page 37, MSC/Circ. 1109/Rev 1.

²⁸⁰ Informations obtenues lors de la visite de la station de pilotage de Port-de-Bouc le mardi 17 mai 2005 selon un pilote de la station de pilotage de Port-de-Bouc membre du syndicat international des pilotes.

Un autre souci lié aux nouvelles mesures de sûreté est la capacité à équilibrer les exigences en matière de sûreté maritime, notamment les contrôles d'accès au navire, et la nécessité de maintenir la libre circulation commerciale et des personnes, ce qui semble incompatible idéologiquement. Il s'agit très probablement d'un des défis majeurs de la mondialisation. Incontournable, il demande une gestion parfaite de tous les instants pour ne pas laisser non plus de côté la notion de rentabilité. Les mesures doivent être viables économiquement afin que chaque intervenant du secteur maritime puisse maintenir sa position concurrentielle sur le marché et que la fluidité des échanges soit respectée.

La question du financement, quant à elle, n'est pas définitivement réglée à l'échelle mondiale. Au niveau européen, elle est toujours en discussion. Il convient d'observer à ce propos que le coût de toutes ces nouvelles mesures a engendré la création d'une surcharge ISPS pour les usagers du transport maritime. Pour la majeure partie des armateurs, le montant de cette nouvelle taxe a été discuté au sein des conférences maritimes et les compagnies qui n'en font pas partie se sont généralement alignées. Le principe de base est l'imposition d'une taxe fixe par conteneur à laquelle s'ajoute celle décidée par certains ports pour couvrir les investissements, plus celle des manutentionnaires qui peut être couplée avec la taxe portuaire. Cette nouvelle surcharge a été relativement mal acceptée de prime abord²⁸¹ puisqu'elle s'ajoute à une liste déjà longue (BAF, CAF, THC, surtaxe pour risque de guerre, pour équipements spéciaux, pour l'encombrement portuaire, etc). De plus, les chargeurs français se sont indignés contre cette pratique visant à imposer une surcharge « arbitraire » commune alors qu'elle devrait dépendre des frais engagés par chaque armateur, ce qui ne peut être uniforme. Les chargeurs voudraient que le fret soit forfaitaire car ils estiment que ces coûts additionnels, censés être des surcharges, sont en réalité des charges à part entière et qu'en tant que telles elles devraient être intégrées dans le prix du transport, et ce pour éviter leur prolifération qualifiée d'« incontrôlable ». Pour ce qui est des passagers²⁸², l'imposition d'une nouvelle taxe²⁸³ est assez critiquée car le trafic passagers est en baisse depuis quelques années et que les compagnies doivent faire face, comme dans tous les secteurs, à la montée en puissance des *low cost*. En France, le sujet est à l'étude au sein du Comité interministériel de la Mer, le CIMER, qui a été instauré par le même décret que le SG Mer, le n°95-1232 du 22 novembre 1995.

Aux éléments vus ci-dessus s'ajoute le fait que la structure éclatée du contrôle maritime pourrait devenir un obstacle à la lutte multilatérale actuellement engagée contre le terrorisme maritime par l'ensemble des Etats. En effet, en plus de l'OMI, qui coordonne l'application de ces règles, l'inspection des conteneurs par scanner relève de l'OMD. Quant à la mise au point d'un passeport infalsifiable destiné au personnel des navires, elle est à la charge de l'OIT. Au niveau national, la problématique est la même, le contrôle est dispersé entre plusieurs intervenants²⁸⁴.

Par ailleurs, le fait que le Code ISPS ne s'applique qu'aux navires de 500 tonneaux de jauge brute effectuant des voyages internationaux ainsi qu'aux installations portuaires les

²⁸¹ Selon l'Association des utilisateurs de transport de fret (AUTF). Site de l'UE : http://europa.eu.int/comm/competition/antitrust/others/maritime/white_paper/autf_french_shippers_council_response_fr.pdf.

²⁸² Site du Sénat : <http://www.senat.fr/cra/s20050215/s20050215H10.html>.

²⁸³ Cf supra 2.2.1 Au niveau national, page 46.

²⁸⁴ Cf supra 2.2.1 Au niveau national, page 46.

desservant est assez limitatif. Il est bien évident que le but est d'éviter un attentat spectaculaire ; toutefois, il faut tenir compte du fait qu'une installation portuaire qui n'est a priori pas destinée à recevoir des navires visés par le Code ISPS soit amenée pour une raison quelconque à le faire. Que se passerait-il ? Elle n'en est légalement pas apte. De plus, les seuls attentats maritimes étant survenus à l'heure actuelle sont le fait de petites embarcations. Ne faudrait-il pas plutôt se recentrer sur ce type de bateaux ? Pour combattre le terrorisme, il faut des moyens efficaces et adaptés tout en gardant bien à l'esprit que l'on n'a pas le droit à l'erreur ; une fois qu'un attentat majeur sera malheureusement survenu, il sera trop tard. Le BMI relève à cet égard dans son rapport annuel pour l'année 2002, publié le 29 janvier 2003, qu'un attentat comme celui perpétré contre le *Limburg* est difficile à empêcher. Il ajoute par ailleurs que la seule réponse possible à ce type d'attaque est que les Etats côtiers s'assurent que les approches de leurs ports sont sécurisées. Il recommande en outre de désigner des chenaux d'accès qui devraient être placés sous la surveillance des garde-côtes ou de la police ; ainsi, toute embarcation non autorisée en serait immédiatement bannie. En effet, « le risque d'attaques terroristes ne pourra probablement jamais être éliminé, par contre, il est possible d'intervenir pour le réduire. La question à se poser est de savoir dans quelle mesure les gouvernements prennent la menace terroriste maritime au sérieux. Après le *Limburg*, nous ne pouvons pas continuer à espérer que le meilleur se produise tout en ignorant les leçons [du passé] ». Il estime que le plus dissuasif restent des veilles anti-pirates vigilantes. En effet, d'après les rapports hebdomadaires fournis par le BMI, de nombreuses tentatives d'attaques sont évitées grâce aux rondes de l'équipage ou à leur seule présence sur le pont.

Enfin, si les grands ports sont désormais aux normes, les ports secondaires, eux, ont plus de difficultés et risquent, à terme, d'être isolés et de ne plus être desservis.

3.3. Comment accroître la sûreté maritime ?

La crainte principale qui est apparue avant même la mise en place effective du chapitre XI-2 et du Code ISPS était que ces nouvelles règles allaient perturber le trafic maritime et ce parce que les taux de conformité ne seraient pas maximaux. Le risque essentiel était que les pays qui appliqueraient strictement les exigences du Code ISPS dès le premier jour de leur entrée en vigueur refuseraient catégoriquement de commercer avec ceux qui ne respecteraient pas les règles et qui peuvent être classés en trois groupes : en premier lieu, certains Etats sont plus laxistes que d'autres ; en second lieu, certains Etats ne se sentent pas du tout concernés ; enfin, il ne faut pas oublier ceux qui n'ont pas les ressources financières suffisantes pour se mettre complètement aux normes. Dans un rapport datant de 2003²⁸⁵, l'OCDE avait prévu que la mise en place de l'ISPS s'élèverait à 1,3 milliards de dollars américains pour les opérateurs de navires au cours de la première année, puis 730 millions les années suivantes – ce qui est astronomique mais nettement inférieur, pour elle, au coût d'un attentat terroriste majeur -. Or, les pays en voie de développement n'ont pas les fonds nécessaires pour réaliser de tels investissements. La résolution 5 de l'OMI, adoptée le même jour que l'ISPS, vise la coopération technique entre Etats : les USA

²⁸⁵ Site de l'OCDE :

http://www.oecd.org/document/45/0,2340,en_2649_34487_4395885_119690_1_1_37407,00.html.

ont donc envisagé de relancer l'ancien *African Coastal Security Program*²⁸⁶ dont le but était d'aider les garde-côtes et marines nationales des pays participants, à savoir le Maroc, l'Algérie et la Tunisie, à s'améliorer, en particulier au niveau de leur patrouille de surveillance. De son côté, l'Allemagne a déployé dès 2004 des navires militaires ainsi que des aéronefs de surveillance maritime à Djibouti et au Kenya. Ne serait-il pas plus pertinent de donner réellement à ces nations les moyens d'agir par elles-mêmes ? Dans ce sens, d'autres Etats ont également contribué à la formation des personnels chargés de la sûreté maritime en envoyant sur place des formateurs. Le travers à éviter étant l'ingérence dans la politique nationale. Il est à noter que l'OMI s'y est également employé dès janvier 2002 notamment au travers de son *IMO's Integrated Technical Co-operation Programme*²⁸⁷. Son implication a permis la formation de près de 3 200 personnes.

A priori, aucun problème de blocage majeur n'a eu lieu, et ce en partie parce que l'OMI a rédigé un certain nombre de circulaires visant à aider les gouvernements contractants dans l'application des nouvelles mesures de sûreté²⁸⁸. L'explication dominante reste toutefois que le fait de ne pas se plier aux normes est gravement pénalisant économiquement. Prenons l'exemple extrême des Etats-Unis : toute marchandise qui ne provient pas d'un port de chargement répondant aux norme ISPS – et même plus avec leurs initiatives unilatérales – est systématiquement refusée et aucun navire étatsunien n'y escalera; de plus, tout navire qui ne suit pas les règles ISPS se verra soit mettre au mouillage en attente de vérification avant de pouvoir pénétrer dans l'enceinte portuaire, parfois en devant remplir certaines conditions d'accès, soit sera formellement interdit d'y entrer. Or, il est clair que le commerce avec les USA représente une part significative des échanges commerciaux pour quasiment toutes les nations du monde ; aucune n'a donc intérêt à se désintéresser des nouvelles mesures de sûreté, ce qui explique par ailleurs qu'il n'était pas nécessaire que le Code ISPS prévoie des sanctions directes en cas d'inexécution des mesures de sûreté. La pression de la sanction économique est telle dans un secteur où la concurrence est féroce que des pénalités supplémentaires n'avaient pas lieu d'être.

Un an plus tard, le défi majeur est la routine. Pour l'instant, la plupart des acteurs semblent jouer le jeu plus ou moins avec complaisance mais qu'en sera-t-il dans un an, cinq ans et plus tard ? Le fait est que le Code ISPS vise à se prémunir contre le terrorisme ; cependant, si rien de concret et/ou de spectaculaire ne se passe, le risque n'est-il pas que la vigilance des uns et des autres se relâche ? C'est alors au moment où ils seront les plus vulnérables que le danger sera d'autant plus grand. C'est dans cette optique que des contrôles effectifs et suivis sont nécessaires pour « ne pas baisser la garde », selon l'expression du Secrétaire général de l'OMI, car la « protection du secteur maritime est un devoir permanent ».

En réalité, la problématique est quasiment enfantine : le monde maritime n'a pas une culture de la sûreté aussi ancrée dans les mœurs que celle du monde aérien, l'ensemble des professionnels concernés s'accorde sur ce sujet. Il lui faut donc la développer, ce qui a déjà commencé mais va encore prendre un certain temps, et ce alors même que tous les acteurs font

²⁸⁶ Programme pour la sûreté des côtes africaines. Site de l'IAGS : <http://www.iags.org/n0124051.htm>.

²⁸⁷ Programme intégré de coopération technique de l'OMI. Site de l'OMI :

http://www.imo.org/includes/blastDataOnly.asp/data_id%3D10606/hesse_chara_sec.pdf.

²⁸⁸ Cf 2.1.3.1.2 Les textes du MSC, page 37.

preuve de bonne volonté. Olivier Halloui estime que, dans ce secteur à la « réputation opaque », l'ISPS est une véritable « révolution culturelle ». C'est toute la mentalité et le mode de fonctionnement séculaire de l'ensemble du secteur maritime qui doit changer. Les mesures adoptées dans le Code ISPS ont été prises pour responsabiliser tous les intervenants, aussi bien les gouvernements que les exploitants d'installations portuaires, les exploitants de navires, les équipages, et les autres parties impliquées dans le transport maritime. Il est donc logique qu'ils y contribuent tous en fournissant le même effort puisque c'est dans l'intérêt de chacun. La tendance actuelle porte même à étendre ces nouvelles règles à la chaîne logistique dans sa totalité, c'est l'étape suivante, le C-TPAT, qui s'apparente à la thèse de l'expéditeur connu de mise dans l'aérien²⁸⁹. Cependant, n'est-il pas un peu trop aisé de réclamer que la provenance des marchandises soit systématiquement et clairement établie quand les propriétaires de navires, eux, continuent à pouvoir impunément dissimuler leur identité ? Toutes les responsabilités et tous les sacrifices ne peuvent pas être demandés toujours aux mêmes personnes. Ce travers du monde maritime est parmi les concepts les plus anciens et il est bien évident qu'il est très dur de lutter contre les pratiques ancestrales ; pourtant, il s'agit d'un objectif vers lequel il est nécessaire de tendre car pour rendre le transport maritime le plus sûr possible, tous les maillons de la chaîne doivent être transparents. La fiche synoptique continue va également dans ce sens.

De manière plus générale, les solutions pour renforcer la sûreté maritime, et donc pour lutter contre le terrorisme, sont diverses. Premièrement, comme le souligne M. Raman²⁹⁰, la coopération régionale et internationale doit primer, et ce notamment sous la forme d'une assistance opérationnelle²⁹¹ et juridique²⁹² mutuelle. Sur ce dernier point, le BMI cite un exemple particulièrement rare²⁹³. Le 25 février 2003, une cour hindoue a condamné 14 pirates indonésiens à sept ans d'emprisonnement chacun pour avoir détourné un navire battant pavillon japonais, l'*Alondra Rainbow*, au large des côtes indonésiennes en octobre 1999, en se basant sur l'article 105²⁹⁴ de la Convention des Nations Unies sur le Droit de la Mer. Il est assez inhabituel qu'une cour nationale se reconnaisse compétente pour un acte réalisé dans les eaux internationales. Le BMI souligne que les autorités hindoues ont « fait preuve de courage quand un Etat avec moins de conviction ne se serait tout simplement pas impliqué étant donné que l'incident concernait un navire étranger, transportant une cargaison étrangère, détourné par des ressortissants étrangers en dehors de sa zone de compétence ». Les garde-côtes de l'Inde ont notamment coopéré avec le BMI et la marine indonésienne pour stopper le navire détourné et arrêter les coupables. M. Raman insiste sur le fait que cette assistance doit devenir la norme plutôt que l'exception sinon la lutte contre le terrorisme maritime et la piraterie restera inefficace.

²⁸⁹ Loi n° 96-151 du 26 février 1996, article 28, modifiée par la loi n° 2002-3 du 3 janvier 2002 consacrant l'expression d'« agent habilité ».

²⁹⁰ Site du SAAG : <http://www.saag.org/papers12/paper1154.html>.

²⁹¹ Actions prises par la marine ou les garde-côtes d'un pays pour appréhender des terroristes impliqués dans des actes de terrorismes maritimes contre une autre nation.

²⁹² Poursuites judiciaires, extradition, remise des terroristes à la police de l'Etat attaqué par l'Etat d'appréhension.

²⁹³ Site du SAAG : <http://www.saag.org/papers12/paper1154.html>.

²⁹⁴ « Tout Etat peut, en haute mer ou en tout autre lieu ne relevant de la juridiction d'aucun Etat, saisir un navire ou un aéronef pirate, ou un navire ou un aéronef capturé à la suite d'un acte de piraterie et aux mains de pirates, et appréhender les personnes et saisir les biens se trouvant à bord. Les tribunaux de l'Etat qui a opéré la saisie peuvent se prononcer sur les peines à infliger, ainsi que sur les mesures à prendre en ce qui concerne le navire, l'aéronef ou les biens, réserve faite des tiers de bonne foi ».

La coopération doit également passer par une intensification des patrouilles communes le long des côtes ainsi qu'aux endroits stratégiques du trafic maritime évoqués antérieurement à plusieurs reprises. L'objectif est d'éviter des « trous » dans la surveillance. Toutefois, le problème reste toujours le même : les régions les plus sensibles sont au large de pays en voie de développement et il leur manque du matériel. C'est pourquoi, estimant que seule l'Indonésie peut résoudre la menace terroriste pesant sur ses eaux territoriales, Aldo Borgu²⁹⁵ considère que la majeure partie de la stratégie antiterroriste australienne doit permettre aux autorités indonésiennes d'en finir avec les organisations terroristes sévissant dans la région. Pour cela, il envisage d'assister les autorités indonésiennes en leur fournissant des bateaux pour patrouiller plus fréquemment, comme dans le cadre du programme *Pacific Patrol Boat* (PPB)²⁹⁶. Cette initiative du gouvernement australien avait en effet permis de renforcer les moyens techniques de surveillance et de patrouille maritime dans la région du Pacifique Sud.

Deuxièmement, le partage même des informations doit être intensifié, notamment par le biais de séminaires, ne serait-ce que parce qu'ils permettent d'échanger des idées sur un mode informel et ainsi de progresser, tel le brainstorming si prisé des praticiens du marketing. Il faut nécessairement avoir conscience des menaces qui pèsent sur la vie humaine, le trafic maritime et le commerce régional et mondial pour les combattre. Le premier pas est donc d'être capable d'identifier le plus clairement possible les organisations terroristes susceptibles d'attaquer le monde maritime. Ensuite, il faut procéder à un suivi de leurs mouvements pour pouvoir les démanteler. Les experts de la lutte anti-terroriste internationale ont déjà répartis les principaux groupes existants en quatre catégories mais uniquement dans l'optique de la menace la plus préoccupante pour la période et pour les USA, à savoir le terrorisme lié aux armes de destruction massive ²⁹⁷. Sur le même modèle, les organisations terroristes susceptibles de commettre des actes de terrorisme maritime pourraient être répertoriées. La première catégorie regrouperait celles qui ont déjà une capacité d'attaque maritime non seulement utilisable sur les côtes et aux abords des ports mais également en haute mer et qui se sont déjà illustrées en la matière, comme par exemple les LTTE. La deuxième catégorie correspondrait à celles qui ont démontré une « capacité sporadique » pour perpétrer certains actes de terrorisme maritime, tels que le détournement de navires, l'attaque de navires au mouillage, etc. Al Qaeda et certains mouvements palestiniens seraient dans cette catégorie. La troisième catégorie viserait celles qui ont témoigné d'un intérêt pour acquérir des compétences d'attaque maritime mais qui ne les ont pas encore. Les divers mouvements jihadistes liés de près ou de loin à Al Qaeda et au Front international

²⁹⁵ Site de l'ASPI : http://www.aspi.org.au/pdf/Maritime_terrorism%20India_AB.pdf.

²⁹⁶ Bateaux de patrouille du Pacifique. Ce programme a été officialisé en août 1983 suite à l'adoption de la Convention de Montego Bay sur le droit de la mer de 1982 qui a créé des ZEE et l'obligation de patrouiller dans ces zones. Site Wikipédia : http://en.wikipedia.org/wiki/Pacific_Patrol_Boat_Program.

²⁹⁷ En premier, viennent ceux qui prônent l'utilisation d'armes de destruction massive et qui en sont en possession, à savoir aucune organisation à l'heure actuelle. En deuxième, il y a ceux qui prônent l'utilisation d'armes de destruction massive ou qui sont susceptibles de les utiliser mais qui ne les ont pas encore ou qui sont en train de les acquérir. Al Qaeda et d'autres organisations jihadistes font partie de cette catégorie. Ceux qui sont déjà en possession d'une sorte d'armes de destruction massive mais qui n'en prônent pas l'utilisation constituent la troisième catégorie. Les LTTE y sont classés à cause de la réserve de cyanure de potassium à leur disposition. Si la quantité qu'ils détiennent reste méconnue, il est certain que s'il est mélangé avec de l'acide, les fumées ou vapeurs toxiques qui en résulteraient seraient suffisantes pour créer une panique collective sans précédent, voire des décès massifs. Enfin, la quatrième catégorie regroupe ceux qui n'ont jamais prôné l'utilisation d'armes de destruction massive et qui n'ont pas plus tenté d'en acquérir, à savoir la majorité des organisations terroristes. Site du SAAG : <http://www.saag.org/papers12/paper1154.html>.

islamique²⁹⁸ appartiendraient à cette catégorie. Enfin, la dernière catégorie contiendrait celles qui n'ont jamais eu d'aptitudes pour commettre des attaques maritimes et qui n'ont pas tenté non plus de les avoir. La plupart des organisations terroristes au niveau mondial rentreraient dans cette ultime catégorie.

Il est à noter, à ce sujet, que seuls des groupuscules ethniques ou religieux, notamment les « formations jihadistes panislamiques », semblent intéressés par l'éventualité de commettre des actes terroristes maritimes. En revanche, aucune formation idéologique ne paraît l'être. Il s'agit là encore d'un point crucial : les autorités des pays attaqués – notamment celles du détroit de Malacca au vu de l'escalade récemment enregistrée au niveau des actes de piraterie motivés par des raisons politiques dans la région – doivent pouvoir déterminer rapidement quels sont les motifs réels qui sous-tendent les actes perpétrés. Ainsi, ils pourront adapter leurs méthodes et les combattre plus efficacement. Pour cela, une collecte efficace de l'information de la part des services de renseignement est nécessaire. Il convient de garder à l'esprit que la menace peut être de deux sortes : soit venir de l'intérieur du pays et dans ce cas seule la compétence des services nationaux de renseignements pourra empêcher l'attaque ; soit être planifiée depuis l'extérieur si bien que pour la faire échouer, l'aide de l'Etat à partir duquel l'acte a été planifié sera tout aussi nécessaires. En tenant compte de cette seconde hypothèse, il apparaît que les services de renseignement devraient, dans une certaine mesure, se compléter. Dans cette optique, M. Raman²⁹⁹ prône l'accentuation de pratiques telles que le repérage commun de nouveaux agents, le recrutement commun, les interrogatoires communs. Il est bien évident que les services de renseignements y sont globalement opposés.

Il est intéressant d'observer, au sujet de la collecte d'informations que, en dehors des actions étatiques, certaines institutions privées s'efforcent pareillement de participer. A titre d'exemple, le Lloyd's Register, basé à Londres, travaille en coordination avec le MI6 britannique³⁰⁰ et la CIA étatsunienne afin de traquer les activités suspectes, en vérifiant entre autre l'acquisition des navires afin de déterminer s'ils n'ont pas été achetés par des terroristes préparant un attentat maritime.

Troisièmement, il faut être opérationnellement apte à gérer une crise majeure due à un attentat terroriste maritime. Il est à noter qu'en pareille situation, M. Raman estime qu'un Etat seul ne fait pas le poids, surtout quand il s'agit de pays aux moyens limités. Il propose donc de mettre en œuvre des cellules régionales de gestion de crise et d'organiser des exercices réguliers pour tester leur efficacité. Il est bien évident que la clé de la réussite de la lutte antiterroriste est la coopération entre toutes les nations du monde et ce parce que le transport maritime est par nature international et que le terrorisme affecte malheureusement tous les pays. Sans cette unanimité, tous les efforts déjà entrepris seraient vains. Comme le souligne Kofi Annan³⁰¹, Secrétaire général des Nations Unies, « le terrorisme ne peut être vaincu que si la communauté internationale a la volonté de s'unir en une large coalition ». La résultante est que cette unanimité n'est efficace que si elle dépasse le syndrome qualifié de « syndrome de la victime finale » par M.

²⁹⁸ *International Islamic Front*.

²⁹⁹ Site du SAAG : <http://www.saag.org/papers12/paper1154.html>.

³⁰⁰ Division experte en désinformation des services secrets britanniques.

³⁰¹ Site de l'ONU : http://www.un.org/french/geninfo/ir/ch2/ch2_txt.htm.

Raman³⁰²: à savoir qu'à l'heure actuelle, chaque pays agit contre le terrorisme quand il est directement concerné, c'est-à-dire quand les victimes sont ses propres citoyens. Si ce n'est pas le cas, la détermination est moins forte, donc nettement moins efficace, ce qui sert les terroristes. Un autre élément affaiblit le consensus général : les diverses lois nationales et accords bilatéraux adoptés par les USA et abordés précédemment, qui créent une distorsion des échanges mondiaux. Le problème s'est principalement posé avant l'entrée en vigueur du Code ISPS car l'échéancier étatsunien était avancé, notamment pour ce qui est de la loi du 14 novembre 2002³⁰³ qui rentrait en application six mois plus tôt que les mesures internationales.

Les USA ont par ailleurs mis en œuvre un certain nombre de mesures de sûreté additionnelles. Ils ont été les premiers à organiser des escortes militaires de super pétroliers, ou d'autre navires marchands. A titre exceptionnel, il est vrai que la manœuvre est efficace et dissuasive. Toutefois, en pratique, ce ne peut être généralisé et sur le long terme, cela devient absolument ingérable, voire impossible dans les eaux territoriales des autres pays. En effet, une telle initiative peut être considérée comme de l'ingérence dans la politique de défense nationale et conduire ainsi à des incidents diplomatiques. Quant à l'extension de la CSI au niveau mondial, il faudrait que le processus soit cadré par une institution internationale qui fixerait des limites afin d'éviter tout abus. Pour le moment, les vérifications de conteneurs sont focalisées sur les boîtes à destination des USA, même si, depuis 2004, le Canada et le Japon ont accepté une proposition étatsunienne consistant à scanner tout conteneur suspect au départ des ports étatsuniens et vers ces deux pays. Dans la même optique, le 22 avril 2004³⁰⁴, l'UE et les USA ont décidé de renforcer l'accord de coopération douanière et d'assistance mutuelle en matière douanière (ACAM) signé le 18 mai 1997. Le but est de rechercher toute solution susceptible d'assurer la sûreté du transport par conteneurs en provenance de n'importe quelle origine au sein de l'UE ou des USA ou en transbordement sur ces deux zones, ce qui couvre déjà une grande partie du commerce mondial pour accroître la sûreté de la chaîne d'approvisionnement. L'objectif étant que les principaux négociants asiatiques s'en inspirent pour que l'ensemble du secteur maritime soit impliqué. Enfin, les USA ont mis au point un détecteur de particules explosives qui est placé à côté des portiques de détection classiques, toutefois, le problème reste le même que pour les scanners, il est impossible de vérifier chaque conteneur.

L'autre partie du problème consiste en ce que les nouvelles mesures physiques de sûreté prises à la suite des attentats du 11 septembre 2001 ont été essentiellement dictées par l'anti-terrorisme étatsunien. Le but pour les USA est d'éviter que les terroristes ne se servent du commerce maritime comme d'un mode de transport d'armes de destruction massive. L'idée est louable mais le raisonnement ne tient globalement pas compte des préoccupations du reste du monde, notamment de l'Asie du Sud-est, où les navires servent à mettre en œuvre des actes terroristes plus classiques et plus tangibles par le biais d'armes plus conventionnelles, comme les explosifs. De même, le manque d'intérêt pour agir contre des organisations comme les LTTE, qui commettent des actes de terrorisme maritime effectifs mais uniquement aux alentours du Sri Lanka – ils ne menacent donc en rien les ressortissants étatsuniens et encore bien moins

³⁰² Site du SAAG : <http://www.saag.org/papers12/paper1154.html>.

³⁰³ Cf supra 2.6.1 Aux USA, page 62.

³⁰⁴ Site de l'UE : <http://europa.eu.int/scadplus/leg/fr/lvb/l06026.htm>.

l'économie des USA – est caractéristique de cet état d'esprit qui démontre bien que les intérêts étatsuniens sont prédominants par rapport aux autres.

Enfin, en dernier recours, il faut être capable de se préparer à l'inattendu et bien garder à l'esprit que les terroristes ciblent leur lieu d'action en fonction de l'opportunité qui se présente. Sans aborder la question en des termes élogieux, bien au contraire, il ne faut pas les sous-estimer et bien prendre en compte le fait que ce sont des individus rationnels, méticuleux et prudents, ce qui rend la lutte antiterroriste d'autant plus épineuse. Ils n'attaqueront que s'ils sont sûrs d'eux à 100% car leur but est de réussir leurs atrocités, si bien qu'ils attendent que leur objectif soit vulnérable. Il apparaît donc clairement que le seul moyen de lutte efficace est d'empêcher toute vulnérabilité. De plus, se concentrer sur leurs actions passées pour prédire leurs attaques futures est dangereux dans la mesure où ils vont rarement taper deux fois au même endroit. Bien au contraire, le propre du terrorisme est qu'il peut frapper n'importe où, n'importe comment, par n'importe quels moyens, ce qui n'a rien de rassurant. Pour les combattre sérieusement, il serait probablement plus pertinent d'essayer d'acquiescer ce que Aldo Borgu qualifie de « compréhension stratégique ». Il faudrait donc continuer à utiliser les informations tactiques obtenues en interrogeant les terroristes actuellement en captivité pour mener une sorte d'étude empirique détaillée à leur sujet. Le but ultime est de parvenir à les comprendre, eux et leur mode opératoire, eux et leurs motivations profondes, eux et ce qui les influence dans le choix des cibles, eux et leurs stratégies de recrutement, eux et la façon dont ils mesurent le succès d'une opération pour pouvoir, au final, mieux les anéantir. Toutefois, il ne faut pas non plus se laisser enfermer dans des schémas d'identification qui proposeraient un terroriste type.

3.4. Les dérives à éviter

Nombreux sont ceux qui voient l'information comme la meilleure arme pour lutter contre le terrorisme. Cependant, tant que la sûreté et la protection des passages maritimes vitaux pour le commerce mondial ne seront pas assurées, la menace du terrorisme maritime planera. Il faut donc agir mais en se basant sur des informations fiables, dans toute la mesure du possible, et ce afin d'éviter toute action démesurée et infondée. Une mesure de sûreté doit être proportionnée (section A/1.2.5 du Code ISPS), et ce en accord avec les principes fondamentaux du droit international et notamment avec le concept de légitime défense. Le préambule du Code ISPS, point 9, est clair sur ce point : « Aucune disposition du présent code ne doit être interprétée ou appliquée d'une manière incompatible avec le respect voulu des libertés et des droits fondamentaux énoncés dans les instruments régionaux, notamment ceux qui ont trait aux travailleurs maritimes et aux réfugiés y compris la Déclaration de l'Organisation Internationale du Travail sur les principes fondamentaux et les droits du travail, ainsi que les normes internationales concernant les travailleurs maritimes et portuaires ».

L'initiative dite de l'Amiral Thomas B. Fargo³⁰⁵ peut être citée à titre de double exemple. Après la chute des Talibans en Afghanistan, les USA ont cherché un certain nombre de solutions pour venir à bout du terrorisme en général, et du terrorisme maritime en particulier. Ils ont de fait

³⁰⁵ Site de l'Institut international d'études stratégiques, <http://www.iiss.org/stratcomfree.php?scID=386>.

adopté une approche régionale du terrorisme pour détruire les éventuels « futurs sanctuaires des terroristes ainsi que leurs bases d'entraînement ». Dans cette optique régionaliste, le Pentagone avait commencé à se pencher sur un projet d'initiative régionale en matière de sûreté maritime³⁰⁶ pour combattre à la fois la piraterie, le terrorisme maritime, le trafic de stupéfiants et le trafic d'êtres humains par mer. L'un des moyens à mettre en œuvre était de renforcer la surveillance des eaux du Sud-est asiatique et notamment celles du détroit de Malacca. Ce programme était censé comprendre non seulement un échange d'informations confidentielles avec les Etats d'Asie du Sud-est mais également le déploiement des forces spéciales et de la marine étatsuniennes, munies de petites vedettes rapides.

La réaction épidermique que ces mesures d'assistance ont immédiatement provoquée peut s'expliquer par le fait que tous les pays de la zone essaient depuis plusieurs années de trouver des solutions régionales à leurs problèmes régionaux de sûreté. De fait, début octobre 2003, les responsables de l'ASEAN³⁰⁷ se sont engagés à renforcer les liens qui les unissent au niveau de la lutte antiterroriste, de la piraterie maritime et des autres délits transnationaux par la création d'une communauté régionale en matière de sûreté. La proposition vient de l'Indonésie et l'un des objectifs prioritaires est d'accroître la coopération en matière de patrouille conjointe. En outre, l'accord *Five Power Defence Arrangement* entre Singapour, la Malaisie, la Grande Bretagne, l'Australie et la Nouvelle Zélande doit être prochainement modifié afin de prendre en compte le terrorisme ainsi que les autres menaces non conventionnelles dirigés contre la sécurité régionale ainsi que contre le monde maritime. Cette coopération régionale est absolument cruciale et doit être encouragée dans la mesure où le découpage administratif des frontières maritimes de ces nations reste un sujet de polémique qui complique la mise en application de certaines mesures. Enfin, Najib Tun Razak, Vice-premier ministre malaisien et ministre de la défense, craint que la présence des forces étatsuniennes dans la région n'augmente au contraire les risques d'insécurité tout en encourageant le fanatisme. Il n'est pas contre le fait de collaborer plus étroitement avec les USA mais il estime que la coopération doit porter sur le partage d'informations ainsi que sur le blocage des réseaux financiers et logistiques des mouvements terroristes plutôt que sur une présence physique comme le souhaitait le secrétaire étatsunien à la défense, Donald Rumsfeld.

Toutefois, la situation peut éventuellement être interprétée en des termes tout à fait différents³⁰⁸. Cette réponse des nations du Sud-est asiatique peut ainsi témoigner d'une certaine forme de ressentiment vis-à-vis de ce qui est considéré comme une initiative intrusive – alors que l'idée de départ était basée sur des intentions tout à fait honorables –. Plus exactement, le fait est que, pour certains gouvernements, il peut ne plus s'agir simplement de respect du droit international et de la non-ingérence mais plutôt de « géopolitique » et de « puissances maritimes qui souhaitent imposer leur volonté aux petits Etats côtiers ». Par le biais « d'excuses et de scénarios cauchemardesques », elles chercheraient à « accroître leur compétence dans les eaux territoriales de ces nations ainsi qu'à modifier les règles prévalant dans les détroits servant à la navigation internationale ». Cette approche en termes d'impérialisme étatsunien est tout aussi plausible au vu de l'histoire mais il convient également d'éviter toute paranoïa collective, aussi

³⁰⁶ La *Regional Maritime Security Initiative*, ou RMSI.

³⁰⁷ *Association of South East Asian Nations* – Association des nations du Sud-est asiatique.

³⁰⁸ Site du blog personnel de Bill Roggio: http://billroggio.com/archives/2005/04/of_pirates_and_1.php.

bien au niveau d'éventuels complots gouvernementaux que d'attentats catastrophes. En effet, une autre erreur à ne surtout pas commettre, même si la menace s'avère tangible, est de construire des scénarios d'horreur qui ne peuvent que compliquer la situation et en aucun cas apporter une quelconque solution. Ce n'est pas de ça dont le monde a besoin à l'heure actuelle eu égard à tous les attentats meurtriers qui se produisent. Il est bien évident qu'aucun pays n'est à l'abri d'actions terroristes dramatiques. Toutefois, il faudrait éviter, dans toute la mesure du possible, de surprojeter les actions malveillantes, notamment celles attribuées à Al Qaeda, tout en déconsidérant d'autres formations terroristes qui existaient bien avant, car ça ne fait que servir les terroristes, ce qui ne signifie pas qu'il faut devenir moins vigilant. Bien au contraire, il faut redoubler d'attention, de prudence et d'intelligence mais en se focalisant sur l'essentiel, sur le factuel et pas sur des fantasmes obsessionnels.

Au-delà de la polémique que cette initiative étatsunienne a soulevé de prime abord, il est un point intéressant : si les autres nations du monde veulent éviter l'ingérence d'un tiers dans leur politique de sûreté, ils ont tout intérêt à développer par eux-mêmes des programmes régionaux de coopération, de partage d'informations et de surveillance commune qui soient indépendants et efficaces. Au final, ce ne peut être que bénéfique et servir la lutte contre les actes malveillants, domaine des plus complexes.

Toute la problématique du terrorisme réside dans le fait qu'il s'agit d'un phénomène si effrayant et si ancré dans l'imaginaire collectif que le jugement en est sérieusement affecté et le désir de vengeance en devient plus fort que la raison. Toutefois, il ne faut pas perdre de vue que, bien que le terrorisme soit une horreur sans nom, ce que personne ne conteste, la lutte contre ce fléau ne doit pas dégénérer ni permettre de graves abus. L'Observatoire pour la protection des défenseurs des droits de l'Homme³⁰⁹ estime que l'année 2004 a été marquée par des lois antiterroristes qui ont « relativis[é], voire (...) ni[é] les droits de l'homme » mais le plus inquiétant est que cette constatation ne s'applique pas uniquement aux pays autoritaires, comme aiment à le penser. Elle rapporte que, depuis août 2004, les juges britanniques considèrent comme étant recevables les preuves résultant d'interrogatoires conduits sous la torture et souligne que « le nombre d'atteinte aux défenseurs des droits de l'Homme » a quasiment été multiplié par deux en comparaison avec 2003. Par ailleurs, il est heureux que le Premier ministre français actuel ait refusé de donner l'ordre aux forces de police de tirer pour tuer, ce qui constitue une grave dérive que rien ne peut expliquer dans une démocratie. La preuve en a été malheureusement faite par la mort de Jean-Charles de Menezes³¹⁰, électricien d'origine brésilienne de 27 ans, abattu à bout portant à Londres le 22 juillet 2005. Soupçonné à tort d'être un terroriste présumé ayant un lien avec les attentats terribles qui ont lieu dans le métro de la capitale britannique, il aurait été pris en chasse par des policiers en civil dans une rame de métro, avant d'être plaqué au sol et tué car il n'aurait pas obéi aux forces de l'ordre qui lui intimaient de s'arrêter. La lutte contre le terrorisme devient une véritable obsession car la pression qu'un attentat majeur se produise est trop forte et il semble que rien ne peut nous en protéger. Cependant, elle ne peut pas justifier de

³⁰⁹ Programme commun à la Fédération internationale des ligues des droits de l'Homme (FIDH) et à l'Organisation mondiale contre la torture (OMCT). Site du Monde : <http://www.lemonde.fr/web/article/0,1-0@2-3220,36-639882@51-635324,0.html>.

³¹⁰ Site du Monde : <http://www.lemonde.fr/web/article/0,1-0@2-669420,36-682158,0.html>.

tels drames, rien ne le peut sinon cela équivaldrait à se rabaisser au même niveau que les terroristes et à totalement déconsidérer la vie humaine.

Conclusion

Ambitionnant un vaste consensus entre les gouvernements, les installations portuaires et les navires, le Code ISPS est le fruit du travail intensif entrepris par le Comité de Sécurité Maritime de l'OMI et son groupe de travail inter-sessionnel pendant un an. Il vise à renforcer la sûreté maritime pour détecter, prévenir et dissuader des actes malveillants pouvant compromettre la sûreté du transport maritime afin que la vulnérabilité soit minimale. Chacun y a rapidement participé car la sûreté s'est vite révélée être un atout majeur pour les ports ainsi qu'un élément indispensable à la poursuite des activités commerciales pour un armateur. Il est cependant à noter que, pour certains pays, dont la France fait partie, il s'agit essentiellement d'une uniformisation à l'échelle internationale dans la mesure où ils appliquaient déjà un certain nombre de mesures similaires à celles nouvellement imposées.

Pour Efthimios Mitropoulos, Secrétaire général de l'OMI, « (...) l'objectif final [est d']élever nos défenses le plus haut possible afin que l'industrie maritime ne devienne pas la cible d'activités terroristes ». Ainsi, le premier pas a été franchi avec le règlement européen (CE) n°725/2004 qui a considérablement étendu l'application du Code ISPS, sans oublier la possibilité – qui deviendra à n'en pas douter obligatoire d'ici là – laissée aux Etats membres de la Communauté européenne d'inclure tous les navires au 1^{er} juillet 2007. L'intérêt serait évidemment que de telles mesures soient généralisées sous peine de renouveler la problématique d'un Code ISPS inégalement appliqué, seule l'uniformité les rendra efficaces. Quant à la sûreté de l'ensemble de la chaîne logistique, elle apparaît de plus en plus comme la prochaine étape. L'OMI a logiquement commencé par le dernier maillon, souvent considéré comme l'un des plus vulnérables, mais il est bien évident qu'une fois le matériel ou les individus chargés de l'attaque terroriste dans l'enceinte portuaire ou à bord du navire, il est trop tard. C'est pourquoi il faut sensibiliser toute la chaîne logistique, un élément seul n'est pas suffisant seule l'implication de tout un chacun est efficace. Il est à espérer que le nouveau projet en cours d'élaboration à l'OMI sur le transport maritime tienne compte de cette problématique.

La situation reste toutefois d'autant plus menaçante actuellement que des « pirates nouvelle génération » s'en prennent de plus en plus fréquemment à des navires marchands transportant des cargaisons dangereuses. Par ailleurs, les attaques contre les navires à passagers gagnent malheureusement en fréquence : un attentat³¹¹ a notamment été perpétré le 28 août 2005 contre le ferry, le *Dona Ramona*, à Lamitan, sur l'île de Basilan, au Sud des Philippines lors de l'embarquement. Un explosif dissimulé à l'arrière du bateau, sous des réservoirs de gaz de pétrole liquéfié (GPL) a blessé 30 personnes – certaines ont des brûlures au troisième degré – et a provoqué un énorme incendie. Ce n'est donc pas le moment de faiblir et l'implication de tous les intervenants reste primordiale sinon la sûreté n'est pas maximale, ce qui est hautement préjudiciable et dangereux. Il est bien évident que la lutte contre la piraterie et le terrorisme international, maritime ou autre, ne peut être que le fruit d'efforts collectifs. Toutefois, il convient

³¹¹ Site de RTL Belgique : <http://www.rtl.be/Site/Index.aspx?LG=1&PageID=209&ArticleID=50756>.

de rappeler que le Code ISPS ne prévoit aucune mesure d'action car ce n'est pas son rôle. L'ISPS n'est que de la prévention.

Il faut également retenir que toute mesure physique de sûreté exige deux composantes essentielles pour être efficace : en premier lieu, une vérification intransigeante des antécédents des nouveaux employés des compagnies maritimes pour éviter toute infiltration de terroristes ou de sympathisants, et plus particulièrement des membres d'équipage, ce qui est des plus difficiles dans la mesure où les navires de commerce recrute dans de nombreux ports en fonction des besoins immédiats. En second lieu, la politique de contrôles aux accès doit être des plus drastiques. Beaucoup souhaitaient la mise en place de mesures de sûreté semblables à celles existant dans un aéroport mais il faut bien être conscient qu'un port est dans une situation diamétralement opposée. Un aéroport est un espace totalement clos, ce que ne sera jamais un port, même avec des barrières et autres grilles ; de plus, le flux de marchandises et de camions qui circulent dans une enceinte portuaire est incomparable avec la situation d'un aéroport qui ne représente qu'à peine 10% du trafic de marchandises à l'échelle mondiale. Par ailleurs, il s'agit essentiellement de marchandises peu volumineuses et qui sont plus rarement conteneurisées que le fret maritime. Toutefois, il n'en demeure pas moins que le monde aérien est une source d'inspiration de par son avancement en la matière.

Pour ce qui est du cas spécifique de la France, le bilan de l'application de l'ISPS est jugé « satisfaisant » par le ministère des transports, de l'équipement, du tourisme et de la mer, et ce en partie du fait que la collaboration entre les exploitants des installations portuaires, les autorités portuaires et les services gouvernementaux en a été considérablement renforcée. Les efforts devraient désormais s'orienter vers le regroupement, sur un lieu de travail commun, des AFFMAR et des ports, comme cela se pratique déjà en Italie notamment, de façon à éviter toute perte d'informations ou du moins de retard dans la transmission. La préoccupation majeure, à l'heure actuelle, reste toutefois l'amélioration de la sûreté des bassins portuaires – dépendant du préfet de département à l'intérieur des limites administratives du port –. En effet, une carence est apparue en matière de surveillance nautique, en tant qu'élément d'intimidation. Il est à noter que cette zone de compétence territoriale dépend de la police nationale si bien que l'une des solutions envisagées serait la création de « brigades de sûreté portuaire ». Elles pourraient être introduites au niveau du PAM et du port autonome du Havre.

L'enjeu est de taille puisque les avantages de l'accroissement de la sûreté du transport maritime vont déjà bien au-delà de la lutte contre le terrorisme, qui, il est vrai était l'objectif central. En effet, la résultante des mesures de sûreté consiste bien souvent en des améliorations en matière de sécurité, la réciproque n'étant pourtant pas vraie. A titre d'exemples, le renforcement de la sûreté maritime a permis de lutter contre le crime organisé, de réduire le nombre de vols de conteneurs sur les terminaux, d'intercepter des passagers clandestins, d'augmenter les capacités en matière de recherche et de sauvetage en mer, d'accroître la protection des pêches et d'affiner la lutte contre la pollution du milieu marin. A titre d'exemple, pour le seul port autonome de Marseille et ce entre janvier et novembre 2004, ce sont quelques

150 passagers clandestins qui ont été interpellés dans l'enceinte portuaire grâce aux diverses opérations de contrôle³¹².

Il est un fait incontournable : un laps de temps supplémentaire est nécessaire pour asseoir définitivement les pratiques les mieux adaptées à une sûreté maximale. Certains sont partagés quant aux méthodes courantes de l'industrie maritime, par exemple l'utilisation de sociétés privées pour contrôler les accès aussi bien des navires que des installations portuaires, qui est à double tranchant : dans un sens, elles seront nettement plus rigoureuses sur l'identité des personnes et ne seront pas influencées dans leur travail, ce qui est un bien. De l'autre, pour le cas spécifique des navires, elles n'ont pas une culture maritime et ne seront probablement pas assez impliquées pour saisir tout le bénéfice à retirer de ces nouvelles mesures. En tout état de cause, la matière reste vivante et ce même d'un point de vue juridique puisque qu'une directive européenne portant sur les unités de chargement intermodales³¹³ est actuellement en cours de discussion pour accroître la sécurisation des conteneurs par des contrôles périodiques et une homologation communautaire uniformisée. Ce texte fait suite, entre autre, à la Convention internationale sur la sécurité des conteneurs des Nations unies (CSC) de 1972 qui a été ratifiée par la plupart des Etats membres. Il ne faut pas oublier non plus la proposition de directive européenne³¹⁴ qui veut que le port, dans sa globalité, soit sécurisé. Maintenant que l'interface mer/terre (navire/installation portuaire) a été traitée, ce texte est sous-tendu par la nécessité d'inclure, dans la sûreté du transport maritime, le dernier tronçon, à savoir la liaison terre/terre matérialisée dans les relations entre le port et l'intérieur du pays.

Enfin, il ne faut pas perdre de vue que si le risque qu'un navire soit utilisé comme bombe flottante est certain, il n'en reste pas moins qu'il ne faut pas oublier trop facilement que les navires modernes sont assez bien équipés d'un point de vue sécuritaire – notamment avec l'avènement des doubles coques – si bien qu'il n'est pas si simple de faire complètement exploser leur chargement ou de les couler.

L'intérêt des différentes mesures de sûreté adoptées est d'être capable d'anticiper de tels périls ainsi que de savoir réagir en cas d'attaque réelle, ce qui passe nécessairement par le partage de renseignements et la coopération internationale. Il est intéressant de noter que, dans un domaine aussi secret que la sûreté, la principale réponse à apporter est paradoxalement l'information.

³¹² Article paru dans Metro, *Opération de contrôle au port*, novembre 2004.

³¹³ Site de l'UE : <http://europa.eu.int/scadplus/leg/fr/lvb/l24271.htm>.

³¹⁴ Cf supra : 2.1.2.3 La proposition de directive du 11 juin 2004, page 35.

Annexes

Tables des annexes

Annexe I : Le Code ISPS, partie A

Annexe II : Chiffres sur la violence en mer

Annexe III: Les autorités impliquées dans le contrôle du navire au port

Annexe IV: Les équipements de sûreté

Annexe V : Les taux de conformité internationaux au Code ISPS

Annexe VI : Exemples de différents certificats internationaux de sûreté du navire

Annexe I³¹⁵

Le Code ISPS, partie A

PRESCRIPTIONS OBLIGATOIRES CONCERNANT LES DISPOSITIONS DU CHAPITRE XI-2 DE LA CONVENTION INTERNATIONALE DE 1974 POUR LA SAUVEGARDE DE LA VIE HUMAINE EN MER TELLE QUE MODIFIÉE

1. Généralités

1.1. Introduction :

La présente partie du Code international pour la sûreté des navires et des installations portuaires contient les dispositions obligatoires auxquelles il est fait référence dans le chapitre XI-2 de la Convention internationale de 1974 pour la sauvegarde de la vie humaine en mer, telle que modifiée.

1.2. Objectifs :

Les objectifs du présent Code sont les suivants :

1. établir un cadre international faisant appel à la coopération entre les Gouvernements contractants, les organismes publics, les administrations locales et les secteurs maritime et portuaire pour détecter les menaces contre la sûreté et prendre des mesures de sauvegarde contre les incidents de sûreté qui menacent les navires ou les installations portuaires utilisés dans le commerce international ;
2. établir les rôles et responsabilités respectifs des Gouvernements contractants, des organismes publics, des administrations locales et des secteurs maritime et portuaire, aux niveaux national et international, pour garantir la sûreté maritime ;
3. garantir le rassemblement et l'échange rapides et efficaces de renseignements liés à la sûreté ;
4. prévoir une méthode pour procéder aux évaluations de la sûreté en vue de l'établissement de plans et de procédures permettant de réagir aux changements des niveaux de sûreté ; et
5. donner l'assurance que des mesures de sûreté maritime adéquates et proportionnées sont en place.

1.3. Prescriptions fonctionnelles :

En vue de réaliser ses objectifs, le Code incorpore un certain nombre de prescriptions fonctionnelles. Celles-ci comprennent, sans toutefois s'y limiter, les fonctions suivantes :

1. rassembler et évaluer des renseignements concernant les menaces contre la sûreté et échanger ces renseignements avec les Gouvernements contractants appropriés ;
2. exiger le maintien de protocoles de communication à l'intention des navires et des installations portuaires ;
3. empêcher l'accès non autorisé aux navires et aux installations portuaires et à leurs zones d'accès restreint ;
4. empêcher l'introduction d'armes, de dispositifs incendiaires ou d'explosifs non autorisés à bord des navires et dans les installations portuaires ;
5. offrir un moyen de donner l'alerte pour réagir aux menaces contre la sûreté ou à des incidents de sûreté ;
6. exiger des plans de sûreté du navire et de l'installation portuaire établis à partir des évaluations de la sûreté ; et
7. exiger une formation, un entraînement et des exercices pour garantir la familiarisation avec les plans et procédures de sûreté.

2. Définitions

2.1. Aux fins de la présente partie, sauf disposition expresse contraire :

1. Convention désigne la Convention internationale de 1974 pour la sauvegarde de la vie humaine en mer, telle que modifiée.
2. Règle désigne une règle de la Convention.
3. Chapitre désigne un chapitre de la Convention.

³¹⁵ Site de la CAMP : http://www.arbitrage-maritime.org/fr/PDF/Code_ISPS.pdf.

4. Plan de sûreté du navire désigne un plan établi en vue de garantir l'application des mesures nécessaires à bord du navire pour protéger les personnes à bord, la cargaison, les engins de transport, les provisions de bord ou le navire contre les risques d'un incident de sûreté.

5. Plan de sûreté de l'installation portuaire désigne un plan établi en vue de garantir l'application des mesures nécessaires pour protéger l'installation portuaire et les navires, les personnes, la cargaison, les engins de transport et les provisions de bord à l'intérieur de l'installation portuaire contre les risques d'un incident de sûreté.

6. Agent de sûreté du navire désigne la personne à bord du navire, responsable devant le capitaine, désignée par la compagnie comme responsable de la sûreté du navire, y compris de l'exécution et du maintien du plan de sûreté du navire et de la liaison avec l'agent de sûreté de la compagnie et les agents de sûreté de l'installation portuaire.

7. Agent de sûreté de la compagnie désigne la personne désignée par la compagnie pour garantir qu'une évaluation de la sûreté du navire est effectuée, qu'un plan de sûreté du navire est établi, est soumis pour approbation et est ensuite appliqué et tenu à jour, et pour assurer la liaison avec l'agent de sûreté de l'installation portuaire et l'agent de sûreté du navire.

8. Agent de sûreté de l'installation portuaire désigne la personne désignée comme étant responsable de l'établissement, de l'exécution, de la révision et du maintien du plan de sûreté de l'installation portuaire ainsi que de la liaison avec les agents de sûreté du navire et les agents de sûreté de la compagnie.

9. Niveau de sûreté 1 désigne le niveau auquel des mesures de sûreté minimales appropriées doivent être maintenues en permanence.

10. Niveau de sûreté 2 désigne le niveau auquel des mesures de sûreté additionnelles appropriées doivent être maintenues pendant une période déterminée en raison d'un risque accru d'incident de sûreté.

11. Niveau de sûreté 3 désigne le niveau auquel de nouvelles mesures de sûreté spéciales doivent être maintenues pendant une période limitée lorsqu'un incident de sûreté est probable ou imminent, bien qu'il puisse ne pas être possible d'identifier la cible précise.

2.2. Le terme « navire », lorsqu'il est employé dans le présent Code, comprend les unités mobiles de forage au large et les engins à grande vitesse, tels que définis à la règle XI-2/1.

2.3. L'expression « Gouvernement contractant » utilisée dans un contexte en rapport avec une installation portuaire, lorsqu'elle figure dans les sections 14 à 18, constitue aussi une référence à l'autorité désignée.

2.4. Les termes et expressions pour lesquels aucune définition n'est donnée dans la présente partie ont le sens qui leur est donné aux chapitres Ier et XI-2 de la Convention.

3. Application

3.1. Le présent Code s'applique :

1. aux types de navires suivants qui effectuent des voyages internationaux :

1. navires à passagers, y compris les engins à grande vitesse à passagers ;

2. navires de charge, y compris les engins à grande vitesse à cargaisons, d'une jauge brute égale ou supérieure à 500 ; et

3. unités mobiles de forage au large ; et

2. aux installations portuaires fournissant des services à de tels navires qui effectuent des voyages internationaux.

3.2. Nonobstant les dispositions de la section 3.1.2, les Gouvernements contractants doivent décider de la portée de l'application de la présente partie du Code aux installations portuaires situées sur leur territoire qui, bien qu'elles soient principalement utilisées par des navires qui n'effectuent pas de voyages internationaux, doivent parfois fournir des services à des navires arrivant d'un voyage international ou partant pour un tel voyage.

3.2.1. Les Gouvernements contractants doivent fonder leur décision, prise en vertu de la section 3.2, sur une évaluation de la sûreté de l'installation portuaire effectuée conformément à la présente partie du Code.

3.2.2. Toute décision prise par un Gouvernement contractant en vertu de la section 3.2 ne doit pas compromettre le niveau de sûreté à atteindre en vertu du chapitre XI-2 ou de la présente partie du Code.

3.3. Le présent Code ne s'applique pas ni aux navires de guerre ou navires de guerre auxiliaires ni aux autres navires appartenant à un Gouvernement contractant ou exploités par lui et affectés exclusivement à un service public non commercial.

3.4. Les sections 5 à 13 et 19 de la présente partie s'appliquent aux compagnies et aux navires de la manière spécifiée à la règle XI-2/4.

3.5. Les sections 5 et 14 à 18 de la présente partie s'appliquent aux installations portuaires de la manière spécifiée à la règle XI-2/10.

3.6. Aucune disposition du présent Code ne porte atteinte aux droits ou obligations qu'ont les Etats en vertu du droit international.

4. Responsabilités des Gouvernements contractants

4.1. Sous réserve des dispositions des règles XI-2/3 et XI-2/7, les Gouvernements contractants doivent établir des niveaux de sûreté et donner des recommandations sur les mesures de protection contre les incidents de sûreté. Des niveaux de sûreté supérieurs dénotent une probabilité accrue de survenance d'un incident de sûreté. Les facteurs à prendre en considération pour l'établissement du niveau de sûreté approprié comprennent notamment :

1. la mesure dans laquelle l'information sur la menace est crédible ;
2. la mesure dans laquelle l'information sur la menace est corroborée ;
3. la mesure dans laquelle l'information sur la menace est spécifique ou imminente ; et
4. les conséquences potentielles de l'incident de sûreté.

4.2. Les Gouvernements contractants, lorsqu'ils établissent le niveau de sûreté 3, doivent diffuser, si nécessaire, des consignes appropriées et fournir des renseignements liés à la sûreté aux navires et aux installations portuaires susceptibles d'être touchés.

4.3. Les Gouvernements contractants peuvent déléguer à un organisme de sûreté reconnu certaines des tâches liées à la sûreté qui leur incombent en vertu du chapitre XI-2 et de la présente partie du Code, à l'exception des tâches suivantes :

1. établir le niveau de sûreté applicable ;
2. approuver une évaluation de sûreté d'une installation portuaire et tout amendement ultérieur à une évaluation approuvée ;
3. identifier les installations portuaires qui seront appelées à désigner un agent de sûreté de l'installation portuaire ;
4. approuver un plan de sûreté d'une installation portuaire et tout amendement ultérieur à un plan approuvé ;
5. exercer des mesures liées au contrôle et au respect des dispositions en application de la règle XI-2/9 ; et
6. établir les prescriptions applicables à une déclaration de sûreté.

4.4. Les Gouvernements contractants doivent, dans la mesure où ils le jugent approprié, mettre à l'épreuve les plans de sûreté du navire ou de l'installation portuaire qu'ils ont approuvés ou, dans le cas des navires, les plans qui ont été approuvés en leur nom, ou les amendements à ces plans, pour vérifier leur efficacité.

5. Déclaration de sûreté

5.1. Les Gouvernements contractants doivent déterminer quand une déclaration de sûreté est requise, en évaluant le risque qu'une interface navire/port ou une activité de navire à navire présente pour les personnes, les biens ou l'environnement.

5.2. Un navire peut demander qu'une déclaration de sûreté soit remplie lorsque :

1. le navire est exploité à un niveau de sûreté supérieur à celui de l'installation portuaire ou d'un autre navire avec lequel il y a interface ;
2. il existe un accord entre les Gouvernements contractants au sujet d'une déclaration de sûreté visant certains voyages internationaux ou navires spécifiques effectuant de tels voyages ;
3. il y a eu une menace pour la sûreté ou un incident de sûreté mettant en cause le navire ou l'installation portuaire, selon le cas
4. le navire se trouve dans un port qui n'est pas tenu d'avoir ou de mettre en oeuvre un plan de sûreté de l'installation portuaire approuvé ; ou

5. le navire exerce des activités de navire à navire avec un autre navire qui n'est pas tenu d'avoir et de mettre en oeuvre un plan de sûreté du navire approuvé.

5.3. L'installation portuaire ou le ou les navires, selon le cas, doivent accuser réception des demandes de déclaration de sûreté pertinentes faites en vertu de la présente section.

5.4. La déclaration de sûreté doit être remplie par :

1. le capitaine ou l'agent de sûreté du navire pour le compte du ou des navire(s) ; et, s'il y a lieu,
2. l'agent de sûreté de l'installation portuaire ou, si le Gouvernement contractant en décide autrement, une autre entité responsable de la sûreté à terre, pour le compte de l'installation portuaire.

5.5. La déclaration de sûreté doit indiquer les mesures de sûreté requises qui pourraient être partagées entre une installation portuaire et un navire ou entre des navires, ainsi que la responsabilité de chacun.

5.6. Les Gouvernements contractants doivent spécifier, compte tenu des dispositions de la règle XI-2/9.2.3, la durée minimale pendant laquelle les déclarations de sûreté doivent être conservées par les installations portuaires situées sur leur territoire.

5.7. Les Administrations doivent spécifier, compte tenu des dispositions de la règle XI-2/9.2.3, la durée minimale pendant laquelle les déclarations de sûreté doivent être conservées par les navires autorisés à battre leur pavillon.

6. Obligations de la compagnie

6.1. La compagnie doit veiller à ce que le plan de sûreté du navire contienne un énoncé clair mettant l'accent sur l'autorité du capitaine. La compagnie doit spécifier, dans le plan de sûreté du navire, que le capitaine a le pouvoir et la responsabilité absolus de prendre des décisions concernant la sécurité et la sûreté du navire et de solliciter l'assistance de la compagnie ou de tout Gouvernement contractant, selon que de besoin.

6.2. La compagnie doit veiller à ce que l'agent de sûreté de la compagnie, le capitaine et l'agent de sûreté du navire bénéficient de l'appui nécessaire pour s'acquitter de leurs tâches et de leurs responsabilités conformément au chapitre XI-2 et à la présente partie du Code.

7. Sûreté du navire

7.1. Un navire est tenu de prendre des mesures correspondant aux niveaux de sûreté établis par les Gouvernements contractants, comme il est indiqué ci-dessous.

7.2. Au niveau de sûreté 1, les activités suivantes doivent être exécutées, par le biais de mesures appropriées, à bord de tous les navires, compte tenu des recommandations énoncées dans la partie B du présent Code, en vue d'identifier et de prendre des mesures de sauvegarde contre les incidents de sûreté :

1. veiller à l'exécution de toutes les tâches liées à la sûreté du navire ;
2. contrôler l'accès au navire ;
3. contrôler l'embarquement des personnes et de leurs effets ;
4. surveiller les zones d'accès restreint pour s'assurer que seules les personnes autorisées y ont accès ;
5. surveiller les zones de pont et les zones au voisinage du navire ;
6. superviser la manutention de la cargaison et des provisions de bord ; et
7. veiller à ce que le système de communication de sûreté soit rapidement disponible.

7.3. Au niveau de sûreté 2, les mesures de protection additionnelles, spécifiées dans le plan de sûreté du navire, doivent être mises en oeuvre pour chacune des activités décrites dans la section 7.2, compte tenu des recommandations énoncées dans la partie B du présent Code.

7.4. Au niveau de sûreté 3, des mesures de protection spéciales supplémentaires, spécifiées dans le plan de sûreté du navire, doivent être mises en oeuvre pour chacune des activités décrites dans la section 7.2, compte tenu des recommandations énoncées dans la partie B du présent Code.

7.5. Chaque fois que l'Administration établit un niveau de sûreté 2 ou un niveau de sûreté 3, le navire doit accuser réception des consignes concernant le changement de niveau de sûreté.

7.6. Avant d'entrer dans un port ou quand il se trouve dans un port situé sur le territoire d'un Gouvernement contractant qui a établi un niveau de sûreté 2 ou un niveau de sûreté 3, le navire doit accuser réception de cette consigne et confirmer à l'agent de sûreté de l'installation portuaire qu'il a commencé à mettre en oeuvre les mesures et procédures appropriées décrites dans le plan de sûreté du navire et dans le cas du niveau de sûreté 3, dans les consignes diffusées par le Gouvernement contractant qui a établi le niveau de sûreté 3. Le navire doit signaler les difficultés éventuelles que pose leur mise en oeuvre. Dans ce cas, l'agent de sûreté de l'installation portuaire et l'agent de sûreté du navire doivent rester en liaison et coordonner les mesures appropriées.

7.7. Si un navire est tenu par l'Administration d'établir, ou a déjà établi, un niveau de sûreté supérieur à celui qui a été établi pour le port dans lequel il a l'intention d'entrer ou dans lequel il se trouve déjà, ce navire doit en informer, sans tarder, l'autorité compétente du Gouvernement contractant sur le territoire duquel l'installation portuaire est située et l'agent de sûreté de l'installation portuaire.

7.7.1. Dans ce cas, l'agent de sûreté du navire doit rester en liaison avec l'agent de sûreté de l'installation portuaire et coordonner les mesures appropriées, si nécessaire.

7.8. Une Administration qui demande aux navires autorisés à battre son pavillon d'établir un niveau de sûreté 2 ou 3 dans un port d'un autre Gouvernement contractant doit en informer ce Gouvernement contractant sans tarder.

7.9. Lorsque les Gouvernements contractants établissent des niveaux de sûreté et veillent à ce que des renseignements sur le niveau de sûreté soient fournis aux navires qui sont exploités dans leur mer territoriale ou qui ont fait part de leur intention d'entrer dans leur mer territoriale, ces navires doivent être invités à rester vigilants et à communiquer immédiatement à leur Administration et à tous les Etats côtiers voisins tous renseignements portés à leur attention qui risqueraient de compromettre la sûreté maritime dans la zone.

7.9.1. Lorsqu'il informe ces navires du niveau de sûreté applicable, un Gouvernement contractant doit, compte tenu des recommandations énoncées dans la partie B du présent Code, informer également ces navires de toute mesure de sûreté qu'ils devraient prendre et, le cas échéant, des mesures qui ont été prises par le Gouvernement contractant pour fournir une protection contre la menace.

8. Evaluation de la sûreté du navire

8.1. L'évaluation de la sûreté du navire est un élément essentiel qui fait partie intégrante du processus d'établissement et d'actualisation du plan de sûreté du navire.

8.2. L'agent de sûreté de la compagnie doit veiller à ce que l'évaluation de la sûreté du navire soit effectuée par des personnes ayant les qualifications voulues pour procéder à une estimation de la sûreté d'un navire, conformément à la présente section et compte tenu des recommandations énoncées dans la partie B du présent Code.

8.3. Sous réserve des dispositions de la section 9.2.1, un organisme de sûreté reconnu peut effectuer l'évaluation de sûreté du navire d'un navire particulier.

8.4. L'évaluation de la sûreté du navire doit comprendre une étude de sûreté sur place et, au moins, les éléments suivants :

1. identification des mesures, des procédures et des opérations de sûreté existantes ;
2. identification et évaluation des opérations essentielles de bord qu'il est important de protéger ;
3. identification des menaces éventuelles contre les opérations essentielles de bord et probabilité de survenance, afin d'établir des mesures de sûreté et de leur donner un ordre de priorité ; et
4. identification des points faibles, y compris les facteurs humains, de l'infrastructure, des politiques et des procédures.

8.5. L'évaluation de la sûreté du navire doit être étayée par des documents, être examinée, acceptée et conservée par la compagnie.

9. Plan de sûreté du navire

9.1. Chaque navire doit avoir à bord un plan de sûreté approuvé par l'Administration. Ce plan doit prévoir des dispositions pour les trois niveaux de sûreté tels que définis dans la présente partie du Code.

9.1.1. Sous réserve des dispositions de la section 9.2.1, un organisme de sûreté reconnu peut préparer le plan de sûreté du navire d'un navire particulier.

9.2. L'Administration peut confier l'examen et l'approbation des plans de sûreté du navire, ou des amendements à un plan précédemment approuvé, à des organismes de sûreté reconnus.

9.2.1. Dans ce cas, l'organisme de sûreté reconnu chargé d'examiner et d'approuver un plan de sûreté du navire, ou des amendements à ce plan, ne doit pas avoir participé à la préparation de l'évaluation de la sûreté du navire ni à la préparation du plan de sûreté du navire, ou des amendements à ce plan, devant faire l'objet de l'examen.

9.3. Tout plan de sûreté du navire, ou tout amendement à un plan approuvé précédemment, qui est soumis aux fins d'approbation doit être accompagné de l'évaluation de la sûreté sur la base de laquelle il a été mis au point.

9.4. Un tel plan doit être élaboré compte tenu des recommandations énoncées dans la partie B du présent Code et être rédigé dans la ou les langues de travail du navire. Si la ou les langues utilisées ne sont ni l'anglais, ni l'espagnol, ni le français, une traduction dans l'une de ces langues doit être fournie. Le plan doit porter au moins sur ce qui suit :

1. les mesures visant à empêcher l'introduction à bord d'armes, de substances dangereuses et d'engins destinés à être utilisés contre des personnes, des navires ou des ports et dont la présence à bord n'est pas autorisée ;
2. l'identification des zones d'accès restreint et des mesures visant à empêcher l'accès non autorisé à ces zones ;
3. des mesures visant à empêcher l'accès non autorisé au navire ;
4. des procédures pour faire face à une menace contre la sûreté ou une atteinte à la sûreté, y compris des dispositions pour maintenir les opérations essentielles du navire ou de l'interface navire/port ;
5. des procédures pour donner suite aux consignes de sûreté que les Gouvernements contractants peuvent donner au niveau de sûreté 3 ;
6. des procédures d'évacuation en cas de menace contre la sûreté ou d'atteinte à la sûreté ;
7. les tâches du personnel du navire auquel sont attribuées des responsabilités en matière de sûreté et celles des autres membres du personnel du navire concernant les aspects liés à la sûreté ;
8. des procédures d'audit des activités liées à la sûreté ;
9. des procédures concernant la formation, les entraînements et les exercices liés au plan ;
10. des procédures concernant l'interface avec les activités liées à la sûreté des installations portuaires ;
11. des procédures concernant l'examen périodique du plan et sa mise à jour ;
12. des procédures de notification des incidents de sûreté ;
13. l'identification de l'agent de sûreté du navire ;
14. l'identification de l'agent de sûreté de la compagnie, y compris les coordonnées où il peut être joint 24 heures sur 24 ;
15. des procédures visant à garantir l'inspection, la mise à l'essai, l'étalonnage et l'entretien de tout matériel de sûreté prévu à bord ;
16. la fréquence de la mise à l'essai ou de l'étalonnage de tout matériel de sûreté prévu à bord ;
17. l'identification des endroits où sont installées les commandes du système d'alerte de sûreté du navire ; et
18. les procédures, instructions et conseils concernant l'utilisation du système d'alerte de sûreté du navire, y compris sa mise à l'essai, son déclenchement ; sa neutralisation et son réenclenchement et la manière de réduire le nombre de fausses alertes.

9.4.1. Le personnel qui procède aux audits internes des activités liées à la sûreté spécifiées dans le plan ou qui évalue sa mise en oeuvre ne doit pas avoir de rapport avec les activités faisant l'objet de l'audit, à moins que cela ne soit pas possible dans la pratique du fait de la taille et de la nature de la compagnie ou du navire.

9.5. L'Administration doit décider quelles sont les modifications qui ne doivent pas être apportées à un plan de sûreté du navire approuvé ou au matériel de sûreté spécifié dans le plan approuvé sans que les amendements pertinents au plan soient approuvés par elle. Ces modifications

doivent être au moins aussi efficaces que les mesures prescrites dans le chapitre XI-2 et dans la présente partie du Code.

9.5.1. La nature des modifications apportées au plan de sûreté du navire ou au matériel de sûreté qui ont été expressément approuvées par l'Administration conformément à la section 9.5 doit être expliquée dans un document indiquant clairement cette approbation. Cette approbation doit être conservée à bord du navire et doit être présentée en même temps que le Certificat de sûreté du navire (ou le Certificat international provisoire de sûreté du navire). Si ces modifications sont provisoires, lorsque les mesures ou le matériel approuvés à l'origine sont rétablis, il n'est plus nécessaire de conserver à bord du navire ce document.

9.6. Le plan peut être conservé sous forme électronique. Dans ce cas, il doit être protégé par des procédures visant à empêcher que ses données soient effacées, détruites ou modifiées sans autorisation.

9.7. Le plan doit être protégé contre tout accès ou toute divulgation non autorisés.

9.8. Les plans de sûreté du navire ne doivent pas faire l'objet d'une inspection par les fonctionnaires dûment autorisés par un Gouvernement contractant à exécuter les mesures liées au contrôle et au respect des dispositions prévues aux termes de la règle XI-2/9, sauf dans les cas prévus dans la section 9.8.1.

9.8.1. Si les fonctionnaires dûment autorisés par un Gouvernement contractant ont des raisons sérieuses de penser que le navire ne satisfait pas aux prescriptions du chapitre XI-2 ou de la partie A du présent Code et si le seul moyen de vérifier ou de rectifier la non-conformité est de réviser les prescriptions pertinentes du plan de sûreté du navire, un accès limité aux sections du plan auquel se rapporte la non-conformité peut être accordé à titre exceptionnel mais uniquement avec l'accord du Gouvernement contractant, ou du capitaine, du navire en question. Toutefois, les dispositions du plan qui se rapportent aux sous-sections 2, 4, 5, 7, 15, 17 et 18 de la section 9.4 de la présente partie du Code sont considérées comme étant des renseignements confidentiels et ne peuvent pas faire l'objet d'une inspection sans l'accord du Gouvernement contractant intéressé.

10. Registres

10.1. Des registres des activités ci-après visées dans le plan de sûreté du navire doivent être conservés à bord au moins pendant la période minimale spécifiée par l'Administration, compte tenu des dispositions de la règle XI-2/9.2.3 :

1. formation, exercices et entraînements ;
2. menaces contre la sûreté et incidents de sûreté ;
3. infractions aux mesures de sûreté ;
4. changements de niveau de sûreté ;
5. communications liées directement à la sûreté du navire, notamment en cas de menaces spécifiques à l'encontre du navire ou des installations portuaires où le navire se trouve ou a fait escale auparavant ;
6. audits internes et examens des activités liées à la sûreté ;
7. examen périodique de l'évaluation de la sûreté du navire ;
8. examen périodique du plan de sûreté du navire ;
9. mise en oeuvre des amendements au plan ; et
10. entretien, étalonnage et mise à l'essai de tout matériel de sûreté prévu à bord, y compris mise à l'essai du système d'alerte de sûreté du navire.

10.2. Les registres doivent être tenus dans la ou les langues de travail du navire. Si la ou les langues utilisées ne sont ni l'anglais, ni l'espagnol, ni le français, une traduction dans l'une de ces langues doit être fournie.

10.3. Les registres peuvent être conservés sous forme électronique. Dans ce cas, ils doivent être protégés par des procédures visant à empêcher que leurs données soient effacées, détruites ou modifiées sans autorisation.

10.4. Les registres doivent être protégés contre tout accès ou toute divulgation non autorisés.

11. Agent de sûreté de la compagnie

11.1. La compagnie doit désigner un agent de sûreté de la compagnie. Une personne désignée comme agent de sûreté de la compagnie peut agir pour un ou plusieurs navires, selon le nombre de navires et les types de navires exploités par la compagnie, sous réserve que les navires dont cette personne est responsable soient clairement identifiés. Une compagnie peut, selon le nombre de navires et les types de navires qu'elle exploite, désigner plusieurs agents de sûreté de la compagnie, sous réserve que les navires dont chaque personne est responsable soient clairement identifiés.

11.2. Outre celles qui sont spécifiées dans d'autres sections de la présente partie du Code, les tâches et responsabilités de l'agent de sûreté de la compagnie comprennent, sans toutefois s'y limiter, ce qui suit :

1. formuler des avis sur les degrés de menace auxquels le navire risque d'être confronté, à l'aide d'évaluations appropriées de la sûreté et d'autres renseignements pertinents ;
2. veiller à ce que des évaluations de la sûreté du navire soient effectuées ;
3. veiller à l'élaboration, à la soumission aux fins d'approbation et puis à la mise en oeuvre et au maintien du plan de sûreté du navire ;
4. veiller à ce que le plan de sûreté du navire soit modifié comme il convient pour en rectifier les lacunes et veiller à ce qu'il réponde aux besoins du navire en matière de sûreté ;
5. prendre des dispositions en vue des audits internes et des examens des activités liées à la sûreté ;
6. prendre des dispositions en vue des vérifications initiales et ultérieures du navire par l'Administration ou l'organisme de sûreté reconnu ;
7. veiller à ce que les déficiences et les non-conformités identifiées lors des audits internes, des examens périodiques, des inspections de sûreté et des vérifications de conformité soient rectifiées rapidement ;
8. accroître la prise de conscience de la sûreté et la vigilance ;
9. veiller à ce que le personnel responsable de la sûreté du navire ait reçu une formation adéquate ;
10. veiller à l'efficacité de la communication et de la coopération entre l'agent de sûreté du navire et les agents de sûreté pertinents des installations portuaires ;
11. veiller à ce que les exigences en matière de sûreté et de sécurité concordent ;
12. veiller à ce que, si l'on utilise des plans de sûreté de navires de la même compagnie ou d'une flotte de navires, le plan de chaque navire reflète exactement les renseignements spécifiques à ce navire ; et
13. veiller à ce que tout autre arrangement ou tout arrangement équivalent approuvé pour un navire ou un groupe de navires donné soit mis en oeuvre et maintenu.

12. Agent de sûreté du navire

12.1. Un agent de sûreté du navire doit être désigné à bord de chaque navire.

12.2. Outre celles qui sont spécifiées dans d'autres sections de la présente partie du Code, les tâches et responsabilités de l'agent de sûreté du navire comprennent, sans toutefois s'y limiter, ce qui suit :

1. procéder à des inspections de sûreté régulières du navire pour s'assurer que les mesures de sûreté sont toujours appropriées ;
2. assurer et superviser la mise en oeuvre du plan de sûreté du navire, y compris de tout amendement apporté à ce plan ;
3. coordonner les aspects liés à la sûreté de la manutention des cargaisons et des provisions de bord avec les autres membres du personnel de bord et avec les agents de sûreté pertinents des installations portuaires ;
4. proposer des modifications à apporter au plan de sûreté du navire ;
5. notifier à l'agent de sûreté de la compagnie toutes déficiences et non-conformités identifiées lors des audits internes, des examens périodiques, des inspections de sûreté et des vérifications de conformité et mettre en oeuvre toutes mesures correctives ;
6. accroître la prise de conscience de la sûreté et la vigilance à bord ;
7. veiller à ce que le personnel responsable de la sûreté du navire ait reçu une formation adéquate, selon qu'il convient ;
8. notifier tous les incidents de sûreté ;
9. coordonner la mise en oeuvre du plan de sûreté du navire avec l'agent de sûreté de la compagnie et avec l'agent de sûreté pertinent de l'installation portuaire ; et
10. s'assurer que le matériel de sûreté est correctement utilisé, mis à l'essai, étalonné et entretenu, s'il y en a.

13. Formation, exercices et entraînements en matière de sûreté des navires

13.1. L'agent de sûreté de la compagnie et le personnel compétent à terre doivent avoir des connaissances et avoir reçu une formation, compte tenu des recommandations énoncées dans la partie B du présent Code.

13.2. L'agent de sûreté du navire doit posséder des connaissances et avoir reçu une formation, compte tenu des recommandations énoncées dans la partie B du présent Code.

13.3. Le personnel de bord chargé de tâches et de responsabilités spéciales en matière de sûreté doit comprendre les responsabilités qui lui incombent à cet égard, telles qu'elles sont décrites dans le plan de sûreté du navire, et il doit avoir des connaissances et des aptitudes suffisantes pour s'acquitter des tâches qui lui sont assignées, compte tenu des recommandations énoncées dans la partie B du présent Code.

13.4. Pour garantir l'efficacité de la mise en oeuvre du plan de sûreté du navire, des exercices doivent être effectués à des intervalles appropriés, compte tenu du type de navire, des changements de personnel du navire, des installations portuaires où le navire doit faire escale et d'autres conditions pertinentes, compte tenu des recommandations énoncées dans la partie B du présent Code.

13.5. L'agent de sûreté de la compagnie doit veiller à la coordination et la mise en oeuvre efficaces des plans de sûreté du navire en participant aux exercices à des intervalles appropriés, compte tenu des recommandations énoncées dans la partie B du présent Code.

14. Sûreté de l'installation portuaire

14.1. Une installation portuaire est tenue de prendre des mesures correspondant aux niveaux de sûreté établis par le Gouvernement contractant sur le territoire duquel elle est située. Les mesures et procédures de sûreté doivent être appliquées dans l'installation portuaire de manière à entraîner le minimum de perturbations ou de retards pour les passagers, le navire, le personnel du navire et les visiteurs, les marchandises et les services.

14.2. Au niveau de sûreté 1, les activités suivantes doivent être exécutées par le biais de mesures appropriées dans toutes les installations portuaires, compte tenu des recommandations énoncées dans la partie B du présent Code, en vue d'identifier et de prendre des mesures de sauvegarde contre les incidents de sûreté :

1. veiller à l'exécution de toutes les tâches liées à la sûreté de l'installation portuaire ;
2. contrôler l'accès à l'installation portuaire ;
3. surveiller l'installation portuaire, y compris la ou les zones de mouillage et d'amarrage ;
4. surveiller les zones d'accès restreint pour vérifier que seules les personnes autorisées y ont accès ;
5. superviser la manutention de la cargaison ;
6. superviser la manutention des provisions de bord ; et
7. veiller à ce que le système de communication de sûreté soit rapidement disponible.

14.3. Au niveau de sûreté 2, les mesures de protection additionnelles spécifiées dans le plan de sûreté de l'installation portuaire doivent être mises en oeuvre pour chacune des activités décrites dans la section 14.2, compte tenu des recommandations énoncées dans la partie B du présent Code.

14.4. Au niveau de sûreté 3, les autres mesures spéciales de protection spécifiées dans le plan de sûreté de l'installation portuaire doivent être mises en oeuvre pour chacune des activités décrites dans la section 14.2, compte tenu des recommandations énoncées dans la partie B du présent Code.

14.4.1. En outre, au niveau de sûreté 3, les installations portuaires sont tenues de suivre et d'exécuter toutes consignes de sûreté spécifiées par le Gouvernement contractant sur le territoire duquel l'installation portuaire est située.

14.5. Lorsqu'un agent de sûreté de l'installation portuaire est informé qu'un navire a des difficultés à satisfaire aux prescriptions du chapitre XI-2 ou de la présente partie du Code ou à mettre en oeuvre les mesures et procédures appropriées décrites dans le plan de sûreté du navire, et dans le cas du niveau de sûreté 3, à la suite de toutes consignes de sûreté données par le Gouvernement contractant sur le territoire duquel l'installation portuaire est située, l'agent de sûreté de l'installation portuaire et l'agent de sûreté du navire doivent rester en liaison et doivent coordonner les mesures appropriées.

14.6. Lorsqu'un agent de sûreté de l'installation portuaire est informé qu'un navire applique un niveau de sûreté supérieur à celui de l'installation portuaire, cet agent le notifie à l'autorité compétente, se met en rapport avec l'agent de sûreté du navire et coordonne les mesures appropriées, si nécessaire.

15. Evaluation de la sûreté de l'installation portuaire

15.1. L'évaluation de la sûreté de l'installation portuaire est un élément essentiel qui fait partie intégrante du processus d'établissement et de mise à jour du plan de sûreté de l'installation portuaire.

15.2. L'évaluation de la sûreté de l'installation portuaire doit être effectuée par le Gouvernement contractant sur le territoire duquel l'installation portuaire est située. Un Gouvernement contractant peut autoriser un organisme de sûreté reconnu à effectuer l'évaluation de la sûreté de l'installation portuaire d'une installation portuaire particulière située sur son territoire.

15.2.1. Si une évaluation de la sûreté de l'installation portuaire a été effectuée par un organisme de sûreté reconnu, le Gouvernement contractant sur le territoire duquel l'installation portuaire est située doit passer en revue cette évaluation et l'approuver pour confirmer qu'elle satisfait à la présente section.

15.3. Les personnes qui effectuent l'évaluation doivent avoir les qualifications nécessaires pour procéder à une estimation de la sûreté de l'installation portuaire conformément à la présente section, compte tenu des recommandations énoncées dans la partie B du présent Code.

15.4. Les évaluations de la sûreté de l'installation portuaire doivent être périodiquement revues et mises à jour, compte tenu des fluctuations de la menace et/ou des changements mineurs affectant l'installation portuaire et doivent toujours être passées en revue et mises à jour lorsque des changements importants sont apportés à l'installation portuaire.

15.5. L'évaluation de la sûreté de l'installation portuaire doit comprendre, au moins les éléments suivants :

1. identification et évaluation des infrastructures et biens essentiels qu'il est important de protéger ;
2. identification des menaces éventuelles contre les biens et les infrastructures et de leur probabilité de survenance, afin d'établir des mesures de sûreté qui s'imposent, en les classant par ordre de priorité ;
3. identification, choix et classement par ordre de priorité des contre-mesures et des changements de procédure ainsi que de leur degré d'efficacité pour réduire la vulnérabilité ; et
4. identification des points faibles, y compris les facteurs humains, de l'infrastructure, des politiques et des procédures.

15.6. Les Gouvernements contractants peuvent accepter qu'une évaluation de la sûreté de l'installation portuaire couvre plusieurs installations portuaires à condition que l'exploitant, l'emplacement, l'exploitation, le matériel et la conception de ces installations portuaires soient similaires. Tout Gouvernement contractant qui autorise un arrangement de ce type doit en communiquer les détails à l'Organisation.

15.7. Lorsque l'évaluation de la sûreté de l'installation portuaire est achevée, il faut établir un rapport qui comprenne un résumé de la manière dont l'évaluation s'est déroulée, une description de chaque point vulnérable identifié au cours de l'évaluation et une description des contre-mesures permettant de remédier à chaque point vulnérable. Ce rapport doit être protégé contre tout accès ou toute divulgation non autorisés.

16. Plan de sûreté de l'installation portuaire

16.1. Un plan de sûreté de l'installation portuaire doit être élaboré et tenu à jour, sur la base d'une évaluation de la sûreté de l'installation portuaire, pour chaque installation portuaire et doit être adapté à l'interface navire/port. Ce plan doit prévoir des dispositions pour les trois niveaux de sûreté qui sont définis dans la présente partie du Code.

16.1.1. Sous réserve des dispositions de la section 16.2, un organisme de sûreté reconnu peut préparer le plan de sûreté de l'installation portuaire d'une installation portuaire particulière.

16.2. Le plan de sûreté de l'installation portuaire doit être approuvé par le Gouvernement contractant sur le territoire duquel l'installation portuaire est située.

16.3. Ce plan doit être élaboré compte tenu des recommandations énoncées dans la partie B du Code et être rédigé dans la langue de travail de l'installation portuaire. Le plan doit comprendre au moins :

1. les mesures visant à empêcher l'introduction, dans l'installation portuaire ou à bord du navire, d'armes, de substances dangereuses et d'engins destinés à être utilisés contre des personnes, des navires ou des ports et dont la présence n'est pas autorisée ;
2. les mesures destinées à empêcher l'accès non autorisé à l'installation portuaire, aux navires amarrés dans l'installation portuaire et aux zones d'accès restreint de l'installation ;
3. des procédures pour faire face à une menace contre la sûreté ou une atteinte à la sûreté, y compris des dispositions pour maintenir les opérations essentielles de l'installation portuaire ou de l'interface navire/port ;
4. des procédures pour donner suite aux consignes de sûreté que le Gouvernement contractant sur le territoire duquel l'installation portuaire est située pourrait donner au niveau de sûreté 3 ;
5. des procédures d'évacuation en cas de menace contre la sûreté ou d'atteinte à la sûreté ;
6. les tâches du personnel de l'installation auquel sont attribuées des responsabilités en matière de sûreté et celles des autres membres du personnel de l'installation portuaire concernant les aspects liés à la sûreté ;
7. des procédures concernant l'interface avec les activités liées à la sûreté des navires ;
8. des procédures concernant l'examen périodique du plan et sa mise à jour ;
9. des procédures de notification des incidents de sûreté ;
10. l'identification de l'agent de sûreté de l'installation portuaire, y compris les coordonnées où il peut être joint 24 heures sur 24 ;
11. des mesures visant à garantir la protection des renseignements figurant dans le plan ;
12. des mesures destinées à garantir la protection effective de la cargaison et du matériel de manutention de la cargaison dans l'installation portuaire ;
13. des procédures d'audit du plan de sûreté de l'installation portuaire ;
14. des procédures pour donner suite à une alerte dans le cas où le système d'alerte de sûreté d'un navire se trouvant dans l'installation portuaire a été activé ; et
15. des procédures pour faciliter les congés à terre pour le personnel du navire ou les changements de personnel, de même que l'accès des visiteurs au navire, y compris les représentants des services sociaux et des syndicats des gens de mer.

16.4. Le personnel qui procède aux audits internes des activités liées à la sûreté spécifiées dans le plan ou qui évalue sa mise en oeuvre ne doit pas avoir de rapport avec les activités faisant l'objet de l'audit, à moins que cela ne soit pas possible dans la pratique du fait de la taille et de la nature de l'installation portuaire.

16.5. Le plan de sûreté de l'installation portuaire peut être combiné avec le plan de sûreté du port ou tout autre plan d'urgence portuaire ou faire partie de tels plans.

16.6. Le Gouvernement contractant sur le territoire duquel l'installation portuaire est située doit décider quelles sont les modifications qui ne doivent pas être apportées au plan de sûreté de l'installation portuaire sans que les amendements pertinents à ce plan soient approuvés par lui.

16.7. Le plan peut être conservé sous forme électronique. Dans ce cas, il doit être protégé par des procédures visant à empêcher que ses données soient effacées, détruites ou modifiées sans autorisation.

16.8. Le plan doit être protégé contre tout accès ou toute divulgation non autorisés.

16.9. Les Gouvernements contractants peuvent accepter qu'un plan de sûreté de l'installation portuaire couvre plusieurs installations portuaires à condition que l'exploitant, l'emplacement, l'exploitation, le matériel et la conception de ces installations portuaires soient similaires. Tout Gouvernement contractant qui autorise un autre arrangement de ce type doit en communiquer détails à l'Organisation.

17. Agent de sûreté de l'installation portuaire

17.1. Un agent de sûreté de l'installation portuaire doit être désigné dans chaque installation portuaire. Une personne peut être désignée comme agent de sûreté d'une ou de plusieurs installations portuaires.

17.2. Outre celles qui sont spécifiées dans d'autres sections de la présente partie du Code, les tâches et responsabilités de l'agent de sûreté de l'installation portuaire comprennent, sans toutefois s'y limiter, ce qui suit :

1. effectuer une étude de sûreté initiale complète de l'installation portuaire en tenant compte de l'évaluation pertinente de la sûreté de l'installation portuaire ;
2. veiller à l'élaboration et à la mise à jour du plan de sûreté de l'installation portuaire ;
3. mettre en oeuvre le plan de sûreté de l'installation portuaire et procéder à des exercices à cet effet ;
4. procéder à des inspections de sûreté régulières de l'installation portuaire pour s'assurer que les mesures de sûreté restent appropriées ;
5. recommander et incorporer les modifications nécessaires au plan de sûreté de l'installation portuaire pour en rectifier les lacunes et mettre à jour le plan pour tenir compte des changements pertinents affectant l'installation portuaire ;
6. accroître la prise de conscience de la sûreté et la vigilance du personnel de l'installation portuaire ;
7. veiller à ce que le personnel responsable de la sûreté de l'installation portuaire ait reçu une formation adéquate ;
8. faire rapport aux autorités compétentes et tenir un registre des événements qui menacent la sûreté de l'installation portuaire ;
9. coordonner la mise en oeuvre du plan de sûreté de l'installation portuaire avec le ou les agent(s) de sûreté compétent(s) de la compagnie et du navire ;
10. assurer la coordination avec les services de sûreté, s'il y a lieu ;
11. s'assurer que les normes applicables au personnel chargé de la sûreté de l'installation portuaire sont respectées ;
12. s'assurer que le matériel de sûreté est correctement utilisé, mis à l'essai, étalonné et entretenu, s'il y en a ; et
13. aider l'agent de sûreté du navire à confirmer, sur demande, l'identité des personnes cherchant à monter à bord du navire.

17.3. L'agent de sûreté de l'installation portuaire doit bénéficier de l'appui nécessaire pour s'acquitter des tâches et des responsabilités qui lui sont imposées par le chapitre XI-2 et par la présente partie du Code.

18. Formation, exercices et entraînements en matière de sûreté des installations portuaires

18.1. L'agent de sûreté de l'installation portuaire et le personnel compétent chargé de la sûreté de l'installation portuaire doivent avoir des connaissances et avoir reçu une formation, compte tenu des recommandations énoncées dans la partie B du présent Code.

18.2. Le personnel des installations portuaires chargé de tâches spécifiques liées à la sûreté doit comprendre les tâches et les responsabilités qui lui incombent à cet égard, telles qu'elles sont décrites dans le plan de sûreté de l'installation portuaire, et il doit avoir des connaissances et des aptitudes suffisantes pour s'acquitter des tâches qui lui sont assignées, compte tenu des recommandations énoncées dans la partie B du présent Code.

18.3. Pour garantir l'efficacité de la mise en oeuvre du plan de sûreté de l'installation portuaire, des exercices doivent être effectués à des intervalles appropriés compte tenu des types d'opérations effectuées par l'installation portuaire, des changements dans la composition du personnel de l'installation portuaire, du type de navires que dessert l'installation portuaire et autres circonstances pertinentes, compte tenu des recommandations énoncées dans la partie B du présent Code.

18.4. L'agent de sûreté de l'installation portuaire doit garantir l'efficacité de la coordination et de la mise en oeuvre du plan de sûreté de l'installation portuaire en participant à des entraînements à des intervalles appropriés, compte tenu des recommandations énoncées dans la partie B du présent Code.

19. Vérification des navires et délivrance des certificats

19.1. Vérifications :

19.1.1. Chaque navire auquel s'applique la présente partie du Code doit être soumis aux vérifications spécifiées ci-dessous :

1. une vérification initiale, avant la mise en service du navire ou avant que le certificat prescrit à la section 19.2 soit délivré pour la première fois, qui comprenne une vérification complète de

son système de sûreté et de tout matériel de sûreté connexe visés par les dispositions pertinentes du chapitre XI-2, de la présente partie du Code et du plan de sûreté du navire approuvé. Cette vérification doit permettre de s'assurer que le système de sûreté et tout matériel de sûreté connexe du navire satisfont pleinement aux prescriptions applicables du chapitre XI-2 et de la présente partie du Code, que leur état est satisfaisant et qu'ils sont adaptés au service auquel le navire est destiné ;

2. une vérification de renouvellement à des intervalles spécifiés par l'Administration mais ne dépassant pas cinq ans, sauf si la section 19.3 s'applique. Cette vérification doit permettre de s'assurer que le système de sûreté et tout matériel de sûreté connexe du navire satisfont pleinement aux prescriptions applicables du chapitre XI-2 de la présente partie du Code et du plan de sûreté du navire approuvé, que leur état est satisfaisant et qu'ils sont adaptés au service auquel le navire est destiné ;

3. au moins une vérification intermédiaire. Si une seule vérification intermédiaire est effectuée, elle doit avoir lieu entre la deuxième et la troisième date anniversaire du certificat telle que définie à la règle I/2 n). La vérification intermédiaire doit comprendre une inspection du système de sûreté et de tout matériel de sûreté connexe du navire, afin de s'assurer qu'ils restent satisfaisants pour le service auquel le navire est destiné. Mention de cette vérification intermédiaire doit être portée sur le certificat ;

4. toute vérification supplémentaire décidée par l'Administration.

19.1.2. Les vérifications des navires doivent être effectuées par les fonctionnaires de l'Administration. L'Administration peut toutefois confier les vérifications à un organisme de sûreté reconnu visé à la règle XI-2/1.

19.1.3. Dans tous les cas, l'Administration intéressée doit se porter pleinement garante de l'exécution complète et de l'efficacité de la vérification et doit s'engager à prendre les mesures nécessaires pour satisfaire à cette obligation.

19.1.4. Le système de sûreté et tout matériel de sûreté connexe du navire doivent être entretenus, après la vérification, de manière à rester conformes aux dispositions des règles XI-2/4.2 et XI-2/6, de la présente partie du Code et du plan de sûreté du navire approuvé. Lorsqu'une des vérifications prescrites aux termes de la section 19.1.1 a été effectuée, aucun changement ne doit être apporté au système de sûreté ou à un quelconque matériel de sûreté connexe ni au plan de sûreté du navire approuvé sans l'accord de l'Administration.

19.2. Délivrance du certificat ou apposition d'un visa :

19.2.1. Un Certificat international de sûreté du navire doit être délivré, après une visite initiale ou une vérification de renouvellement effectuée conformément aux dispositions de la section 19.1.

19.2.2. Ce certificat doit être délivré ou visé soit par l'Administration, soit par un organisme de sûreté reconnu agissant pour le compte de l'Administration.

19.2.3. Un Gouvernement contractant peut, à la demande de l'Administration, faire vérifier le navire. S'il est convaincu que les dispositions de la section 19.1.1 sont respectées, il doit délivrer au navire un Certificat international de sûreté du navire ou autoriser sa délivrance et, le cas échéant, apposer un visa ou autoriser son apposition sur le certificat du navire, conformément au présent Code.

19.2.3.1. Une copie du certificat et une copie du rapport de vérification doivent être communiquées dans les meilleurs délais à l'Administration qui a fait la demande.

19.2.3.2. Tout certificat ainsi délivré doit comporter une déclaration établissant qu'il a été délivré à la demande de l'Administration. Il doit avoir la même valeur et être accepté dans les mêmes conditions qu'un certificat délivré en vertu de la section 19.2.2.

19.2.4. Le Certificat international de sûreté du navire doit être établi selon le modèle qui figure en appendice au présent Code. Si la langue utilisée n'est ni l'anglais, ni l'espagnol, ni le français, le texte doit comprendre une traduction dans l'une de ces langues.

19.3. Durée et validité du certificat :

19.3.1. Le Certificat international de sûreté du navire doit être délivré pour une période dont la durée est fixée par l'Administration, sans que cette durée puisse excéder cinq ans.

19.3.2. Lorsque la vérification de renouvellement est achevée dans un délai de trois mois avant la date d'expiration du certificat existant, le nouveau certificat est valable à compter de la date d'achèvement de la vérification de renouvellement jusqu'à une date qui n'est pas postérieure de plus de cinq ans à la date d'expiration du certificat existant.

19.3.2.1. Lorsque la vérification de renouvellement est achevée après la date d'expiration du certificat existant, le nouveau certificat est valable à compter de la date d'achèvement de la vérification de renouvellement jusqu'à une date qui n'est pas postérieure de plus de cinq ans à la date d'expiration du certificat existant.

19.3.2.2. Lorsque la vérification de renouvellement est achevée plus de trois mois avant la date d'expiration du certificat existant, le nouveau certificat est valable à compter de la date d'achèvement de la vérification de renouvellement jusqu'à une date qui n'est pas postérieure de plus de cinq ans à la date d'achèvement de la vérification de renouvellement.

19.3.3. Si un certificat est délivré pour une durée inférieure à cinq ans, l'Administration peut en proroger la validité au-delà de la date d'expiration, jusqu'à concurrence de la période maximale indiquée dans la section 19.3.1, à condition que les vérifications mentionnées dans la section 19.1.1, qui sont applicables lorsqu'un certificat est délivré pour cinq ans, soient effectuées selon qu'il convient.

19.3.4. Si, après l'achèvement d'une vérification de renouvellement, un nouveau certificat ne peut pas être délivré ou fourni au navire avant la date d'expiration du certificat existant, l'Administration ou l'organisme de sûreté reconnu agissant pour le compte de l'Administration peut apposer un visa sur le certificat existant et ce certificat doit être accepté comme valable pour une nouvelle période, qui ne peut excéder cinq mois à compter de la date d'expiration.

19.3.5. Si, à la date d'expiration de son certificat, le navire ne se trouve pas dans un port dans lequel il peut subir une vérification, l'Administration peut proroger la validité de ce certificat. Toutefois, une telle prorogation ne doit être accordée que pour permettre au navire d'achever son voyage vers le port dans lequel il doit être vérifié et ce, uniquement dans le cas où cette mesure semble opportune et raisonnable. Aucun certificat ne doit être ainsi prorogé pour une période de plus de trois mois et un navire auquel cette prorogation a été accordée n'a pas le droit, en vertu de cette prorogation, après son arrivée dans le port dans lequel il doit être vérifié, d'en repartir sans en avoir obtenu un nouveau certificat. Lorsque la vérification de renouvellement est achevée, le nouveau certificat est valable jusqu'à une date qui n'est pas postérieure de plus de cinq ans à la date d'expiration du certificat existant avant que la prorogation ait été accordée.

19.3.6. Un certificat délivré à un navire effectuant des voyages courts qui n'a pas été prorogé en vertu des dispositions précédentes de la présente section peut être prorogé par l'Administration pour une période de grâce ne dépassant pas d'un mois la date d'expiration indiquée sur ce certificat. Lorsque la vérification de renouvellement est achevée, le nouveau certificat est valable jusqu'à une date qui n'est pas postérieure de plus de cinq ans à la date d'expiration du certificat existant avant que la prorogation ait été accordée.

19.3.7. Lorsqu'une vérification intermédiaire est achevée dans un délai inférieur à celui qui est spécifié dans la section 19.1.1 :

1. la date d'expiration figurant sur le certificat est remplacée au moyen d'un visa par une date qui ne doit pas être postérieure de plus de trois ans à la date à laquelle la vérification intermédiaire a été achevée ;
2. la date d'expiration peut rester inchangée, à condition qu'une ou plusieurs vérifications supplémentaires soient effectuées de telle sorte que les intervalles maximaux entre les vérifications prescrites aux termes de la section 19.1.1 ne soient pas dépassés.

19.3.8. Un certificat délivré en vertu de la section 19.2 cesse d'être valable dans l'un quelconque des cas suivants :

1. si les vérifications pertinentes ne sont pas achevées dans les délais spécifiés dans la section 19.1.1 ;
2. si les visas prescrits aux termes des sections 19.1.1.3 et 19.3.7.1, si elles s'appliquent, n'ont pas été apposés sur le certificat ;
3. lorsqu'une compagnie assume la responsabilité de l'exploitation d'un navire qui n'était pas exploité précédemment par cette compagnie ; et
4. si le navire passe sous le pavillon d'un autre Etat.

19.3.9. Dans les cas où :

1. un navire passe sous le pavillon d'un autre Gouvernement contractant, le Gouvernement contractant dont le navire était autorisé précédemment à battre le pavillon, doit, dès que possible, adresser à l'Administration cessionnaire des copies du Certificat international de sûreté du navire ou tous les renseignements relatifs au Certificat international de sûreté du navire dont le navire était pourvu avant le transfert, ainsi que des copies des rapports de vérification disponibles, ou
2. une compagnie assume la responsabilité de l'exploitation d'un navire qui n'était pas exploité auparavant par elle, la compagnie antérieure doit, dès que possible, adresser à la nouvelle compagnie exploitante des copies de tout renseignement concernant le Certificat international de sûreté du navire ou faciliter les vérifications décrites dans la section 19.4.2.

19.4. Délivrance d'un certificat provisoire :

19.4.1. Les certificats décrits dans la section 19.2 ne doivent être délivrés que si l'Administration qui délivre le certificat est pleinement convaincue que le navire satisfait aux prescriptions de la section 19.1. Toutefois, après le 1er juillet 2004, pour :

1. un navire sans certificat ou un navire à sa livraison ou avant sa mise ou sa remise en service ;
2. un navire battant le pavillon d'un Gouvernement contractant qui passe sous le pavillon d'un autre Gouvernement contractant ;
3. un navire battant le pavillon d'un Etat qui n'est pas un Gouvernement contractant qui passe sous le pavillon d'un Gouvernement contractant, ou
4. une compagnie qui assume la responsabilité de l'exploitation d'un navire qui n'était pas exploité auparavant par elle, jusqu'à ce que le certificat visé à la section 19.2 soit délivré, l'Administration peut faire délivrer un Certificat international provisoire de sûreté du navire établi sur le modèle figurant en appendice à la présente partie du Code.

19.4.2. Un Certificat international provisoire de sûreté du navire ne doit être délivré que si l'Administration ou l'organisme de sûreté reconnu, au nom de l'Administration, a vérifié que :

1. l'évaluation de la sûreté du navire prescrite par la présente partie du Code a été effectuée ;
2. une copie du plan de sûreté du navire satisfaisant aux prescriptions du chapitre XI-2 et de la présente partie du Code se trouve à bord du navire, le plan ayant été soumis pour examen et approbation et étant appliqué à bord du navire ;
3. le navire est doté d'un système d'alerte de sûreté du navire qui satisfait aux prescriptions de la règle XI-2/6, si un tel système est exigé ;
4. l'agent de sûreté de la compagnie :

1. s'est assuré :

1. que le plan de sûreté du navire a été examiné pour vérifier qu'il satisfait à la présente partie du Code ;
2. que le plan a été soumis aux fins d'approbation ; et
3. que le plan est appliqué à bord du navire ; et

2. a mis en place les arrangements nécessaires, y compris en ce qui concerne les exercices, les entraînements et les vérifications internes, moyennant lesquels il estime que le navire subira avec succès la vérification prescrite conformément à la section 19.1.1.1 dans un délai de six mois ;

5. des dispositions ont été prises pour procéder aux vérifications requises aux termes de la section 19.1.1.1 ;

6. le capitaine, l'agent de sûreté du navire et autre personnel de bord responsables de tâches spécifiques liées à la sûreté sont familiarisés avec leurs tâches et responsabilités telles que spécifiées dans la présente partie du Code ; et avec les dispositions pertinentes du plan de sûreté du navire qui se trouve à bord, ces renseignements ayant été fournis dans la langue de travail du personnel du navire ou dans une langue qu'il comprend ; et

7. l'agent de sûreté du navire satisfait aux prescriptions de la présente partie du Code.

19.4.3. Un Certificat international provisoire de sûreté du navire peut être délivré par l'Administration ou par un organisme de sûreté reconnu autorisé à agir en son nom.

19.4.4. Un Certificat international provisoire de sûreté du navire est valable pour une période de six mois, ou jusqu'à la date de délivrance du certificat prescrit aux termes de la section 19.2, si cette date est antérieure, et il ne peut pas être prorogé.

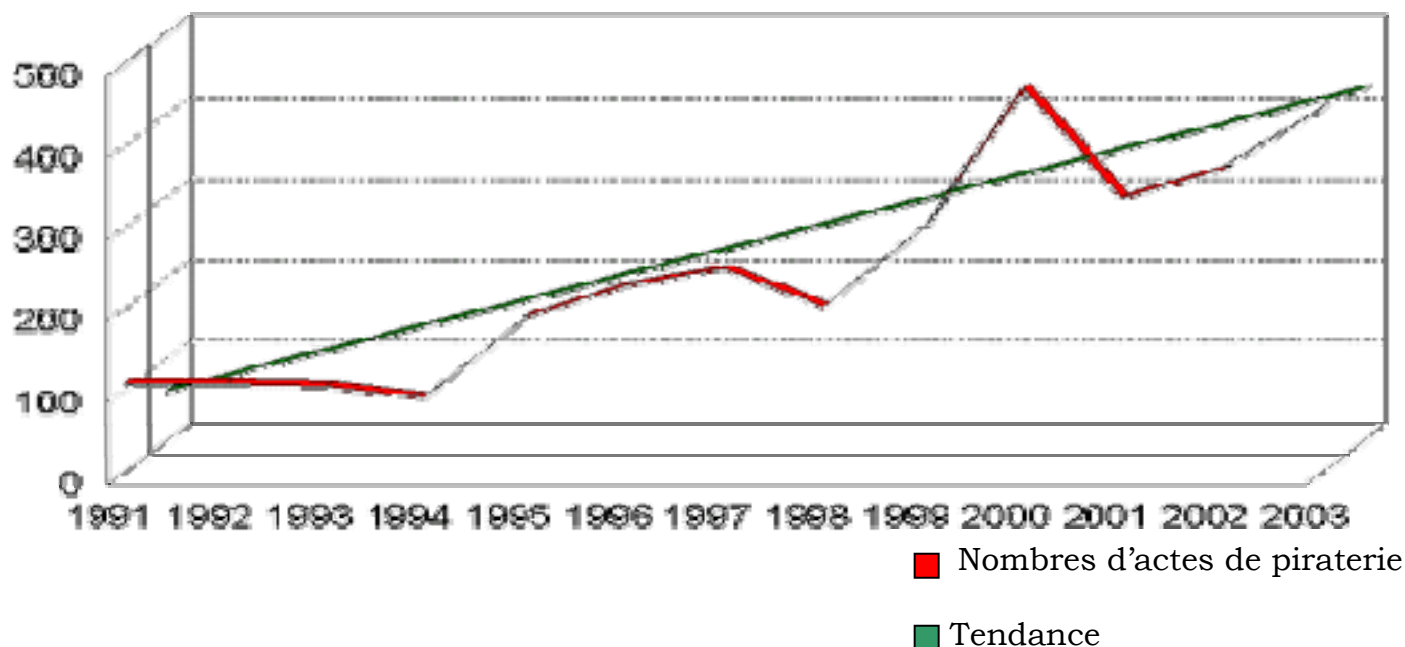
19.4.5. Aucun Gouvernement contractant ne doit accepter qu'un autre certificat international provisoire de sûreté du navire soit délivré par la suite à un navire si, de l'opinion de l'Administration ou de l'organisme de sûreté reconnu, l'une des raisons pour lesquelles le navire ou la compagnie sollicite un tel certificat est de se soustraire à l'obligation de satisfaire pleinement au chapitre XI-2 et à la présente partie du Code au-delà de la période de validité du Certificat provisoire initial décrit dans la section 19.4.4.

19.4.6. Aux fins de l'application de la règle XI-2/9, les Gouvernements contractants peuvent, avant d'accepter un Certificat international provisoire de sûreté du navire en tant que certificat valable, s'assurer que les conditions prescrites aux termes des sections 19.4.2.4 à 19.4.2.6 ont été remplies.

Annexe II³¹⁶

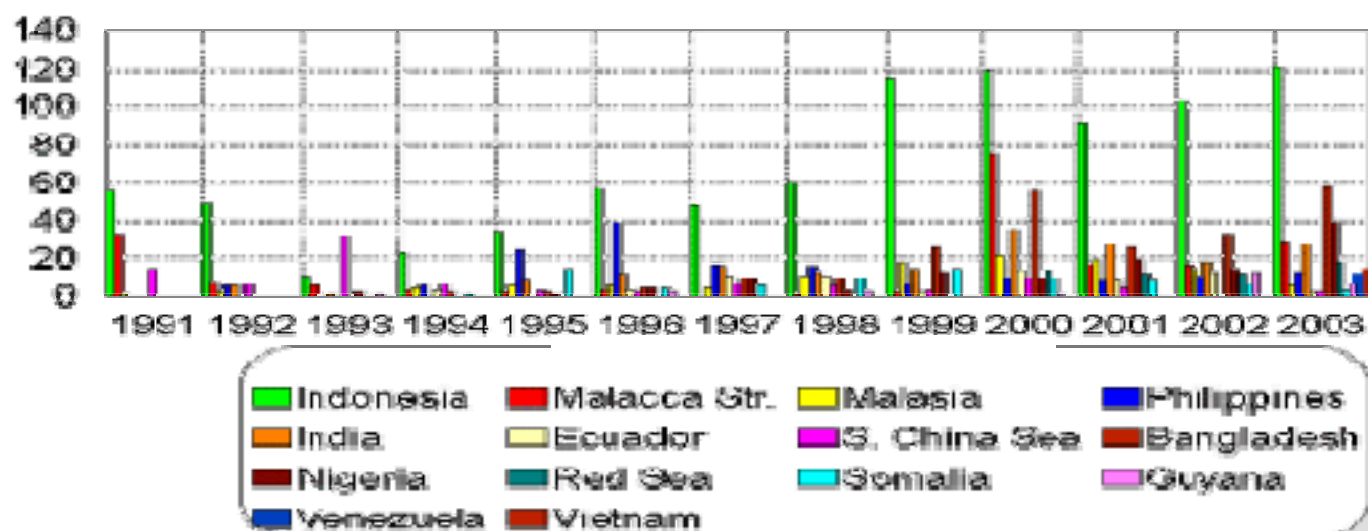
Statistiques sur les actes de violence en mer

Nombre d'actes de piraterie



<http://www.secure-marine.com/statistics/attack.htm>

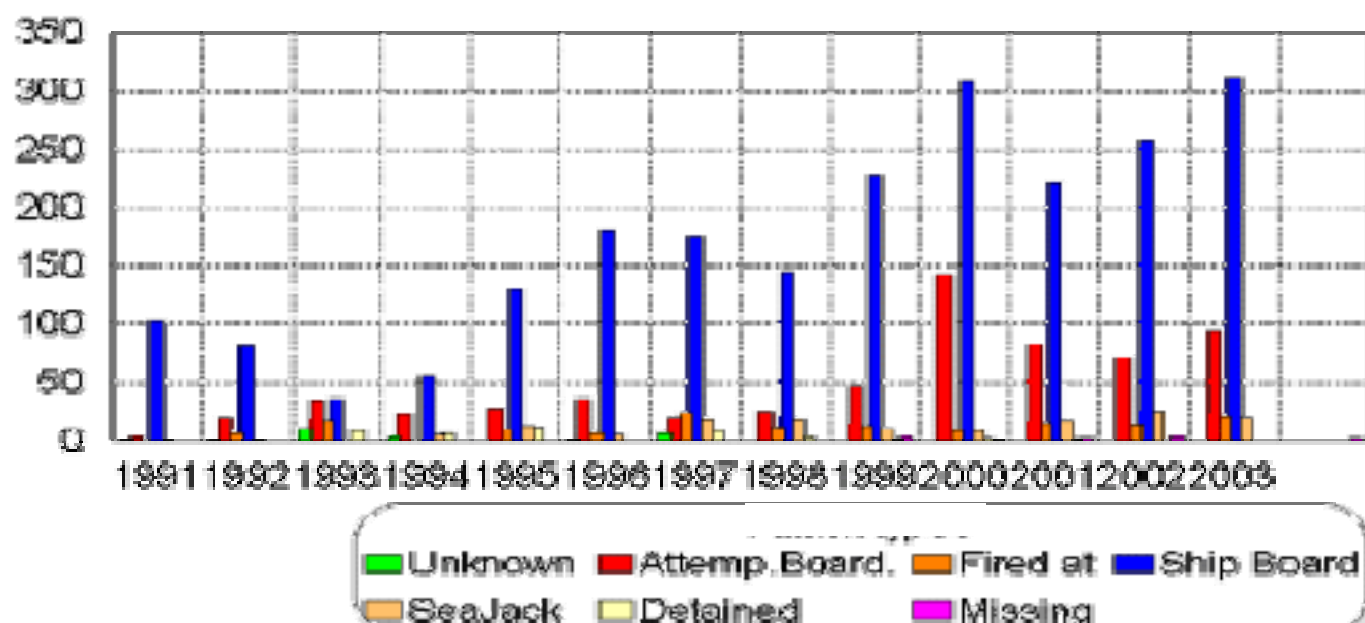
Pays dénombrant plus de 10 attaques par an



<http://www.secure-marine.com/statistics/countries.htm>

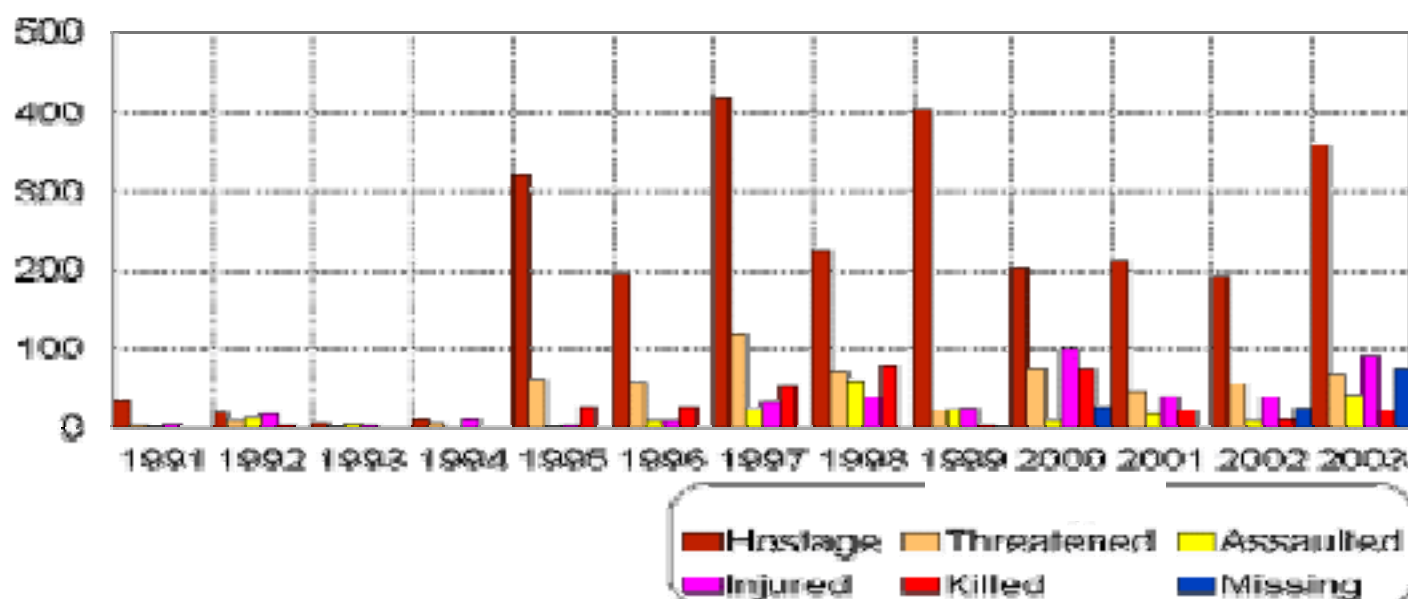
³¹⁶ Les informations sont essentiellement issues des rapports du BMI et disponibles sur le site de Secure Marine, un consultant néerlandais en sûreté maritime, recommandé sur le site du BMI : <http://www.secure-marine.com/history.htm>.

Types d'attaques perpétrées contre les navires



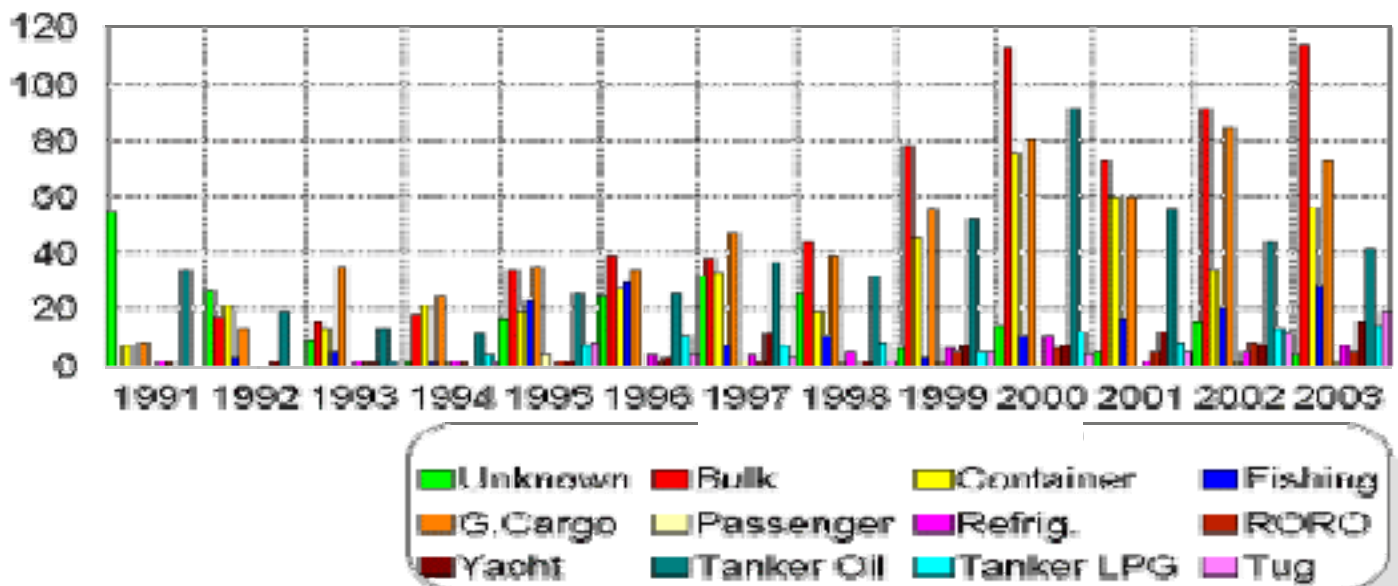
http://www.secure-marine.com/statistics/attack_types.htm

Types d'attaques perpétrées contre les équipages



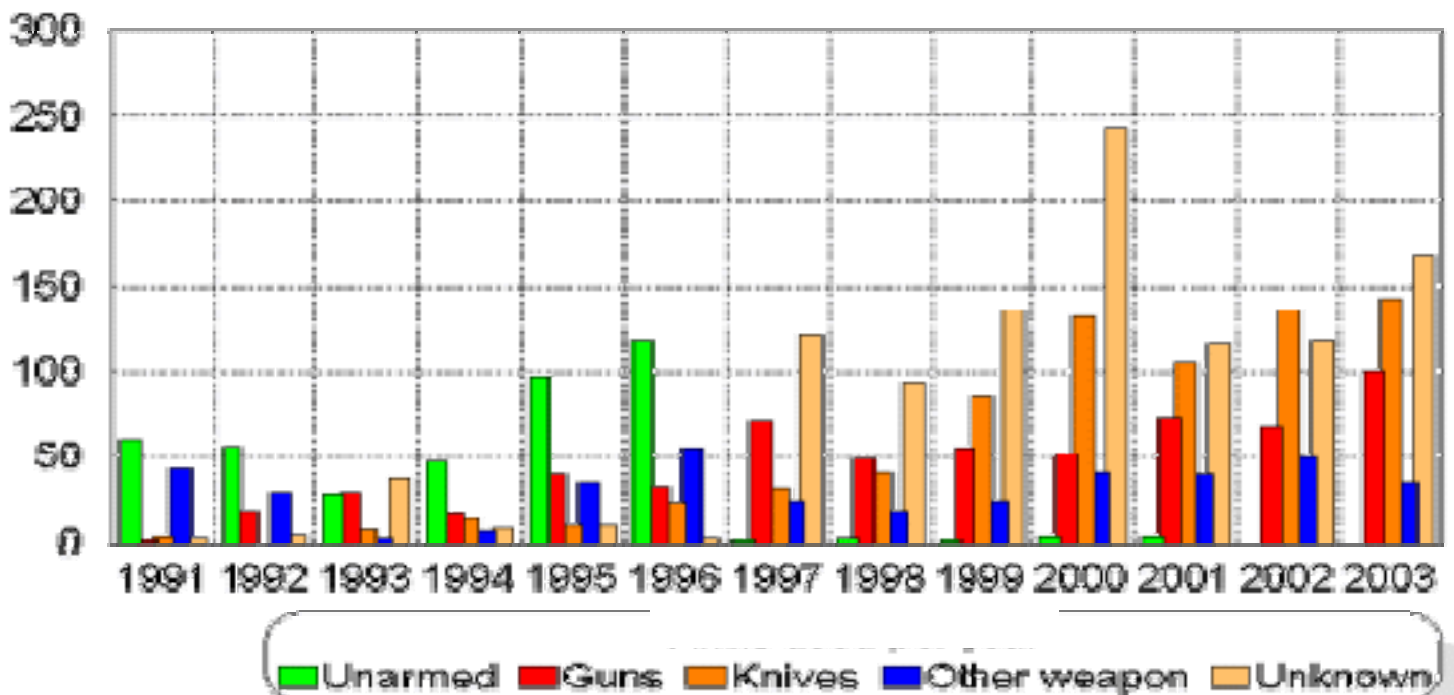
http://www.secure-marine.com/statistics/attack_crew.htm

Type de navires attaqués



<http://www.secure-marine.com/statistics/ships.htm>

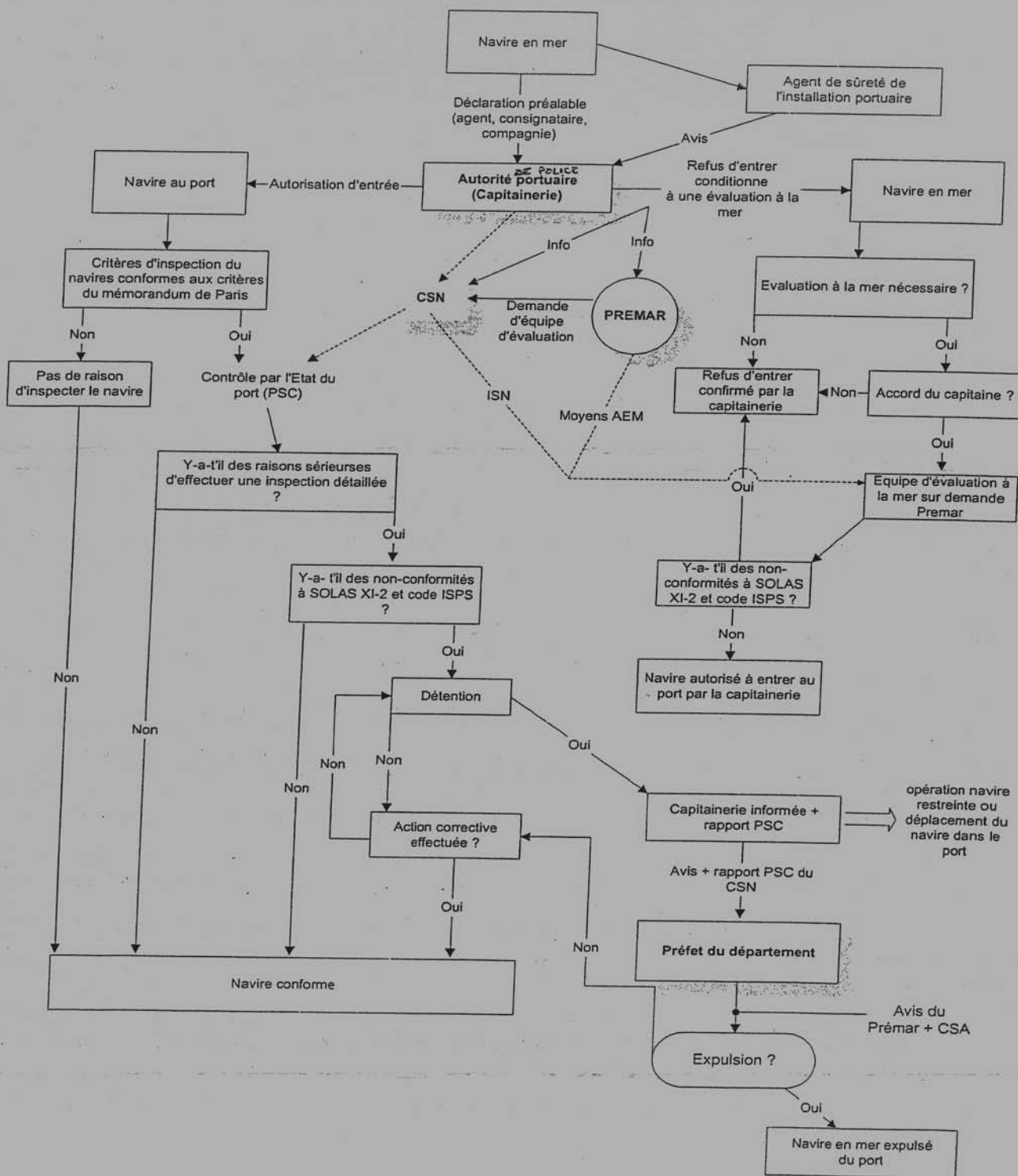
Type d'armes utilisées



http://www.secure-marine.com/statistics/arms_used.htm

Annexe III

Les autorités impliquées dans le contrôle du navire au port



Annexe IV

Les équipements de sûreté

1. LE SCANNER DU PAM³¹⁷



2. COUPEE SECURISEE³¹⁸



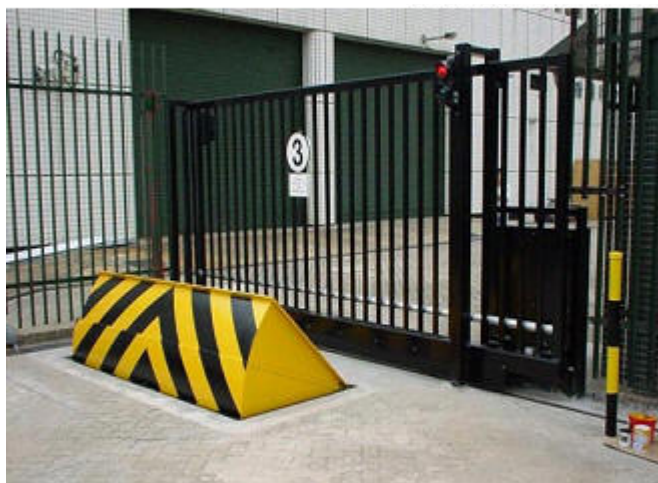
³¹⁷ Photo fournie par Laurent Bauer (PAM).

³¹⁸ Les équipements suivants viennent du site de Secopex :
<http://www.isps.fr/ISPS-materiel-equipement-securite-protection.htm>.

3. BARRAGE ELECTRIQUE



4. DISPOSITIF ANTI BELIER



Annexe V

Les taux de conformité internationaux au Code ISPS

Taux de conformité au Code ISPS à 09h00 le **30 juin 2004**

NAVIRES		
Gouvernements (46 réponses)		
Nombre de navires astreints au Code	22539	
Plans de sûreté des navires (PSN) soumis	19377	
Certificats international de sûreté des navires (CISN) émis	11996	53.2% (contre 41.3% le 25 juin)
IACS		
Nombre de navires astreints au Code		
Plans de sûreté des navires (PSN) soumis	16784	
Certificats international de sûreté des navires (CISN) émis	13005 11639	69.3% (contre 60.8% le 25 juin)
INTERCARGO		
Nombre de navires astreints au Code		
Plans de sûreté des navires (PSN) soumis	916	
Certificats international de sûreté des navires (CISN) émis	769 513	56% (même % depuis le 11 juin)
INTERTANKO		
Nombre de navires astreints au Code		
Plans de sûreté des navires (PSN) soumis	2175	
Certificats international de sûreté des navires (CISN) émis	2175 1547	71% (contre 56% le 25 juin)
IPTA		
Nombre de navires astreints au Code		
Plans de sûreté des navires (PSN) soumis	429	
Certificats international de sûreté des navires (CISN) émis	425 425	99.0% (contre 71.1% le 25 juin)
ICCL		
Nombre de navires astreints au Code		
Plans de sûreté des navires (PSN) soumis	118	
Certificats international de sûreté des navires (CISN) émis	118 118	100.0% (contre 88.9% le 25 juin)
BIMCO		
Nombre de navires astreints au Code		
Plans de sûreté des navires (PSN) soumis	2622	
Certificats international de sûreté des navires (CISN) émis	2189 488	18.6% (même % depuis le 11 juin)
INSTALLATIONS PORTUAIRES		
Gouvernements (86 réponses)		
Nombre d'installations portuaires	7974	
Plan de sûreté de l'installation portuaire (PSIP) soumis	4688	
PSIP approuvés	4260	53.4% (contre 31.9% le 25 juin)

Tableau comparatif des résumés généraux³¹⁹

(au 1^{er} septembre 2004 et au 29 novembre 2004)

	au	
Renseignements généraux	01/09/2004	29/11/2004
Nombre d'Etats qui sont des gouvernements contractants	153	153
Nombre de gouvernements contractants qui n'ont pas de littoral	13	13
Etats pour lesquels la Convention entre en vigueur après le 1 ^{er} juillet 2004	6	6
Etats pour lesquels la Convention n'est pas encore entrée en vigueur	5	0
Nombre d'Etats contractants qui ont notifié un point de contact national unique	129	134
en % du nombre total d'Etats qui sont des gouvernements contractants	84,31%	87,58%
Renseignements concernant les installations portuaires		
Gouvernements contractants ayant signalé qu'ils avaient des installations portuaires	122	133
en % du nombre total d'Etats qui sont des gouvernements contractants	79,74%	93,66%
Gouvernements contractants ayant signalé qu'ils avaient approuvé des PFSP	119	132
en % du nombre total d'Etats qui sont des gouvernements contractants	77,78%	92,96%*
Nombre d'installations portuaires déclarées (estimation)	9 108	9 541
- nombre de PFSA approuvés	8 674	9 394
en % du nombre d'installations portuaires déclarées	95,23%	98,46%
- nombre de PFSP soumis	8 587	9 388
en % du nombre d'installations portuaires déclarées	94,28%	98,40%
- nombre de PFSP approuvés	8 413	9 261
en % du nombre d'installations portuaires déclarées	92,37%	97,07%

*chiffre revu afin de prendre en compte les Etats sans littoral, à l'exception de ceux qui bordent des mers fermées.

³¹⁹ Site de Secopex : http://www.isps.fr/Actualité/tableau_code_ISPS.pdf.

Etat comparatif de la mise en œuvre par régions géographiques

(au 1^{er} septembre 2004 et au 29 novembre 2004)

Au 1^{er} septembre 2004

Région	Afrique	Etats arabes et méditerranéens	Asie et Pacifique	CEI et Europe orientale	Amérique latine et Caraïbes	Nord-ouest de l'Europe	Amérique du Nord
Nombre d'Etats	30	22	31	19	30	19	2
Etats sans littoral*	2	0	1	4	1	3	0
Etats qui ont approuvés des PFSP	17	20	27	12	28	16	2
Etats qui ont approuvés des PFSP (%)*	60,71	90,91	90,00	80,00	96,55	100,00	100,00
Installations portuaires déclarées	177	425	2931	493	813	3819	459
PFSP approuvés	165	338	2683	445	674	3658	459
PFSP approuvés (%)	93,22	79,53	91,54	90,26	82,90	95,78	100,00

Au 29 novembre 2004

Région	Afrique	Etats arabes et méditerranéens	Asie et Pacifique	CEI et Europe orientale	Amérique latine et Caraïbes	Nord-ouest de l'Europe	Amérique du Nord
Nombre d'Etats	30	22	31	19	30	19	2
Etats sans littoral*	2	0	1	4	1	3	0
Etats qui ont approuvés des PFSP	23	21	28	13	29	16	2
Etats qui ont approuvés des PFSP (%)*	82,14	95,45	93,33	86,67	100,00	100,00	100,00
Installations portuaires déclarées	239	414	3084	608	861	3868	467
PFSP approuvés	225	346	2927	580	850	3866	467
PFSP approuvés (%)	94,14	83,57	94,91	95,39	98,72	99,95	100,00

*chiffre revu afin de prendre en compte les Etats sans littoral, à l'exception de ceux qui bordent des mers fermées.

Renseignements fournis concernant les questions visées à
la règle XI-2/13 de la Convention SOLAS
 (au 29 novembre 2004)

Règle	Nom et coordonnées des autorités	Gouvernements contractants	
		Nombre	Pourcentage
XI-2/13.1.1	Responsables de la sûreté du navire	125	81,70%
XI-2/13.1.1	Responsables de la sûreté des installations portuaires	114	74,51%
XI-2/13.1.3	Désignées pour recevoir les communications relatives à l'évaluation de la sûreté des navires et leur donner suite	103	67,32%
XI-2/13.1.4	Désignées pour recevoir les communications d'autres gouvernements et leur donner suite	111	72,55%
XI-2/13.1.5	Désignées pour donner des conseils et prêter assistance aux navires	103	67,32%
XI-2/13.2	Nombre de gouvernements contractants utilisant des organismes de sûreté reconnus	96	62,75%
	Nombre d'organismes de sûreté reconnus associés	205	-----

Bibliographie

Doctrine

- BOISSON Philippe, *La sûreté des navires et la prévention des actes de terrorisme dans le domaine maritime*, DMF n° 640, p. 723, septembre 2003.
- BOISSON Philippe, *Les clauses de sûreté maritime dans les chartes-parties*, Gazette n°6 de la Chambre Arbitrale Maritime de Paris (CAMP), page n° 3.

Presse

- *Le dispositif d'approbation des plans de sûreté des navires de commerce*, Amarres, 4^{ème} trimestre 2004, pages 3 à 5.
- *Opération de contrôle au port*, Metro novembre 2004

Sites Web

- Asia Times, http://www.atimes.com/atimes/Front_Page/FF16Aa02.html
- Association of Canadian Port Authorities, http://www.acpa-ports.net/pr/releases/release_07052004-funding-f.html
- BBC, <http://news.bbc.co.uk/1/hi/world/asia-pacific/1804146.stm>
- Bibliothèque virtuelle sur la mer de Chine du Sud, <http://community.middlebury.edu/~scs/docs/Ong-Preempting%20Terrorism%20and%20Piracy,%20ISEAS.pdf>
- Biométrie on Line, http://biometrie.online.fr/Faq_index.htm
- CAMP :
<http://www.arbitrage-maritime.org/fr/gazette.htm>
http://www.arbitrage-maritime.org/fr/PDF/Code_ISPS.pdf
- Cèdre (Centre de documentation, de recherche et d'expérimentations sur les pollutions accidentelles des eaux), <http://www.le-cedre.fr/>
- Centre de géostratégie de l'Ecole Normale Supérieure, <http://www.geostrategie.ens.fr/membres.php>
- CGVMSL :
http://www.greatlakes-seaway.com/fr/navigation/isps_adv.html
http://www.greatlakes-seaway.com/fr/navigation/isps_bg.html
- CCI de Rouen, http://www.rouen.cci.fr/club_risques/cr_mai_2005.pdf
- Chambre de Commerce Internationale :
http://www.iccwbo.org/home/news_archives/2003/stories/piracy%20_report_2002.asp
<http://www.icc-ccs.org/main/news.php?newsid=40>
<http://www.icc-ccs.org.uk/>
- Check Point, site d'information militaire suisse, <http://www.checkpoint-online.ch/CheckPoint/Monde/Mon0072-TerrorismeMaritime.html>

- CommentÇaMarche.net, <http://www.commentcamarche.net/wifi/wifiintro.php3>
- Commission économique pour l'Europe de l'ONU, <http://www.unece.org/trans/bcf/wp30/documents/TRANS-WP30-218f.pdf>
- *Department of Homeland Security*, http://www.dhs.gov/interweb/assetlibrary/HSSTAC_MtgNotice_2005May18-19.pdf
- Douane australienne, <http://www.customs.gov.au/site/page.cfm?u=4238>
- Entreprise Euronext, http://www.euronext.com/file/view/0,4245,1626_53424_637231306,00.pdf
- GIGN, <http://www.gign.org/unites-francaises/cos.php>
- Gouvernement luxembourgeois, http://www.gouvernement.lu/salle_presse/actualite/2004/03/25sommet/
- Groupe Canada Newswire, <http://www.newswire.ca/fgov/fr/releases/archive/May2004/21/c6623.html>
- IAGS, <http://www.iags.org/n0124051.htm>
- Institut australien de politique stratégique, http://www.aspi.org.au/pdf/Maritime_terrorism%20India_AB.pdf
- Institut d'études internationales de Montréal :
<http://www.er.uqam.ca/nobel/cepes/pdf/BULL71.pdf>
<http://www.er.uqam.ca/nobel/cepes/pdf/BULL72.pdf>
- Institut international d'études stratégiques, <http://www.iiss.org/stratcomfree.php?scID=386>
- Le Monde :
<http://www.lemonde.fr/web/article/0,1-0@2-3220,36-639882@51-635324,0.html>
<http://www.lemonde.fr/web/article/0,1-0@2-669420,36-682158,0.html>
http://www.lemonde.fr/web/recherche_breve/1,13-0,37-851377,0.html
- Libération : <http://www.liberation.fr/page.php?Article=282361>
- Marine canadienne, http://www.marine.forces.gc.ca/mspa_news/news_issues_f.asp?category=4&title=30
- Ministère des transports canadien: <http://www.tc.gc.ca/vigilance/spu/maritime/rehaussement/systeme.htm>
- Ministère français de la défense, http://www.defense.gouv.fr/sites/das/dossiers/strategies_regionales_americaines_apres_le_11_septembre825
- Ministère français des transports, de l'équipement, du tourisme et de la mer :
http://www.mer.equipement.gouv.fr/commerce/01_ports_francais/01_organisation_portuaire/index.htm
http://www.mer.equipement.gouv.fr/securite/03_navigation/02_cross/trafic2000.pdf
- Net Marine, <http://www.netmarine.net/forces/commando/hubert/>
- OCDE :
<http://www.oecd.org/dataoecd/19/61/33949707.pdf>
<http://www.oecd.org/dataoecd/39/4/34029659.pdf>
http://www.oecd.org/document/45/0,2340,en_2649_34487_4395885_119690_1_1_37407,00.html

- OMD, <http://www.wcoomd.org/ie/Fr/Presse/OMD%20-%20CADRE%20DE%20NORMES%20juin%2021%20final.pdf>
- OMI :
<http://www.imo.org/home.asp>
http://www.imo.org/includes/blastDataOnly.asp/data_id%3D10606/hesse_chara_sec.pdf
http://www.imo.org/Newsroom/mainframe.asp?topic_id=583&doc_id=2689
http://www.imo.org/Newsroom/mainframe.asp?topic_id=892&doc_id=3687
http://www.imo.org/Newsroom/mainframe.asp?topic_id=892&doc_id=3760
http://www.imo.org/Newsroom/mainframe.asp?topic_id=892&doc_id=4714
<http://www2.imo.org/ISPSCode/ISPSInformation.aspx>
- ONU, http://www.un.org/french/geninfo/ir/ch2/ch2_txt.htm
- Port de Halifax, <http://www.portofhalifax.ca/AbsPage.aspx?id=1152&siteid=1&lang=2>
- RTL Belgique, <http://www.rtl.be/Site/Index.aspx?LG=1&PageID=209&ArticleID=50756>
- Salvanos,
<http://www.salvanos.org/modules.php?op=modload&name=News&file=article&sid=523&mode=thread&order=0&thold=0>
- Secopex :
http://www.isps.fr/Actualité/tableau_code_ISPS.pdf
<http://www.isps.fr/ISPS-materiel-equipement-securite-protection.htm>
<http://www.isps.fr/supply-chain-security.htm>
- Secure Marine :
<http://www.secure-marine.com/history.htm>
<http://www.secure-marine.com/statistics/attack.htm>
<http://www.secure-marine.com/statistics/countries.htm>
http://www.secure-marine.com/statistics/attack_types.htm
http://www.secure-marine.com/statistics/attack_crew.htm
<http://www.secure-marine.com/statistics/ships.htm>
http://www.secure-marine.com/statistics/arms_used.htm
- Sénat français :
<http://www.senat.fr/cra/s20050215/s20050215H10.html>
<http://www.senat.fr/rap/a04-076-20/a04-076-2016.html>
http://www.senat.fr/rap/a04-076-20/a04-076-20_mono.html#toc0
<http://www.senat.fr/rap/r03-388/r03-3882.html>
- South Asia Analysis Group, <http://www.saag.org/papers12/paper1154.html>
- Terrorisme.Net, http://www.terrorisme.net/p/article_136.shtml
- The Economist, http://www.economist.com/agenda/displayStory.cfm?story_id=2804108
- Union Européenne :
http://europa.eu.int/comm/competition/antitrust/others/maritime/white_paper/autf_french_shipping_council_response_fr.pdf
http://europa.eu.int/comm/taxation_customs/customs/customs_controls/drugs_precursors/index_fr.htm
<http://europa.eu.int/scadplus/leg/fr/lvb/l06026.htm>
<http://europa.eu.int/scadplus/leg/fr/lvb/l24271.htm>

Tables des matières

<u>Sommaire</u>	p.2
<u>Glossaire</u>	p.3
<u>Introduction</u>	p.5
<u>I La menace actuelle</u>	p.7
1.1 Historique	p.7
1.1.1. Le terrorisme maritime	p.7
1.1.2. La piraterie	p.10
1.2 La situation actuelle	p.14
1.2.1 La situation en France	p.18
1.2.2 La situation dans le reste du monde	p.19
1.2.2.1 La situation en Asie	p.19
1.2.2.1.1 La situation en Asie du Sud-est	p.19
1.2.2.1.2 La situation en Inde	p.22
1.2.2.2 La situation en Australie	p.23
1.2.2.3 La situation au Canada	p.24
1.2.2.4 La situation en Turquie	p.24
1.3 Les objectifs principaux	p.25
<u>II La mise en application au quotidien</u>	p.26
2.1 Les textes complémentaires en matière de sûreté du transport maritime	p.26
2.1.1 La législation française	p.27
2.1.1.1 Les arrêtés	p.28
2.1.1.2 Les circulaires conjointes de la DTMPL et du HFD Mer	p.29
2.1.1.3 Le décret 2004-290 du 26 mars 2004	p.30
2.1.1.4 L'instruction n° 412	p.30
2.1.1.5 L'instruction n° 413	p.30
2.1.1.6 Les ordonnances	p.32
2.1.2 La législation européenne	p.33
2.1.2.1 Le règlement (CE) n° 724/2004	p.33
2.1.2.2 Le règlement (CE) n° 725/2004	p.33
2.1.2.3 La proposition de directive du 11 juin 2004	p.35
2.1.2.4 Le règlement (CE) n° 884/2005	p.36
2.1.3 La législation internationale	p.36
2.1.3.1 La législation de l'OMI	p.36
2.1.3.1.1 La résolution 1	p.36
2.1.3.1.2 Les textes du MSC	p.37
2.1.3.1.3 Proposition d'amendement	p.41
2.1.3.2 La législation de l'OIT	p.41
2.1.3.3 La législation de l'OMD	p.42

2.1.3.4 La législation étatsunienne	p.43
2.1.3.4.1 La <i>Container Security Initiative</i> , ou CSI	p.43
2.1.3.4.2 La <i>Proliferation Security Initiative</i> , ou PSI	p.44
2.1.3.4.3 Le <i>Custom-Trade Partnership against Terrorism</i> , ou C-TPAT	p.45
2.1.3.4.4 La règle des préavis	p.45
2.1.3.4.5 Le <i>Public Health Security and Bioterrorism Preparedness and Response Act</i> , dit <i>Bioterrorism Act</i> , ou BTA	p.46
2.2 L'organisation française	p.46
2.2.1 Au niveau national	p.46
2.2.2 Au niveau local	p.51
2.3 Les navires/ les armateurs	p.51
2.4 Les ports	p.55
2.4.1 L'exemple du Port Autonome de Marseille	p.60
2.5 Les gouvernements	p.62
2.6 Les grandes lignes de l'application dans le reste du monde	p.62
2.6.1 Aux USA	p.62
2.6.2 Au Canada	p.63
2.6.3 A Singapour	p.66
2.6.4 En Chine	p.66
2.6.5 En Australie	p.67
2.6.6 L'OTAN	p.69
2.6.7 Les taux de conformité	p.71
2.6.7.1 Au niveau français	p.71
2.6.7.2 Au niveau international	p.72
<u>III Conséquences et solutions</u>	p.74
3.1 Les nouvelles clauses des chartes parties	p.74
3.1.1 Les obligations des parties	p.74
3.1.2 Le refus d'accès au port	p.75
3.1.3 La NOR	p.75
3.1.4 La notion de port sûr	p.75
3.2 Les difficultés nées de l'application directe	p.76
3.3 Comment accroître la sûreté maritime ?	p.78
3.4 Les dérives à éviter	p.84
<u>Conclusion</u>	p.88
<u>Annexes</u>	p.91
<u>Table des annexes</u>	p.92
<u>Annexe I</u> : Le Code ISPS, partie A	p.93
<u>Annexe II</u> : Statistiques sur les actes de violence en mer	p.108
<u>Annexe III</u> : Les autorités impliquées dans le contrôle du navire au port	p.111
<u>Annexe IV</u> : Les équipements de sûreté	p.112

<u>Annexe V :</u> Les taux de conformité internationaux au Code ISPS	p.114
<u>Bibliographie</u>	p.118
<u>Tables des matières</u>	p.121