

Contexte : la piraterie maritime, une menace avérée pour l'économie de l'énergie en mer

La production mondiale pétrolière est répartie sur plus de 10.000 champs offshore, impliquant chacun d'une part un ensemble d'équipements pour extraire, traiter et stocker provisoirement le pétrole et d'autre part des navires chargés d'effectuer le transport maritime d'hydrocarbures entre lieux de production et de consommation. La piraterie maritime moderne représente à l'heure actuelle le risque majeur pour la sécurisation de ces sites de production énergétique et du transport maritime pétrolier.

1. La piraterie maritime : un risque majeur sur le milieu maritime

Loin des images fantasmagoriques qui placent la piraterie dans l'univers romancé des bateaux à voiles, la piraterie moderne est un phénomène violent dont la recrudescence inquiète les autorités maritimes internationales.

La piraterie est « l'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 soit contre un autre navire ou aéronef, ou contre des personnes ou des biens à leur bord, en haute mer, soit contre un navire ou aéronef, des personnes ou des biens, dans un lieu ne relevant de juridiction d'aucun État¹ ».

Force est donc de constater que les individus et organisations qui pratiquent des attaques contre des pêcheurs, des navires de commerce, des plaisanciers ou des plateformes pétrolières sont particulièrement déterminés, souvent suréquipés (moyens de locomotion, moyens de communications, armements...), et leurs « chefs » expérimentés assurent la pérennité de cette activité délictueuse en gérant les attaques comme s'il s'agissait d'une entreprise « mondiale ».

¹ Article 15 de la Convention sur la haute mer.

Les bateaux utilisés par les pirates sont des vedettes très puissantes, des « speed-boats », capables de rattraper aisément un lourd navire de commerce, qui ne peut que ralentir, incapable de virer de bord ou d'augmenter la vitesse au point de semer l'embarcation légère. Ces « dollars flottants » sont des proies faciles, croisant dans des eaux peu fréquentées par les autorités côtières [Onuoha, 2010]. Les « bateaux-mères », des pirates, postés en arrière du champ des « opérations », sont équipés des dernières technologies en matière de repérage dans l'espace, ce qui leur permet de cibler et d'organiser très précisément une attaque en prenant au dépourvu le navire attaqué, en envoyant des vedettes souvent indétectables par les navires assaillis.

Les actes de piraterie ne cessent de se multiplier. En 2013, 264 attaques ont été recensées par le Bureau maritime international (BMI), dont 141 en Asie du Sud-Est et 51 en Afrique de l'Ouest. 85 % des attaques ont eu lieu de nuit et les principales cibles sont les navires de commerce (pétrolier, vraquier et remorqueurs avec barge) au mouillage ou naviguant à faible vitesse. Dans la majorité des cas, les pirates cherchent à voler du matériel facile à revendre, ou à piller les navires, ou leur cargaison mais aussi à kidnapper certains membres d'équipage. Selon le BMI, une attaque sur 4, lorsqu'elle n'est pas interrompue par les forces gouvernementales navales de sécurité, est menée avec succès.

Au début des années 2000, les pirates étaient armés de couteaux. Aujourd'hui, ils attaquent leurs proies à l'arme automatique. La constatation, bien que peu surprenante, est alarmante. A la date du 18 août 2014, selon le rapport du BMI, les pirates ont mené 148 attaques.

2. La maritimisation de l'énergie, nouveaux territoires, nouveaux enjeux et nouvelles menaces

« La sécurité énergétique fait partie des challenges économiques et sécuritaires les plus sérieux, aussi bien aujourd'hui que dans le futur. La croissance des économies du monde et des sociétés va de pair avec l'importance de l'énergie et de pair avec les infrastructures qui produisent et fournissent cette énergie. Les infrastructures énergétiques critiques fournissent le carburant qui permet à l'économie globale d'avancer et à nos sociétés de fonctionner ». C'est en ces termes que s'est ouverte

l'allocation de l'OSCE (Organization for Security and Cooperation in Europe) lors de la réunion du comité économique de l'OTAN du 22 septembre 2008 à Bruxelles.

Plusieurs catastrophes ont démontré la vulnérabilité que peuvent avoir de telles infrastructures et l'impérieuse nécessité d'une profonde rigueur dans le respect des procédures, la conception et l'exploitation de ces systèmes « critiques ». La question de la maritimisation de l'énergie se révèle donc comme un enjeu considérable [Napoli., 2014].

La production offshore joue un rôle important dans l'approvisionnement énergétique des sociétés modernes. Si la majorité de la production est opérée par moins de 500 mètres d'eau, l'offshore dit « profond », dans des zones situées par plus de 1 000 m de hauteur d'eau, se développe depuis quelques années grâce à des avancées technologiques majeures, notamment dans le domaine de la sismique ou des installations sous-marines. Pour donner un ordre d'idée, la production d'huile par plus de 1 000 mètres de fond a augmenté de 12 % entre 2006 et 2008. Pour le gaz, la production par plus de 1 000 mètres représente moins de 2 % de la production mondiale et les réserves sont estimées à 2,7 Tm³ (mille milliards).

Les compagnies pétrolières s'intéressent à l'offshore car c'est l'une des rares zones d'accès aux réserves naturelles et car il permet aussi de se protéger des conflits à terre (comme par exemple dans le golfe de Guinée où il est plus sûr de produire en mer qu'à terre). La production offshore devrait poursuivre son développement, ainsi près de 30 nouveaux champs situés sous plus de 1 000 mètres d'eau devraient être mis en production tous les ans d'ici à 2020, soit plus du double de la décennie 2000-2010.

Le domaine de sécurité maritime présente des multiples risques, comme le risque de naufrage, causés par le tonnage qui devient de plus en plus élevé ou la vitesse croissante des navires. Citons comme exemple le naufrage du traversier sénégalais le *Joola* au large des côtes de Gambie le 26 septembre 2002, faisant officiellement 1 863 morts et disparus, et officieusement plus de 2 000 victimes. La capacité légale du traversier était de 550 personnes...

Les risques de naufrage sont aussi liées aux erreurs humaines ou aux dysfonctionnements de systèmes technologiques comme dans le cas du ferry-boat grec *Express Samina* au large de Paros (Grèce), le 26 septembre 2000, faisant 82 morts. La

coque du navire se déchira en deux endroits et coula en une heure, uniquement parce que 9 portes étanches sur 11 n'étaient pas fermées au niveau des salles de machines et des soutes. À la suite de ce naufrage, l'installation de boîtes noires deviendra une obligation sur tous les navires transporteurs de passagers.

Le risque de collision avec des objets flottants (navires, conteneurs tombés à l'eau, etc.) est aussi connu. Durant la Première Guerre mondiale, une terrible explosion se produisit dans le port d'Halifax, en Nouvelle-Écosse au Canada, lorsqu'un navire français transportant des munitions, le *Mont-Blanc*, entra en collision avec un navire norvégien qui se rendait en Belgique. L'explosion des munitions du *Mont-Blanc* advint 19 minutes plus tard : elle rasa 2,5 km² de la ville, tua 2 000 personnes et en blessa des milliers d'autres. Un raz-de-marée de 18 mètres de haut déclenché par l'explosion fut si puissant qu'il emporta des arbres, plia des rails de chemin de fer et démolit des édifices, transportant des débris en tout genre sur des centaines de mètres.

Le risque des catastrophes naturelles (séisme, cyclone, etc.) et aux aléas météorologiques (tempête, vague scélérate, etc.), représente aussi de réels dangers au quotidien comme cela fut le cas pour le ferry-boat *Princess of the Stars*, de la compagnie Sulpicio Lunes faisant 828 morts le 21 juin 2008, le navire a sombré en raison d'énormes vagues provoquées par le typhon Fengshen aux Philippines.

Les pollutions dues à l'extraction ou au transport des hydrocarbures sont encore présentes dans nos mémoires. Citons pour exemples l'accident en 2010 sur la plateforme pétrolière *Deepwater Horizon* dans le golfe du Mexique causant la perte de 4,9 millions de barils, 11 personnes portées disparues, 17 blessés et plusieurs zones polluées (littoraux de la Louisiane, du Mississippi, de l'Alabama et de la Floride).

De nouveaux risques, comme le risque sanitaire, qui se présentent avec le transport de déchets nucléaires, d'eaux de ballast et la circulation de navires ou sous-marins à propulsion nucléaire, et éventuellement armés d'engins nucléaires complètent dramatiquement le panorama des menaces.

A ces accidents et catastrophes, s'ajoute le risque de piraterie, toujours présent dans les espaces stratégiques comme le golfe d'Aden ou encore le golfe de Guinée, haut lieu de la production de pétrole offshore dans le monde.

La plupart des sources d'énergie nécessaires au fonctionnement de nos sociétés modernes sont fournies par le gaz et le pétrole. La dépendance mondiale à l'égard du pétrole est énorme, il alimente nos moyens de transport, chauffe ou refroidit des bâtiments et sert à créer des produits chimiques industriels et domestiques. 60% de la production de pétrole est utilisée pour le transport, essentiellement les voitures et les camions. Le pétrole est une énergie non renouvelable dont la consommation actuelle atteint 70 millions de barils par jour, certaines estimations en prévoyant le doublement d'ici 2025.

La production offshore représente 30 % de la production mondiale de pétrole (avec 25 millions de barils par jour) et 27 % de celle de gaz. L'offshore représente par ailleurs 20 % des réserves mondiales de pétrole et 30 % de celles de gaz. Environ 450 champs ont été découverts à plus de 1 000 mètres de profondeur, dont 38 % dans le golfe du Mexique aux États-Unis, 26 % dans le golfe de Guinée en Afrique et 18 % au Brésil. Ils ne représentent pour l'instant que 3 % de la production mondiale de pétrole, mais ce chiffre ne fera que croître dans les années à venir compte tenu des réserves estimées de l'ordre de 72 livre sterling.

La construction, le transport, le fonctionnement d'une plate-forme génèrent divers risques. D'éventuels incidents ou accidents peuvent aggraver des impacts sur l'environnement, les marins ou les biens comme le risque sismique, le risque des rejets et de toxicité, le risque d'incendie ou d'explosion qui est le risque le plus redouté et le risque de pollution qui perturbe la vie marine comme par exemple le cas du *Pasha Bulker*, cargo de 40 000 tonnes transportant du charbon, échoué le 8 juin 2007 sur le littoral australien avec encore 700 tonnes de pétrole à bord. Les 21 personnes de l'équipage ont été hélitreuillées. Restait à traiter le risque de pollution.

A ces accidents et catastrophes [Gordon et al., 1996], s'ajoute depuis le début des années 2000, le risque de piraterie Hansen, 2009], très présent dans les espaces stratégiques comme le golfe d'Aden ou le golfe de Guinée, haut lieu de la production de pétrole offshore dans le monde. Compte tenu des enjeux économiques liés aux hydrocarbures, les champs de production offshore sont devenus une cible de choix pour la piraterie maritime voire la menace terroriste [Anifowose et al., 2012]. Or si les plateformes pétrolières et navires associés forment un réseau industriellement abouti en

ce qui concerne l'exploitation, ils sont démunis face aux actes de malveillance intentionnels : de ce point de vue, ce sont des cibles de choix, isolées et donc très exposées.

3. Revue de littérature sur les attaques de piraterie contre les infrastructures énergétiques en mer, le cas des champs pétroliers

Les cas d'attaques d'infrastructures énergétiques offshore, s'ils restent pour le moment moins fréquents et moins médiatisés que ceux d'attaque de navires, n'en sont pas moins extrêmement inquiétants en ce sens qu'ils dévoilent une grande vulnérabilité des infrastructures.

Les attaques sur les navires transportant de l'énergie représentent un pourcentage significatif. En 2006, elles avoisinaient environ 12 % des attaques pour atteindre plus de 24 % en 2007. La plupart des attaques sont des actes visant à dérober un bien de valeur. Elles se déroulent dans les ports mêmes ou à l'aide de petites embarcations très rapides. Le nombre de détournements et de prises d'otages ainsi que de demandes de rançon a aussi fortement augmenté. En août 2003, le tanker malaisien *Penrider* a été abordé au large de l'Indonésie et une rançon demandée pour un montant de 100 000 dollars. Les cas où le navire est attaqué pour les biens qu'il transporte est clairement un objectif des pirates. En 1998, le *Petro Ranger* a été attaqué hors des eaux territoriales de Singapour. Il transportait près de 12 000 tonnes de produits pétroliers. Les pirates sont allés jusqu'à le débaptiser et le renommer *Wilby* en lui attribuant un pavillon hondurien. Le *Petro Ranger* devient ainsi, pour un temps, un navire fantôme [Nincic., 2009].

La grande majorité des attaques contre des navires transportant de l'énergie concerne les tankers de pétrole et le transport de gaz liquide. Par rapport au nombre total de la flotte de tankers (environ 120 000), 4 000 (3 %) sont des tankers énergétiques. En 2007, les pirates se sont aussi intéressés avec succès aux plateformes pétrolières mobiles et aux transporteurs de gaz liquide. Ainsi, deux ont été attaqués en 2007, l'un en Indonésie, l'autre au large de Singapour. Trois plateformes fixes de forage ont aussi été attaquées, deux au Nigeria (avec un kidnapping et une rançon à la clef) et une en Inde. Ces

événements démontrent que les pirates sont désormais en capacité de s'attaquer à tout type de cible.

La piraterie à l'encontre des installations pétrolière en mer a depuis 1988 pris une ampleur considérable.

Dans la Figure 0-1, un exemple de scénario d'attaque par 14 pirates lourdement armés contre un navire conteneur est donné. Les pirates ont utilisé deux bateaux dont un navire de ravitaillement et un navire de haute vitesse. Ils sont aisément montés à bord du conteneur. Malgré le déclenchement du système d'alerte et le repli de l'ensemble de l'équipage au sein d'une « citadelle », les pirates ont réussi à pénétrer dans cette dernière et ont enlevé cinq personnes dont le maître de l'équipage. Ils se sont enfin échappés en emportant la trésorerie de l'équipage.

Outre des navires transportant le pétrole ou du matériel en liaison avec l'activité de production, plusieurs plateformes pétrolières ont aussi été attaquées ces dernières années. Le navire-citerne français *Gascogne*, battant pavillon luxembourgeois (il appartient à la société Sea-Tankers), a été attaqué le 4 février 2013. Ce navire de 119 m de long dispose d'un équipage de 17 ou 19 personnes.

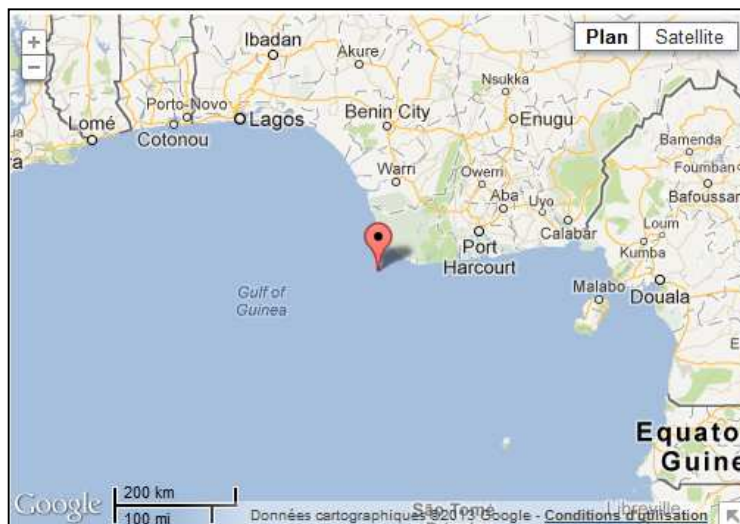


Figure 0-1 : Attaque de pirate contre un navire conteneur le 25 avril 2013 (Source Bureau maritime international)

Selon le ministre des Transports, de la Mer et de la Pêche Frédéric Cuvillier, « *il y a 19 personnes à bord, tous des Togolais (...). Nous n'avons pas reçu de revendication pour*

l'instant », a-t-il ajouté en précisant que le bateau naviguerait « à la hauteur du sud du Ghana et se dirigerait vers le Togo », tout proche.

C'est le troisième cas de capture d'un pétrolier au large de la Côte d'Ivoire. Dans les deux premiers cas, le navire a été vidé de sa cargaison, au large du Ghana, puis libéré par les ravisseurs. En octobre 2013, un tanker grec avait été attaqué alors qu'il mouillait devant le port d'Abidjan, tandis qu'en janvier, c'est un tanker battant pavillon panaméen qui avait été la cible des pirates.

Malgré la diminution de nombre d'attaques de piraterie (439 en 2011, 297 en 2012 contre 264 en 2013), la dangerosité et la gravité des conséquences de ces actes sur l'équipage des cibles attaqués restent constantes en évolution.

Force est de constater que les marins des navires de commerce ne sont ni équipés, ni formés pour repousser une attaque armée. Même si des formations de prévention et d'intervention sont réalisées pour les équipages transitant dans des zones à risques, et même si des équipements sont apportés aux navires, il n'appartient pas aux marins de devoir faire face à la violence d'une attaque pirate.

Les pirates ne se limitent plus à l'heure actuelle à piller les marchandises et les effets personnels contenus sur les navires. Après avoir pris le contrôle du navire, ils réclament désormais des rançons pour libérer les équipages. Certains pirates vont même jusqu'à tuer tout l'équipage pour revendre la marchandise et se servir du navire détourné pour faire transiter en toute impunité une marchandise qui sera détournée à nouveau, et ainsi de suite, en modifiant à chaque fois l'immatriculation grâce à des pavillons de complaisance attribués sans aucun contrôle. Les transporteurs, seuls face à leurs décisions, se retrouvent désemparés, et finissent souvent par verser les rançons demandées après les avoir négociées.

Aujourd'hui, une nouvelle forme de piraterie voit le jour : un groupe organisé, hiérarchisé, maîtrisant les dernières technologies en matière de repérage maritime, doté d'informatique dans le monde, d'armes puissantes et de bases à terre sur des territoires de non-droit. La question se pose de savoir comment il est possible d'éradiquer ce phénomène pourtant vivement condamné qui fait frémir les marins du monde, hésiter les armateurs, et méditer les assureurs.

4. Des solutions technologiques innovantes qui se déploient progressivement

A ce jour, il existe deux types de systèmes opérationnels dédiés à la protection des cibles maritimes :

- La détection d'une menace ;
- La gestion d'une attaque.

4.1 La détection d'une menace

Dans le domaine de la détection en environnement marin, il existe de nombreux systèmes. Citons :

- Des systèmes à base de radar à impulsions tels que par exemple les radars de veille ou de navigation de type TERMA, RURUNO, RACAL ou DECA, ou encore le système Sea-Giraffe d'Ericsson [Saab, 2005]. Ces systèmes sont destinés à détecter en priorité des mobiles coopératifs de taille importante ou moyenne. Ils ont des performances médiocres face à de petites cibles marines non coopératives évoluant dans une mer formée (fouillis de mer) et sont pénalisés par une zone aveugle à faible distance du porteur. Par ailleurs, les systèmes à balayage sont généralement relativement lents pour analyser un domaine étendu.
- Des systèmes de surveillance optronique (développés par exemple par SAGEM, EADS, THALES, RADAMEC, ALENIA, HGH, FLIR Systems, etc. [Sagem, 2012]). Ces systèmes sont handicapés par les problèmes de réflexion solaire sur la mer et restent sensibles aux conditions météorologiques, leur portée étant rapidement réduite en présence de brume ou brouillard et d'embruns.

A titre d'exemple, le projet SCANMARIS ([Morel et al., 2010] et [Morel et al., 2008]) a permis de tester en milieu marin des modules innovants de détection de comportements suspects d'embarcations de tailles variables de manière globale et à long terme en analysant le trafic maritime régulier et en le croisant avec des bases de données sur les navires, pour identifier des suites spatio-temporelles d'anomalies.

4.2 La gestion d'une attaque

Les solutions élaborées reposent principalement sur des outils de diagnostic convoquant des raisonnements probabilistes et/ou à base de connaissances expertes. Les algorithmes rencontrés dans la littérature révèlent des insuffisances dans l'évaluation et la planification de la réaction [Giraud et al., 2013].

Les exemples d'attaques cités précédemment sont de parfaites illustrations de la faiblesse des dispositifs anti-piraterie actuellement mis en place. La sécurité des installations pétrolières est donc à ce jour assurée par des dispositifs dits classiques. Ces derniers, malgré leurs points forts pour l'aide à la détection, ne traitent pas des différents types de menaces (bateau de pêche, jet ski, tanker, etc.) et leur efficacité dépend de nombreux paramètres liés à l'environnement ainsi qu'aux contraintes techniques et opérationnelles [Giraud et al., 2010].

La solution consiste donc à augmenter le degré de protection des infrastructures en développant un système capable de prévenir la menace et de générer des réactions internes et externes en cas d'intrusion confirmée ([Morel et al., 2007] et [Giraud et al., 2012]).

Problématique et objectifs de recherche

Cette thèse se concentre sur la façon dont une approche bayésienne de l'estimation, de l'inférence et du raisonnement dans l'analyse des risques pourrait compléter avantageusement les approches classiques sous-tendues par des modèles « fréquentistes » [Pichard, 1998].

La fréquence n'est pas une probabilité. Une fréquence est une proportion d'observations alors qu'une probabilité est la mesure d'une incertitude sur un événement.

Les deux cadres classiques, dans lesquels la probabilité intervient avec sa sémantique, sont les suivants :

- Le cadre fréquentiste : la probabilité porte exclusivement sur les observations, conditionnellement à des valeurs hypothétiques des paramètres ; sémantiquement les probabilités sont conçues comme des fréquences. Dans sa version radicale, le cadre fréquentiste exclut toute probabilité sur les paramètres, et partant toute probabilité des hypothèses. Le cadre fréquentiste, mis en place à la fin du XIX^{ème} siècle, reste encore le cadre dominant de la statistique.
- Le cadre bayésien : la probabilisation porte aussi bien sur les observations que sur les paramètres. Le cadre bayésien est un enrichissement du cadre fréquentiste ; il restitue la sémantique naturelle des probabilités et permet les probabilités des hypothèses. Le cadre bayésien, plus ancien que le cadre fréquentiste, remonte au XVIII^{ème} siècle.

Les méthodes bayésiennes permettent de répondre directement aux questions sur les paramètres et les modèles : « Quelle est la probabilité d'un ensemble de paramètres compte tenu des données observées? ». Les méthodes fréquentistes permettent, elles, de répondre aux questions sur : « Quelle est la probabilité des données sans aucune hypothèse ? ».

Les deux approches bayésienne et fréquentiste sont généralement combinées comme techniques d'estimation et d'inférence ([Efron, 2005] et [Little, 2006]).

Le couplage de l'approche fréquentiste et de l'estimation bayésienne dans le cadre de notre problématique de lutte contre la piraterie apparaît donc pertinent. Il fournit une compréhension conceptuelle utile à la pluralité des données et connaissances convoquées

dans la prévention du risque et conduit à développer une boîte à outils statistiques particulièrement polyvalente à fin d'aide à la décision.

Afin de démontrer cette hypothèse, l'objectif principal de ce travail de thèse est de proposer une nouvelle approche permettant d'améliorer la prévention, le diagnostic, le management et la prise de décision face au risque de piratage maritime. Plus précisément, les objectifs de la thèse sont :

- D'étudier la faisabilité d'intégrer, au sein d'un outil de conception des réseaux bayésiens statiques, des données et des retours d'expériences des attaques de pirateries sur différents types de navires. Cela permettra ainsi de mieux comprendre l'environnement maritime, de préciser et de décrire des actes réels de piraterie et surtout de présenter les avantages de l'approche fréquentiste.
- De coupler des modèles quantitatifs d'analyse des risques avec des données et connaissances qualitatives acquises auprès d'experts du domaine maritime. Ce qui permettra de concevoir à l'aide d'un réseau bayésien dit « statique » un modèle de diagnostic de la menace plus adapté à la protection des champs pétroliers. Le couplage permettra de présenter la complémentarité entre l'approche fréquentiste et l'approche probabiliste.
- De concevoir un modèle dynamique d'aide à la décision grâce aux potentiels des réseaux bayésiens dits « dynamiques ». Ce modèle permettra l'amélioration des résultats obtenus à partir du modèle « statique ».
- De valider le couplage entre le modèle statique et le modèle dynamique afin d'obtenir un système performant pour le management du risque de piraterie maritime.

Organisation du manuscrit de thèse

Le manuscrit est organisé en 6 chapitres.

Le chapitre 1 présente une vue d'ensemble du projet de publications qui a sous-tendu ce travail de thèse.

Le chapitre 2 situe le premier article publié dans la revue « *Radio Science Bulletin*² ». Ce chapitre est constitué de deux sections, dont la première décrit en français le travail accompli pour concevoir un système de management du risque de piraterie basé sur les potentiels des réseaux bayésiens; la seconde livrant l'article tel que publié en langue anglaise par la revue.

Le chapitre 3 est lui aussi composé de deux sections. La première décrit en français le travail réalisé afin de démontrer l'adaptation à chaque type d'attaque de la planification générée par le système conçu. La seconde livre l'article tel que publié dans la revue « *Safety Science*³ ».

Les résultats obtenues dans les chapitres 2 et 3 ont permis la construction d'un réseau bayésien « statique » pour le management du risque de piraterie contre les champs pétroliers et a permis de discuter des résultats acquis au plan tant méthodologique qu'opérationnel.

Le chapitre 4 présente l'article soumis à la revue « *International Journal of Critical Infrastructure Protection*⁴ » qui propose un système de management du risque de piraterie basé sur les réseaux bayésiens dits « dynamiques ».

Enfin, le chapitre 5 décrit le couplage entre le réseau bayésien « statique » et le réseau bayésien « dynamique ». Les résultats sont présentés dans le cadre d'un article soumis à la revue « *Ocean Engineering*⁵ ».

Les chapitres 4 et 5 sont composés de deux sections comme les précédents.

² http://www.ursi.org/en/publications_rsb.asp

³ <http://www.journals.elsevier.com/safety-science/>

⁴ <http://www.journals.elsevier.com/international-journal-of-critical-infrastructure-protection/>

⁵ <http://www.journals.elsevier.com/ocean-engineering/>

Le chapitre 6 synthétise en français l'intégralité du travail effectué pendant cette thèse. Nous avons présenté le contexte général, le modèle conçu basé sur les réseaux bayésiens statiques, le modèle final basé sur les réseaux bayésiens dynamiques et enfin le couplage entre réseaux bayésiens statiques et réseaux bayésiens dynamiques.

Le manuscrit se termine par une conclusion qui pose le bilan de ce travail, met en avant les principales contributions et présente des perspectives de recherche.

MCours.com