Ecole Supérieure de Navigation

HOGERE ZEEVAARTSCHOOL ANTWERPEN

La sécurité maritime mondiale au 21ème siècle :

Un focus sur la piraterie et la cyberpiraterie, leur évolution et leur endiguement

Jorys Reubrecht

Mémoire présenté
Pour l'obtention du titre de
Master en Sciences Nautiques

Promoteur : Capitaine Guido Delvaux
Co-promoteur : Madame Anne-Pascal Mornard
Année académique 2021–2022

Avant-propos

La sécurité maritime est un sujet très vaste et très intéressant.

J'ai décidé d'étudier ce qui me semble être les deux plus grands acteurs de l'insécurité maritime, soit la piraterie et la cyberpiraterie.

Plus particulièrement la piraterie dans le Golfe de Guinée car elle se trouve en pleine évolution et touche également l'intégralité de l'industrie maritime.

En qualité de futur officier de la marine marchande, cette réalité m'interpelle et le sujet m'interroge. C'est la raison pour laquelle j'ai souhaité décrypter et analyser ses origines, son développement et les moyens mis en œuvre pour la combattre dans cette zone du monde.

Je ne pense pas que la piraterie sera un jour totalement éradiquée, cependant, pour la combattre il faut en comprendre les causes racines.

Depuis quelques années maintenant, l'industrie maritime constate également, à ses dépens, l'importance et la progression de la cybersécurité dans son milieu.

Dans le cadre de ce travail, je tiens à remercier mon promoteur Capitaine G. Delvaux ainsi que mon co-promoteur Madame A.P. Mornard, pour leurs conseils et relectures au cours de l'année. Également S. Reubrecht pour ses relectures et son aide, ainsi que R. et S. Charmont pour leurs points de vue critiques.

Résumé

En qualité de futur officier, la sécurité maritime est un sujet qui me préoccupe tout particulièrement.

Quelles sont les causes de l'insécurité maritime au 21ème siècle et quels sont les principaux moyens mis en œuvre pour la combattre ? Comment la piraterie se développe et pourquoi le monde ne trouve pas de solutions durables ? En quoi la cybersécurité représente les enjeux de demain ?

Les données, rapports et articles que j'ai consultés et rassemblés ainsi que les témoignages de certains professionnels m'ont permis de comprendre le point de vue des populations atteintes par ce fléau et également que le phénomène de la piraterie est la résultante d'années de misère économique et sociale ainsi que de dissensions politique.

L'augmentation de la présence militaire est un premier pas admirable. Cependant une approche qui traite les causes plutôt que les conséquences de la piraterie, aurait un effet plus durable.

L'industrie maritime est également une cible parfaite pour les cybercriminels. La disruption des entreprises de transport peut-être d'une grande valeur pour certains criminels. Les navires et leurs systèmes connectés sont également des cibles faciles pour les pirates.

Les mesures prises pour contrer la cyberpiraterie dans le secteur maritime sont nouvelles pour la plupart. Mais c'est l'éducation du personnel maritime qui jouera le plus grand rôle dans le combat contre la cybercriminalité.

Abstract

As a future officer, maritime safety is a subject of particular concern to me.

What are the causes of maritime insecurity in the 21st century and what are the main means implemented to combat it? How does piracy grow and why can't the world find lasting solutions? How does cybersecurity represent the challenges of tomorrow?

The data, reports and articles consulted in combination with the information collected by certain professionals have enabled me to understand the point of view of the populations touched by this scourge.

My research has enabled me to understand that the phenomenon of piracy arises from years of economic and social misery as well as political dissension.

The increased military presence is an admirable first step. However, an approach that addresses the causes rather than the consequences of piracy would have a more lasting effect.

The shipping industry is also a perfect target for cybercriminals. Disrupting transportation companies can be of great value to some criminals. Ships and their connected systems are also easy targets for pirates.

The measures taken to counter cyberpiracy in the maritime sector are for the most part new, but it is the education of maritime personnel that plays the biggest role in the fight against cybercrime.

Table des matières

Liste des figures

Liste des abréviations

AIS : Automatic Identification System

ARPA : Automatic Radar Plotting Aid

BIMCO : Baltic and International Maritime Conference

BMP WA : Best Management Practice West Africa

CCTV : Close Circuit Television

CSO : Company Security Officer

DGNSS : Differential Global Navigation Satellite System

ECCAS : Economic Community of Central African States

ECDIS : Electronic Chart Display and Information System

ECOWAS : Economic Community of West African States

ENISA : European Network and Information Security Agency

EUROPOL : European Police Office

FMI : Fonds Monétaire International

FPSO : Floating Production Storage and Offloading

GGC : Gulf of Guinea Commission

GIGN : Groupe d'Intervention de la Gendarmerie Nationale

GISIS : Global Integrated Shipping Information System

GMDSS : Global Maritime Distress System

GNSS : Global Navigation Satellite System

GPS : Global Positioning System

H&M Insurance : Hull and Machinery Insurance

IACS: International Association of Classification Societies

IBS : Integrated Bridge System

ICC : International Chamber of Commerce

ICS : International Chamber of Shipping

IDH : Indice de Développement Humain

IGP&I Clubs : International Group of Protection and Indemnity Clubs

IMB : International Maritime Bureau

INTERPOL : International police

ISC : Information Sharing Centre

ISPS : International Ship and Port Facility Security Code

IT : Information Technology

LRAD : Long-Range Acoustic Device

MDAT-GoG : Maritime Domain Awareness for Trade - Gulf of Guinea

MEND : Movement for the Emancipation of the Niger Delta

MODU : Mobile Offshore Drilling Unit

MRU : Motion Reference Unit

MSC : Maritime Security Council

MSRF : Maritime Security and Response Flotilla

NAS : Network Attached Storage

OCIMF : Oil Companies International Marine Forum

OMI : Organisation Maritime Internationale (IMO)

ONU : Organisation des Nations Unies

OPEP : Organisation des Pays Exportateurs de Pétrole

OT : Operational Technology

OTAN : Organisation du Traité de l'Atlantique Nord

P&I Insurance : Protection and Indemnity Insurance

PIB : Produit Interieur Brut

PRC : Piracy Reporting Centre

PRS : Position Reference System

RADAR : Radio Detection And Ranging

ReCAAP : Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia

RPG : Rocket Propelled Grenade

SATCOM : Satellite Communication

SEV : Security Escort Vessels

SOMS : Straits of Malacca and Singapore

SSA : Ship Security Assessment

SSA : Secure Anchorage Area

SSAS : Ship Security Alert System

SSP : Ship Security Plan

STS : Ship To Ship

UKHO : United Kingdom Hydrographic Office

UNCLOS : United Nations Convention on the Law of the Sea

UNODC : United Nations Office on Drugs and Crime

UNSC : United Nations Security Council

VHF : Very High Frequency

VHP : Vessel Hardening Plan

VLAN : Virtual Local Area Network

VPD : Vessel Protection Detachment

VPN : Virtual Private Network

VRA : Voluntary Reporting Area

YAMS : Yaounde Architecture for Maritime Security and Safety

Introduction

Le monde maritime connait une insécurité grandissante depuis ces dernières décennies.

La piraterie moderne révèle une alarmante croissance depuis la fin du 20ème siècle. L'OMI et l'ONU sont les premières organisations à nous avoir alerté sur le sujet.

Aujourd'hui, comme par le passé, les pays en voie de développement sont les plus touchés. Malgré une large médiatisation des actes de piraterie somalienne au large de la Corne de l'Afrique au début des années 2010, le sujet reste encore largement méconnu tant du grand public que de certains professionnels de la mer.

Certes, la piraterie est aussi vieille que la navigation elle-même. Cependant, la fin du 20ème siècle et le début du 21ème siècle sont marqués par une augmentation très importante du nombre d'incidents de piraterie et de brigandage. Les principaux foyers de piraterie dans le monde sont l'Afrique de l'Est, l'Afrique de l'Ouest, l'Asie du Sud-Est ainsi que les Amériques. Ces régions ont de nombreux points communs ; économie fragile, inégalités sociales, dissensions politiques et insécurité latente.

Le 21e siècle a également connu des enjeux concernant la cybersécurité. Le monde maritime, soufrant de son éternel retard technologique, fait les frais de ces cyberattaques. Les navires restent à ce jour des proies faciles pour les cybercriminels.

Ce travail a pour but d'étudier les enjeux de la sécurité maritime au 21ème siècle, en deux parties.

Dans la première partie nous analyseront les causes et conséquences de la piraterie moderne dans le monde et les différentes régions touchées. Nous verrons comment la piraterie se développe et pourquoi le monde ne trouve-t-il pas de solution durable.

Dans un premier temps, nous verrons comment la piraterie s'est développée en Somalie au début des années 2010. Son mode opératoire particulièrement violent qui mettait en péril la vie de tous les marins naviguant dans cette région. Avant qu'elle ne soit maîtrisée par les efforts conjoints de différentes puissances.

Dans un deuxième temps, nous analyserons en détails le cas du Golfe de Guinée, aujourd'hui le point chaud de la piraterie mondiale, avec des attaques toujours plus violentes qui reprennent en partie le mode opératoire somalien. Cette région est très représentative de la piraterie au 21ème siècle. Nous étudierons alors la géopolitique des pays du Golfe de Guinée et plus particulièrement du Nigeria afin d'apporter une vision plus claire et compréhensible quant aux causes de la piraterie dans cette région. Nous observerons l'évolution des modes opératoires des pirates. Cette mutation et les méthodes des auteurs de ces incidents permettrons de mettre en exergue l'impact de la piraterie sur le commerce maritime. Pour clore cette étude de cas, nous observerons quelles sont les différentes mesures prises pour lutter contre ce fléau dans le Golfe de Guinée.

Dans un troisième temps, nous verrons comment les pirates opèrent en Asie du Sud-Est, la deuxième région la plus active en termes de piraterie. Comment les organisations internationales ont réussi à éradiquer la menace dans le détroit de Malacca, et comment cette dernière s'est insidieusement glissée vers le détroit de Singapour.

Finalement nous observerons comment l'Amérique du Sud et l'Amérique Centrale font face aux risques de piraterie, et comment ces incidents pourraient être reliés au crime organisé d'Amérique latine.

Dans la seconde partie, nous nous pencherons sur l'analyse des enjeux de la cybersécurité dans le contexte maritime du 21ème siècle. Nous verrons en quoi la cyberpiraterie représente un danger pour la sécurité maritime.

Dans un premier temps, nous verrons qui sont les cybercriminels et de quels moyens ils disposent pour perturber l'industrie maritime. Nous analyserons les conséquences potentielles des cyberattaques à bord et au sein-même des entreprises à travers le prisme de plusieurs études de cas.

Nous verrons également comment la sécurité des navires autonomes pourrait être grandement impactée par ce genre d'incidents.

Puis nous verrons quels sont les moyens mis en œuvre pour se protéger et lutter contre la cyberpiraterie.

Pour clore cette partie, nous démontrerons dans une dernière étude de cas que le danger de ces attaques vient aussi de la facilité d'accès aux outils de piratage.

Les ressources proviennent d'organisations, de journaux référents et reconnus, de rapports et ouvrages. Les données dynamiques ont été vérifiées à plusieurs reprises au cours de la rédaction de ce travail. On peut noter que l'obtention d'informations n'est pas toujours aisée, spécialement lors des recherches sur la piraterie. Les données en provenance des états concernés sont rares. Ceci est sûrement dû au fait des dissensions politiques et de la communication difficile entre agences régionales et internationales. Il en est de même pour les entreprises maritimes qui préfèrent éviter d'ébruiter les incidents les concernant. Ce travail a pu cependant être bonifié grâce au témoignage d'un membre de l'US Navy concernant la lutte contre la piraterie somalienne. Ainsi qu'avec les informations fournies par le Capitaine W. Justers concernant les assurances maritimes.

Partie I : La piraterie

CHAPITRE 1 : La piraterie en général

1.1 L'histoire de la piraterie

C'est dans l'antiquité classique que nous remonterons, pour trouver l'origine de la piraterie, apparue avec la navigation elle-même. Réputés pour leurs actes de piraterie, les Phéniciens ou Tyrrhéniens agissaient déjà en ce sens. L'Odyssée d'Homère, au 8ème siècle avant J.C. y fait déjà référence.

En mer méditerranée, la piraterie s'est rapidement heurtée aux civilisations grecques et romaine, qui fortes d'un commerce déjà florissant, se sont dressées contre ces flibustiers afin de protéger leurs marchés.

Encouragé par la découverte des Amériques et d'une route maritime entre l'Europe et les Indes, l'âge d'or de la piraterie atteint un premier pic entre le 17ème et le 18ème siècle. Loin des terres, remplis de richesses et peu protégés, ces navires devenaient des proies attrayantes parfois rentables. De quoi susciter quelques vocations pour certains hommes de l'époque. Utopie pour certains, dystopie pour d'autres.

Aujourd'hui, « Queen Anne's Revenge » et autres « Hollandais volant » ont laissé place à des vedettes rapides. Les assaillants ont abandonné leurs sabres et pistolets à silex pour s'armer de fusils d'assaut. Les pirates des temps modernes sont tout autant violents que leurs prédécesseurs. Menaçant, blessant, séquestrant, tuant l'équipage des navires qui ont eu la malchance de croiser leur route.

1.2 La piraterie d'un point de vue légal

De façon générale, une distinction est faite entre actes de piraterie et de brigandage.

La Convention des Nations Unies sur le Droit de la Mer (**UNCLOS**), entré en vigueur en 1994, définit la piraterie par ses actes situés en haute mer et à des fins privées. En limitant sa définition aux termes « haute mer » et « privé » l'UNCLOS exclu les actes de brigandage et de terrorisme.

Selon les ressources, les données peuvent variées. En effet, certaines organisations internationales, telle l'Organisation Maritime Internationale (**OMI**), distinguent dans leurs

études, « piraterie » et « acte de brigandage ». Tout autant illicite, ce dernier est commis dans les eaux intérieures, archipélagiques ou mers territoriales.

Le Bureau Maritime International (**IMB**), lui, ne fait pas de distinction dans ses rapports trimestriels et annuels entre les actes de « piraterie » et de « brigandage ».

Définition de la piraterie[1]

On entend par piraterie 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 État ;
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 points 1 a) ou b) ou commis dans l'intention de les faciliter.

Définition du brigandage[2]

(a) Tout acte illicite de violence ou détention ou acte de déprédation ou menace de celui-ci, autre qu'un acte de piraterie, commit à des fins privés et dirigé contre un navire ou une personne ou propriété à bord d'un tel navire dans la limite des eaux intérieures d'un état, eaux archipélagiques et mer territoriale ;
(b) Tout acte incitant ou facilitant intentionnellement un acte décris ci-dessus.

Par abus de langage, le terme « acte de piraterie » pourra-être utilisé pour définir un « acte de brigandage », ou un « vol à main armée ».

Selon certains spécialistes du droit, la piraterie pourrait aussi être incluse dans la définition de crime contre l'humanité, comme caractérisé dans le Statut de Rome[3]. Etant un crime qui affecte l'humanité entière par ses conséquences, économiques entre autres.

[1] ONU, Convention des Nations unies sur le droit de la mer
[2] OMI, Code of Practice for the investigation of crimes of piracy and armed robbery against ships A.1025
[3] S.J. Pertuet, The challenges of criminalising piracy & armed robbery at sea under International Criminal Law

1.3 Qui comptabilise les incidents ?

Plusieurs organisations internationales publient régulièrement des rapports des activités de piraterie et de vols à main armée en mer. Notamment l'IMB, qui est une branche de la Chambre de Commerce Internationale (**ICC**) établi en 1981. En 1992 l'IMB contribuera à l'ouverture du *Piracy Reporting Centre* (**PRC**) à Kuala Lumpur, suite à l'augmentation des incidents en Asie du Sud-Est. Le PRC a l'avantage d'être un service gratuit indépendant de la juridiction d'un état en particulier et fournit aux navires un lieu de rapport international.

L'OMI rassemble les données avec leur module sur la piraterie et les vols à main armée du *Global Integrated Shipping Information System* (**GISIS**) et agit en collaboration avec l'IMB.

Indépendamment de l'IMB, l'état de Singapour sponsorise la création de l'*Information Sharing Centre* (**ISC**) en 2006, avec l'aide du *Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia* (**ReCAAP**). Ce centre fournis des rapports beaucoup plus complet que l'IMB mais ne comptabilise cependant que les incidents s'étant déroulés dans l'Asie du Sud-Est.

1.4 Compilation par l'IMB PRC

Les données présentes dans la suite de ce travail seront essentiellement en provenance des rapports annuels de l'IMB, nous verrons donc comment l'agence classe les différents incidents.

Par type :

- Abordé : lorsque les assaillants gagnent l'accès au navire.
- Détourné : lorsque les assaillants gagnent l'accès au navire et prennent le contrôle du navire à l'équipage.
- *Fired upon* : lorsque les assaillants utilisent des armes contre un navire en essayant de gagner l'accès au navire.
- *Attempted* : lorsque les assaillants approchent le navire avec l'intention apparente de l'aborder, dont l'attaque reste infructueuse dû à l'action de l'équipage.

Par conséquence :

- Equipage : lorsque le personnel est ; kidnappé, pris en otage, tué, menacé, agressé, blessé ou disparu.
- Navire : particulièrement lorsque le navire a été la cible d'armes à feu, ou lorsque les assaillants endommagent délibérément les équipements à bord.
- Cargaison : lorsque la marchandise à bord est volée ou endommagée.

Les incidents sont également classés par sévérité, de niveau 1 à 3. Le niveau de sévérité 1 étant le plus grave et le niveau 3 le moins grave. Ainsi que le type d'arme utilisé lors de l'attaque.

L'IMB récolte également les informations comprenant le type de navire attaqué, leur pavillon ainsi que la nationalité de leur armateur.

La dernière catégorie de classification est la localisation géographique des incidents, information élémentaire lorsqu'il s'agit de déterminer quelle région est dangereuse à la navigation (se référer à l'Annexe 1). L'IMB classe les attaques par pays, ou par région géographique, comme le Golfe d'Aden, ou le détroit de Singapour. Il est relativement aisé de classer ces informations lorsque les attaques se déroulent dans les eaux territoriales des états, cependant certains incidents se déroulent en haute mer, et ce faisant, hors de la juridiction de quelconque état. Ces incidents sont donc généralement attribués par extension, à l'état dont la Zone Economique Exclusive est la plus proche.

Aussi, l'Asie du Sud-Est étant composée d'archipels et d'îlots sous la juridiction d'états différents, il peut être difficile d'attribuer un incident à un état ou un territoire en particulier. L'Indonésie en particulier, comprenant plus de 13 000 îles[4]. Même si les délimitations des eaux territoriales et de la Zone Economique Exclusive sont définies par la Convention sur le Droit de la Mer de 1982, il existe encore des disputes entre l'Indonésie et ses voisins concernant quelques territoires[5].

[4] CIA, Indonésie
[5] Reuters, Indonesia says could also take China to court over South China Sea

1.5 L'imperfection des données

L'IMB n'est pas le seul à éditer des rapports sur la piraterie. Plusieurs organisations recensent également les données. Toutefois, ces différentes instances ne sont pas toutes d'accord sur leur validité. Selon certains observants, les données de l'IMB seraient à revoir à la hausse[6]. En effet chaque incident signalé entre dans un processus de vérification complexe qui peut parfois ignorer, volontairement ou non, quelques incidents.

On voit notamment la limitation de l'IMB lorsque l'on compare les données fournies lors de leurs rapports annuels, à ceux fournis par l'ISC, dans l'Asie du Sud-Est. En 2021, l'ISC rapportait 82 incidents dans la région[7], alors que l'IMB en rapportait seulement 56[8].

Aussi, la présence du PRC et de l'ISC en Asie du Sud-Est dû à l'émergence de la piraterie dans la région, mène surement à la surreprésentation du problème dans la région, et la sous-représentation dans les autres zones de piraterie au début de leur mise en place[9].

Également, certains pirates misent sur la furtivité pour mener à bien leurs raids, cela signifie qu'une opération réussie ne sera sans doute jamais notifiée. Le détective Karsten Von Hösslin, après avoir infiltré un réseau de piraterie dans l'Asie du Sud-Est, affirmait qu'une majeure partie de ces incidents ne seront jamais rapportés aux institutions[10]. C'est aussi le discours tenu par Peter Gwin, journaliste pour National Geographic[11]. L'IMB elle-même suggère que seulement deux tiers des incidents leur sont rapportés[12].

Les entreprises elles-mêmes peuvent refuser de communiquer ces informations par crainte de subir une augmentation de leurs primes d'assurance. Les navires attaqués par des pirates sont souvent arrêtés par les autorités pour inspection, faisant perdre aux compagnies de précieuses heures, voire jours. Les états dans lesquels les incidents se déroulent pourraient également craindre une mauvaise publicité[13]. Ou bien des individus pourraient être infiltrés à l'intérieur des organisations afin d'empêcher la divulgation de telles informations qui pourraient causer du tort aux réseaux criminels.

[6] S.Bateman, Safety and security in the Malacca and Singapore Straits
[7] ISC, Piracy and Armed Robbery against Ships in Asia Annual Report 2022
[8] ICC-IMB, 2021 Annual IMB Piracy Report
[9] M. Murphy, Small boats, weak states, dirty money
[10] R. Spiess, Black Spots
[11] P. Gwin, Writer Tracks Modern-Day Pirates in Malaysia
[12] M. Murphy, Small boats, weak states, dirty money
[13] M. Murphy, Small boats, weak states, dirty money

Les compagnies maritimes victimes d'attaques de pirates sont très reluctantes à discuter de leurs informations. Nous avons essayé de contacter plusieurs entreprises de transport maritime à ce sujet, mais sans réponse.

Bien que les chiffres rapportés par les organisations internationales soient sûrement à revoir à la hausse, nous utiliserons ici uniquement les données officielles pour analyser la situation.

1.6 Les différentes régions touchées par la piraterie

La piraterie dans l'ère moderne est souvent représentée avec la Somalie, cependant, l'Afrique de l'Est n'a pas été la seule région touchée durant le 21^{e} siècle. L'Afrique de l'Ouest, l'Asie du Sud-Est, l'Amérique du Sud et Centrale connaissent depuis quelques dizaines d'années une recrudescence du nombre d'acte piraterie ou de vol à main armée dans leurs eaux. Ces régions ont de nombreuses similarités ; instabilité politique, économie incertaine, inégalités sociales… Mais elles possèdent toutes leur propre piraterie avec de caractéristiques bien précises.

CHAPITRE 2 : La Somalie

La Somalie représente très certainement la première image qui apparait au grand public lorsque l'on parle de la piraterie au 21e siècle. Les médias ont énormément couvert le sujet dans cette région lors des pics d'incidents au début des années 2010. Indirectement, l'industrie hollywoodienne du cinéma s'est emparée du sujet, quand elle a retracé dans le film « Captain Phillips » en 2013, l'abordage et la prise d'otages du *Maersk Alabama* au large des côtes somaliennes. On peut dire que les pirates ont été mis à l'affiche à cette occasion.

2.1 Géopolitique de la Somalie

Situé entre l'Océan Pacifique et l'Océan Atlantique, l'Océan Indien est un lieu riche d'activités maritimes.

Grande comme deux fois la France, avec ses 638 000 kilomètres carrés[14], la Somalie, pays de la Corne de l'Afrique, offre une des routes maritimes les plus fréquentées au monde. Du golfe d'Aden au nord jusqu'à l'Océan Indien au sud. Ce pays, marqué par les colonisations, est l'un des plus pauvres au monde avec un **PIB** par habitant estimé à 277 $ en 2020[15]. Cette situation résulte pour une bonne part de l'histoire mouvementée de ce pays, en proie aux guerres civiles et une quasi-inexistence de richesses intrinsèques, avec cependant, des eaux somaliennes très poissonneuses.

2.2 La piraterie en Somalie

La piraterie dans les eaux somaliennes a émergé à la suite de l'effondrement du gouvernement somalien de Siad Barre en 1991, conclusion de la guerre civile en Somalie, entrainant notamment une inflation énorme de la monnaie somalienne. La Somalie étant un état côtier et peu arable, la population était obligée de pêcher pour se nourrir. Mais sans gouvernement, la marine somalienne n'était plus là pour protéger les eaux territoriales, laissant le champ libre aux pêcheurs venus de l'Est pour attraper les réserves somaliennes. La quantité de nourriture apportée par la pêche devenait bien trop faible pour survivre. Les populations locales, privées de leurs ressources, ont soumis les pêcheurs étrangers à ce qu'ils

[14] Macro Trends, Somalia Surface Area 1961-2022
[15] Trading Economics, Somalia GDP per capita

appelaient des « taxes ». À savoir le vol de leur cargaison ou de leurs effets personnels. Celles-ci seront très vite perçues comme des actes de brigandage et de piraterie, à commencer dans le début des années 1990. De plus en plus loin des côtes, les pirates se développent rapidement, attaquant des navires de plus en plus gros. Comme lors la prise du tristement célèbre Maersk Alabama en 2009, à une distance de 240 miles nautiques des terres. C'est en 2010 avec quelque 445 incidents recensés dont 217 attribués aux pirates Somaliens[16], que les actes ont connu un pic. Cette même année, on estimait que 0,02% de la population somalienne faisait partie de groupes engagés dans la piraterie[17]. Ces groupes répondant aux ordres d'un petit nombre de seigneurs de guerre locaux[18].

2.2.1 Modus Operandi

Les pirates sévissant au large de la Corne de l'Afrique ont rapidement adopté un mode opératoire qui leur est propre.

Ils ciblent d'abord un navire de la marine marchande qui navigue près des côtes, avant d'en prendre le contrôle et de le transformer en vaisseau-mère. Navire qui servira de centre d'opérations aux pirates et depuis lequel ils pourront lancer davantage d'attaques, toujours plus loin des côtes.

Les équipages sont généralement pris en otage puis ramené à terre, où ils seront détenus dans des conditions de vie effroyables avant de les échanger contre une rançon.

En 2011, 3863 marins furent agressés par des pirate, 968 d'entre eux ont été en contact rapproché avec les assaillants à bord de leur navire. 1206 personnes étaient détenues par des groupes pirates, incluant 555 marins pris en otage en 2011 et 645 marins capturés en 2010 ou avant, dont plusieurs dizaines d'entre eux étaient retenu en otage depuis plusieurs années. On nota également le décès de 35 otages, dont la majorité perdirent la vie lors d'opérations de sauvetage visant à les sauver[19]. La durée moyenne de détention des marins était de 316 jours[20].

Pendant leur séquestration, 10% des victimes furent sujets à des actes de torture. Comme être laissé attaché sous le soleil pendant plusieurs heures, enfermé dans une pièce réfrigérée,

[16] ICC-IMB, 2011 Annual Piracy Report
[17] One Earth Future, The Human Cost of Somali Piracy 2011
[18] M. Murphy, Small boats, weak states, dirty money
[19] One Earth Future, The Human Cost of Somali Piracy 2011
[20] One Earth Future, The Human Cost of Somali Piracy 2011

ou même se faire arracher les ongles. La quasi-totalité des otages furent victime de violences psychologiques et certains d'entre eux nécessitent encore à ce jour une attention médicale[21].

2.2.1.1 La demande de rançon comme business model

En 2010, on déterminait que la totalité des rançons payées aux pirates pour libérer des marins, pour cette année-là, approchait 238 millions de dollars. La valeur moyenne d'une rançon étant de plus de 5 millions de dollars. L'année suivante a connu une diminution, on estime le nombre de rançons payées à 31, avec un total de près de 160 millions de dollars et une moyenne de 5 millions de dollars par rançon. En 2012, les chiffres chutaient encore pour atteindre un total de 32 millions de dollars avec une moyenne de 4 millions de dollars[22]. Les Nations Unies estiment entre 300 et 400 millions de dollars la totalité des rançons payées à des groupes de pirates somaliens entre 2005 et 2012. Avec 179 navires détournés sur la même période. Des rançons furent payées pour 152 d'entre eux, soit un taux de « réussite » de 85%[23].

RANSOMS PAID IN 2012					
Ship Name	Date Hijacked	Date Released	Days Held	Ship Type	Ransom Amount (millions)[12]
Free Goddess	February 7, 2012	October 11, 2012	247	Bulk Carrier	$5.7
M/T Liquid Velvet	October 31, 2011	June 5, 2012	218	Chemical Tanker	$4
MV Olib G	September 8, 2010	January 8, 2012	487	Chemical Tanker	$3
MT Fairchem Bogey	September 20, 2011	January 12, 2012	114	Oil/Chemical Tanker	$8
MT Enrico Ievoli	December 27, 2011	April 23, 2012	118	Oil/Chemical Tanker	$9
Leila	February 15, 2012	April 11, 2012	56	Roll on, Roll off (RO/RO)	$.25
Albedo	November 25, 2010	July 31, 2012	614	Container Ship	$1.2
Orna	December 15, 2010	October 19, 2012	674	Bulk Carrier	$.6
				TOTAL	$31.75

Figure 1 Rançons payées aux pirates somaliens en 2012
Source : One Earth Future (2013)

Cependant, le paiement des rançons ne représente seulement que 1% des coûts économiques totaux de la piraterie à cette époque. Les dépenses liées à l'emploi de gardes armés, aux opérations militaires et à la consommation accrue de carburant représentant plus de 75% des dépenses à elles trois[24].

Certains pays, comme les Etats-Unis, sont connus pour leur politique très stricte lorsqu'il touche aux prises d'otages et la demande de rançons. Ils « ne négocient pas avec les

[21] One Earth Future, The Human Cost of Somali Piracy 2011
[22] One Earth Future, The Human Cost of Somali Piracy 2011
[23] CyberKeel, Virtual pirates at large on the cyber seas
[24] One Earth Future, The Economic Cost of Somali Piracy 2012

terroristes ». C'est, selon la large majorité des experts, la meilleure façon de réduire le nombre de demandes de rançons. Cependant, arrêter de payer des rançons n'est pas aussi simple. D'un côté, les armateurs ne souhaitent pas nourrir un cycle de prises d'otages rentables. Malgré cela, ils doivent faire tout ce qui est en leur pouvoir pour réduire le coût humain de ces incidents en s'assurant de la libération des marins.

Le rançonnage est ultimement la fonction de la réussite des précédentes prises d'otages. L'argent reçu par les pirates ne les encourage pas seulement à continuer de perpétrer leurs attaques, mais leur permet également d'investir dans de meilleurs équipements pour faciliter de futures prises d'otages. Il faut donc adopter une politique stricte de non-négociation pour rendre cette activité non-profitable[25].

2.2.1.2 La prise d'otages du Ponant

On peut, durant cette période, noter le détournement du Ponant, du 4 au 11 avril 2008 dans le Golfe d'Aden, au large du Puntland.

Prise d'otages survenue le 4 avril 2008, dans le Golfe d'Aden, contre le Ponant, un navire de croisière voilier battant pavillon français, avec à son bord trente personnes, dont 22 Français, six Philippins, une Ukrainienne et un Camerounais.

Le capitaine, Patrick Marchesseau, navigue tous feux éteints et **AIS** coupé depuis plusieurs nuits. Mais en plein jour, une douzaine de pirates somaliens, armés de fusils d'assaut et lance-roquettes, attaquent le voilier qui se rendait en Mer Méditerranée. Dû à l'usage inefficace de lances à incendie pour repousser l'attaque et face aux tirs des pirates, le capitaine décide de se rendre après avoir diffusé un message de détresse. La marine française qui patrouille dans la zone reçoit l'alerte et les opérations s'enchainent[26]. Un navire des forces canadiennes de la *Combined Task Force 150*[27], engagées dans la lutte contre le terrorisme, dépêche un hélicoptère qui confirme l'attaque. À cet instant[28], aucune rançon n'est exigée et le voilier, aux mains des pirates, fait route vers le sud pour jeter l'ancre le long des côtes somaliennes du Puntland. Le Premier ministre français déclenche immédiatement l'alerte *Pirate-Mer* et l'aviso *Commandant Bouan*[29] reçoit l'ordre de se rendre sur zone en observation car il ne

[25] Raymond, Piracy and Armed Robbery in the Malacca Strait
[26] de La Grange, Le Ponant : l'histoire secrète d'une libération
[27] defense.gouv.fr, TF 150 : Opération commune de sécurité maritime
[28] Le Journal Du Dimanche, Les secrets de l'opération Thalathine
[29] Mer et Marine, Détournement du Ponant : Bateau au mouillage et contact établi avec les pirates

dispose pas de capacité d'intervention. Le navire école *Jeanne d'Arc*, possédant un hôpital embarqué et des hélicoptères, sera également détourné pour se rendre sur place. Les autorités locales accordent à la France le droit de poursuivre les pirates. Le *Commandant Bouan* est chargé de récupérer les dix-huit commandos marine parachutés au large de l'île de Socotra. Les hauts responsables des commandos marine et du Groupe d'Intervention de la Gendarmerie Nationale (**GIGN**) se rendent sur place pour superviser les opérations. Parallèlement, et sous les conseils avisés de spécialistes, l'armateur négocie avec les pirates.

Figure 2 Image tirée de l'Opération Thalathine avec Le Ponant et le Commandant Bouan au large de la côte somalienne Source : youtube.com (2010)

Selon les négociations, décisions et consignes prises en haut lieu[30], une semaine plus tard, les otages sont autorisés à quitter le voilier après le paiement d'une rançon qui aurait été de plus de deux millions de dollars versée par l'assureur[31]. Le capitaine sera retenu le temps pour les pirates de recompter l'argent. C'est une fois tous les passagers du Ponant en sécurité et les pirates en fuite que les armées de terre, mer et air se mettent en action pour les intercepter « sans usage excessif de la force », lors de l'Opération *Thalathine*, selon les recommandations

[30] Le Point, L'histoire secrète du « Ponant »
[31] Le Point, L'histoire secrète du « Ponant »

du Président Nicolas Sarkozy. Une seule balle aura suffi pour stopper la voiture de 6 pirates repéré par un avion espion, qui seront envoyés à Paris pour y être jugés[32].

Cette opération est largement regardée comme étant une démonstration de force de la part de la France. Cependant, il est important de rappeler que plus de la moitié des décès d'otages se déroule pendant les opérations militaires visant à les sauver. Ce fût le cas en 2009 lors de l'opération de sauvetage du voilier français *Tanit*, où Florent Lemaçon, un des otages, décéda des suites d'un tir en provenance des forces françaises[33].

C'est également après cette période que les pirates somaliens commencèrent une vendetta contre la France et les Etats-Unis, qu'ils considèrent responsables pour les opérations militaires en Somalie. En 2009, un pirate reconnaissait au micro de Ross Kemp n'avoir que peu d'intérêt pour rançonner des otages français et américains, mais préfère les exécuter pour faire exemple. « From now on I think that if a French or American national is taken hostage, they won't ask for a ransom. […] They will either give them back or treat them in the same way that their friends were treated »[34].

2.2.2 Les mesures prises

Alarmé par cette augmentation d'incidents, le Conseil de Sécurité des Nations Unies (**UNSC**) adopte depuis 2008 des résolutions pour combattre cette crise. La résolution 1816 en 2008 exprimait l'inquiétude des Nations Unies quant à l'augmentation d'incidents liés à la piraterie et rattachée à la présence de pêcheurs illégaux dans les eaux somaliennes. C'est non sans réaffirmer le respect des Nations Unies pour la souveraineté et l'indépendance politique de la Somalie, qu'elle condamne tout acte de piraterie et de brigandage dans les eaux somaliennes ainsi qu'en haute mer. Elle appelle tous les états à aider les autorités locales et organisations régionales à combattre la piraterie[35].

Avec l'augmentation du budget injecté dans le combat contre la piraterie dans les années qui suivirent et la diminution du nombre d'incidents, le coût « par incident » augmente de 28,6 millions de dollars en 2011 à 82,7 millions de dollars en 2012. Alors que le nombre d'incident chutait de 236 à 75 sur la même période. En 2012, il y avait une présence permanente de 21

[32] Libération, La force et la réactivité des armées
[33] Le Monde, Le skipper du "Tanit" a bien été tué par une balle française
[34] Kemp, Ross Kemp in the Search of Pirates
[35] UNSC, Resolution 1816

à 30 bâtiments militaires dans l'Ouest de l'Océan Indien, patrouillant une surface équivalente à 1,5 fois la surface de l'Europe continentale[36]. Avec l'*Opération Atalante* de l'Union Européenne, de 2008 à 2012, l'*Opération Ocean Shield* de l'Organisation du Traité de l'Atlantique Nord (**OTAN**), de 2009 à 2016 ainsi que la *Combined Task Force 151*, initiée en 2009. Ces opérations militaires, surnommées « big three » auraient couté environ 3 milliards de dollars par an à cette époque[37].

Au regard des chiffres de l'IMB, on peut admettre que les mesures prises par l'UNSC couplées à la présence militaire des États membres ont permis de démanteler le réseau de piraterie en Somalie. Même si la résolution 2554 de 2020 reconnaît « […] that piracy off the coast of Somalia has been repressed but not eradicated […] »[38], elle affirme que des résolutions précédentes, a résulté une baisse des attaques pirates depuis 2011. En effet, quasi inexistantes aujourd'hui, les attaques attribuées aux pirates somaliens représentent 1,49 % du total des attaques entre 2013 et 2021 (soit 27 incidents), quand on enregistrait 45,15 % de 2008 à 2012 (soit 851 incidents)[39].

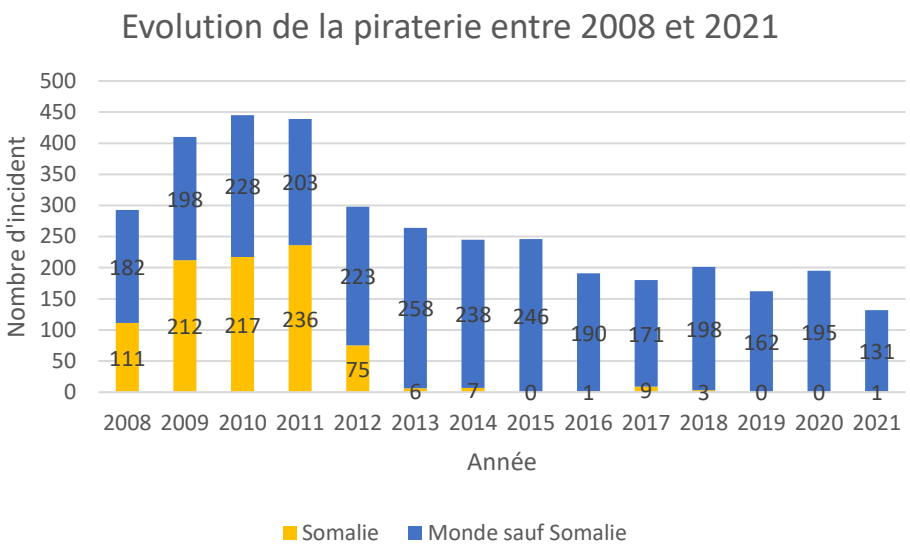

Figure 3 Evolution de la piraterie mondiale entre 2008 et 2021
Source : propre graphique, basé sur les données de l'ICC-IMB (2022)

Cependant, encore en 2019, les otages d'un navire de pêche furent libérés après près de 5 années de détention[40]. Malgré cela, les quelques incidents survenus en Mer Rouge ces

[36] Operation Ocean Shield, Operation Ocean Shield
[37] One Earth Future, The Economic Cost of Somali Piracy 2012
[38] UNSC, Resolution 2554
[39] ICC-IMB, 2020 Annual Piracy Report
[40] Joubert, The State of Maritime Piracy 2019

dernières années sont attribués aux conflits ayant lieu au Moyen-Orient, mais pas reliés à des actes de piraterie ou de brigandage[41].

Les criminels de l'Est de l'Afrique ont su profiter des tensions politiques présentes en Somalie depuis les années 1990 pour développer un réseau de piraterie régional. Ces activités se sont rapidement développées, de petites attaques visant des navires de pêche, jusqu'au détournement et à la prise d'otages d'équipages d'imposants navires de la marine marchande. Les pirates somaliens ont su instaurer un climat de terreur dans les eaux du Golfe d'Aden et de l'Ouest de l'Océan Indien. Cette époque fût une des plus dangereuses pour les marins du monde entier, en travaillant avec le risque constant de kidnapping et de potentiellement rester emprisonné pendant plusieurs centaines de jours.

Cependant, il ne faut pas crier victoire trop tôt, même si la piraterie somalienne est aujourd'hui considérée comme éradiquée, la plupart des moyens mis en œuvre pour lutter ne traitent pas des causes racines du problème. Les solutions impliquant la présence militaire sont efficaces uniquement à court et moyen terme. La Somalie reste un des pays les plus pauvres et dangereux au monde. Il n'est donc pas impossible que la piraterie réémerge dans la région. L'IMB reconnait encore en 2022 que les groupes de pirates somaliens possèdent toujours les capacités leur permettant potentiellement de reprendre leurs activités[42].

[41] Joubert, The State of Maritime Piracy 2019
[42] ICC-IMB, 2021 Annual IMB Piracy Report

CHAPITRE 3 : Etude de cas : Le Golfe de Guinée

La piraterie dans la région du Golfe de Guinée s'est largement développée depuis cette dernière décennie, devenant le nouveau centre mondial de la piraterie dans la fin des années 2010, avec en 2018, plus de 40% des actes de pirateries qui se déroulaient dans le Golfe de Guinée. Le monde maritime voit encore une fois, après la Somalie, une zone géographique affaiblie se tourner vers la violence.

3.1 Géopolitique du Golfe de Guinée

Le Golfe de Guinée est très représentatif des enjeux sociaux, politiques et économiques qui peuvent amener une telle région à devenir le plus grand centre de la piraterie du monde.

3.1.1 La ruée vers l'or noir

Le golfe de Guinée est une région pétrolifère, du delta du Niger jusqu'en Angola. On estimait en 2012 à 38 milliards de barils[43] la quantité de pétrole restante dans ses sols.

L'économie de ces pays est très largement basée sur le commerce du pétrole. En 2018, l'Angola tirait 25,62 % de son PIB du pétrole, et 9,025 % pour le Nigéria[44]. Pourtant, en favorisant l'emploi d'expatriés sur les exploitations pétrolières, les populations locales, elles, sont considérablement lésées et ne peuvent que trop marginalement profiter des emplois générés par les exploitants. Un des problèmes majeurs étant que l'industrie pétrolière a marginalisée les autres secteurs d'activités tels l'agriculture, le commerce et autres industries manufacturières. Si l'on considère également une maintenance défaillante des équipements qui engendre une pollution des sols, des eaux et des airs, on comprend comment ces pays s'enfoncent dans ce cercle vicieux et se raccrochent au secteur pétrolier.

L'Organisation des Pays Exportateurs de Pétrole (**OPEP**) estime que 70 % des recettes publiques et 83 % des recettes d'exportation viennent de l'industrie pétrolière[45]. Cependant, même si cette industrie représente la majeure source des revenus du pays, le secteur reste encore largement sous exploité. Le manque d'investissement couplé à une maintenance

[43] Ademefi Isumonah, Armed Society in the Niger Delta
[44] La Banque Mondiale, Bénéfices tirés du pétrole (% du PIB) - Nigeria, Angola
[45] BNP PARIBAS, Nigéria : Le contexte économique

désastreuse ne permet pas à la région d'exploiter l'industrie pétrolière au maximum de ses capacités.

Une telle dépendance au pétrole fragilise ces pays, chaque choc pétrolier déstabilisant un peu plus leur économie. On note une baisse du prix du pétrole de 2014 à 2016, le prix du baril Brent chutant de 115,680 à 27,080 USD[46].

Figure 4 Prix du pétrole brut Brent en USD de 2005 à 2021
Source : Tradingview.com (données du FXCM) (2021)

On pouvait relever en 2016 un taux de croissance négatif du PIB pour le Nigéria de - 4,168 % et de l'Angola de - 5,816 %[47]. Des données qui parlent d'elles-mêmes et mettent en exergue la corrélation entre le prix du pétrole et l'économie de ces pays, fortement mise à mal à chaque choc pétrolier.

En multipliant les emprunts pour relancer son économie, l'agence de notation financière *Moody's* s'interroge quant aux conséquences de la dette, et les capacités du pays à honorer ses remboursements. Malgré les promesses de diversifier l'économie, faites au Fonds Monétaire International (**FMI**) et à la Banque Mondiale, le Nigéria, pays le plus peuplé d'Afrique, reste encore extrêmement dépendant de l'or noir.

[46] FCXM, CFDs sur Pétrole Brut (Brent)
[47] La Banque Mondiale, Croissance du PIB par habitant (% annuel) - Nigeria, Angola

3.1.2 Des problématiques sociales…

Pays le plus peuplé d'Afrique avec 206 millions d'habitants en 2020[48], le Nigeria affiche un autre triste record. Son taux de chômage de 33,3 %[49] en janvier 2021 dont une augmentation de 6,2 points depuis le premier semestre 2020, le positionne comme un des pays les plus touchés au monde. Depuis 2019, le pays semblait sortir de cette période de récession engendrée par la dernière chute du prix du pétrole en 2016. Cependant, ce rebond paraissait trop faible pour répondre aux besoins d'une population toujours plus nombreuse et un taux de chômage des jeunes approchant les 55 % en 2020[50].

3.1.3 … et politiques

À ces difficultés économiques et sociales, s'ajoutent les dissensions politiques. En effet, le Mouvement pour l'Emancipation du Delta du Niger (**MEND**), groupe armé basé dans le delta du Niger, « dont les actions ciblées contre le secteur pétrolier – sabotage d'infrastructures pour réduire ou paralyser la production, attaques de navires et enlèvements d'employés – visent, selon le MEND, à faire pression sur le gouvernement nigérian »[51]. Même si une amnistie fût signée en 2009 entre eux et le gouvernement nigérian et une grande quantité d'armes fût remise aux autorités, le groupe n'a jamais été démantelé[52]. Les peuples du delta du Niger pâtissent énormément de l'industrie pétrolière, la pollution des eaux ne permet plus aux pêcheurs de vivre de leur activité. Les investisseurs sont étrangers et l'emploi d'expatriés dans les puits de pétroles est largement favorisé au détriment des populations locales.

Fweley Diangitukwa, docteur en science économique et sociale, dénonce l'incapacité des pays à assumer efficacement leurs fonctions régaliennes. Les actes de piraterie maritime font écho à la misère et la paupérisation et signent une révolte contre la corruption des élites locales, les injustices et le désarroi face aux malversations et l'incompétence des dirigeants politiques[53].

[48] Trading Economics, Nigeria - Population
[49] Trading Economics, Taux de chômage - Liste des pays
[50] Trading Economics, Nigeria - Taux de chômage des jeunes
[51] M. Luntumbue, Piraterie et insécurité dans le golfe de Guinée : défis et enjeux d'une gouvernance maritime régionale
[52] Terra Firma, Risk Focus : Kidnap and Ransom
[53] Diangituwka, Terrorisme et piraterie dans le golfe de Guinée : esquisses de solutions

Le *bunkering*, une technique qui consiste à percer les pipe-lines pour détourner les approvisionnements, est une pratique répandue au Nigéria, qui viserait à récupérer ce dont l'État a privé les populations locales.

Militant écologiste, activiste et co-fondateur d'*Environmental Rights Action*, *Les amis de la Terre*, Nnimmo Bassey, déclare, lors d'une interview donnée pour *Afrique Renouveau* en 2014, « le gouvernement doit mettre un terme au vol de pétrole qui n'est pas le fait des habitants des régions concernées, mais d'une mafia internationale qui compte en son sein des nigérians haut placés ». Personnalité reconnue par ses pairs, il affirme « le Nigéria possède autant de pétrole volé que de pétrole officiellement vendu sur le marché »[54]. C'est sans compter ses pertes de matière première amplifiées par un entretien déficient des installations.

Pour ces deux observateurs, les faits de brigandage sont la résultante de pays corrompus qui profitent des soutiens de la manne pétrolière entretenant les élites et appauvrissant toujours plus les populations locales.

Les problématiques économique, sociale et politique montrent combien les populations locales peuvent se sentir délaissées par leurs gouvernements.

La détérioration des ressources halieutiques engendre la paupérisation d'importantes couches de la population. Pour certains, trouver refuge auprès de groupes organisés dans la piraterie, peut sembler une facilité pour tenter de survivre.
Même si les causes fondamentales du développement de la piraterie dans le Golfe de Guinée sont différentes de celles en Somalie, on remarque certains points communs. En effet, l'augmentation des actes de piraterie en Afrique de l'Ouest est majoritairement associée à l'augmentation de l'instabilité dans la région.

3.2 La piraterie dans le Golfe de Guinée

3.2.1 Un successeur à la piraterie Somalienne ?

Même si la piraterie est présente dans le Golfe de Guinée depuis des années, la région est devenue la zone rouge de la piraterie mondiale à la suite de l'extinction de la piraterie somalienne. Cependant c'est autant le nombre d'incidents en augmentation que le mode

[54] Akinbobola, Le Nigeria n'a pas besoin de nouveaux puits de pétrole

opératoire toujours plus violent, semblable à ce qu'on avait pu observer lors de l'épisode de piraterie somalienne, qui inquiète le monde maritime.

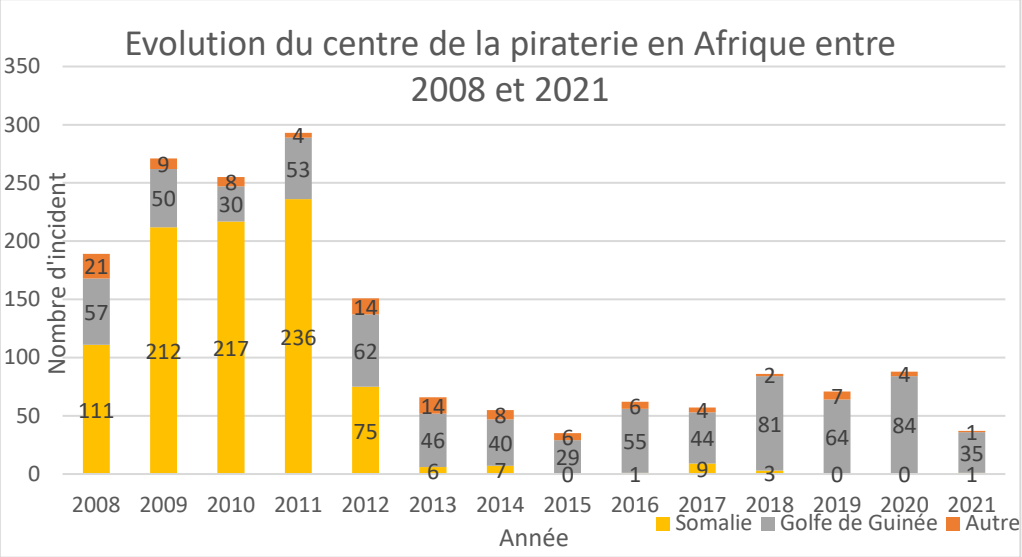

Figure 5 Evolution du centre de la piraterie en Afrique entre 2008 et 2021
Source : propre graphique, basé sur les données de l'IMB (2022)

À l'instar de leurs homologues somaliens, ces pirates opérant dans le Golfe de Guinée, fortement armés, ne craignent pas d'aborder de gros navires à pleine vitesse, et n'ont aucun scrupule à agresser l'équipage.

3.2.2 Un modus operandi différent

Un but identique, s'enrichir… Mais des modes opératoires différents selon les régions du monde.

Alors que les pirates somaliens profitaient de l'absence de forces de l'ordre pour garder les navires détournés près des côtes, leurs homologues à l'Ouest ne peuvent pas profiter de cet état. En effet, bien que l'instabilité grandissante puisse offrir de nombreux avantages aux pirates, elle n'est pas mesurable à celle qu'a pu subir la Somalie.

3.2.2.1 L'industrie du kidnapping

À l'Est comme à l'Ouest, l'objectif premier des pirates est l'obtention de rançons en échange d'otages. Mais si les somaliens cherchaient aussi à s'emparer des navires, dans le Golfe de Guinée, ils misent tout sur la cargaison la plus rentable et la plus légère : son équipage. En effet, en 2020, ce ne sont pas moins de 96 % des enlèvements en mer qui se déroulaient dans

le Golfe de Guinée[55]. Soit 130 membres d'équipage dans 22 différents incidents. Le plus souvent en pleine nuit, les pirates abordent le navire, même en route, avant de maîtriser l'équipage et le ramener à terre. Une « monnaie d'échange », retenue parfois plusieurs mois, dans l'attente des négociations opérées entre ravisseurs et armateurs. Selon certains pirates, la vie humaine est tarifée. Ces groupes armés le savent, les assurances sont en capacité de payer le prix cher. Les rançons pouvant aisément excéder les 200 000 $ pour un marin Français, et encore plus pour un Américain[56]. La valeur d'un otage semble être lié à sa couleur de peau et les kidnappeurs préfèrent capturer les membres d'équipage avec la peau la plus claire[57]. Les assaillants n'hésitent pas non plus à emmener des marins africains, mais les rançons demandées sont généralement plus faibles. On estime en 2021 à 1 million de dollars par an, la valeur des rançons demandées pour des otages africains[58]. Malgré ces estimations, il est difficile de vérifier la valeur des rançons demandées en échange d'otages non-africains car aucune des parties ne souhaite médiatiser cet échange, de par leur nature illégale. Cependant, on peut affirmer que les pirates du Golfe de Guinée demandent des rançons bien plus faible que leurs homologues somaliens lors du pic de la piraterie du début des années 2010.

Les otages sont détenus dans de pauvres conditions de vie pendant généralement trois à quatre semaines, pouvant aller jusqu'à six. Même s'ils ne souffrent que rarement de torture ou de maltraitement délibéré, ils sont parfois frappés et humiliés. La principale menace vient des conditions de détention non-hygiéniques. Les camps d'otages sont généralement situés dans des régions marécageuses, à grande distance des villes et villages. La jungle est très épaisse, le sol boueux. La faune est également dangereuse, on y retrouve multitudes d'insectes porteurs de maladies comme les moustiques, on peut d'ailleurs noter que la Malaria est extrêmement présente sur les côtes ouest-africaines. Un médecin basé dans le Delta du Niger conduisant des tests sur les marins libérés affirmait que 60 à 70% des otages contractait la Malaria lors de leur détention[59]. Les otages « habitent » dans des cabanes insalubres et se partagent parfois un matelas pour coucher. La nourriture est également pauvre, principalement constituée de pâtes et de riz. Le manque d'hygiène couplé à la

[55] ICC-IMB, 2020 Annual Piracy Report
[56] Etevenard et Bassompierre, A l'abordage des pirates du Golfe de Guinée
[57] Terra Firma, Risk Focus : Kidnap and Ransom
[58] Bell, Pirates of the Gulf of Guinea: A Cost Analysis for Coastal States
[59] Terra Firma, Risk Focus : Kidnap and Ransom

malnutrition mène souvent les otages à des inflammations du système digestif pendant leur captivité.

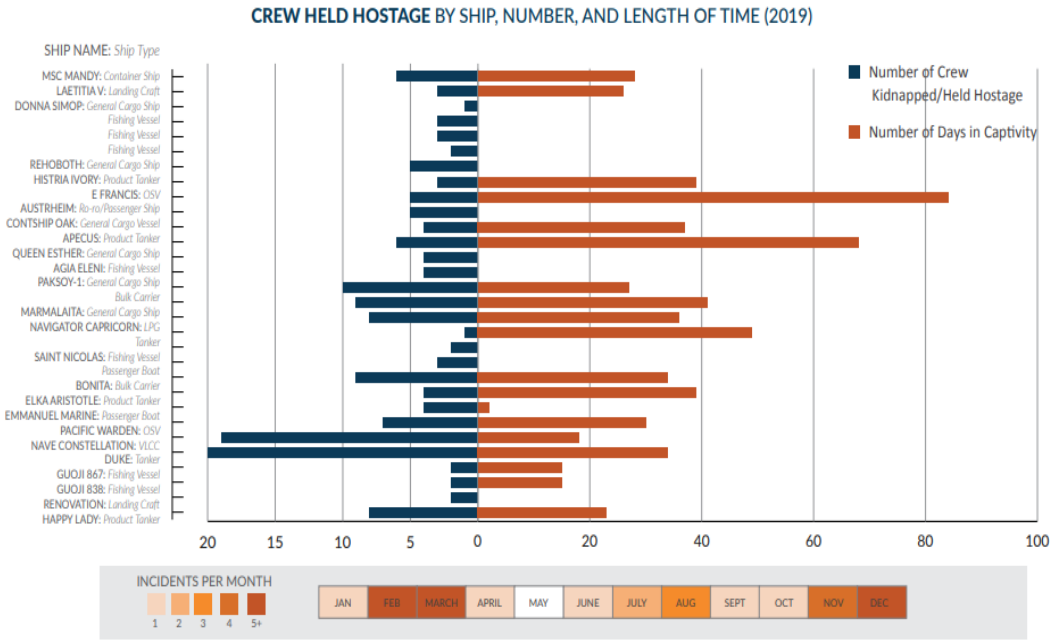

Figure 6 Membres d'équipage retenu en otage en 2019 par navire, nombre et durée
Source : One Earth Future (2020)

Les marins sont généralement capturés pendant les saisons sèches, afin d'éviter les difficultés supplémentaires à garder les otages en bonne santé, résultant des fortes chutes de pluie. Ils préfèreront donc éviter de s'occuper de leurs victimes de fin-mars à fin-juillet, ainsi que de début-septembre à mi-octobre[60].

Heureusement pour les marins, les kidnappeurs savent que la santé des otages est primordiale pour le bon déroulé des opérations de rançonnage. Il n'est pas dans leurs meilleurs intérêts d'affaiblir leurs otages. Les marins survivent, en grande partie, à leur détention. En réalité, un seul décès d'otage fût documenté après le kidnapping de marins dans le Golfe de Guinée. Cependant, les survivants souffriront des dégâts psychologiques pendant toute leur vie et pourraient être atteints de Syndrome de Stress Post-Traumatique, d'anxiété, ou d'autres troubles psychologiques[61].

Les otages ne peuvent pas s'échapper, déjà affaibli par leurs conditions de détention, leur survie dans la jungle est impossible. Des interventions militaires dans les camps d'otages ont déjà été réalisées dans le passé, cependant, elles mettent les victimes dans une situation bien

[60] Terra Firma, Risk Focus : Kidnap and Ransom
[61] Terra Firma, Risk Focus : Kidnap and Ransom

trop dangereuse. En réalité, les ravisseurs ne craignent pas tant les autorités que les groupes de kidnappeurs rivaux, qui pourrait « voler » leurs otages[62].

Une fois la rançon payée, les victimes sont remises à des équipes spécialisées dans la prise en charge d'otages. Elles sont ensuite accompagnées en lieux sûrs pour des examens médicaux, avant de prendre l'avion pour retrouver leur famille.

L'argent est ensuite utilisé par les kidnappeurs pour acheter navires, essence, munitions, ou bien pour corrompre les autorités locales, au moins l'équivalent de 10 000 $ par attaque[63]. Les rançons obtenues sont partagées entre les pirates et leur famille, mais aussi avec les autres personnes faisant partie de la communauté.

Bien que les pirates du Golfe de Guinée utilisent des méthodes similaires à leurs homologues somaliens, ils restent bien moins dangereux pour les marins. Les victimes sont traitées avec plus d'humanité que les otages détenus en Afrique de l'Est. Les kidnappeurs traitent leurs prisonniers comme une « marchandise », qu'il faut bien entretenir afin d'en garder la valeur.

3.2.2.2 Mode opératoire

Très bien préparés, ces pirates sont en mesure de maitriser tout type de navire sans discrimination quant à leur pavillon ou cargaison.

Des vaisseaux mères sillonnent les eaux à la recherche de cibles potentielles, équipés de radar, d'un **GPS** et parfois d'un AIS pour repérer des navires à une grande distance. Les vaisseaux-mères utilisés par ces pirates sont bien loin de la taille de ceux de leurs homologues somaliens, qui eux, n'hésitaient pas à détourner des navires de la marine marchande à cet effet. Ces navires-ci sont au plus souvent de petits navires de pêche arrangés pour cette activité. Ils sont cependant assez imposants pour permettre la présence de vedettes amarrées leur permettant de passer à l'attaque plus rapidement une fois leur cible repérée. Ces dernières sont généralement équipées de puissants moteurs hors-bord leur permettant de suivre les navires les plus rapides. Les moyens grandissants des pirates leur permettent de cibler des victimes toujours plus loin des côtes. Même si la majorité des incidents se déroule toujours près des côtes, comme illustré dans la figure suivante.

[62] Terra Firma, Risk Focus : Kidnap and Ransom
[63] Monnet, Rencontre avec « Black Devil », le pirate du delta du Niger

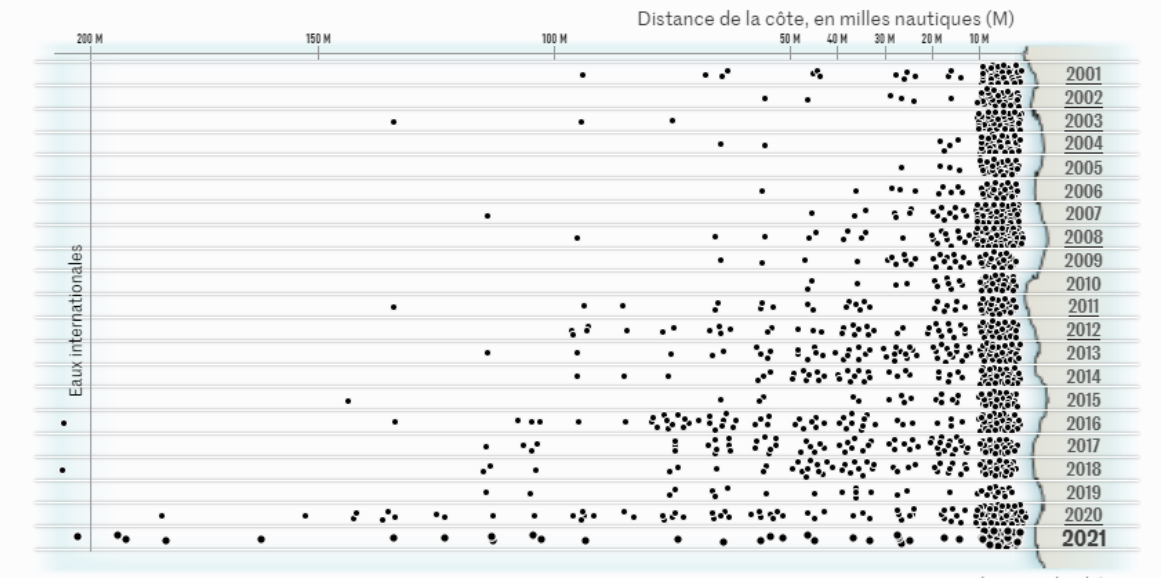

Figure 7 Distance des actes de piraterie et de brigandage dans le Golfe de Guinée de 2001 à 2021
Source : Le Monde (2021)

Équipés d'échelles, de cordes ou de perches, pour monter à bord, nous remarquons que les assaillants peuvent utiliser des armes d'assaut de catégorie militaire ou de *rocket propelled grenades* (**RPG**s) *avec* lesquelles ils visent généralement la passerelle[64]. Ils peuvent ainsi organiser l'abordage de navires avec de grands franc-bord, en route ou à l'ancre. Une fois à bord, ils cherchent à maîtriser l'équipage en atteignant la passerelle de navigation. Ralentir le navire permet aux autres pirates d'aborder, pour parfois voler la cargaison et autres objets de valeur. Il n'est pas rare que ces hommes armés restent à bord plusieurs jours et cherchent à déplacer le navire en dehors de la juridiction des états pour ainsi procéder au transfert de cargaison en **STS**[65].

La piraterie et les vols à main armée en mer touchent aussi les navires à l'ancre. Lagos, au Nigeria est le plus gros port d'Afrique de l'Ouest. Ses installations permettent une prise en charge de différents types de cargo, la compagnie *Maersk* y détient un terminal de containeurs et le groupe *BUA*, une raffinerie. On peut compter quotidiennement une cinquantaine de navires dans sa zone d'ancrage, avec un temps d'attente moyen de 1 jour et demi[66]. Cotonou (Bénin), Abidjan (Côte d'Ivoire), ou Tema (Ghana), sont également des ports majeurs d'Afrique du Golfe de Guinée. La congestion générée par ce trafic intense place les navires en situation de danger. À l'ancre ou en attente proche des côtes, là où la piraterie sévit davantage.

[64] ICC-IMB, 2021 Annual IMB Piracy Report
[65] ICS et al., BMP WA
[66] Marine Traffic, LAGOS Port

En 2021, le nombre d'incident rapporté a drastiquement chuté. 35 incidents dans la région du Golfe de Guinée, soit une diminution de 60% par rapport à l'année 2020. 57 membres d'équipage furent kidnappés, représentant 100% des kidnappings en mer dans le monde. Cependant, les pirates ont causé la mort d'un marin lors de l'abordage d'un navire au large des côtes de Guinée Equatoriale dans la nuit du 30 décembre 2021, avant d'avoir kidnappé plusieurs membres d'équipage, dont leur capitaine[67].

3.2.3 Petro-piracy

10,9 milliards de dollars[68]. C'est la perte estimée par la Marine nigériane, due à la *petro-piracy*[69]. Riche de ses puits d'hydrocarbures et de gaz naturel, la région du delta du Niger attire toutes les convoitises. Puiser dans les pipelines, les ruines d'anciens puits à l'abandon ou directement depuis les pétroliers et plateformes offshore, est une pratique répandue[70]. La fréquence de cette pratique dépend majoritairement du prix du baril, on trouve une diminution du vol de pétrole lors des crises pétrolières, comme entre 2014 et 2016 ou plus récemment dû à l'épidémie de Covid-19[71]. On pourrait craindre une recrudescence de ce type de crime avec l'augmentation du prix du pétrole dû aux tensions entre la Fédération de Russie et l'Occident.

Ces pirates, dotés d'équipements adéquats, sont en mesure de raffiner eux-mêmes le pétrole détourné dans des raffineries clandestines, parfois même, directement sur les pétroliers ou plateformes offshore.

Installées au milieu de nulle part, ces raffineries clandestines offrent un paysage de désolation. Ces installations rudimentaires n'épargnent ni l'environnement ni les hommes qui y travaillent. La cargaison volée est jetée dans des fours improvisés à même le sol, le produit distillé est ensuite récolté à la main.

Outre les pertes financières engendrées par cette pratique, pour les producteurs mais également pour l'économie locale, la *petro-piracy* porte également un fort préjudice à l'environnement, et aux populations.

[67] The Maritime Executive, One Crew Member Killed, Six Kidnapped in New Gulf of Guinea Incident
[68] BNP PARIBAS, One Crew Member Killed, Six Kidnapped in New Gulf of Guinea Incident
[69] Nigerian Navy, Nigerian Navy Ships
[70] Pietsch et Pichon, Piracy in the Gulf of Guinea
[71] ICC-IMB, 2021 Annual IMB Piracy Report

Figure 8 Raffinerie clandestine au Nigéria
Source : adapté d'Etevenard et Bassompierre (2016)

3.2.4 A la frontière entre piraterie et terrorisme

Il peut être difficile de comparer la piraterie au terrorisme maritime, principalement car ce dernier manque de définition internationale. Alors que les pirates sont en grande partie guidés par des raison financières, c'est majoritairement des objectifs idéologiques et politiques que suivent les terroristes[72]. Les terroristes souhaitent changer la structure de leur société. Ce faisant, ils requièrent d'être entendu par les gouvernements et inspirer la terreur dans le cœur de la population civile. Pour cela, ils ont besoin de médiatiser au maximum leurs activités, avec des crimes toujours plus choquants. Alors que les pirates préfèreront garder leurs activités secrètes, profitant de garder profil-bas pour continuer leurs attaques impunément.

Cependant la piraterie et le terrorisme maritime peuvent se rejoindre sur certains points.

Les pirates ont généralement des motivations financières. Cependant, en Afrique de l'Ouest, certains groupes de pirates se mélangent étrangement à des groupes armés politisés et pouvant être qualifiés de groupes terroristes, comme le MEND. Les pirates ne manquent pas de moyens, et son reconnus comme étant les mieux armés du monde. En 2021, 65% des incidents dans la région du Golfe de Guinée comportait la présence d'armes à feu, contre

[72] Moreels, The insurability of maritime terrorism

seulement 19% dans les Amériques et 5% dans le détroit de Singapour[73]. Malgré cela, les pirates ouest-africains ont largement plus de motivations financières que politiques.

3.3 Un impact sur le commerce

L'insécurité générée par les fréquentes attaques pirates à un impact non négligeable sur l'économie du secteur maritime et donc l'économie mondiale.

3.3.1 Les assurances, un coût non négligeable

Les contrats d'assurance dans l'industrie maritime sont divers, et ils peuvent couvrir différents risques.

Une *Hull and Machinery* (**H&M**) *Insurance* couvre les dangers à l'intégrité physique du navire, tels que les explosions, incendies et les périls de la mer. Ces assurances couvrent les dangers liés à la piraterie. Une *Protection and Indemnity* (**P&I**) *Insurance* couvre entre autres les dommages causés à la cargaison durant le transport et les risques de dégâts environnementaux et exclue le plus souvent les dangers liés à la piraterie et aux vols à main armée. Ces derniers sont généralement couverts par une *War Risks Insurance*. Cette assurance couvre les pertes et dégâts sur *Hull & Machinery* résultants, entre autres, de guerres, guerres civiles ou acte de piraterie. Elle couvre également les réclamations P&I liées aux risques de guerres comme par exemple, les décès, blessures et toutes dépenses résultantes de la détention de membres d'équipages[74].

Toutefois, les *War Risks Insurances* ne couvrent généralement pas les rançons dans le cadre de piraterie, sauf en cas d'avarie commune. Selon les règles du *UK* et *Hellenic War Risks*, le remboursement de rançons est laissé à la libre appréciation des directeurs de ces compagnies d'assurances. Il n'est donc garanti ni sur le principe ni sur le montant. Il est préférable selon le Capitaine Justers, responsable d'une compagnie d'assurance maritime, de souscrire une *Kidnap and Ransom* (**K&R**) *Insurance* spécifique, couvrant non seulement le coût de la rançon mais également tous les frais liés, y compris la perte d'exploitation engendrée par de tels incidents[75].

[73] ICC-IMB, 2021 Annual IMB Piracy Report
[74] UK War Risks, War risks cover details
[75] Justers, Interview personnelle

Cependant, du point de vue des assureurs, distinction est faite entre actes de piraterie et de guerre. Ces derniers sont des incidents spécifiques au regard des assurances bien que la frontière entre les deux soit infiniment mince. En 2020, le *Joint War Comitee*, constitué du *Lloyd's Market Association* et de *l'International Underwriting Association*, intégrait une large partie du Golfe de Guinée dans la liste des « Hull War, Piracy, Terrorism and Related Perils Listed Areas »[76]. Les armateurs sont alors contraints de supporter des frais supplémentaires s'ils souhaitent naviguer dans ces eaux.

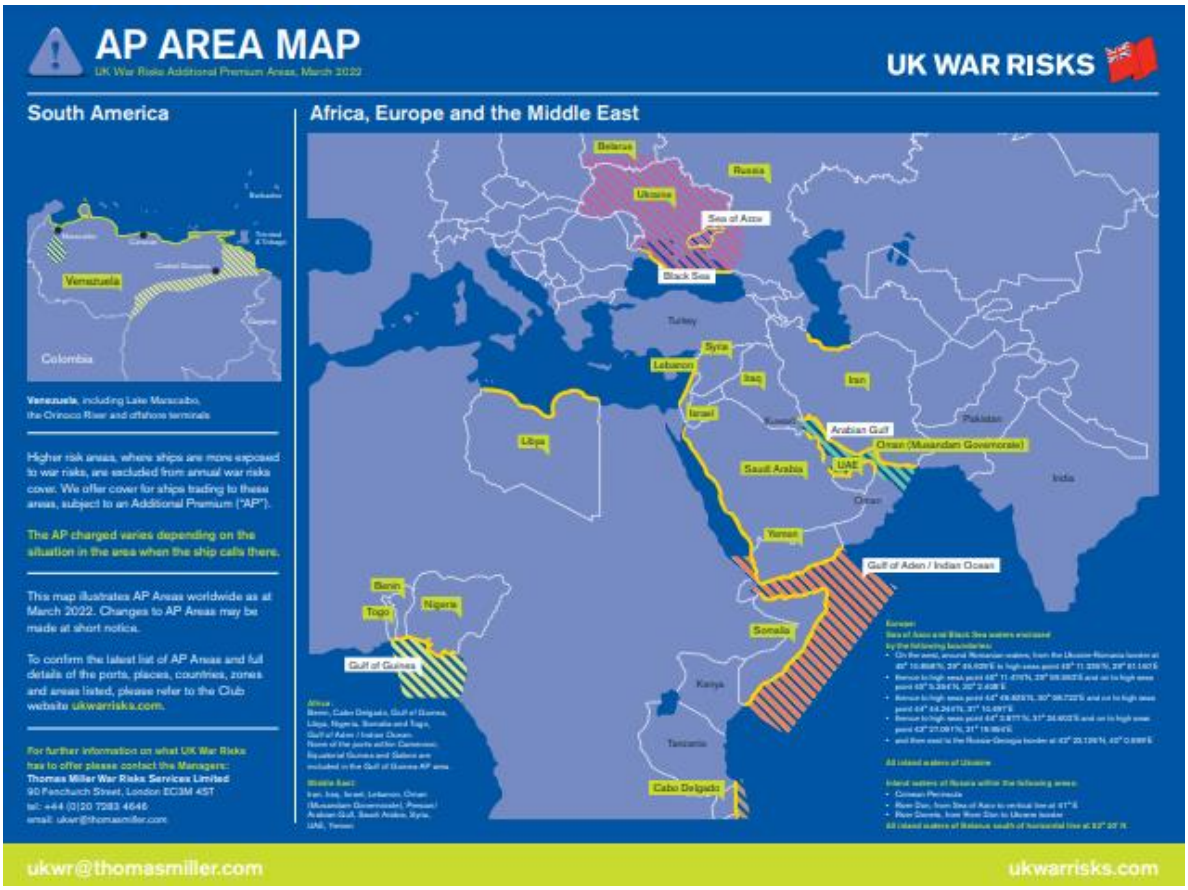

Figure 9 UK War Risks Additional Premium (AP) Areas 2022
Source : UK War Risks (2022)

Le coût de cette prime additionnelle est calculé en fonction des négociations entre le coutrier et la compagnie concernant, entre autres, le taux, les remises, la présence d'une assurance K&R sous-jacente. Le coût dépend également de la taille de la flotte à assurer ainsi que le nombre d'escales dans les zones concernées. Si l'on exclut les éventuelles remises, le taux additionnel brut peut être estimé à 0,06% (de la valeur assurée du navire et pour une période de 7 jours) au large des côtes du Nigeria. A titre de comparaison, ce taux est estimé à 0,09%

[76] LMA ; IUA, Hull War, Piracy, Terrorism and Related Perils Listed Areas

dans le Golfe d'Aden, 0,30% dans le Golfe Persique et 1,50% à Novorossiysk, en Mer Noire (cette prime exceptionnellement élevée est attribuée à la guerre entre la Fédération de Russie et l'Ukraine)[77].

On a pu constater, lors de l'épisode de piraterie en Somalie, une diminution des coûts des assurances de 635 millions de dollars en 2011 à 550 millions en 2012. Une diminution attribuée à l'augmentation de la présence de personnel armé à bord.

3.3.2 L'impact du Covid-19

La pandémie de Covid-19 a atteint les terres nigérianes au début de l'année 2020, avec le premier cas avéré le 25 février 2020[78]. Le virus a été beaucoup moins virulent en Afrique de l'Ouest que dans d'autres régions du monde[79]. Cependant, la vie des populations, déjà en situation de précarité économique et sociale a été bouleversée au même titre qu'en occident. Les mesures sanitaires prises par les gouvernements n'ont pas facilité la résolution des conflits déjà existants.

Comme nous avons vu dans les chapitres précédents, la stabilité économique de certains pays du Golfe de Guinée est ultra-dépendante du commerce international et du prix du pétrole brut. Malheureusement cette pandémie a considérablement ralenti le commerce international[80]. Lorsque les gouvernements mondiaux étaient en gestion de crise, les ports restaient inaccessibles. Les navires devaient alors attendre à l'ancre pendant de longues semaines, parfois des mois, avant de reprendre leur route. Les navires à l'ancre ou à la dérive demeurent des cibles faciles pour les pirates et les équipages ont fortement été touchés sur un plan physique et psychologique[81].

L'épidémie mondiale de Covid-19 a rapidement été suivie d'une vague de confinement dans le monde entier, limitant considérablement les déplacements de chacun. L'importante restriction du trafic, qu'il soit maritime, routier ou aérien, a généré un surplus de pétrole dans les réserves de carburant. Cette crise a engendré une chute drastique de la demande de l'or noir, conduisant à un effondrement du prix du baril. En atteignant des valeurs records à 15,905

[77] Justers, Interview personnelle
[78] AllAfrica, Nigeria Records First Coronavirus Case
[79] Worldometer, Nigeria Records First Coronavirus Case
[80] Organisation Mondiale du Commerce, La COVID-19 et le commerce mondial
[81] Whiting, Stuck at sea: How to save the world's seafarers and the supply systems they support

USD le baril Brent[82] la semaine du 20 avril 2020, l'économie du Golfe de Guinée se voyait une nouvelle fois fortement impactée.

Figure 10 Prix du pétrole brut Brent en USD
Source : Tradingview.com (données du FXCM) (2021)

Avec une contraction de son PIB de plus de 9 % durant les deux premiers trimestres de 2020, le Nigéria entre en récession pour la seconde fois depuis 2016[83]. L'inflation anéantit l'économie du pays avec une augmentation de 12,34 % en avril 2020 à 18,17 % en mars 2021[84].

La hausse fulgurante du chômage au Nigeria pourrait devenir un motif suffisant pour certaines populations qui se tourneraient alors vers la piraterie.

Les professionnels des activités maritimes naviguant dans les eaux du Golfe de Guinée ont été fortement éprouvés par ces désastres économiques.

En effet, la *petro-piracy*, une des activités essentielles des pirates s'est vue fortement déstabilisée à la suite de cette nouvelle baisse du prix du baril. Eux-mêmes, subissant la crise, ont enregistré des pertes importantes de bénéfices générés habituellement par leurs activités criminelles. Ils ont cependant rebondi très rapidement, et se sont tournés vers une alternative rémunératrice, le kidnapping.

[82] FXCM, CFDs sur Pétrole Brut (Brent)
[83] Le Point Afrique, COVID-19 : Le Nigéria en récession accuse le coup
[84] Trading Economics, Nigeria Inflation Rate

C'est ainsi que le Golfe de Guinée a noté une augmentation de 31 % du nombre d'incidents de 2019 à 2020[85].

Le PIB du Nigeria a augmenté de près de 4% dans le dernier trimestre de 2021, il s'agit du cinquième trimestre consécutif qui fait apparaitre un PIB positif. Un effort méritoire compte tenu de la relance économique après la crise engendrée par la pandémie. Cette expansion continue d'être tirée par le secteur non-pétrolier et on note une augmentation de 8% des recettes engendrées par l'industrie pétrolière, souffrant de la baisse de production. Malgré la remontée des prix du pétrole, le Nigeria a du mal à atteindre ses objectifs de production en raison de l'insécurité résultante de la déprédation des équipements pétroliers. On peut espérer que le pays continue son développement en restant de moins en moins dépendant du cours du pétrole. Bien qu'il pourrait profiter de la récente explosion du prix du baril, une des conséquences des évènements en Ukraine et des tensions entre la Fédération de Russie et l'Occident[86]. Ce dernier facteur est à suivre avec attention.

3.4 Les mesures prises

Toutes les organisations, nationales et internationales, se doivent de prendre leur part de responsabilité dans la prévention de la piraterie et la protection de leurs eaux.

3.4.1 Par les organisations locales…

En 2011, le UNSC encourageait les états de l'*Economic Community of West African States* (**ECOWAS**), *Economic Community of Central African States* (**ECCAS**) et le *Gulf of Guinea Commission* (**GGC**) à prendre des mesures pour lutter contre la piraterie. Et, en 2021, le Président de l'*ECOWAS*, Nana Addo Dankwa, en appelait à tous les états membres pour combattre cette menace qui met à mal la sécurité de leurs régions.

Le gouverneur de l'état de Rivers au Nigeria, Rotimi Amaechi, annonçait en 2009 vouloir rétablir la peine de mort pour tous les auteurs de kidnapping. « It may be unpopular with the NGOs, Civil rights or human rights movements but it's popular with our population » affirmait ce dernier dans un reportage pour la BBC[87].

[85] ICC-IMB, 2019 Annual Piracy Report, 2020 Annual Piracy Report
[86] National Bureau of Statistics, National Gross Domestic Product Q4 2021
[87] Kemp, Ross Kemp in the Search of Pirates

Le *Yaounde Code Of Conduct*, signé en 2013 par 25 pays d'Afrique Centrale et d'Afrique de l'Ouest, définit la forme du combat contre la piraterie et permet à ses différents membres de s'allier contre des ennemis communs. Sous ce code, a été fondé le *Yaounde Architecture for Maritime Security and Safety* (**YAMS**) qui vise, à faciliter la communication entre les différents acteurs de la lutte contre la piraterie, entrainer un personnel qualifié et faciliter la documentation des incidents.

Les états du Golfe de Guinée ont instauré un *Voluntary Reporting Area* (**VRA**) afin de faciliter la communication et augmenter la capacité des forces armées à répondre à temps. Certains états ont aussi mis en place des *Secure Anchorage Area* (**SAA**) et donnent l'accès à des *Security Escort Vessels* (**SEV**), qui sont des vaisseaux transportant des gardes armés, escortant le navire. Ils peuvent aussi permettre l'utilisation de *Vessel Protection Detachments* (**VPD**)[88], qui sont des détachements armés à bord du navire, pour garantir un accès sécuritaire aux navires de la marine marchande dans les eaux du Golfe de Guinée.

3.4.2 …et les organisations internationales

Comme nous l'avons vu plus haut, les organisations internationales sont très sensibles à la piraterie. Elles avaient déjà rapidement réagi au moment des attaques en Somalie, et prennent le sujet très au sérieux.

L'OMI est un des principaux acteurs dans la sensibilisation et la mise en place de standards contre la piraterie. En 2021, son secrétaire général, Kitack Lim, conforte l'urgence de la situation. L'OMI facilite la communication entre les organisations régionales et internationales et porte assistance aux États membres concernant les mesures de sécurité mises en place. Le Comité de la Sécurité Maritime (**MSC**) se retrouvait en mai 2021 pour réévaluer les problématiques en causes, rapportées dans la Résolution MSC.489(103)[89].

Mise en place en 1990, la mission Corymbe assure son 150ème mandat. Le bâtiment militaire Français, patrouilleur de haute mer *Commandant Bouan*, opère dans cette partie du monde pour, entre autres, protéger les eaux de la piraterie et renforcer la coopération internationale dans la zone. En accord avec le Processus de Yaoundé, pas moins de 17 bâtiments ont été déployés pour répondre à cette mission de 2018 à 2021.

[88] ICS et al., BMP WA
[89] MSC, RECOMMENDED ACTION TO ADDRESS PIRACY AND ARMED ROBBERY IN THE GULF OF GUINEA

En 2021, la *Marine Nationale* française et la *Royal Navy* britannique accompagnaient la Marine nigériane lors d'un exercice à grande échelle dans les eaux du Golfe de Guinée. Cet entraînement eût pour but de renforcer la collaboration entre les différentes puissances qui se battent contre les activités criminelles dans leurs eaux[90]. En associant leurs connaissances et compétences respectives, ce type d'action permettra d'accroitre les résultats dans leur lutte contre la piraterie.

3.4.3 La formation des unités locales

En 2015, l'Organisation internationale de police criminelle (**INTERPOL**) lance le projet *AGWE*. Avec un budget de 8,1 millions d'euros réparti sur 8 ans, il a pour mission de former les autorités maritimes du Golfe de Guinée ; du Bénin, de la Côte d'Ivoire, du Ghana, du Nigéria et du Togo[91].

Les experts en sciences criminelles d'INTERPOL ont pour objectif d'instaurer un réseau régional de spécialistes dans ce domaine. Formation, simulation, concertation et coordination, sont les activités primordiales à la bonne réalisation du projet AGWE. À terme, ces nouveaux réseaux régionaux seront aptes à gérer les enquêtes dans le domaine de la criminalité maritime et les poursuites pénales qui en découlent[92].

Depuis quelques années, certaines forces navales du Golfe de Guinée ont pu bénéficier de formations. Mieux informées et davantage sensibilisées, ces forces peuvent ainsi apporter une réponse appropriée face aux attaques pirates visant des navires de la marine marchande. La *Marine Nationale* française présente dans la région, œuvre aussi dans ce sens en apportant son soutien depuis plusieurs années aux marines locales. La Marine nigériane est devenue la plus compétente et la plus respectée d'Afrique de l'Ouest grâce à son prestige et son organisation, avec une flotte comprenant 109 patrouilleurs[93].

3.4.4 ISPS Code

L'*International Ship and Port Facility Security Code* (**ISPS)** représente le résultat d'années de travail par le MSC de l'OMI. Son but est de faciliter la coopération entre les différents gouvernements, administrations locales et l'industrie maritime en termes de sécurité.

[90] Agency Report, Pirates' Attacks: Navy deploys 13 warships, 1,500 troops in Gulf of Guinea
[91] INTERPOL, PROJECT AGWE
[92] INTERPOL, Project AGWE, West Africa
[93] Global Fire Power, 2022 Nigeria Military Strength

Ce Code définit le *Ship Security Plan* (**SSP**), approuvé par l'Administration, instaure des exigences quant aux niveaux de sécurité établis par l'ISPS. Il définit les mesures à prendre afin d'empêcher les dangers internes ou externes de nuire à l'intégrité du navire ou de son équipage. Ces mesures délimitent également les actions à mener pour freiner l'accès illicite à bord, aussi bien en port qu'en mer. Le SSP définit aussi les responsabilités du personnel lors de brèches de sécurité.

Ce Plan se doit d'être régulièrement mis-à-jour, et c'est le but du *Ship Security Assessment* (**SSA**), qui développe et renforce le SSP. Le SSA intègre des études réalisées à bord afin d'identifier les mesures existantes, les équipements importants à protéger ainsi que toutes les déficiences constatées.

Analyser le risque est une étape nécessaire, il faut, pour cela, identifier les menaces et leurs probabilités d'exécution. Un des rôles du SSA est donc de classer ces risques afin de prioriser les mesures de sécurité[94].

Il est du devoir du Company Security Officer (**CSO**) de s'assurer que le SSP est bien respecté à bord et que les SSA sont correctement menés et à intervalles adéquats.

La gestion du *risk assessment* est capitale pour une compagnie. Cependant, toutes les entreprises ne portent pas la même analyse du risque sur la piraterie, pourtant très active dans le Golfe de Guinée. Certains armateurs estiment que la probabilité de voir ses navires se faire attaquer est très faible, ainsi la navigation dans ces eaux est extrêmement conséquente.

3.4.5 Best Management Practice

En 2020, l'*International Chamber of Shipping* (**ICS**), *Baltic and International Maritime Conference* (**BIMCO**), *International Group of Protection and Indemnity Clubs* (**IGP&I Clubs**), *INTERCARGO*, *INTERTANKO* et l'*Oil Companies International Marine Forum* (**OCIMF**) ont publié le *Best Management Practice West Africa* (**BMP WA**). Un document qui se présente sous la forme d'une liste de conseils, similaire au BMP 5, qui lui traite de la région autour du Golfe d'Aden. Il répertorie les options en termes de prévention et protection contre la piraterie. Notons cependant que malgré le caractère officiel de ce document, le capitaine reste le seul responsable quant aux décisions prises sur le navire.

[94] OMI, ISPS Code

3.4.5.1 L'importance de la veille

Le plus sûr pour éviter une attaque de pirate est de l'anticiper, de rester en tous points vigilant et de la voir arriver.

Un des moyens pour repérer des navires pirates est le radar. Le **RADAR** utilise des ondes électromagnétiques pour déterminer l'azimut et la distance d'un objet. Composé d'un émetteur, d'un récepteur et d'une antenne. Les radars sont aujourd'hui associés à l'**ARPA**, permettant de suivre les échos affichés. L'ARPA est un des outils les plus précieux au marin pour assurer une bonne veille. Son association avec l'AIS augmente les informations à la disposition de l'officier de quart. Même si la possession d'AIS par de petits navires n'est pas obligatoire[95]. Ces outils permettent de différencier les navires suspects. Cependant ils seront beaucoup moins utiles dans des zones de fort trafic, où l'écran du radar peut devenir submergé de cibles et de vecteurs. En haute mer, où dans des zones d'ancrage, on pourra beaucoup plus facilement détecter un potentiel navire pirate.

Les pirates utilisent le plus souvent de petites vedettes, leur surface de réflexion des ondes radar est donc très mince. De plus leurs esquifs sont parfois construits de bois, ce qui reflète beaucoup moins les ondes qu'une coque en métal et sont facilement confondu par le *wave clutter* du Radar. Il pourrait également être très facile de manquer un écho dû à un mauvais réglage du gain. Aussi, le secteur aveugle du radar induit par la présence de la cheminée est à prendre en considération lorsque les vedettes sont trop proches du navire.

Maintenir une vigie permanente est le moyen le plus sûr de détecter de potentiels assaillants. Si certaines vedettes sont trop petites pour être détectées par le Radar, un marin observateur pourra sans doute les apercevoir. Les vigies doivent donc rester sur leurs gardes, et pour ce faire elles devraient être remplacées régulièrement pour éviter la lassitude, qui pourrait engendrer un défaut de surveillance. La présence de vigies est aussi une dissuasion supplémentaire pour les pirates, s'ils se savent observés, ils pourraient renoncer à l'abordage. Même lorsque l'équipage n'observe pas activement la mer à la recherche de potentiels assaillants, il est possible de placer des mannequins à des emplacements stratégiques à bord[96]. Des pirates épiant le navire à l'aide de jumelles ne pourraient pas faire la différence entre ceux-ci et de vraies vigies.

[95] OMI, IMO Res A 917 (22)
[96] ICS et al., BMP WA

L'équipage doit être formé pour repérer tous navires suspects de jour comme de nuit. Des exercices doivent être menés afin d'entrainer les hommes à réagir rapidement et efficacement lors d'une attaque pirate. Pour permettre à l'officier de quart d'engager les manœuvres adéquates, la vigie se doit d'être réactive dès l'observation d'une embarcation suspecte.

3.4.5.2 Le choix de la discrétion

Le meilleur moyen d'éviter d'être pris pour cible par des pirates, reste la discrétion. Ne pas se faire remarquer

Les pirates utilisent principalement le Radar pour détecter leurs cibles potentielles à de longues distances. Il existe des technologies permettant à un navire d'éviter d'apparaître sur un Radar ou à tout le moins, de diminuer sa signature. C'est le cas du plaquage en fibre de carbone ou fibre de verre. Un navire peut également être construit dans une forme particulière, évitant les surfaces verticales qui reflèteraient les ondes vers leur source. Cependant, ces mesures ne sont pas répandues à bord des navires marchands mais sont plutôt réservées aux bâtiments militaires de haute technologie.

Les capitaines peuvent aussi choisir d'éteindre l'AIS du navire pour éviter de fournir des informations à de potentiels assaillants. L'OMI affirme que l'AIS peut être éteint si son opération normale risque de compromettre la sécurité du navire ou de son équipage[97]. Cependant, cette technique est à double tranchant car elle empêche également les navires aux alentours, militaires comme civils, de recevoir ces informations. Aussi, si l'AIS n'est pas réactivé avant que l'équipage se réfugie dans la citadelle, les autorités pourraient avoir plus de difficultés pour repérer le navire en danger. C'est ce qu'affirme l'OTAN, qui encourage les capitaines à laisser l'AIS activé durant le transit à travers des zones de danger[98].

Malgré son interdiction par les règles de navigation et le BMP WA, certains capitaines choisissent d'éteindre leurs feux de navigation pendant la nuit, lors du passage dans des zones sensibles. Cela aura pour effet de diminuer la distance de détection des pirates, qui ne possèdent généralement pas de Radar sur leurs vedettes, ce genre d'équipement est ordinairement réservé au vaisseau mère. Bien que proscrite par les règles, la méthode reste

[97] OMI, IMO Res A 917 (22)
[98] NATO Shipping Centre, Piracy - Revised Guidance on the use of AIS in the High Risk Area off Somalia

malgré tout utilisée[99]. Bien entendu, l'extinction des feux de navigation est à proscrire (encore d'avantage) en présence de trafic, par soucis de sécurité.

3.4.5.3 Les Ship Protection Measures (SPM)

Le BMP WA fournit une liste d'équipements ayant prouvé leur efficacité. Ils visent à apporter des moyens de défense contre des attaques de pirates. Même si les navires sont particulièrement vulnérables quand ils sont à l'ancre, les différents SPMs se doivent de répondre à toutes les éventualités[100]. Le CSO a la responsabilité de dresser un *Vessel Hardening Plan* (**VHP**), en accord avec les régulations fournies par la compagnie et le ISPS Code. Ce plan assure une bonne préparation du navire et de son équipage pour contrer toutes tentatives d'attaques.

La défense du navire s'organise en trois étapes. La première a pour but d'empêcher les assaillants d'aborder le navire, la deuxième de ralentir leur progression dans le navire, et la dernière de garder l'équipage en sécurité jusqu'à l'intervention des secours.

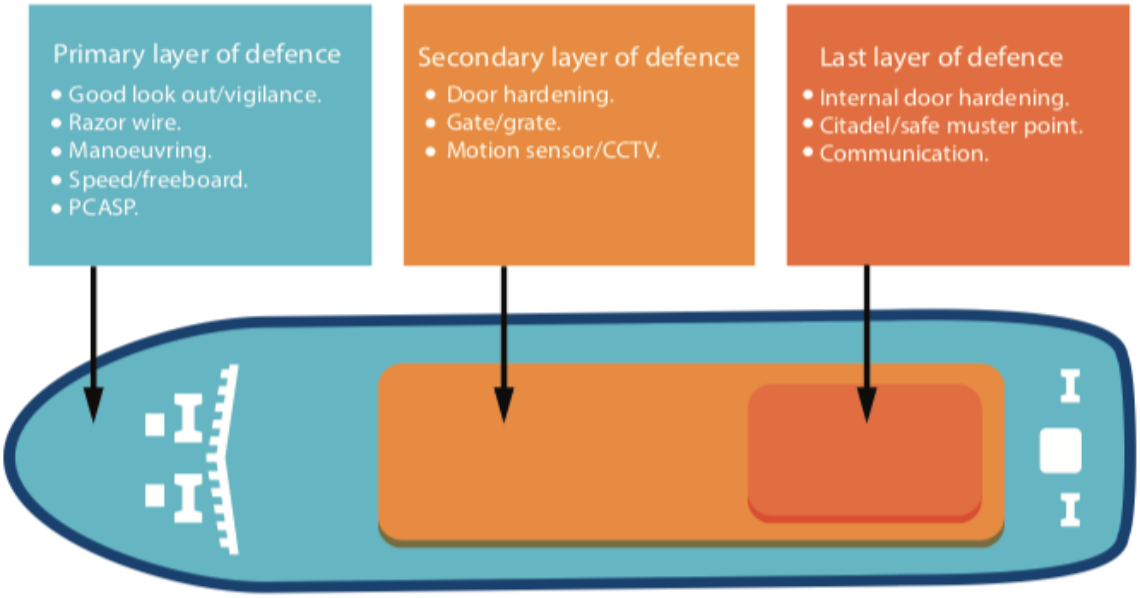

Figure 11 Les 3 couches de protection contre une attaque pirate
Source : BMP WA (2020)

Lorsque des assaillants ont été identifiés par l'équipage, l'officier de quart doit sonner l'alarme d'urgence afin d'informer le reste du personnel, et le rassembler. Il doit aussi émettre un appel de détresse via les systèmes radio ou satellite appropriés. Le *Ship Security Alert System* (**SSAS**)

[99] Jeff, 10 Ways Sailors Use to Fight Pirates
[100] ICS et al., BMP WA

est également un équipement utile lors d'une attaque, il permet d'émettre une alarme silencieuse à la terre pour l'informer de la situation du navire.

La plupart des attaques sont menées depuis de petits navires très rapides. C'est pourquoi il est conseillé de mettre la machine en avant toutes et de manœuvrer de façon à créer des vagues, déstabilisant les esquifs pirates[101]. Cependant, il faut garder à l'esprit que l'utilisation intensive des machines couplée pendant de longues périodes pourrait endommager le système de propulsion et mener à une potentielle panne.

Il est également important de noter que des pirates choisissant une approche furtive préfèreront aborder le navire par sa poupe, cependant, les turbulences créées par l'hélice les empêcheront de garder une position stable. C'est pourquoi la plupart des pirates lors d'abordage à grande vitesse, choisiront d'aborder le navire par son côté. Lors de la navigation, le milieu du navire connait une diminution de pression hydrostatique induite par le principe de Bernoulli[102]. Cette baisse de pression induit un vide entre le navire et l'esquif pirate, permettant à ce dernier de garder sa position sans effort. Toutefois cet effet de ventouse peut s'estomper avec du roulis[103].

Des barrières physiques sont aussi présentes. On peut retrouver des barbelés à lames destinés à empêcher les abordages. Des jets d'eau ou de mousse pouvant être opérés à distance afin de déstabiliser les assaillants. Bien que peu conventionnel, on a pu noter lors de plusieurs abordages de pirates que l'équipage disséminait des bris de verre sur le navire, espérant blesser certains assaillants ne portant pas de chaussures.

Certains équipements plus modernes peuvent être utilisés. Le *Long-Range Acoustic Device* (**LRAD**) est une arme à énergie dirigée non létale pouvant aussi être utilisé comme dispositif de communication. Certains équipements peuvent produire des ondes sonores jusqu'à plus de 150 dB[104]. Le LRAD est principalement utilisé à bord des navires militaires. On peut noter son utilisation notamment lors de l'abordage du *Magellan Star* dans le Golfe d'Aden en 2010, dont les détails ont été discutés lors de notre interview avec membre de l'US Navy, où les

[101] ICS et al., BMP WA
[102] Lataire, Propulsion (Part 2)
[103] M. Murphy, Small boats, weak states, dirty money
[104] HyperSpike, HS-18 RAHD

forces américaines utilisèrent le LRAD pour harceler les pirates pendant plusieurs jours, les exténuant avant l'arrivée d'une équipe d'assaut pour reprendre le navire[105].

Certains navires sont également équipés d'armes laser à longue distance. Cet équipement est utilisé pour aveugler les assaillants, sans pour autant causer des dégâts oculaires à long-terme[106].

Cependant, ce genre de technologie n'est pas utilisée à bord des navires de la marine marchande. On les retrouve davantage sur les bâtiments militaires.

L'OMI conseille la présence d'une citadelle à bord des navires[107]. Il s'agit une pièce fortifiée dans laquelle l'équipage non nécessaire à la navigation peut se réfugier au début de l'abordage. La pièce doit être équipée d'équipements de communication, **VHF** et téléphone satellite. Lors d'un abordage, le capitaine décide quand l'équipage nécessaire à la navigation doit se protéger dans la citadelle, car dans l'éventualité d'une réponse militaire, les forces armées doivent être assurées que l'entièreté de l'équipage se trouve en sécurité dans la citadelle.

Une fois en sécurité dans la citadelle, l'équipage doit pouvoir surveiller la position des assaillants. C'est pourquoi un système de **CCTV** doit pouvoir couvrir le navire, et des écrans situés dans les points importants. Ceci est le seul système qui permet aux marins de savoir si les pirates ont quitté le navire tout en restant en sécurité dans la citadelle. Cependant, les caméras sont souvent détruites ou mises hors service lors des abordages.

3.4.5.4 La présence d'armes à bord

La présence de militaires ou paramilitaires à bord est aussi, pour les compagnies, une possibilité à considérer. Toutefois, elle doit être autorisée par l'état pavillon en consultation avec les armateurs concernés. La France interdit la présence de gardes armés privés, alors que la Belgique autorise la présence de services de sécurité privés sur les navires battant pavillon belge et sous certaines réserves. Ceci est une arme dissuasive, les forces armées tirent sur le moteur du navire pirate les empêchant de mener à bien leur opération. Généralement, la seule présence de militaires suffit à dissuader les assaillants[108]. Certains navires peuvent aussi

[105] Anthony, Interview personnelle
[106] Daniel, 20 Anti-Piracy Weapons Deployed In Ships To Fight Pirates
[107] OMI, MSC.1/Circ.1332
[108] Anthony, Interview personnelle

prévenir de la présence de personnel armé à bord par AIS, afin de décourager de potentiels pirates équipés pour recevoir ces communications.

L'efficacité de la présence de gardes armés a largement fait ses preuves durant l'épisode intense de piraterie somalienne. On estimait alors que les équipes de sécurité auraient empêché 43% des tentatives de détournement de navire en 2011[109]. Cependant, quelques autres rapports démontraient que la présence de forces armées à bord augmente la probabilité qu'a l'équipage à se faire tirer dessus[110].

On estimait la proportion des navires engageant des gardes armés pendant leur passage dans des zones sensibles, à 30% en 2011 et au moins 50% en 2012, lors de l'épisode de piraterie somalienne. Ainsi que le coût de ces services à 1,5 milliards de dollars en 2012.

Toutefois, l'OMI déconseille fortement la présence d'armes à bord qui pourrait générer une escalade de l'armement[111]. On remarque également que la présence de personnel de sécurité peut donner un sentiment de sécurité au capitaine du navire, qui négligera volontairement les mesures conseillées par le BMP[112].

3.4.5.5 Le signalement

Comme abordé précédemment, les États du Golfe de Guinée ont introduit un VRA ainsi qu'une liste de formulaires à remplir pour rapporter des activités suspectes. Couplé avec le *Maritime Domain Awareness for Trade - Gulf of Guinea* (**MDAT-GoG**), établit en 2016 par les forces navales britanniques et françaises dont les centres sont établis à Portsmouth et Brest et avec le support du *Yaounde Process*. Le but du MDAT-GoG est de faciliter la communication et supporter l'industrie maritime dans le Golfe de Guinée. Ce centre de coopération fournit aux compagnies et aux capitaines un numéro d'urgence à contacter en cas d'attaque. Les informations recueillies sont disponibles gratuitement sur le site internet du MDAT-GoG ainsi que dans des rapports hebdomadaires. En 2018, 300 navires par jour rapportaient à ce centre[113].

[109] One Earth Future, The Human Cost of Somali Piracy 2011
[110] Bockmann et Katz, Shooting to Kill Pirates Risks Blackwater Moment
[111] OMI, Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships
[112] One Earth Future, The Human Cost of Somali Piracy 2011
[113] MDAT-GoG, ReCAAP Brief

On peut aussi noter que l'Institut Hydrographique du Royaume-Uni (**UKHO**) a travaillé en collaboration avec le MDAT-GoG pour fournir des Cartes de Sureté Maritime présentant les informations basiques quant au signalement des navires, telle la carte Q6114.

3.4.5.6 Le Voyage Planning

Le voyage planning reste le meilleur moyen pour les compagnies d'éviter les incidents. Le Golfe de Guinée est défini par le *Joint War Comitee* de *Lloyd's* dans le document « Hull war, piracy, Terrorism and Related Perils Listed Areas ». Les armateurs sont conscients des risques et de la dangerosité quant à la navigation dans cette zone. Les primes d'assurance extrêmement conséquentes le leur rappel à leur bon souvenir. Même s'il est de la responsabilité des officiers de préparer le Voyage Planning, le travail peut être simplifié à terre.

Les côtes du Golfe de Guinée sont congestionnées par le trafic. Lagos, un des ports le plus important d'Afrique de l'Ouest, reste un point névralgique. L'importance du trafic oblige un très grand nombre de navires à patienter. Ils se retrouvent à l'ancre au large des côtes Nigérianes attendant leur tour. Et c'est bien ici que règne principalement le danger et que les navires sont les plus vulnérables. Cette attente offre plus d'opportunité aux pirates d'approcher facilement. La vitesse nulle permet aux assaillants d'aborder le navire sans résistance. C'est pourquoi le BMP WA conseille à tous les navires en attente d'une place au port de se positionner à plus de 200 miles nautiques des côtes.

Lors de l'épisode de piraterie somalienne, certaines compagnies ont pu re-router leurs navires pour éviter de les faire passer par le Golfe d'Aden, préférant passer par le Cap de Bonne Espérance. En 2012, on estimait les coûts de ces changements de route à 290 millions de dollars[114]. Cependant, la position géographique du Golfe de Guinée ne permet pas ce genre de considérations aux armateurs, en effet, le Golfe de Guinée reste le centre névralgique du commerce en Afrique de l'Ouest et cette recommandation peut sembler difficile à appliquer.

Le Golfe de Guinée, devant ses faiblesses économiques et sociales ainsi que son insécurité, est devenu l'épicentre de la piraterie dans la seconde moitié des années 2010. C'est en prenant

[114] One Earth Future, The Economic Cost of Somali Piracy 2012

pour modèle le mode opératoire de leurs homologues somaliens que les pirates de l'Ouest de l'Afrique ont su s'affirmer comme les plus dangereux de ces dernières années. Les nombreux marins et personnels d'unités offshores souffrent du danger grandissant que représente les pirates et leur règne de terreur. Nombreuses sont les personnes kidnappées au large des côtes…

L'industrie maritime a son rôle à jouer parmi la pléthore d'agences internationales et de gouvernements locaux qui essayent de rétablir une sécurité dans les eaux du Golfe de Guinée. Elle prit notamment l'initiative de rédiger le BMP WA, ouvrage rassemblant la totalité des informations nécessaires à la protection d'un navire et de son personnel contre la menace pirate.

On pourrait attribuer la diminution d'incidents durant l'année 2021 à la présence militaire intensive, qu'elle soit locale, avec la marine nigériane, ou internationale, avec la Marine Nationale française ou la Royal Navy britannique. Cependant, la multiplication d'opérations militaires dans la région n'est pas une solution durable, comme nous avons observé avec le cas de la Somalie.

Les causes fondamentales de la présence de la piraterie, comme la pauvreté et l'insécurité n'ont pas été traitées, et celles-ci se règlent sur le long terme. Les quelques plans de relance économique proposés par les gouvernements locaux et agences internationales font pâle figure devant le budget injecté dans la présence militaire dans la région du Golfe de Guinée.

CHAPITRE 4 : L'Asie du Sud-Est

L'Asie du Sud Est, le détroit de Malacca, le détroit de Singapour, étaient des zones de pirateries avant même leur colonisation par les européens. Passage obligatoire entre l'Orient et l'Occident, région archipélagique, peuplée par des marins et des commerçants. Le territoire parfait pour des pirates. On observe d'ailleurs des témoignages d'actes de piraterie dans le détroit de Malacca et la Mer de Chine Méridionale depuis au moins le 5e siècle[115].

4.1 Géopolitique de l'Asie du Sud Est

Le détroit de Malacca et de Singapour sont bordés par trois états très hétérogènes. La Malaise insulaire au Nord, l'Indonésie avec l'île de Sumatra au Sud, et la cité-État de Singapour. Ces pays remettent régulièrement en question leur souveraineté sur les détroits de Malacca et de Singapour (**SOMS**). Bien que la Convention sur le Droit de la mer de 1982 en définisse clairement les limites. Même si en 1971, l'Indonésie et la Malaisie, en accord respectif, déclarent que les SOMS ne sont pas des détroit internationaux[116].

Cette région est bien différente des deux décrites précédemment. La Malaisie, l'Indonésie et Singapour sont loin de posséder les mêmes problématiques économiques et sociales que l'Afrique de l'Ouest et la Somalie. Singapour, la Malaisie et l'Indonésie ont respectivement un Indice de Développement Humain très élevé, élevé et moyen. Alors que le Nigeria possède un **IDH** faible, et la Somalie, un des plus faible du monde[117].

Cependant, ces trois états sont marqués par des différences de richesse importante. La cité-état de Singapour est reconnu comme l'état le plus riche d'Asie du Sud-Est et également le plus riche d'Asie[118] devant le Qatar avec un PIB par habitant de 58 000 $ en 2020[119]. Alors que son voisin, la Malaisie, possède un PIB par habitant six fois moindre[120]. L'Indonésie, quant à elle, se place dans les derniers de la liste avec un PIB par habitant de 3 700 $ en 2020[121].

[115] Chalk, GREY-AREA PHENOMENA IN SOUTHEAST ASIA: PIRACY, DRUG TRAFFICKING AND POLITICAL TERRORISM
[116] Sun, Regulation of Shipping in the Straits of Malacca and Singapore
[117] UNDP, Human Development Report 2020
[118] Trading Economics, PIB PAR HABITANT - LISTE DES PAYS - ASIE
[119] Trading Economics, Singapour - PIB par habitant
[120] Trading Economics, Malaisie - PIB par habitant
[121] Trading Economics, Indonésie - PIB par habitant

Les populations du Sud-Est de l'Asie se reposent essentiellement sur la pêche pour fournir des emplois et répondre aux besoins alimentaires de la population. Cependant, ces dernières années, la région a connu un appauvrissement conséquent de ses eaux dû à la surpêche, très présente au sein de la zone. Les méthodes adoptées par les pêcheurs sont catastrophiques pour l'environnement et les ressources halieutiques. Avec l'utilisation de produits chimiques comme le cyanure de sodium, étourdissant les poissons pour les rendre plus facile à pêcher[122]. L'utilisation de chaluts sur tous types de fonds, causant la destruction des coraux, ou encore la pêche à la dynamite. La région fait désormais face à l'épuisement de ses eaux. Les populations sont donc poussées à se tourner vers d'autre emplois.

La région possède également de nombreuses insécurités. Ces dernières décennies ont été marquées par le développement de nombreux groupes de crime organisé avec une forte influence dans les domaines du trafic de drogues, trafic d'êtres humains et la contrefaçon de médicaments[123].

La différence de richesse, accompagnée par la faible sécurité[124] et l'appauvrissement des eaux sont indéniablement des facteurs qui poussent les peuples de l'Asie du Sud-Est à se livrer aux vols à main armée et à la piraterie[125].

4.2 Piraterie en Asie du Sud-Est

Espace stratégique permettant de relier l'Orient à l'Occident, la mer de Chine méridionale est une région clé du transport maritime international. Les détroits de Malacca et de Singapour sont les détroits les plus longs empruntés pour la navigation internationale, et aussi les plus animés. On estime que plus de 130 000 navires s'arrêtent au port de Singapour, et que la moitié du flux de pétrole mondial passe à travers son détroit[126]. La piraterie est présente depuis longtemps dans cette région. Il est estimé que 60% des incidents maritimes de 1993 à 2015 se sont déroulés en Asie du Sud-Est. Alors que « seulement » 17% sont attribués au pirates Somaliens sur cette même période[127].

[122] Barber et Pratt, Poison and Profits - Cyanide Fishing in the Indo-Pacific
[123] UNODC, Transnational Organized Crime in Southeast Asia: Evolution, Growth and Impact
[124] Carnegie, Human Insecurities in Southeast Asia
[125] Writer Tracks Modern-Day Pirates in Malaysia
[126] Wong, Sea robbery attempt in Singapore Strait foiled by Singapore and Indonesian navies
[127] Spiess, Black Spots

Si elle se situait principalement dans le détroit de Malacca, c'est désormais à proximité du port de Singapour que l'on retrouve la zone de piraterie la plus active en 2021. En effet, y ont été rapportés 35 incidents, soit 27% des actes de pirateries mondiaux, ou 63% des actes de pirateries et de vols à main armée dans la région de l'Asie du Sud-Est[128]. On retrouve également une partie des incidents dans les eaux philippines, notamment à proximité de la zone d'ancrage du port de Manille.

Contrairement à leurs homologues africains, les pirates actuels de cette région ne privilégient pas les kidnappings. On observe seulement quelques occurrences ces dernières décennies[129]. Cependant, si les pirates se livrent à ce genre d'actes, ils préfèrent cibler les populations locales sur de petits navires de pêche[130].

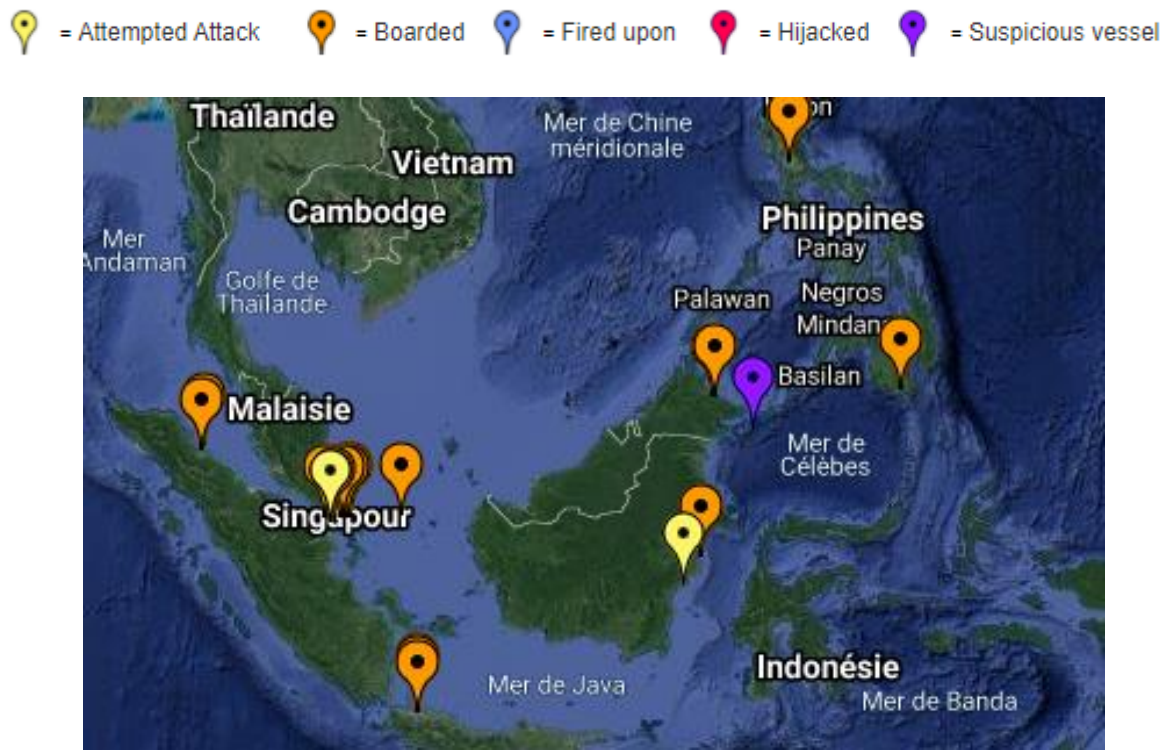

Figure 12 Carte de la piraterie en Asie du Sud-Est en 2021
Source : ICC-IMB (2022)

4.2.1 Le détroit de Malacca

La configuration géographique du détroit de Malacca permet de façon naturelle le développement des actes de piraterie et de vols à main armée. Le trafic de forte densité dans cet espace relativement étroit laisse libre cours aux pirates qui privilégient les attaques de

[128] ICC-IMB, 2021 Annual IMB Piracy Report
[129] ReCAAP et al., Regional Guide to Counter Piracy and Armed Robbery Against Ships in Asia
[130] Joubert, The State of Maritime Piracy 2019

navires les plus vulnérables. Le lourd trafic a été encore plus agglutiné à la suite de la création du dispositif de séparation du trafic en 1998, la vitesse étant réduite à 12 nœuds dans certaines zones par les régulations internationales[131].

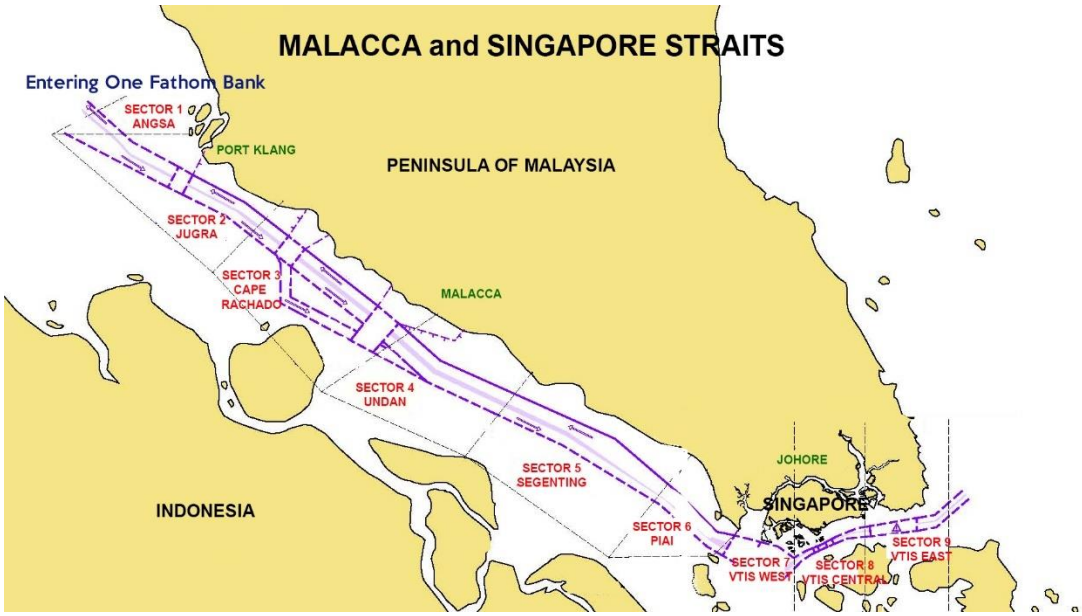

Figure 13 Dispositif de Séparation du Trafic au détroit de Malacca et de Singapour
Source : pac-venture.com (2018)

C'est dans cette région géographique que le 21e siècle connaîtra la première explosion de la piraterie, une décennie avant la Somalie, et deux décennies avant le Golfe de Guinée.

Peter Gwin, journaliste pour National Geographic expliquait en 2007 lors d'une interview que le détroit de Malacca laissait cours à plusieurs types de piraterie. Majoritairement, les pirates associés au crime organisé ciblaient certains pétroliers, profitant de la montée du prix du baril principalement dû à l'invasion de l'Irak par les Etats-Unis. Les pirates pouvaient aborder le navire avant de maitriser l'équipage et transférer une partie de la cargaison en STS vers un autre navire ou dans un port à proximité. Les assaillants pouvaient aussi kidnapper l'équipage avant de les séquestrer sur des îlots aux alentours[132]. De 2002 à 2007, l'IMB a recensé 258 incidents dans le détroit de Malacca, dénombrant 200 marins pris en otage et 8 morts[133].

[131] OMI, SN/Cir.198
[132] Gwin, Writer Tracks Modern-Day Pirates in Malaysia
[133] ICC-IMB, 2007 Piracy and Armed Robbery Against Ships Annual Report

On peut notamment citer la prise d'otage du capitaine et chef mécanicien du vraquier *Ocean Bridge* en 2005 au niveau de Kuala Lumpur. Les pirates auraient demandé une somme proche de 150 000 euros pour leur libération[134].

Un autre incident majeur dans le détroit de Malacca en 2003 montre les moyens que possédaient les criminels. Lorsque 50 pirates équipés d'armes automatiques, sur 2 navires différents, ont attaqués le navire de pêche *MV Dong Yih* pendant près de 2 heures. Le capitaine fût blessé et la superstructure criblée d'une centaine de balles[135].

La piraterie dans le détroit de Malacca s'est largement développée à la fin des années 1990 et au début des années 2000. Les incidents toujours plus violents ont donc motivé les organisations internationales à prendre certaines mesures. Le risque de la présence terroriste est aussi présent. L'espace restreint des détroits permettant aisément à des individus malintentionnés de détourner un navire et de l'utiliser à des fins criminelles, utilisant par exemple un chargement de nitrate d'ammonium comme explosif. Ce produit chimique fût notamment la cause d'un incident survenu à Brest en 1947[136] et également de l'explosion au port de Beyrouth en 2020[137].

4.2.1.1 Le terrorisme maritime dans la région

La crainte du développement du terrorisme maritime dans la l'Asie du Sud-Est n'est pas sans fondements. En effet, depuis la fin des années 1980, plusieurs groupes religieux radicalisés ont reçu l'aide d'Al Qaïda, le groupe le plus notable étant *Jemaah Islamiyah* (JI), littéralement « Communauté Islamiste »[138]. Le groupe fût formé dans les années 1960 alors que l'un de ses fondateurs militait pour l'établissement de la *sharia* en Indonésie[139]. Il est principalement connu pour être le commanditaire des attentats de Bali de 2002 et 2005 et pour avoir planifié de nombreux actes de terrorisme maritime visant des bâtiments militaires de l'US Navy présent en Asie du Sud-Est[140].

[134] Permal, Piracy and Sovereingty in the Strait of Malacca
[135] Herbert-Burns, Compound piracy at sea in the early twenty-first century
[136] Séré, En 1947, un cargo chargé de nitrate d'ammonium explosait à Brest
[137] Pompeo, Explosion in Beirut – Secretary Pompeo's Statement
[138] M. Murphy, Small boats, weak states, dirty money
[139] CFR, Jemaah Islamiyah (a.k.a. Jemaah Islamiah)
[140] M. Murphy, Small boats, weak states, dirty money

4.2.1.2 La lutte contre la piraterie

C'est en 2005 que le Lloyd's Joint War Risks Committee listait les détroits de Malacca et Singapour comme « high risk war zone ». En 2006 qu'on verra la création du *Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia* et de l'*Information Sharing Centre* ReCAAP ISC, à Singapour. On peut noter que l'Indonésie et la Malaisie ont refusé de faire partie de l'accord visant à combattre militairement la présence pirate dans leurs eaux. Ils préféraient s'appuyer sur leurs propres marines nationales pour protéger leurs eaux. Le premier ministre Malaisien Abdullah Ahmad Badawi affirmant en 2004 « I think we can look after our own area »[141]. D'aucuns pensent également qu'une des raisons supplémentaires que l'Indonésie soit réticente au combat contre la piraterie était potentiellement que de 70 à 75% des dépenses militaires du pays étaient couvertes par des activités illégales, telle la piraterie[142].

Cependant, d'autres états, comme entre autres Singapour, la Chine, l'Inde mais aussi la Norvège, les Pays-Bas et les Etats-Unis, ont décidé d'utiliser leur puissance navale pour aider les puissances locales. Il n'est pas surprenant de voir les Américains participer à un accord militaire multilatéral. En effet, après les évènements du 11 septembre 2001, les Etats-Unis souhaitent renforcer leur présence militaire dans le monde. L'antiterrorisme et l'antiprolifération étant au cœur de la stratégie de sécurité militaire des Etats-Unis[143].

La région a connu un pic d'incident en 2000, attribué à la crise économique connue par l'Asie en 1997[144]. Elle est vite devenue l'épicentre de la piraterie mondiale. Cependant les états ont su répondre efficacement aux problématiques en adoptant une politique agressive contre la piraterie et les vols à main armée en mer. Il en a résulté, de 2016 à 2020, l'absence totale d'incidents. On ne peut cependant assurer avec certitude que ces patrouilles resteront efficaces sur le long terme[145].

[141] Ramachandran, Divisions over Terror Threat in Malacca Straits
[142] Liss, The Challenges of Piracy in Southeast Asia and the Role of Australia
[143] Badot, La sécurisation du détroit de Malacca : un défi pour l'Asie
[144] Raymond, Piracy and Armed Robbery in the Malacca Strait
[145] ICC-IMB, 2021 Annual IMB Piracy Report

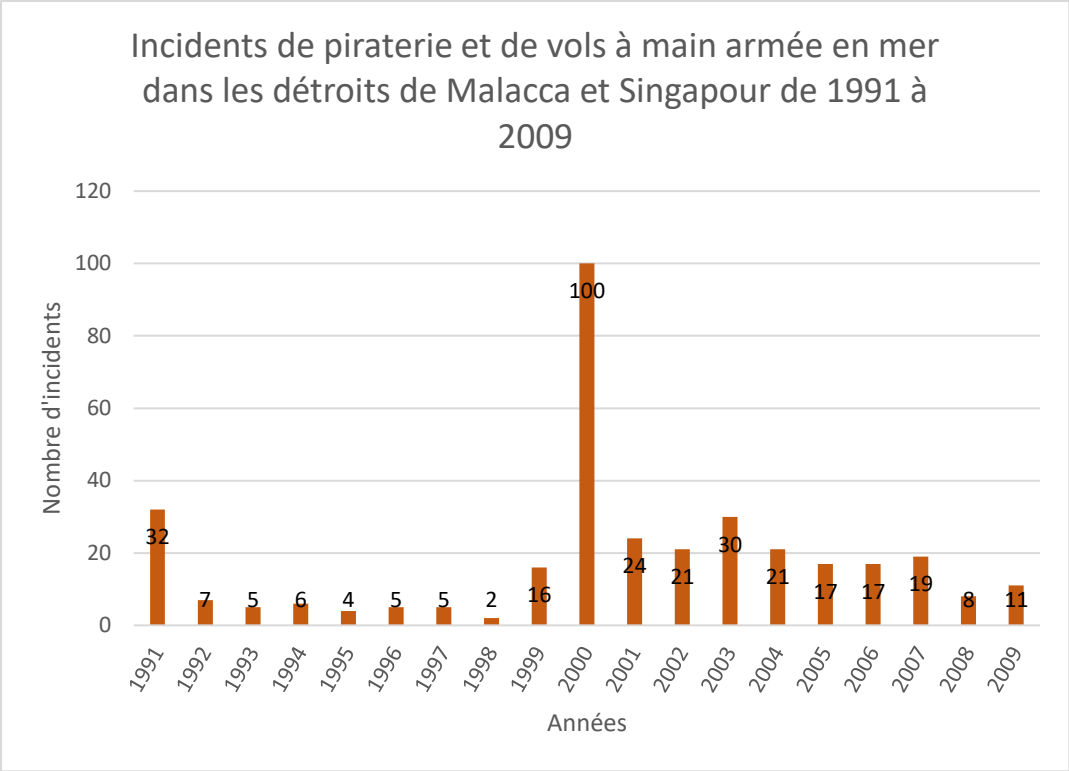

Figure 14 Incidents de piraterie et de vols à main armée en mer dans les détroits de Malacca et Singapour de 1991 à 2009
Source : propre graphique, basé sur les données de Nokerman (2010)

4.2.2 Le détroit de Singapour

À ce jour, l'épicentre de la piraterie asiatique s'est déplacé du détroit de Malacca vers celui de Singapour.

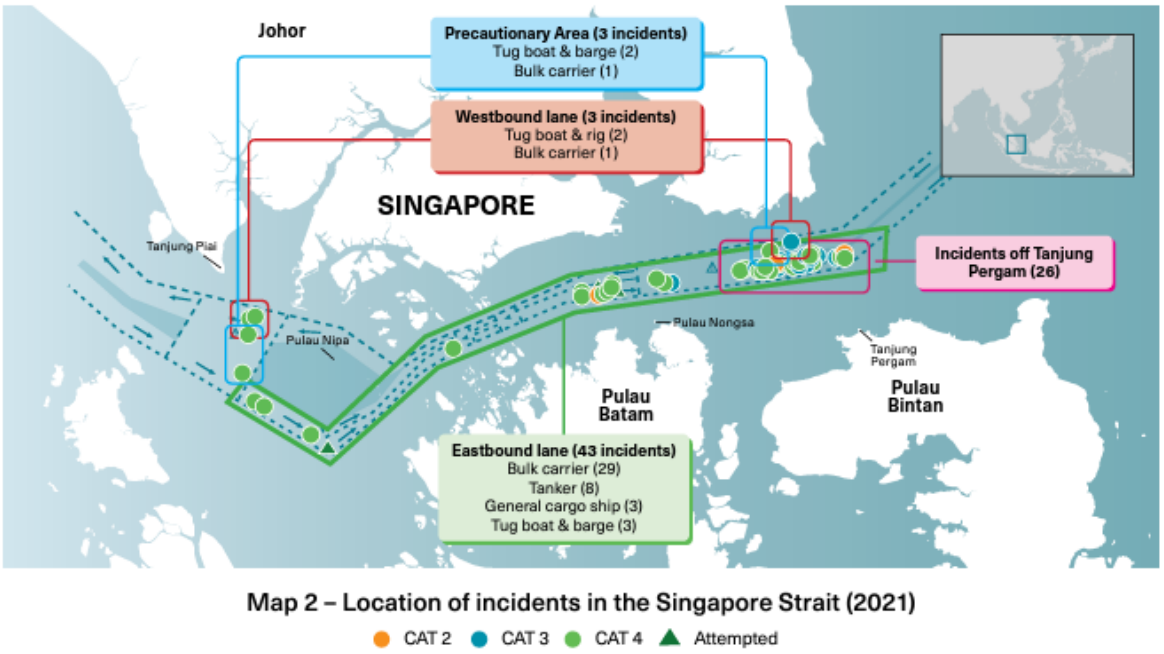

Figure 15 Carte de la piraterie dans le Détroit de Singapour en 2021
Source : ReCAAP ISC (2022)

Les pirates qui agissent dans le détroit de Singapour ont un mode opératoire qui leur est propre. À bord de navires de pêche non-ostentatoires (appelés *pancung* en Indonésie[146]) équipés d'un ou plus moteurs hors-bord, ils agissent fréquemment de nuit (en 2021, 27 des 35 incidents rapportés se déroulaient entre 21h et 06h heure locale[147]), généralement pourvus d'armes blanches. Les pirates n'ont pas forcément besoin d'échelles pour aborder les navires qui circulent à allure réduite dans le dispositif de séparation du trafic. Ils peuvent aussi simplement utiliser une tige de bambou munie d'un crochet pour se hisser à bord[28]. Ils repèrent les navires les plus lents, au franc-bord réduit et les abordent généralement par la poupe[148]. Lorsque les esquifs utilisés par les pirates sont de trop faible puissance, ces derniers peuvent utiliser une méthode d'approche alternative. Ils positionnent deux de leurs navires de chaque côté de la proue de la cible, un câble tendu de l'un à l'autre. La force du navire victime est utilisée pour rapprocher les deux bateaux pirates le long de la coque de ce dernier[149].

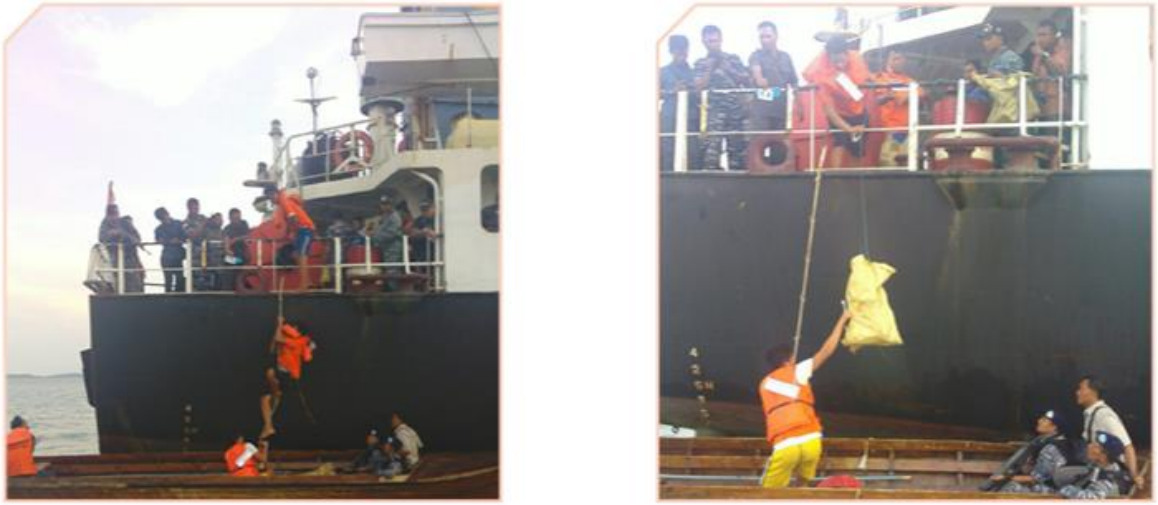

Figure 16 Simulation d'abordage utilisant une corde nouée et un grapin (à gauche) et du transfert du butin (à droite) par des pirates arrêtés par la marine Indonésienne
Source : ReCAAP (2016)

Leur objectif est bien précis. Ils recherchent les objets précieux de l'équipage. Ils n'hésitent aucunement à faire usage de leurs armes en menaçant voire en blessant le personnel à bord qui tenterait de les en empêcher. Cependant, les pirates opérant dans le Sud-Est de l'Asie sont de loin les moins violents, en 2021 on ne compte « que » 7 violences infligées à l'équipage,

[146] M. Murphy, Small boats, weak states, dirty money
[147] ICC-IMB, 2021 Annual IMB Piracy Report
[148] Kemp, Ross Kemp in the Search of Pirates
[149] Davis, Piracy in Southeast Asia shows signs of increased organisation

contre près du double dans les Amériques et 9 fois plus au total dans le Golfe de Guinée[150]. Même si les pirates abordant les navires en Asie du Sud-Est sont généralement armés, il est très rare que leurs opérations finissent par des blessures sérieuses. La non-violence aide subtilement les assaillants à garder profil-bas. Plus leurs opérations sont violentes, plus les autorités voudront stopper ces incidents[151]. Les pirates veulent à tout prix éviter de reproduire les causes qui ont mené à l'éradication de la piraterie dans le détroit de Malacca.

Leur particularité, la rapidité. En effet ils agissent en quelques minutes avant de repartir et repérer leur prochaine victime, ils n'hésitent pas à stopper l'opération et fuir le navire s'ils se savent repérés. Nommée « shopping » par les pirates eux-mêmes, cette opération est répétée à volonté par les assaillants. En effet, en 2021, on compte 6 dates avec 2 incidents la même journée, avec un intervalle de temps entre 2h et 4h[152]. À l'abri des autorités dans ces eaux indonésiennes parsemées d'ilots où il est aisé de se cacher, les pirates peuvent ainsi spolier de nombreuses cibles.

Un incident typique dans le détroit de Singapour se déroule comme suit :

« Four robbers boarded the ship underway. They assaulted and injured the fourth engineer, stole engine spares and escaped. Alarm raised, PA announcement made, and crew mustered. On searching the ship no robbers were found. Incident reported to VTS. »[153]

Les pirates de l'Asie du Sud-Est se sont transformés en quelques années de criminels opportunistes en des syndicats professionnalisés. Les voleurs sont la plupart du temps payés comme des salariés. Ils perçoivent une rémunération référencée par un taux horaire, pouvant atteindre jusqu'à 500 dollars de l'heure[154].

La baisse du nombre d'incidents dans la seconde moitié des années 2010 aurait pu en son temps permettre de croire en l'essoufflement de la piraterie dans la région. Toutefois, depuis 2018, on constate une augmentation majeure d'actes criminels qui confirme combien cette activité délictueuse est toujours réelle en Asie du Sud Est.

[150] ICC-IMB, 2021 Annual IMB Piracy Report
[151] Spiess, Black Spots
[152]ICC-IMB, 2021 Annual IMB Piracy Report
[153] ICC-IMB, 2021 Annual IMB Piracy Report
[154] von Hoesslin, Lawless Oceans

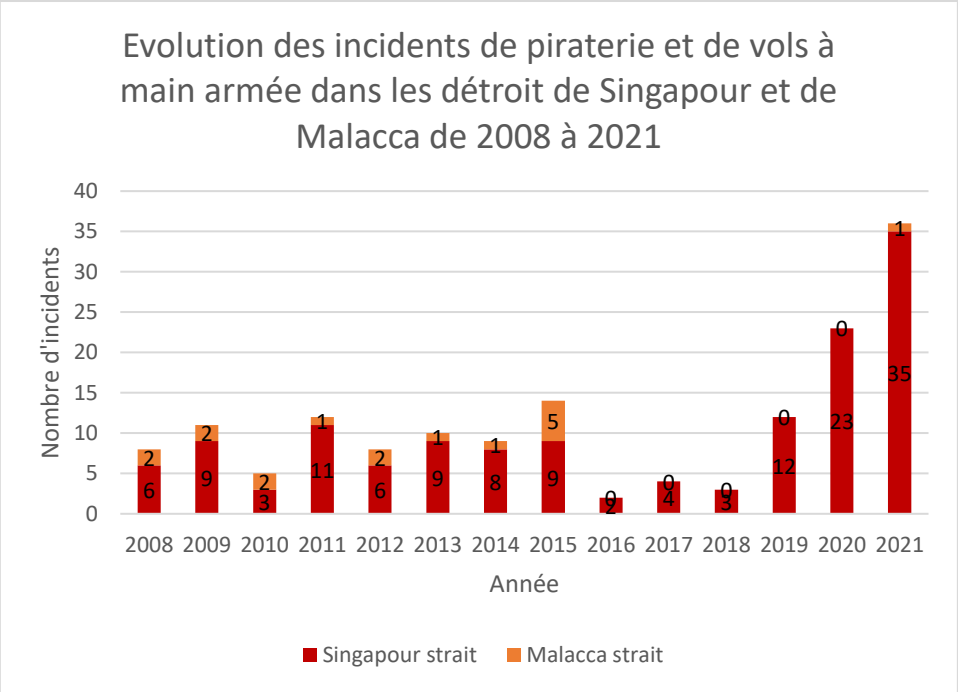

Figure 17 Evolution des incidents de piraterie et de vols à main armée dans les détroits de Singapour et de Malacca
Source : propre graphique, basé sur les données de l'IMB (2021)

4.2.2.1 La lutte contre la piraterie

Alors que leurs homologues africains privilégient le détournement de navires et la prise d'otage des équipages, les activités criminelles dans ces eaux sont bien moins agressives. Même si les modes opératoires des criminels du Sud-Est de l'Asie ne changent pas beaucoup, on peut lire quelques tendances. L'augmentation d'incidents impliquant des remorqueurs et des barges de 2008 à 2011, c'est ce constat qui initiera la rédaction du « Tug Boats and Barges (TaB) Guide Against Piracy and Sea Robbery » par le ReCAAP en 2013[155]. Suivra en 2015, l'édition du « Guide for Tankers Operating in Asia against Piracy and Armed Robbery Involving Oil Cargo Theft » motivée par l'augmentation du vol de pétrole entre 2014 et 2015[156].

L'Asie du Sud-Est profite également de son équivalent du BMP, avec la parution en 2016 du « Regional Guide to Counter Piracy and Armed Robbery Against Ships in Asia » née de la coopération entre le ReCAAP et plusieurs agences maritimes[157]. Cette publication, comme celles que nous retrouvons sur le continent africain, a pour but de faciliter l'opération de navires dans les zones de pirateries de l'Asie du Sud-Est. Fournissant des détails quant au *risk*

[155] ReCAAP ; IFC, Tug Boats and Barges (TaB) Guide Against Piracy and Sea Robbery
[156] ReCAAP ; IFC ; RSIS, Guide for Tankers Operating in Asia against Piracy and Armed Robbery Involving Oil Cargo Theft
[157] ReCAAP et al., Regional Guide to Counter Piracy and Armed Robbery Against Ships in Asia

assessment, à la préparation des défenses physiques du navire pour retarder voire empêcher un abordage, ainsi qu'aux actions à prendre lors d'une attaque.

Cet ouvrage est la Bible du marin qui souhaite se préparer à lutter contre un acte de piraterie ou de vol à main armée en Asie du Sud-Est.

La sécurité du détroit de Singapour a su profiter de la présence militaire internationale dans le détroit de Malacca et la Mer de Chine Méridionale. Depuis 2002 et chaque année, la Marine singapourienne s'entraine avec des marines internationales, dont la Navy américaine, afin d'améliorer leur efficacité de réponse contre des incidents de piraterie[158]. Cependant, le détroit de Singapour ne possède pas autant de patrouilles militaires que le détroit de Malacca et c'est principalement la Marine singapourienne en coopération avec l'Indonésie, la Malaisie et la Thaïlande qui assurent la sécurité des eaux territoriales de Singapour. C'est la vague d'incidents de piraterie et de vols à main armée depuis 2019 qui a galvanisé les autorités singapouriennes pour développer leur sécurité, en lançant le *Maritime Security and Response Flotilla* (**MSRF**)[159].

L'Asie du Sud-Est a toujours subi des actes de piraterie dans ses eaux. Depuis ces dernières décennies, avec l'augmentation de la pauvreté et de l'insécurité, la pratique s'est largement démocratisée. Le taux de pauvreté dans cette partie du monde n'est certes pas similaire aux autres territoires où la piraterie sévit, cependant il connait d'immenses inégalités entre Singapour et les pays voisins. Cette différence de richesse couplée à l'insécurité peut mener les populations à se tourner vers ces activités enrichissantes que sont la piraterie et le brigandage. L'augmentation des incidents dans le détroit de Malacca à la fin des années 1990 a su être réprimée par l'augmentation de la présence militaire dans la région. La piraterie a cependant réussi à se déplacer dans le détroit voisin. Le détroit de Singapour est désormais la région la plus densément impactée par les attaques. Le mode opératoire des assaillants est cependant moins agressif que dans les autres territoires dans le monde. La méthode et

[158] Menon, Singapore navy takes part in exercise with 20 countries to boost regional maritime security against terrorism, piracy
[159] Abke, Singapore counters pirates with new maritime flotilla

l’absence de violence explique le manque de volonté des institutions internationales à trouver des solutions pour endiguer le phénomène dans cette région du monde.

CHAPITRE 5 : L'Amérique du Sud

5.1 Géopolitique des Amériques

Davantage connue pour son trafic de narcoleptiques, l'Amérique latine n'en est pas moins une zone à risques en matière de piraterie.

L'Amérique Centrale et l'Amérique du Sud sont des régions très hétéroclites et la piraterie fait rage dans plusieurs de leurs pays, notamment le Venezuela, la Colombie, l'Equateur et le Pérou.

5.2 Piraterie en Amériques

L'Amérique Centrale est, elle aussi, une région stratégique pour le transport maritime. C'est en effet par le canal de Panama qu'une route s'ouvre aux navires entre les Océans Atlantique et Pacifique. On note cependant que le Panama ne souffre pas de la piraterie.

Ce fléau touche majoritairement la côte Nord de la Colombie et particulièrement Carthagène, l'Équateur à Guayaquil, Callao au Pérou et Port-au-Prince en Haïti. Ces zones particulièrement réduites laisseraient à penser que ces actes de pirateries sont le fait de groupes isolés.

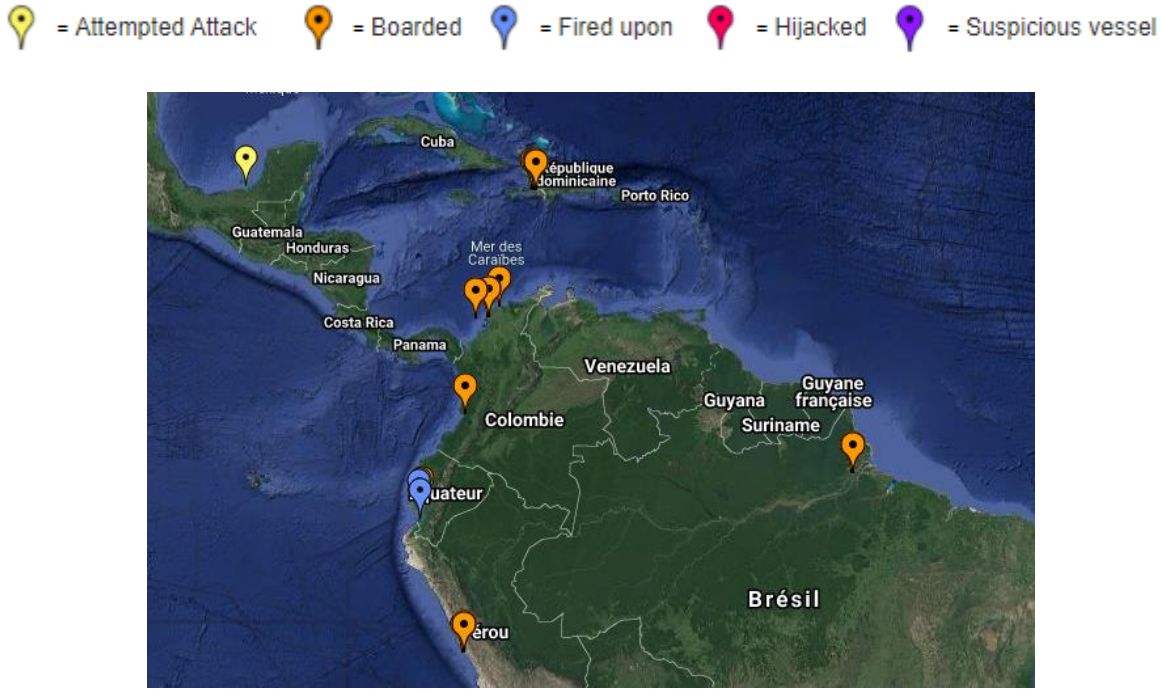

Figure 18 Carte de la piraterie aux Amériques en 2021
Source : ICC-IMB (2022)

À chaque secteur géographique son mode opératoire. C'est équipé d'armes blanches ou d'armes à feu que les pirates abordent, généralement de nuit (en 2021, 60% des navires abordés aux Amériques l'étaient entre 21h et 06h heure locale[160], les navires au mouillage. On relève que les pirates de cette région préfèreront cibler les navires à l'ancre, en 2021 77% des incidents se déroulaient sur des navires à l'ancre, contrairement aux autres zones comme le détroit de Singapour où, en 2021, 100% des navires attaqués étaient en route. Similairement au Golfe de Guinée, ce fait est en grande partie dû au temps d'attente que subissent de nombreux navires chaque jour, avant qu'une place ne se libère au port. Pour exemple ; au port de Callao au Pérou, on compte plusieurs de dizaines de navires à l'ancre tous les jours[161]. La figure suivante montre clairement la propension des pirates des Amériques à attaquer les navires à l'ancre, comparativement à leurs homologues dans le reste du monde.

CHART F: Region specific type of incident in relation to the status of vessel movement January – December 2021

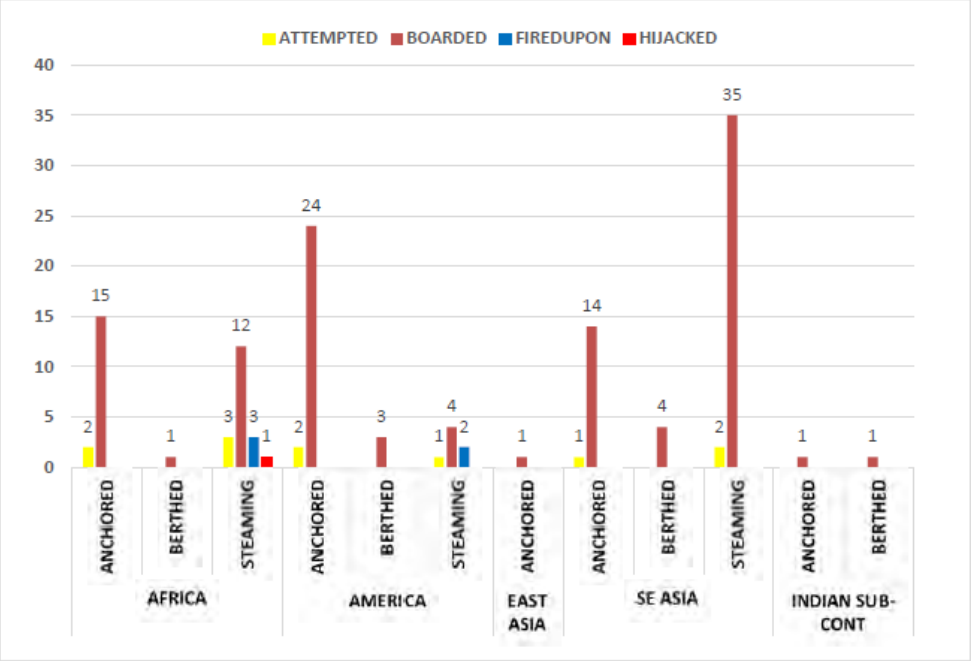

Figure 19 Type d'incident par région en relation avec le statut du mouvement du navire en 2021
Source : ICC-IMB (2022)

La côte Nord-Est du Mexique est aussi une région particulière, même si elle ne comptabilise que peu d'incidents, 4 en 2020 et 1 en 2021. On remarque que les pirates s'en prennent

[160] ICC-IMB, 2021 Annual IMB Piracy Report
[161] Marine Traffic, Callao Port

uniquement aux unités offshores, comme des navires poseurs de canalisations ou navires d'approvisionnement offshore[162].

Le Venezuela est de plus en plus calme, seulement 2 incidents ont été recensés depuis ces deux dernières années. On peut remarquer un pic en 2017 et 2018 avec respectivement 12 et 14 incidents[163].

Même si ces valeurs peuvent sembler faibles au regard du nombre d'incidents dans le Golfe de Guinée ou en Asie du Sud-Est, l'Amérique du Sud et l'Amérique Centrale figurent encore dans les régions les plus sensibles à la piraterie.

Le port de Guayaquil en Equateur possède lui aussi ses spécificités. En 2020 et 2021, 100% des navires abordés étaient des porte-conteneurs (les porte-conteneurs ne représentant que 34% des navires à faire escale dans ce port). Les attaques ont toutes le même déroulé : les assaillants abordent le navire, en route, dérobent le contenu de plusieurs conteneurs avant de s'enfuir.

On pourrait déceler ici un rapport potentiel avec un autre fléau de la région.

5.2.1 Les pirates en lien avec les narcotrafiquants

Le crime organisé est particulièrement développé en Amérique du Sud et Amérique Centrale. Toute la chaine du trafic de drogue est implantée dans cette région, culture, production, raffinement et trafic. En 2010, l'Amérique du Sud est considérée comme la seule productrice de cocaïne mondial, le Mexique et la Colombie comme les principaux exportateurs d'opiacés en direction des Etats-Unis et le Mexique comme la principale source d'amphétamines étrangères vers les Etats-Unis[164]. Cependant, ce sont l'Amérique du Nord et l'Europe de l'Ouest qui sont considérées comme les plus grands consommateurs de ces produits. Une partie importante des drogues en direction de l'Europe passe par l'Afrique de l'Ouest[165]. *European Police Office* (**EUROPOL**) estimait en 2007 qu'entre 25 et 30% de la production mondiale de cocaïne, soit environ 250 tonnes, arrivaient sur le marché européen chaque année, principalement en provenance du Venezuela et du Brésil. Le trafic se fait principalement par voie maritime, les produits illicites cachés parmi la cargaison des

[162] ICC-IMB, 2021 Annual IMB Piracy Report
[163] ICC-IMB, 2021 Annual IMB Piracy Report
[164] Congressional Research Service, Latin America and the Caribbean: Illicit Drug Trafficking and U.S. Counterdrug Programs
[165] Congressional Research Service, Illegal Drug Trade in Africa: Trends and U.S. Policy

conteneurs. L'Office des Nations Unies contre les drogues et le crime (**UNODC**) affirme que 55% des saisies de cocaïne se font dans le transport maritime[166]. Ce sont donc les ports européens majeurs, comme Hambourg, Anvers ou Le Havre, qui se partagent une quantité importante des saisies de la drogue en provenance d'Amérique latine[167].

La sécurité des ports est un enjeu majeur dans les Caraïbes et l'Amérique du Sud. Souvent dû au manque de ressources, la complicité potentielle du personnel avec les trafiquants locaux et à l'ingéniosité des criminels pour cacher leur marchandise. Les autorités portuaires détectent rarement les produits illicites présents au sein de leur territoire. Les conteneurs sont rarement inspectés[168].

Pourtant, 420 millions de conteneurs sont transportés autour du monde chaque année. Si une large majorité transporte des marchandises licites, certains sont utilisés pour transporter drogues, armes et mêmes des êtres humains[169]. L'Organisation des Nations Unies (**ONU**) a développé en 2003 le Programme de Contrôle des Conteneurs afin d'assister les autorités à renforcer leurs défenses contre l'exploitation des conteneurs par le crime organisé.

On peut noter l'aide de l'ONU à la saisie de 4,5 tonnes de cocaïne à Guayaquil en octobre 2021, à destination d'Anvers[170]. Cependant, la majeure partie des interceptions de marchandises illicites par les autorités sont réalisées dans le pays d'arrivée du conteneur. Comme en février 2021 au port de Hambourg, où les autorités Allemandes ont saisi 16 tonnes de cocaïne, d'une valeur estimée entre 1,5 et 3,5 milliards d'euros, en provenance du Paraguay. La drogue fut trouvée dans plus de 1 700 boîtes de conserves normalement remplies de mastic[171]. En 2020, un total de 65,48 tonnes de cocaïne a été saisi par les autorités belges au port d'Anvers[172].

Les criminels changent très régulièrement les méthodes pour dissimuler leur marchandise dans les conteneurs. Les trafiquants dirigent généralement des compagnies d'exportation, leur permettant de cacher la drogue directement dans des contenants, mélangée à la marchandise. Les conteneurs réfrigérés sont le plus souvent utilisés, facilitant la dissimulation

[166] UNODC, Transnational Organized Crime in Southeast Asia: Evolution, Growth and Impact
[167] EUROPOL, EU Drug Markets Report
[168] France Télévisions, Complément d'enquête, Le Havre, coke en stock
[169] UNODC, Container Control
[170] Belga, Saisie de 4,5 tonnes de cocaïne à destination d'Anvers
[171] The Guardian, Twenty-three tonnes of cocaine seized in Europe's biggest haul
[172] Expatica, Cocaine seized at key European port busts records

de cargaison illicite dans les unités de réfrigération. Des conteneurs sains peuvent aussi être utilisés, c'est ce qu'on appelle la contamination de conteneurs, représenté dans la figure suivante. Dans ce cas-ci, un employé du port, recruté par les criminels, accèdera au contenu du conteneur en brisant son scellé de sécurité. Puis introduira un nombre de sacs remplis de drogue avant de refermer le conteneur avec une réplique du scellé de sécurité[173].

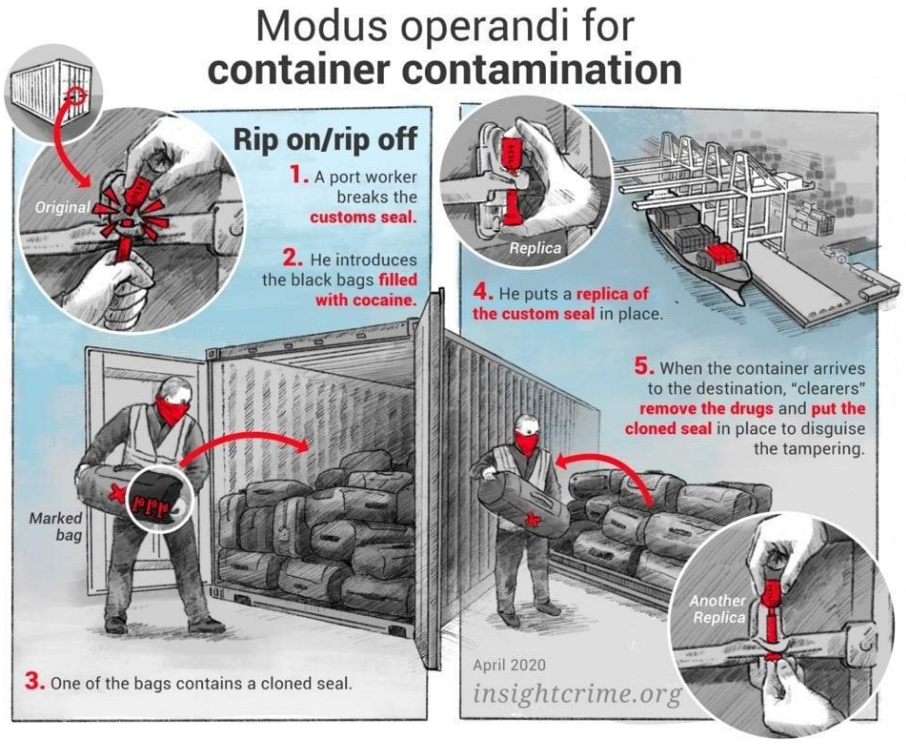

Figure 20 Mode opératoire pour la contamination d'un conteneur
Source : insightcrime.org (2021)

Certains cartels de drogue contrôlent même l'intégralité des dockers de certains ports, c'est le cas du Gang de Barrio King au Pérou, ce qui leur assurait un monopole sur le trafic de drogue à Callao, le plus grand port du pays[174].

La corruption du personnel n'est pas seulement présente dans les ports. Certains trafiquants en viennent à engager les membres d'équipages pour récupérer et cacher de la marchandise illicite à bord, dans des conteneurs, ou même au sein du navire. Ce fut le cas à bord du *MSC Gayane*, où certains marins utilisèrent la grue du navire pour hisser plusieurs tonnes de cocaïne avant de les cacher dans divers conteneurs. Le navire fut arrêté au port de

[173] France Télévisions, Complément d'enquête, Le Havre, coke en stock
[174] Ramirez, Container Shipping: Cocaine Hide and Seek

Philadelphie par les autorités américaines, où 20 tonnes de drogue, d'une valeur d'1 milliard de dollars, purent être saisies[175].

Avec toutes ces données, on pourrait extrapoler que la série de vols à main armée se déroulant en Equateur à proximité du port de Guayaquil, comme décrit dans le chapitre précédent, pourrait avoir un rapport avec le trafic de drogue. L'abordage des porte-conteneurs étant un moyen pour les narcotrafiquants de récupérer leurs produits illicites avant leur arrivée au port. Il n'y a malheureusement pas d'archives stipulant l'origine de ces conteneurs, ce qui pourrait appuyer cette théorie.

Un incident typique en Equateur se déroule comme suit :

> Eight armed robbers in two speed boats approached the ship underway. Master raised the alarm and activated the SSAS. The robbers fired warning shots, managed to board the ship, and opened 15 containers. When the search lights were directed towards the robbers, they opened fire towards the bridge. Port Control and Coast Guard notified. The robbers stole part of the cargo and escaped. Later, the Coast Guard boarded the ship for investigation. No injuries to crew.[176]

Alors que leurs voisins sud-américains préfèrent l'utilisation d'armes blanches, les pirates équatoriens se munissent d'armes automatiques. Ce type d'armement peut laisser à penser que les assaillants pourraient appartenir, servir ou collaborer avec des groupes de narcotrafiquants, ce qui pourrait expliquer les moyens mis en œuvre pour récupérer le contenu des conteneurs.

Il fut aussi reporté que des bandes armées à proximité du port de Guayaquil abordaient certains navires, avant de forcer l'équipage à récupérer des produits illicites sous la menace d'une arme[177]. Ces dernières informations soutiennent la théorie du lien entre les pirates et les trafiquants de drogue équatoriens.

[175] justice.gov, MSC Gayane Crew Member Pleads Guilty to Cocaine Trafficking Stemming from One of the Largest Drug Seizures in U.S. History
[176] ICC-IMB, 2020 Annual Piracy Report
[177] Ramirez, Container Shipping: Cocaine Hide and Seek

Bien que la piraterie dans les Amériques ne possède pas la même virulence que dans les autres régions du monde, elle n'en est pas moins un danger à l'industrie maritime. Ici, les pirates préfèrent se concentrer sur des larcins de faible envergure, plutôt que de s'attaquer aux marins. Cependant, on peut deviner un lien entre la piraterie et le trafic de narcoleptiques, autre fléau de cette région. Les trafiquants utilisent des méthodes toujours changeantes pour duper les autorités. Parfois en impliquant les marins eux-mêmes dans leurs exactions. C'est le port de Guayaquil en Equateur qui représente au mieux ce type d'incidents qui relie brigandage et trafic de drogue.

Lors de cette première partie, nous avons vu quelles sont les causes du développement de la piraterie et comment elle représente un des principaux enjeux de la sécurité maritime au 21ème siècle. Insécurités économiques, sociales, politiques, sont tous des facteurs qui favorisent le développement de groupes pirates dans les différentes régions affaiblies dans le monde. Les groupes criminels somaliens ont su profiter de l'absence de gouvernement pour perpétrer leurs exactions et se développer rapidement jusqu'à atteindre l'épisode de piraterie le plus intense du 21ème siècle. Les états du Golfe de Guinée, souffrant de leur économie fragile, n'a pas su contrer l'élan de piraterie qui s'est développé après l'éradication de la menace sur la Corne de l'Afrique. La piraterie représente aujourd'hui une industrie à part entière dans cette région du monde, où l'on échange une vie pour une mallette d'argent. L'Asie du Sud-Est possède également une large insécurité ainsi que de grandes différences de richesse. Les pirates dans cette région se livrent généralement au vol d'équipement et objets personnels de l'équipage. Au même titre, les pirates qui opèrent dans les Amériques se contentent généralement de voler le navire et l'équipage. Même si quelques incidents semblent être liés au trafic de drogue, très présent dans la région.

Pour contrer la piraterie, les organismes internationaux répondent de la même manière. Ils augmentent la présence militaire dans les territoires touchés afin de diminuer l'insécurité maritime. Cependant, ces opérations sont très couteuses, et ne traitent pas les causes

fondamentales du problème de la piraterie, qui sont généralement les faiblesses sociaux-économiques et politiques des états.

Partie II : La Cyberpiraterie

CHAPITRE 6 : La Cyberpiraterie en général

En plus de la sécurité maritime menacée par la piraterie mondiale, l'industrie maritime doit également faire face aux enjeux de la cybersécurité.

L'industrie maritime connait depuis plusieurs années un développement accru de ses systèmes informatiques. Les navires adoptent et profitent de plus en plus des systèmes digitaux et automatisés, que ce soit pour l'aide à la navigation et la facilitation des opérations de chargement. Bien qu'apportant un confort non négligeable, le développement de ces « nouvelles technologies » augmente les risques quant à la sécurité à bord. En effet, les *Operational Technologies* (**OT**)[i] et *Information Technologies* (**IT**)[ii] sont de plus en plus souvent connectées à Internet, multipliant le risque d'attaques visant les systèmes du navire. Les risques peuvent venir de l'extérieur, comme de l'intérieur, avec l'introduction de *malwares* par des périphériques de stockage personnels.

6.1 Différents types de cyberattaques

Les navires et entreprises maritimes peuvent être la cible de deux types d'attaques ;

Les attaques non-ciblées exploitent des vulnérabilités répandues dans les systèmes informatiques en utilisant des outils facilement disponibles. Elles incluent entre-autres[178] :

- Le *Malware*, littéralement « logiciel malveillant », décrit une catégorie de cyber-attaques comprenant spywares, ransomwares, virus, cheval de Troie… Les spywares espionnent les activités de l'utilisateur et peuvent enregistrer ses données personnelles. Les ransomwares cryptent les données de l'utilisateur jusqu'à ce qu'une rançon soit payée. Les virus se multiplient et se propagent vers d'autres systèmes informatiques pouvant détruire des données voire détruire le système lui-même. Les chevaux de Troie persuadent l'utilisateur de sa nature sécurisée jusqu'à son installation, puis pourront altérer, détruire ou voler des données.

[178] BIMCO et al., The Guidelines On Cyber Security On Board Ships V4.0 ; FORTINET, Cyberglossary
i Les IT sont les systèmes et logiciels qui se concentrent sur des données comme information
ii Les OT utilisent le matériel et les logiciels pour gérer les équipements et systèmes à bord

- Le *water holing* consiste à reproduire ou compromettre un site internet afin de forcer l'utilisateur de lui communiquer des informations à son insu.
- Le *phishing* consiste à envoyer un grand nombre de courriers électroniques frauduleux en faisant croire en leur légitimité afin d'obtenir des informations personnelles. Cette technique peut être associée à d'autres pratiques.
- Le *Drive-by Download* consiste à injecter un malware depuis un site internet qui s'intègrera dans le navigateur de l'utilisateur pour analyser les failles de sécurité dans le système.

Les attaques ciblées sont souvent plus sophistiquées et utilisent des outils spécifiquement *conçus* pour atteindre les entreprises ou navires. Elles incluent entre-autres[179]:

- Le *Spear-phishing*, semblable au *phishing*, utilise des informations personnelles, généralement récoltées sur les réseaux-sociaux. Il permet d'atteindre plus facilement les victimes. Le *Whaling* est une technique de *Spear-phishing* consistant à cibler des personnes au poste à responsabilité, comme le PDG ou le capitaine d'un navire.
- Le *Denial-of-Service* (DoS) consiste à surcharger les ressources d'un système en le noyant sous des requêtes de connexion. Le *Distributed Denial-of-Service* (DDoS), encore plus insidieux, ils utilisent plusieurs appareils informatiques afin de dissimuler ses origines.
- Le *Brute-Force* est le type de cyberattaque le moins complexe. Il s'agit d'un logiciel qui tente d'accéder à des informations numériques en testant toutes les combinaisons possibles d'un mot de passe. Cette méthode peut facilement être utilisée conjointement avec des *malwares* ou *phishing*, après avoir appris connaissance d'informations personnelles sur la cible. La plupart des sites internet et logiciels enregistrent les mots de passes des utilisateurs dans une base de données hachée par la fonction MD5, cette fonction permet de transformer une suite de caractères en 32 caractères en notation hexadécimale. Cette fonction est très difficilement renversée, on peut donc considérer que les mots de passes sont efficacement protégés. L'utilisation de mots de passe complexes et différents est donc plus efficace pour

[179] BIMCO et al., The Guidelines On Cyber Security On Board Ships V4.0

contrer ce genre d'attaques. Un simple code à 4 chiffres possèdera $10^{(4)}$ possibilités, alors qu'un mot de passe à 10 caractères utilisant lettres minuscules, majuscules, chiffres et caractères spéciaux tous compris dans la table ASCII possèdera $94^{(10)}$ possibilités. Il est aussi possible d'utiliser des clés de chiffrement qui cryptent les données jusqu'à $2^{(128)}$ ou même $2^{(256)}$ possibilités, empêchant même les plus puissantes machines de cracker le code.

6.2 Qui sont ces « cyberpirates » ?

On peut classer les criminels qui se cachent derrière ces cyberattaques en quatre catégories :

- Les criminels ordinaires sans compétences spécifiques ne sont en soit pas une menace. Toutefois, ils ont facilement accès à un marché noir, qui lui peut fournir les compétences nécessaires à une cyberattaque. La société de Cybersécurité *Trend Micro* estimait en 2012 les coûts pour commander certaines activités illégales[180]. Entre 100 et 550 $ pour installer un *Malware* sur 1 000 ordinateurs, et 1 300 $ pour l''implantation d'un Cheval de Troie dans un compte bancaire. Tout type de cyberattaques peuvent être commandés par des organisations criminelles ne possédant pas les capacités à le faire elles-mêmes. C'est ce genre de criminels qu'on retrouvera dans l'industrie maritime, généralement impliqués dans le vol de marchandises ou d'informations ou même le détournement de navires[181]. Leurs attaques sont donc principalement un moyen d'optimiser leurs activités criminelles existantes, comme l'extorsion ou le trafic de drogue.
- Les cybercriminels avec toutes les compétences nécessaires peuvent soit travailler pour les criminels énoncés ci-dessus ou à leur propre compte. La société de cybersécurité *CrowdStrike* indiquait en 2013 que le cybercrime était dominé par 50 groupes[182]. Ces groupes ont les ressources et les compétences pour organiser n'importe quel type d'attaque. Cependant, ils sont généralement motivés par l'argent et préfèreront les *Ransomwares*[183]. Le piratage n'est pas forcément l'activité principale de ces individus, il peut être simplement un hobby. Notamment, nous avons remarqué

[180] Trend Micro, Russian Underground 101
[181] CyberKeel, Virtual pirates at large on the cyber seas
[182] CSO, Global cybercrime dominated by 50 core groups, CrowdStrike report finds
[183] CyberKeel, Virtual pirates at large on the cyber seas

une augmentation de 400% du nombre de cyberattaques contre l'industrie maritime, cette hausse peut être attribuée aux confinements dû à l'épidémie de SARS-COV2[184]. Les cybercriminels ayant davantage de temps libre pour perpétrer leurs exactions.

- Le groupe des *hacktivistes* représente tous les groupes utilisant les cyberattaques comme moyen de supporter leur idéologie politique. Ces personnes pourraient cibler des entreprises qu'ils considèrent qu'elles méritent une punition. Par exemple une compagnie étant impliquée dans un incident maritime avec des conséquences environnementales, estimant que les sanctions prises par les autorités à son égard n'ont pas été assez sévères. Ce groupe sera principalement motivé par la destruction des données ou par la perturbation du fonctionnement global d'une entreprise.
- Les états possèdent bien plus de moyens dans ce domaine. Ils disposent généralement de services de renseignements et de personnel qualifié pour mener à bien n'importe quelle opération de cyberattaque. Ceci leur permet d'espionner un autre état ou de ralentir significativement son économie en attaquant sa capacité de transport maritime.

Les attaques peuvent provenir de différentes personnes avec des motivations diverses. Des activistes qui voudraient s'en prendre à l'intégrité et la réputation de l'entreprise, ou des criminels cherchant à s'emparer de données sensibles monnayables. Ces pratiques peuvent également s'appliquer dans le cadre d'espionnage industriel d'une entreprise concurrente cherchant à obtenir des données importantes. Notons cependant qu'il existe des cabinets de sécurité informatique et des communautés de hackers qui cherchent des failles de sécurité dans les réseaux, avant d'en informer les propriétaires, afin de renforcer la qualité des défenses mises en place.

[184] BlueVoyant, Supply Chain Disruptions and Cyber Security in the Logistics Industry

CHAPITRE 7 : Operational Technology

La plupart des systèmes OT à bord sont connectés sur un réseau local virtuel (**VLAN**) et sont donc moins sujets à des cyberattaques. Cependant, le système informatique local n'est pas invulnérable, et son infection pourrait être dévastatrice.

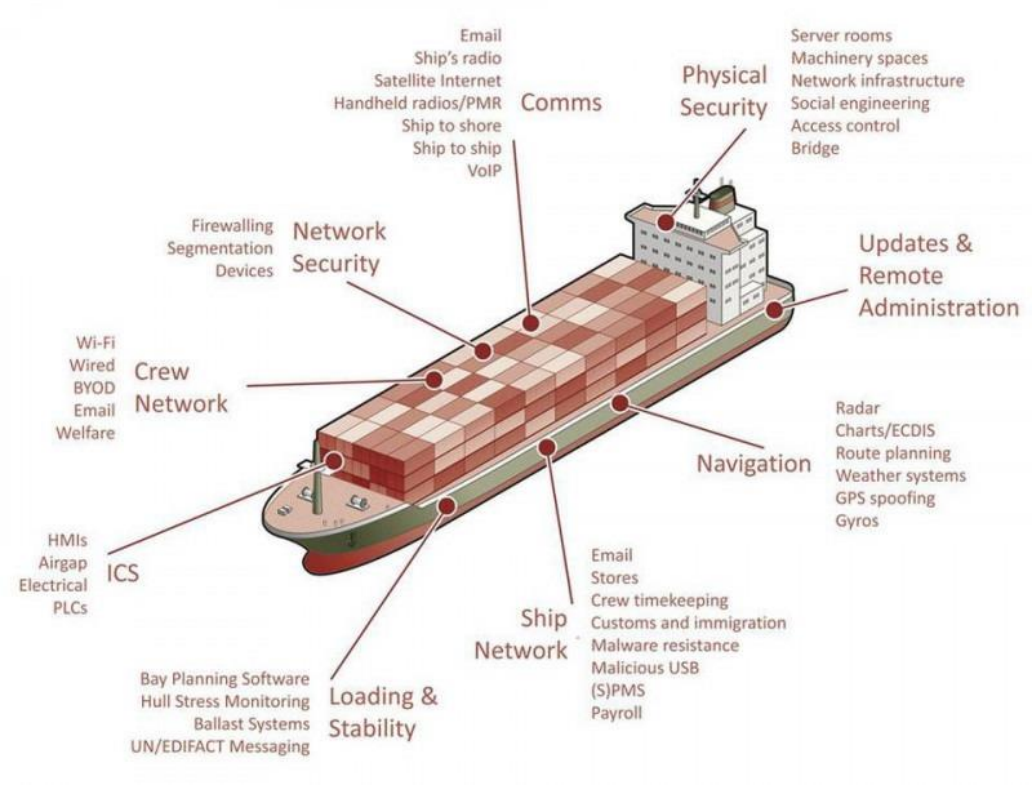

Figure 21 Systèmes connectés à bord
Source : pentestpartners.com (2017)

7.1 Brouillage et usurpation d'identité GNSS

Le brouillage (ou *Jamming*) empêche la cible de recevoir les signaux émis par les satellites par l'émission de bruits. Le **GNSS** utilise une puissance très faible ce qui le rend relativement simple à brouiller. Cependant, le brouillage est aussi un risque naturel de l'utilisation de systèmes de positionnement par satellite. En effet, l'activité solaire ou la présence de particules ionisées dans l'ionosphère peut être la cause d'effets similaires au brouillage intentionnel.

C'est en 2015 que la Corée du Sud subit le plus gros incident de brouillage GPS, alors que plus de 250 navires et 1 000 aéronefs ont été affectés. Selon la victime, un acteur parrainé par l'état Nord-Coréen aurait été l'auteur de cette attaque.

Le Professeur David Last du *General Lighthouse Authorities* mesura l'effet des brouilleurs sur les systèmes à bord. Dans un test, un brouilleur fut installé sur un phare. Les effets furent notables sur les récepteurs GNSS de navires jusqu'à une distance de 30 km. Certains récepteurs cessèrent simplement de fonctionner, alors que d'autres donnèrent de fausses positions, affirmant que le bateau naviguait sur la terre[185].

Lors d'un second test, des brouilleurs furent placés sur des navires, causant la panne de plusieurs systèmes comme le système de navigation, les horloges électroniques et l'AIS.

Ces séries de tests ont permis de souligner que la navigation moderne se repose essentiellement sur le GNSS. Si le système tombe en panne, le risque d'accident augmente énormément[186].

L'usurpation d'identité GNSS (ou *GNSS Spoofing*) envoie de fausses données à la cible en imitant les signaux satellites, par l'utilisation de stations fixes.

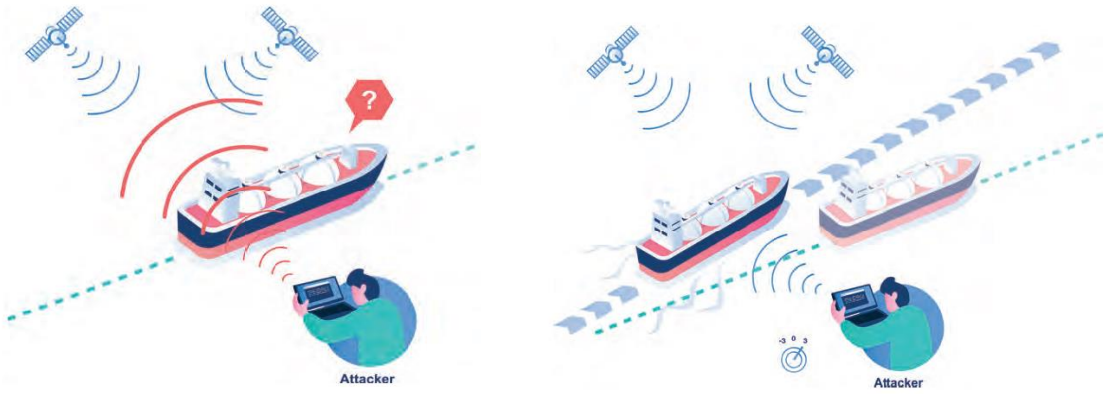

Figure 22 Brouillage (à gauche) et Usurpation d'identité GNSS (à droite)
Source : INTERTANKO (2019)

Dans le premier cas, un émetteur à courte ou longue portée empêchera la cible de recevoir les signaux des satellites. Cette pratique est relativement simple à détecter par l'officier de quart, puisque le navire n'affichera plus de position GNSS.

Dans le second cas, l'antenne GNSS transmet de fausses données au système qui affichera donc une position et/ou un cap erroné. Tous les sous-systèmes utilisant le GNSS souffriront de cette erreur. Cette méthode est plus insidieuse car le navire affichera une position légèrement erronée qui s'aggravera avec le temps. En 2013, des chercheurs de l'université

[185] CyberKeel, Virtual pirates at large on the cyber seas
[186] Graham, Shipping industry vulnerable to cyber attacks and GPS jamming

d'Austin ont réussi à détourner le GPS d'un yacht d'une valeur de 80 millions de dollars situé à 30 miles nautique des côtes en utilisant un équipement d'une valeur de 2 000 $[187]. Ces derniers ont réussi à détourner le cap du navire de 3 degrés. Même si le changement de cap fût notifié par le système de navigation et que l'équipage essaya de corriger l'erreur, la route du yacht resta sous le contrôle de l'équipe de chercheurs[188]. Le navire finira avec une position éloignée de plusieurs centaines de mètres de celle indiquée par le GPS.

En 2015, des fonctionnaires du gouvernement américain affirmaient que des trafiquants de drogue utilisaient la technologie de *GNSS Spoofing* afin de masquer leurs activités proches de la frontière mexicaine.[189] C'est cependant la Fédération de Russie qui est la pionnière dans ces technologies, on peut noter le déploiement de tels équipements sur des théâtres de guerre comme la Syrie ou l'Ukraine[190].

Un officier avertit quant aux risques et conséquences de brouillage ou d'usurpation d'identité GNSS possède plusieurs moyens de vérifier l'intégrité des données reçues par l'antenne. Si la terre est visible ou à portée du radar, il peut, conjointement à l'utilisation de l'ARPA, s'appuyer sur l'emploi d'une carte électronique ou papier afin de vérifier sa position. Il lui sera aussi possible d'utiliser l'*overlay* de l'ARPA sur l'**ECDIS**. En considérant le cap gyro et la distance parcourue indiquée par le log, l'officier peut également vérifier sa position GNSS avec sa position calculée à l'estime. A noter également que si le navire en est équipé, il est préférable de privilégier un autre moyen de positionnement, à micro-ondes ou hydroacoustique. Certains récepteurs GNSS peuvent être équipés d'antennes adaptatives qui peuvent atténuer les interférences.

7.2 Usurpation d'identité AIS

A l'instar du GNSS, l'usurpation d'identité AIS est aussi possible. Les données émises sont modifiables par l'officier de quart. En général, l'altération de données AIS se fait pendant le transit dans des zones sensibles comme des zones de piraterie afin d'éviter de potentiels assaillants de détecter un signal et d'utiliser ces informations à leur avantage. Cependant, l'AIS

[187] C4ADS, Above Us Only Stars
[188] UT News, UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea
[189] Tucker, DHS: Drug Traffickers Are Spoofing Border Drones
[190] OSCE, Latest from the OSCE Special Monitoring Mission to Ukraine (SMM), based on information received as of 19:30, 19 January 2017

ne peut être coupé dans certaines zones de pirateries où la circulation est trop dense, comme le détroit de Singapour.

En 2013, la société de cybersécurité *Trend Micro* démontrait la facilité d'accès au système AIS[191]. Elle put modifier les données émises par le navire comme sa position, son cap, sa vitesse ou son nom. Déclencher une fausse alerte de collision. Imiter la signature d'autorités maritimes afin de demander à un navire de désactiver leur AIS. Ou même de créer une balise factice d'homme à la mer.

A noter que la problématique de la plupart des systèmes AIS réside en l'absence de sécurité intégrée. En effet, le système ne vérifié pas l'intégrité des données reçues, il émet le signal sans en vérifier l'authenticité.

7.3 HSMS Hull Stress Monitoring Systems

C'est après la perte de nombreux vraquiers dans les années 1980 et 1990 attribuées à la répartition inappropriée des charges sur le navire que les HSMS furent implémentés, et ainsi permettre de s'assurer que les contraintes ne dépassent pas les limites spécifiées. Les senseurs installés sur le navire envoient au système les valeurs mesurées. Ces connections se font généralement par le système informatique local du navire.

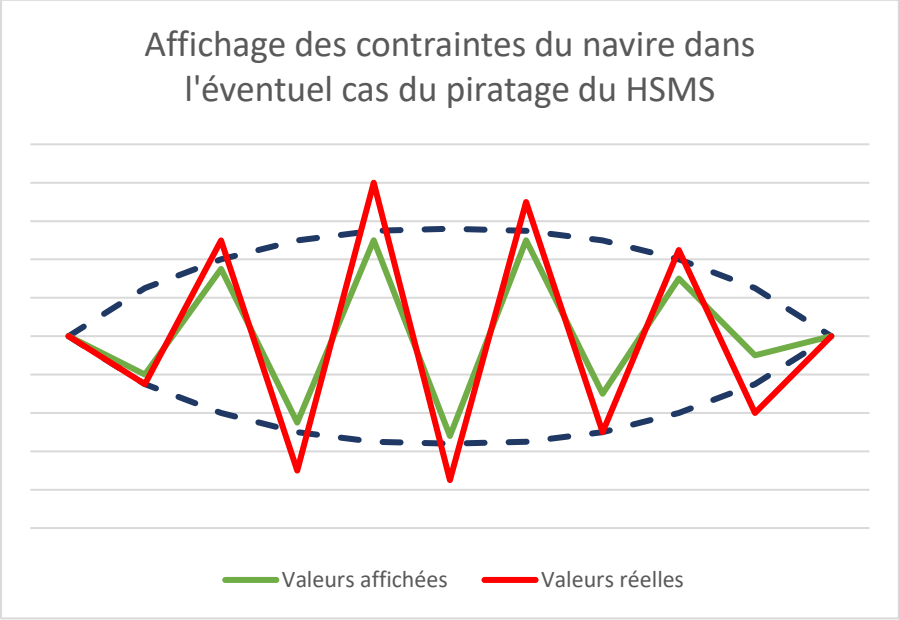

Figure 23 Affichage des contraintes du navire dans l'éventuel cas du piratage du HSMS
Source : Propre figure (2022)

[191] CyberKeel, Virtual pirates at large on the cyber seas

Comme vu précédemment, l'infection du réseau VLAN du navire est une possibilité. Dans une telle situation, les informations rapportées par les capteurs peuvent être manipulées

La manipulation ou la destruction de ces données pourraient avoir un impact désastreux sur l'intégrité du navire et de son équipage.

7.4 VDR Voyage Data Recorder

Le VDR agit comme la preuve la plus fiable pour connaître les raisons d'un incident à bord. Ces équipements ont notamment été utilisés pour prouver la culpabilité du commandant du Costa Concordia lors de son naufrage en 2012[192].

Cependant, l'intégrité du VDR peut potentiellement être altérée. Des recherches ont été effectuées sur le VR-3000 de *Furuno* après que deux militaires Italiens, à bord du pétrolier Enrica Lexie, aient été accusés du meurtre de deux pêcheurs Indiens. Affirmant penser que les victimes étaient des pirates, or, ces témoignages n'ont pas pu être vérifiés car les données du VDR étaient corrompues[193].

Une analyse du groupe de cybersécurité *IOActive* mis en exergue un nombre de vulnérabilités dans le VR-3000 ;

- Un mauvais chiffrement des données audio.
- Une faille de sécurité permettant de supprimer des conversations audio, images radar et d'altérer les données de vitesse et de position.
- Il fût également remarqué que le VDR pouvait être utilisé par des malfaiteurs pour espionner l'équipage via son réseau de microphones[194].

7.5 ECDIS Electronic Chart Display and Information System

L'ECDIS, comme la plupart des systèmes informatiques du navire, est connecté au réseau local. Capital pour la navigation, son intégrité l'est d'autant plus que certains navires ne possèdent plus de cartes en papier.

[192] ANSA, Sub al lavoro, recuperata 'scatola nera' plancia
[193] Gallagher, Hacked at sea: Researchers find ships' data recorders vulnerable to attack
[194] Gallagher, Hacked at sea: Researchers find ships' data recorders vulnerable to attack

Il est de plus en plus courant que les clés USB utilisés pour la mise à jour de l'ECDIS soient infectées par des *Malwares*. Il est donc fortement recommandé d'analyser tous les périphériques de stockage avant de les introduire dans le système[195].

L'entreprise de cybersécurité israélienne *Naval Dome* réussi à accéder au système d'un navire en envoyant un courrier électronique au capitaine. Le virus fût transféré à l'ECDIS pendant la mise-à-jour des cartes. L'attaque visait à déplacer la position affichée par l'ECDIS pendant le passage d'un chenal étroit en pleine nuit. Les profondeurs indiquées sur la carte ont pu être changées, ainsi que les paramètres du navire, comme sa position, son cap, son tirant d'eau et sa vitesse[196].

Certaines compagnies choisissent la méthode la plus sûre pour éviter la corruption des données de l'ECDIS. Leurs navires utilisent principalement des cartes à papier pour la navigation.

7.6 Navires à positionnement dynamique

La plupart des navires de l'industrie offshore ont la nécessité de garder une position très précise pour de longues périodes, notamment les plates-formes flottantes, **FPSO**s, câbliers et certaines dragues. Ce système se base sur un système informatique complexe composé de capteurs, consoles, systèmes de management de puissance, dont la redondance est assurée. Le système de positionnement dynamique se doit d'être indépendant et ségrégué, cependant, comme vu précédemment, les systèmes à bord ne sont jamais totalement protégés contre une attaque extérieure ou intérieure.

Le navire possède entre autres des anémomètres pour mesurer le vent, des gyrocompas pour mesurer le cap, un *Motion Reference Unit* (**MRU**) pour mesurer les mouvements du navire, et parfois des courantomètres pour mesurer le courant. Tous les navires à positionnement dynamique possèdent également des *Position Reference Systems* (**PRS**) afin de mesurer leur position, géographique ou relative. Si le navire utilise le système de *Diffenretial GNSS* (**DGNSS**) comme PRS, il peut aussi être la cible de brouillage ou usurpation d'identité GNSS comme indiqué précédemment.

[195] Baraniuk, How hackers are targeting the shipping industry
[196] The Maritime Executive, Tests Show Ease of Hacking ECDIS, Radar and Machinery

Les capteurs envoient les données mesurées au système. Lors du fonctionnement normal du navire, il est possible qu'un de ces senseurs retourne une valeur fausse. Toutefois, le système est programmé pour refuser cette valeur. Ce dernier devra donc comparer les valeurs des différentes unités. Puis, après une série de test, choisir quelle valeur est la plus probable. Si un capteur semble fautif, il sera exclu afin d'éviter la lecture de mauvaises données[197].

Le système est donc conçu pour gérer la défaillance des équipements. Cependant, une personne malintentionnée ayant accès au système informatique du navire pourrait altérer les données. Le système de positionnement dynamique serait incapable de remarquer l'erreur car tous les capteurs indiqueraient la même valeur fausse. Toutefois, il est nécessaire au bateau d'utiliser au minimum deux types de PRS différents, si le GNSS devait être infecté, le système le mettrait de côté et préfèrera utiliser les autres systèmes de position.

La perte de position des navires à positionnement dynamique peut avoir des conséquences dramatiques en fonction du travail qu'ils effectuent. La collision entre deux navires ou avec une plate-forme. La rupture d'un tuyau sous-marin, initiant une catastrophe écologique. Ou même la section du cordon ombilical reliant un plongeur à son navire, l'alimentant en air.

C'est donc la qualité de la ségrégation des navires à positionnement dynamique qui les protège contre les attaques extérieures. Une personne malveillante ne pourrait pas transmettre de *Malware* depuis l'Internet du navire jusqu'à son réseau Ethernet. La plus grande vulnérabilité vient donc de l'intérieur, lorsque le personnel introduit sans le savoir des périphériques infectés, notamment lors de la mise-à-jour des logiciels.

En 2013, un *Mobile Offshore Drilling Unit* (**MODU**) dériva à la suite de l'infection du système par un *Malware* introduit par les périphériques personnel de l'équipage. Le logiciel désactiva la liaison jusqu'aux propulseurs, ce qui causa à la plate-forme une perte de position[198].

En réalité, l'industrie offshore possède une meilleure protection contre les risques cybernétiques que le reste du monde maritime[199]. Les compagnies investissent des sommes colossales pour la construction et l'exploitation des navires et structures. Le budget injecté

[197] Dotselaere, DP BASIC COURSE
[198] Knox, Coast guard commandant on cyber in the maritime domain
[199] Data Journalism Team, Cybersecurity hiring levels in the offshore industry rose in April 2022

dans la cybersécurité est donc bien plus important que dans le reste de l'industrie maritime[200]. Les risques viennent donc d'avantage de l'intérieur que du reste des équipements connectés.

7.7 Autres systèmes

Un incident surgissant dans n'importe lequel des systèmes connectés du navires aurait la capacité de s'étendre à tout le réseau.

- Les navires récents possèdent généralement un système de pont intégré (**IBS**). Cet équipement permet de centraliser les informations relatives à la navigation en rassemblant divers sous-systèmes. Même s'il n'est généralement pas connecté à un réseau externe, l'IBS est régulièrement mis-à-jour par des médias amovibles pouvant être infectés par des *malwares*.
- Le **GMDSS**, utilisé pour émettre les messages de détresse suite à une collision, inondation, incendie ou un naufrage, est un système critique à la sureté du navire. Il pourrait être compromis par des personnes malintentionnées qui empêcheraient l'émission. Ou détourné pour émettre de faux messages de détresse[201].
- Le Radar, pourrait être infecté via le réseau local du navire. Des équipes de l'agence de cybersécurité *Naval Dome* réussirent à pénétrer le Radar d'un navire en passant par le réseau Ethernet. Elles parvinrent à éliminer les cibles radar sans déclencher aucune alarme[202].
- Certains terminaux de conteneur utilisent le GNSS pour automatiser la logistique, le brouillage ou usurpation d'identité GNSS pourrait perturber le bon fonctionnement de ces ports.
- Les logiciels utilisés pour gérer la cargaison et les opérations de chargement peuvent également générer des risques quant à l'intégrité du système informatique à bord, ces programmes fonctionnant souvent en interface avec d'autres programmes à terre. Si un pirate venait à modifier les plans de chargement, cela pourrait totalement modifier

[200] offshore-technology.com, Cybersecurity in Oil & Gas
[201] Lagouvardou, Maritime Cyber Security: concepts, problems and models
[202] The Maritime Executive, Tests Show Ease of Hacking ECDIS, Radar and Machinery

les contraintes et la stabilité du navire, pouvant potentiellement causer le naufrage du navire.

- Souffrant toujours de son retard technologique, la plupart des systèmes à bord, comme les systèmes GPS, le pilote automatique ou l'AIS utilisent le système d'exploitation Windows XP. Ce système, commercialisé en 2001 est connu pour son nombre de vulnérabilités, dont une liste est disponible gratuitement sur Internet[203].
- Certains logiciels à bord sont fournis avec des licences renouvelables. L'émission de fausses données de temps pourrait les amener à une expiration prématurée.

La plupart des OT à bord ne présente que peu d'opportunité pour les cyberpirates de monnayer leurs attaques. Cependant, les assaillants pourraient facilement instaurer le chaos en modifiant les données de navigation et ainsi initiant des collisions entre navires ou avec une plateforme offshore. L'usurpation d'identité GNSS pourrait aussi être utilisée pour attirer un navire dans des eaux dangereuses.

[203] CVE Details, Security Vulnerabilities

CHAPITRE 8 : Information Technology

Selon le BIMCO, la plupart des cyberattaques envers des systèmes IT ne sont pas considérées dangereuses pour la sécurité du navire et de son équipage[204], elles peuvent cependant engendrer de lourdes pertes financières pour l'entreprise.

8.1 Incident au Port d'Anvers

De 2011 à 2013, le port d'Anvers a été la cible de cyberattaques liés au trafic de stupéfiants. Les malfaiteurs auraient engagé des hackers afin de récupérer des IT contrôlant la position des conteneurs. En possession de ces informations, les trafiquants ont pu envoyer des conducteurs complices afin de récupérer la marchandise illégale avant que le propriétaire ne récupère sa cargaison.

Les pirates auraient envoyé des *malwares* via courriers électroniques au personnel du port afin d'espionner les données du système. Ils ont ainsi pu obtenir les identifiants de connexion en utilisant des logiciels de *keylogging* qui observent et enregistrent ce que les employés tapaient sur leur clavier.

Les procureurs en charge de cette affaire affirmaient qu'un groupe de trafic de drogue basé au Pays-Bas cachait cocaïne et héroïne parmi la cargaison de conteneurs en provenance d'Amérique du Sud.

La brèche de sécurité fût décelée lorsque plusieurs conteneurs furent détectés manquants. Un employé du port fût visé par des tirs d'arme automatique après avoir déplacé un conteneur rempli de cocaïne, alors qu'il en ignorait la contenance. Dans une opération jointe entre les forces de police belges et néerlandaises, les fonctionnaires de police saisissaient plusieurs armes à feu, accompagnées d'une arme automatique, silencieux, un gilet pare-balles ainsi que 1,3 millions d'euros en liquide dans une mallette. Le chef de l'unité de la lutte contre le crime organisé d'Anvers, Danny Decraene, estimait à 155 millions d'euros le montant des saisies de plus d'une tonne de cocaïne en 2013.

[204] BIMCO et al., The Guidelines On Cyber Security On Board Ships V4.0

8.2 Maersk

En 2017, le système IT de Maersk fut touché par l'attaque du *Ransomware NotPetya*, avec une flotte de plus de 700 navires[205] il est le plus grand armateur du monde[206]. Le *Malware* a été infiltré dans le système avant d'encrypter tous ses fichiers, demandant une rançon sous la forme de BitCoins. L'infection arriva via la mise-à-jour du logiciel de comptabilité de l'entreprise.

L'armateur fut forcé d'éteindre tous ses systèmes afin de contenir l'incident. La cessation des activités ainsi que la réinstallation des plus de 60 000 équipements informatiques couta à la compagnie de 200 à 300 millions de dollars[207].

Cet incident eut pour effet de rappeler à toutes les entreprises l'importance de la cybersécurité. *Maersk* pense qu'avec le développement des technologies et l'augmentation de la digitalisation, les vulnérabilités ne feront qu'augmenter. Et conseille une amélioration racinaire de la cybersécurité des infrastructures technologiques.

8.3 L'incident Zombie Zero

En 2014, l'entreprise de cybersécurité *TrapX* découvrait l'infection par un *Malware* de scanners en provenance de fabricants chinois, touchant au moins 8 compagnies de logistique dans le monde[208].

Une étude spécifique, menée par *TrapX* a permis d'en mesurer l'incidence. Un tiers des scanners avait été infecté par un *Malware* préinstallé sur les équipements avant leur livraison à l'entreprise de logistique.

Lorsque les scanners étaient branchés au réseau de la compagnie, le logiciel lançait une série d'attaques automatisées à la recherche du serveur responsable pour la gestion de la chaîne logistique, et du commerce. Il établissait ensuite une connexion vers la Chine qui permettait la visualisation et la corruption des données commerciales[209].

[205] Placek 2022, The world's leading container ship operators as of March 31, 2022, based on number of owned and chartered ships
[206] Reiff, 10 Biggest Shipping Companies
[207] Lagouvardou, Maritime Cyber Security: concepts, problems and models
[208] TrapX, ANATOMY OF AN ATTACK Zombie Zero Weaponized Malware Targets ERP Systems
[209] CyberKeel, Virtual pirates at large on the cyber seas

Cet incident a causé de nombreuses réactions dans l'industrie de la logistique, car la pièce d'équipement était infectée depuis sa fabrication. Il peut donc devenir difficile d'instaurer un climat de confiance avec les entreprises qui pourraient fournir des appareils dont la fiabilité pourrait être mise en cause.

8.4 L'attaque de l'industrie énergétique

En janvier 2022, plusieurs compagnies pétrolières, dont le géant allemand *Oiltanking* ont été la cible d'une attaque du *Ransomware BlackCat*. Plusieurs dizaines de terminaux pétroliers dans le monde entier se sont trouvés affectés pendant plusieurs jours[210]. L'entreprise s'est vue contrainte d'opérer dans des conditions limitées durant la période de l'attaque.

Cet incident eu l'effet d'une bombe pour l'industrie pétrolière qui souffrait, déjà à l'époque, des tensions politiques entre la Fédération de Russie et l'Ukraine alors que les prix de l'énergie commençaient à grimper.

Europol, chargé de l'enquête, nota que les programmeurs du logiciel *BlackCat* utilisaient la langue russe. Toutefois, ce constat ne peut à lui seul suffire pour affirmer la culpabilité de la Russie. En effet, les hackers fournissent souvent de faux indices pour couvrir leurs traces. Cependant, en juin 2021, les autorités américaines affirmèrent avoir intercepté la rançon payée par *Colonial Pipeline* en direction de *Darkside*, un groupe d'extorqueurs basé en Fédération de Russie[211].

8.5 Le développement des documents électroniques

L'industrie maritime utilise les mêmes bons de chargement depuis plusieurs siècles. Ce document a plusieurs rôles, majoritairement définis par les *Hague-Visby Rules*. Il est la preuve du contrat de transport existant entre le chargeur et le transporteur, c'est aussi un reçu pour la marchandise, et donne à son titulaire les droits exclusifs sur la livraison. Ce document doit être envoyé en multiples exemplaires aux différentes parties du contrat, et se doit d'être présentée à la récupération de la cargaison. Et c'est bien sur ce dernier point qu'on constate l'obsolescence du bon de chargement. Avec le développement du secteur maritime, il n'est

[210] TIdy, European oil facilities hit by cyber-attacks
[211] Demeestere, European oil port terminals hit by cyberattack

pas rare que les navires arrivent à leur destination avant le document, rendant la livraison de la marchandise très compliquée, si ce n'est impossible.

L'industrie maritime essaye donc depuis quelques années d'engager une transition numérique avec notamment les systèmes *Bolero* et *essDOCS*[212]. Ces documents sont donc transformés en IT et deviennent une nouvelle mine d'or pour les cyberpirates, qui voient dans cette digitalisation une nouvelle opportunité de s'approprier des informations.

8.6 Lien avec la piraterie

Une entreprise qui remarqua le changement de mode opératoire de certains pirates demanda à l'entreprise *Verizon* d'analyser la situation. Il fut remarqué que les pirates ciblaient précisément certains conteneurs lors de leurs abordages. L'enquête a démontré que les pirates avaient eu accès au système de gestion de la cargaison, ils ont ainsi pu obtenir des informations sur les bons de chargement des conteneurs à bord[213].

[212] UKP&I, Electronic Bills of Lading - An Update: Part II
[213] Verizon, Data Breach Digest, Scenarios from the field

CHAPITRE 9 : La sécurité des navires autonomes

Les industries du transport essayent depuis quelques années de développer des véhicules automatisés, la plupart étant lié au secteur automobile, avec les *Google Cars* ou *Tesla*, et de l'aviation, avec *Xwing*. Cependant, le monde maritime reste en retard dans ce domaine des nouvelles technologies. A noter que, l'objectif de la plupart des compagnies qui développent ces navires autonomes, est bien d'équiper ces derniers de supports lors de la prise de décisions, de réduire l'erreur humaine et d'augmenter la sécurité d'un point de vue global. Il s'agit bien d'un choix stratégique quant à la navigation et non le projet de remplacer l'équipage.

Figure 24 Maritime Autonomous Surface Ship (MASS) en développement par Kongsberg
Source : Kongsberg (2022)

L'OMI définit quatre degrés d'autonomie[214] :

- Degré Un : *Navire avec processus automatisés et aide à la décision*, l'équipage à bord fait fonctionner le navire. Certaines opérations peuvent être automatisées et entreprises sans surveillance mais l'équipage doit être prêt à reprendre le contrôle.

[214] OMI, Outcome Of The Regulatory Scoping Exercise For The Use Of Maritime Autonomous Surface Ships (MASS)

- Degré Deux : *Navire contrôlé à distance avec un équipage à bord*, le navire est télécommandé depuis un autre lieu. L'équipage est disponible pour prendre le contrôle.
- Degré Trois : *Navire contrôlé à distance sans équipage à bord*, le navire est télécommandé depuis un autre lieu mais ne possède pas d'équipage.
- Degré Quatre : *Navire totalement autonome*, le système est capable de prendre lui-même les décisions.

L'équipage à bord d'un navire peut facilement détecter la cyberattaque d'un OT, comme le GNSS, l'ECDIS ou l'ARPA, en comparant les données informatiques avec d'autres capteurs déconnectés du système électronique, comme le gyro ou simplement visuellement, lorsque des aides à la navigation sont observables. Un navire autonome aura beaucoup plus de difficulté à repérer et contrer ce genre d'attaque. Les risques courus par les navires automatisés restent bien supérieurs à ceux des autres bateaux. En effet, leur grande dépendance au système informatique, le niveau d'intégration de leurs systèmes ainsi que leur connectivité avec la terre et Internet les rendent plus vulnérables. Il reste important de noter que, pour le moment, les législations concernant la cybersécurité à bord des navires autonomes ne sont pas plus strictes que pour le reste des navires et que le sujet manque encore beaucoup de documentation.

Afin de traiter avec ces nouvelles technologies, il est impératif d'étudier les problématiques et risques que pourrait engendrer le développement de l'automatisation dans le secteur maritime.

Cependant, nous avons vu précédemment que les infections de *Malwares* venaient souvent de l'imprudence de l'équipage. Un navire avec un personnel réduit, et plus informé, pourrait diminuer ces risques. Cependant nous n'aurons pas l'occasion d'en discuter plus en détails, un tel sujet pourrait faire à lui seul l'objet d'un mémoire.

CHAPITRE 10 : Les assurances contre la cybercriminalité

Sachant qu'une majorité des leaders de l'industrie a déjà subi des attaques (entre autres *Maersk*, *MSC*, *COSCO*, *CMA CGM*[215]), on comprend la nécessité d'engager des contrats d'assurances incluant la protection contre les cyberattaques.

Le risque de cyberattaque est généralement exclu des assurances H&M, avec la clause d'exclusion des risques cybernétiques de 2003, et plus récemment avec « War, Cyber War and Cyber Operation Exclusion » de Lloyds en 2021. Excluant les pertes et dommages, recours de tiers ou dépenses résultant de cyberattaques[216].

Les assurances P&I quant à elles, n'excluent pas les risques cybernétiques à moins qu'ils ne soient considérés comme actes de guerres, par exemple s'ils sont perpétrés par des organisations terroristes. Selon le Capitaine Justers, responsable d'une compagnie d'assurance maritime, dans le cas où le risque est exclu par le P&I, il peut être couvert par l'extension *bio-chem* de l'assurance, à hauteur de 30 millions de dollars, s'il est la cause de maladies, blessures, ou décès[217]. Dans ce cas-ci, l'assuré devra prouver elle-même que l'attaque est un acte de guerre ou un acte terroriste.

Une attaque visant IT ou OT sur le navire serait donc couverte, sauf si l'assureur arrivait à prouver que le système n'était pas suffisamment protégé pour contrer ce type de risques.

Depuis le 20 février 2022, la couverture P&I de base est disponible pour la cybercriminalité sans restriction jusqu'à une valeur de 550 millions de dollars. Au-delà de laquelle une limite globale sera appliquée[218].

Cependant, les polices d'assurances *RG* contiennent généralement une clause d'exclusion de risques cybernétiques, les assurances War P&I de *RG* ne couvrent donc pas les cyberattaques. Cela-dit, certains assureurs *RG*, tel le *UK War Risks Associations*, proposent une couverture limitée des risques cybernétiques de 50 millions de dollars par an[219].

[215] Cimpanu, All four of the world's largest shipping companies have now been hit by cyber-attacks
[216] LMA, War, Cyber War and Cyber Operation Exclusion
[217] Justers, Interview personnelle
[218] Justers, Interview personnelle
[219] Justers, Interview personnelle

Certains risques restent exclus des assurances maritimes. On peut noter en exemple, le cas d'une entreprise qui serait amenée à payer une rançon suite à une infection par un *Ransomware*. En réalité, les assurances maritimes ne couvrent pas les risques *onshore*, qui se déroulent au sein de la compagnie. A cet effet, une compagnie devra souscrire une assurance couvrant les risques cybernétiques non-maritime[220].

En se spécialisant dans les risques liés aux cyberattaques, le secteur des assurances a dû élargir ses offres et évoluer. On peut noter en exemple *Chubb*, *AIG* ou *AXIS*[221].

Néanmoins, il existe sur le marché, des assureurs spécialisés couvrant aussi bien les risques *onshore* qu'offshore[222].

[220] Justers, Interview personnelle
[221] Harvey, Top 8 Cyber Insurance Companies for 2020
[222] Justers, Interview personnelle

CHAPITRE 11 : La facilité d'accès aux outils de piratage

La hauteur du risque liée aux cyberattaques réside également dans la facilité avec laquelle il est possible de se procurer des outils adaptés à l'objectif. Les didacticiels qui permettent de se former à l'utilisation de ces outils sont eux aussi facilement récupérables en ligne et donnent un pouvoir non négligeable à toutes personnes malintentionnées cherchant à pirater des données.

Dans cette partie, nous essaierons de montrer la facilité que pourraient avoir certaines personnes malintentionnées à pirater des données.

11.1 Les réseaux sociaux comme source d'information

De nos jours, et dans cette ère numérique grandissante, il devient normal et coutumier de partager quotidiennement sa vie sur Internet. Cette évolution à double tranchant, qui laisse la part belle aux réseaux sociaux, offre une fenêtre ouverte aux individus peu scrupuleux. En effet, ces derniers peuvent aisément, et surtout à moindre coût, obtenir des informations nécessaires à leurs activités de piratage. Il est donc capital de filtrer les informations transmises sur les réseaux afin de ne pas faciliter l'accès aux IT du navire.

Un navire transitant par la Mer Rouge en direction du Golfe d'Aden avait coupé ses émissions d'AIS afin de rester caché de potentiels pirates. Il fut remarqué avant d'entrer dans le Golfe d'Aden qu'un nombre signifiant d'images du navire et de ses systèmes avait été mis en ligne sur Facebook. Ces photographies fournissant une vue détaillée des mesures de sécurité en place sur le navire, le capitaine décida de prendre une route différente afin d'éviter de potentielles attaques[223].

11.2 Logiciel de Brute Force

Ne possédant que quelques bases de programmation en langage *Python*, un logiciel de *Brute Force*, le type le plus simple de cyberattaque, a été créé[iii].

[223] CyberKeel, Virtual pirates at large on the cyber seas

iii Création personnelle d'un logiciel de type *Brute Force* en *Python*

Comme expliquée dans la partie 6.1, une attaque de *Brute Force* consiste à essayer toutes les combinaisons possibles d'un mot de passe. On peut optimiser le code en y insérant des bases de données comprises des mots de passes les plus employés, le programme testera donc en priorité les mots de passes les plus probables.

En quelques minutes de recherches on peut facilement trouver une liste des mots de passes les plus utilisés de ces dernières années[224].

```
import os
import time
dico=['123456','password','123456789','12345678','12345','111111','1234567','sunshine',
      'qwerty','iloveyou','princess','admin','welcome','666666','abc123','football',
      '123123','monkey','654321','!@#$%^&*','charlie','aa123456','donald','password1','qwerty123']
def dictionnary_brute_force(word,lenght):
    if lenght<=1:
        for letter in dico:
            if mdp==word + letter:
                print("Votre mot de passe est " +word+letter)
                print("--- %s seconds ---" % (time.time() - start_time))
                os.system("pause >null")
                quit()
            else:
                print(word+letter)
                dictionnary_brute_force(word+letter,lenght+1)

os.system("cls")
mdp=input("\n mdp:")
start_time = time.time()
dictionnary_brute_force('',1)
```

Figure 25 Code Python d'un logiciel de Brute Force basique avec une base de données
Source : Création personnelle (2022)

Il est probable que le mot de passe de la cible ne soit pas compris dans la base de données, si c'est le cas, on pourra exécuter le prochain script. Ce dernier demande la longueur du mot de passe, et testera une par une toutes les combinaisons possibles. Ce programme n'est pas exploitable en l'état pour trouver un mot de passe sur un site internet. Il faudrait pour ce faire, lui intégrer une interface connectée au navigateur. Notons que la plupart des sites internet à connexion privée empêchent les multiples tentatives de connexion provenant d'une même adresse IP. Cependant cela est facilement contournable par l'utilisation d'un réseau privé virtuel (**VPN**).

[224] SplashData, Les mots de passe les plus utilisés de 2018 : les vôtres y figure nt-ils?

```
import os
import time
liste=['a', 'b', 'c', 'd', 'e','f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n',
       'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z',
       'A','B','C','D','E','F','G','H','I','J','K','L','M','N',
       'O','P','Q','R','S','T','U','V','W','X','Y','Z',
       'é', 'è', 'à', 'â', 'ë', 'ï', '1', '2', '3', '4', '5', '6', '7', '8', '9', '0',
       '^','¨','$','£','¤','µ','%','ù','!','§','/',':',',','?','°','=',
       '}','{','(',')','~','&','é','²',' ','`','|','ç', '-', '_','*','@','#']
longueur=int(input("Entrez la longueur du mot de passe "))
def brute_force(word,lenght):
    if lenght<=longueur:
        for letter in liste:
            if mdp==word + letter:
                print("Votre mot de passe est " +word+letter)
                print("--- %s secondes ---" % (time.time() - start_time))
                os.system("pause >null")
                quit()
            else:
                print(word+letter)
                brute_force(word+letter,lenght+1)

os.system("cls")
mdp=input("\n mdp:")
start_time = time.time()
brute_force('',1)
```

Figure 26 Code Python d'un logiciel de Brute Force basique
Source : Création personnelle (2022)

Un processeur de faible puissance, *Intel® Core™ i3-7100* à 2 cœurs, avec une vitesse de 2,40 GHz, qui utilise 30% de ses capacités, avec une carte graphique bas-de-gamme *Intel® HD Graphics 620* peut tester en moyenne 140 possibilités par secondes[iv]. Soit 103 possibilités en 0,81 secondes, 103^2 possibilités en 76,17 secondes et 103^3 possibilités en 7 613 secondes. Par extrapolation on peut déterminer que cette machine prendra plus de 9 jours pour cracker un mot de passe à seulement 4 caractères, à cette vitesse. Ces 9 jours peuvent paraitre énorme, mais il est toutefois important de préciser que ce type de matériel est un des moins puissants du marché. De plus, les hackers utilisent généralement plusieurs machines pour accélérer le processus.

Dans la pratique, les cyberpirates utilisent des ordinateurs extrêmement puissants leur permettant de gagner beaucoup de temps et d'être très réactifs dans leur tâche. Equipés des cartes graphiques les plus puissantes du marché, comme la *NVIDIA TITAN V*[225]. On voit dans la figure ci-dessous que le temps pour déchiffrer un mot de passe, même complexe, devient dérisoire.

iv Ordinateur personnel utilisé pour ces tests
[225] NVIDIA, NVIDIA TITAN V

Figure 27 Temps qu'un hacker prendra pour trouver par Brute Force votre mot de passe chiffré par méthode MD5
Source : hivesystems.io (2022)

La technologie d'aujourd'hui offre encore davantage d'opportunités pour les hackers. Avec la démocratisation du Cloud, certaines entreprises comme Amazon, proposent la location de clusters informatique dématérialisés comme les « Instances P4d Amazon EC2 » avec une puissance de calcul 1,5 fois supérieure à celle d'un ordinateur physique[v] [226].

La méthode la plus efficace pour éviter qu'un hacker ne *Brute Force* notre mot de passe est toujours de renforcer sa sécurité en utilisant des mots de passes plus longs avec des caractères spéciaux. Cependant, c'est le site internet ou le logiciel qui aura le plus d'impact dans la sécurité de ses bases de données, en utilisant des fonctions de hachage plus complexe. En effet la fonction MD5 est largement considérée comme trop faible et il est recommandé d'utiliser d'autres fonctions de hachage, comme *bcrypt*. Malheureusement, encore beaucoup de sites internet utilisent cette technologie dépassée, ce qui est alertant en sachant que les gens utilisent souvent les mêmes mots de passe pour différents sites[227].

v P4d EC2 comparé à NVIDIA RTX 2080
[226] Hive Systems, Are Your Passwords in the Green?
[227] Have I Been Pwnd, ';--have i been pwned?

11.3 Exploitation de la connexion satellite

En 2017, un membre de la communauté de « consultants en sécurité » *Pen Test Partners* réussi à accéder au système informatique d'un vraquier en quelques heures en utilisant seulement des outils disponibles sur internet[228]. Après avoir trouvé des failles de sécurité dans le système **SATCOM** *Sailor 900*, il a pu s'infiltrer dans le terminal *CommBox*™ vendu par l'entreprise *KVH*. L'interface de *CommBox*™ permettant de voir le nom des personnes connectées, il repéra un cadet utilisant le système. Quelques instants sur les réseaux sociaux ont permis aux hackers de trouver toutes les informations nécessaires à une tentative de phishing. Puis prendre le contrôle de son ordinateur personnel, trouver une faille dans la ségrégation entre Internet et l'Intranet du navire, pour atteindre les systèmes de navigation.

L'auteur de l'attaque affirme qu'il ne devrait pas être aussi simple d'accéder au système informatique d'un navire. Il insiste sur le fait que la présence de protocoles de sécurisation des données devrait être obligatoire dans les équipements de communication satellite. Il conseille aux constructeurs de mettre à jour d'urgence leurs équipements afin de les protéger contre les cyberattaques[229].

[228] Munro, OSINT from ship satcoms
[229] Munro, OSINT from ship satcoms

CHAPITRE 12 : La protection contre les cyberattaques

En 2011, l'*European Network and Information Security Agency* (**ENISA**) publiait le premier rapport de l'Union Européenne sur les aspects et challenges de la cybersécurité dans le monde maritime[230]. En affirmant que l'industrie maritime représentait un secteur critique de la société Européenne, l'agence reconnaissait déjà une mauvaise sensibilisation des parties concernées, comme les gouvernements, les autorités portuaires, ou les entreprises elles-mêmes. Que la menace cybernétique grandissait et évoluait beaucoup plus rapidement que les moyens de la combattre.

L'ENISA pointait également le fossé entre la menace cybernétique grandissante qui évoluait beaucoup plus rapidement que les moyens mis en œuvre pour la combattre. À l'occasion de ce rapport, l'agence préconisait une série de conseils. Entre autres, renforcer la sensibilisation du personnel de l'industrie maritime quant aux aspects de la cybersécurité, ou développer les capacités du secteur à se défendre contre une cyberattaque.

En 2017, le Comité de la Sécurité Maritime MSC, de l'OMI développait une circulaire pour aider à la gestion des risques liés aux cyber-attaques[231]. Ces lignes directrices restent cependant de simples recommandations. En l'absence d'obligation, les entreprises maritimes restent libres de gérer ces risques en adéquation avec leurs propres stratégies. Il est possible de faire la distinction entre la *Cyber-Security*, qui protège contre l'accès et la manipulation des données, IT et OT, et la *Cyber-Safety*, qui protège contre la perte de l'intégrité et la disponibilité des données et OT liées à la sureté. La cybersécurité doit être vue comme complémentaire aux exigences de sécurité des codes ISM et ISPS.

L'*International Association of Classification Societie*s (**IACS**) développe en 2016 « On Board Use and Application of Computer Based Systems », puis en 2020, « Recommendation on Cyber Resilience » qui préconisent les prérequis concernant le design, la construction et l'entretien des OT à bord des navires sous classe. Ces recommandations ont pour but de concevoir des navires dont la « cyber-résilience » peut être maintenue toute leur vie.

L'IACS, afin de protéger le système informatique à bord, propose le plan suivant[232] :

[230] ENISA, ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR
[231] OMI, Guidelines On Maritime Cyber Risk Management
[232] IACS, Recommendation on Cyber Resilience

- Identifier : Il est capital d'identifier les systèmes vulnérables aux cyberattaques. Mais également, de connaître quelles informations se déplacent entre les différents OT à bord. Enfin, de déterminer les interdépendances entre les systèmes critiques au bon fonctionnement du navire, qui influent sur sa sécurité et celle de son équipage ainsi que de l'environnement.
- Protéger : Il est déterminant de concevoir des systèmes IT et OT supportant une configuration, une intégration et une maintenance sécurisée. De segmenter en plusieurs réseaux les différentes infrastructures à bord. Ainsi que de restreindre les accès aux systèmes OT, qu'ils soient physiques ou numériques.
- Détecter : Il devrait être fourni des moyens de surveiller l'opération des systèmes OT à bord, afin d'augmenter les chances de détection dans le cas d'une cyberattaque.
- Répondre : Dans le cas où le navire serait la cible d'une cyberattaque, l'impact de l'incident devrait être contenu dans le réseau d'arrivée afin d'empêcher son développement dans les systèmes adjacents.
- Récupérer : Les équipements devraient être conçus pour faciliter leur restauration et rétablir le navire dans des conditions sécurisées.

Le navire, durant sa vie, sera soumis à diverses visites par des agents, techniciens et pilotes. Il n'est pas improbable que l'introduction de *Malwares* soit due à l'utilisation de périphériques de stockage personnels de certaines de ces personnes se rendant à bord. Ces visites ne sont pas toujours contrôlables, par exemple si elles se déroulent en cale sèche. C'est la raison pour laquelle il devrait toujours exister une sauvegarde des données critiques, et qu'il est recommandé d'analyser régulièrement le système contre de potentiels *malwares*[233].

Les entreprises sont encouragées à sensibiliser leur personnel quant aux risques liés à la sécurité informatique. En effet, le choix de mots de passe sécurisés et la vigilance pendant l'utilisation de la messagerie, entre autres, devraient être des réflexes acquis pour tous les personnels de la compagnie. Elles sont aussi encouragées à sauvegarder leurs données régulièrement, les données à bord peuvent être enregistrées sur un *Network Attached Storage*

[233] BIMCO et al., The Guidelines On Cyber Security On Board Ships V4.0

(**NAS**) comportant plusieurs disques de sauvegarde qui pourraient être utilisés suite à la perte ou au vol des données du navire[234].

Les comptes administrateurs offrent à l'utilisateur le contrôle total sur les fichiers, répertoires et services d'un ordinateur. Leur attribution devrait être strictement limitée au personnel dont les besoins sont avérés, les comptes utilisateurs quant à eux, devraient être utilisés dans l'utilisation quotidienne.

Les entreprises fournissant les logiciels étudient constamment les potentielles failles de sécurité que pourraient engendrer ces programmes et développent régulièrement des mises-à-jour pour les en débarrasser. C'est pourquoi ils devraient être régulièrement révisés afin d'éviter toute défaillance de sécurité, mais toujours avec beaucoup de prudence. Ces mises-à-jours sont généralement transmises au navire par courrier électronique, par Internet. Il faut donc s'assurer de l'intégrité du poste informatique sur lequel sont récupérés les fichiers, ainsi que du périphérique de stockage qui sera utilisé. Car comme vu précédemment, un grand nombre de *Malwares* sont insérés lors de la mise-à-jour de ces logiciels.

L'accès au Wi-Fi à bord, bien que majoritairement positif pour les membres d'équipage afin de rester en lien avec le reste du monde, peut aussi être source de failles de sécurité. La protection du réseau devrait également faire preuve d'une attention toute particulière. En utilisant une clé de chiffrement utilisant le protocole WPA2, qui permet d'éviter l'accès au réseau par des individus malintentionnés lors d'escales[235]. De plus, le réseau Wi-Fi devrait être réservé aux utilisations personnelles de l'équipage, de ce fait, si le réseau venait à être infecté par un *malware*, il ne pourrait pas se propager au reste du système informatique du navire. A bord, les réseaux professionnel et personnel sont dissociés en deux VLAN distincts. Ce fonctionnement permet d'éviter la mise en danger des systèmes de navigation par une potentielle infection d'un poste de travail à usage personnel. Il est important de ségréguer totalement les réseaux Internet et Ethernet afin d'éviter toute infection pouvant s'étendre réciproquement de l'un vers l'autre.

[234] Ministère de l'Environnement, de l'Energie et de la Mer ; ANSSI, Guide des bonnes pratiques de sécurité informatique à bord des navires

[235] Ministère de l'Environnement, de l'Energie et de la Mer ; ANSSI, Guide des bonnes pratiques de sécurité informatique à bord des navires

12.1 Quand l'attaque se termine-t-elle ?

Un autre écueil questionne. Il est, en effet, difficile de savoir quand une cyberattaque peut être considérée comme contenue voire maitrisée et si elle peut se reproduire. Il peut être complexe de déterminer la source d'une attaque et de repérer les failles de sécurités au sein du système informatique de l'entreprise et du navire. Cela encourage les compagnies à faire appel à des sociétés de cybersécurité, pour vérifier l'intégrité de leurs réseaux et fournir un rapport des défauts résidents au sein de leur sécurité informatique.

Dans le cas d'une cyberattaque venant de l'intérieur, avec par exemple, l'introduction d'un *Malware* depuis le périphérique d'un membre du personnel, l'entreprise devra nettoyer l'intégralité de ses réseaux et équipements à la recherche du dit logiciel. Précisons que certains *Malwares* peuvent aisément se cacher, et ainsi échapper aux systèmes de nettoyage[236]. Certains de ces logiciels ont aussi la capacité d'analyser le système informatique à la recherche des différentes failles de sécurité avant d'en communiquer à l'attaquant[237]. C'est pourquoi le réseau devrait être inspecté et réparé entièrement, pas uniquement la brèche utilisée lors de cet incident en particulier.

Dans le cas d'une « *hardware attack »* comme *Zombie Zero*, où une pièce d'équipement est directement infectée par un *Malware* et non par faute du personnel, il est majeur de connaître la portée de l'infection. Quels sont les équipements infectés ? Le fabricant ayant produit ces appareils est-il toujours digne de confiance ?

[236] Computer Forensics World, Can Malware Hide From Antivirus?
[237] CyberKeel, Virtual pirates at large on the cyber seas

Conclusion

Le monde maritime souffre depuis ces deux dernières décennies d'une augmentation de l'insécurité, autant physique, avec la piraterie, que virtuelle, avec la cyberpiraterie.

L'industrie maritime a connu plusieurs émergences de la piraterie au cours des deux dernières décennies. Le détroit de Malacca au début des années 2000, puis la Corne de l'Afrique à la fin des années 2000. Elle a su y faire face avec l'aide des puissances internationales, avec la sensibilisation des marins et la présence de forces armées.

La piraterie est un phénomène économique et social. Les pirates sont eux-mêmes les victimes des décennies de dissentions politiques. Notamment en Somalie, où les populations ont souffert des dissensions politiques et de la pêche illégale au large de leur côtes. Ou dans le Golfe de guinée, les états ayant une économie tournée vers le commerce du pétrole, leur économie fluctue énormément avec le cours du baril. Mais c'est aussi la présence du crime organisé, notamment dans les Amériques et dans l'Asie du Sud-Est, qui favorise le développement des actes de piraterie et de vols à main armée dans ces régions du monde.

Les pirates ont tous leur propre mode opératoire. Les pirates d'Amérique latine et du Sud-Est de l'Asie préfèreront perpétrer des séries de larcins silencieux. C'est cependant en Afrique qu'on retrouve les attaques les plus violentes. Notamment dans le Golfe de Guinée, qui devient le centre névralgique de la piraterie mondiale depuis le début des années 2010. Après la suppression de la menace autour de la Corne de l'Afrique.

Le kidnapping reste selon moi le plus gros danger au commerce international, les pirates mettant en danger la santé physique et mentale des marins. Les victimes restent pendant plusieurs dizaines de jours dans de pauvres conditions de vie, traités comme des marchandises.

La *petro-piracy* est également une activité très importante de la piraterie en Golfe de Guinée, les pays du Golfe étant de gros producteurs et exportateurs de pétrole. En dérobant le pétrole brut depuis les installations, les criminels mettent en danger leur propre santé, celle des populations alentours, ainsi que celle de l'environnement.

La piraterie dans le Golfe de Guinée étant une problématique mondiale, les organisations internationales ont su s'allier aux institutions politiques locales. A l'image des côtes

somaliennes et du détroit de Malacca, la région se militarise de plus en plus, tant par des marines étrangères que par les armées locales, nouvellement formées par ces dernières.

Cependant, avant d'être un problème maritime, la piraterie prend généralement naissance en réponse à des problématiques à terre.

Malheureusement, la piraterie est un problème qui perdure. Les cadres institutionnels des régions touchées sont entravés par le manque de moyens financiers et l'abondance d'institutions inefficaces empêchent le développement d'une approche plus profonde.

Les institutions internationales n'arrivent pas à régler le problème de la piraterie à une échelle mondiale et sur le long terme. Les initiatives régionales et internationales touchent, à ce jour, principalement l'Afrique de l'Ouest, et très peu les autres régions affectées comme les Amériques et l'Asie du Sud-Est.

Selon moi, la lutte contre la piraterie devrait commencer par le développement économique et social ainsi que par le combat du crime organisé dans les régions affectées. Particulièrement dans la région du Delta du Niger, qui reste très nettement sous-développé malgré les richesses présentes dans ses terres. Ainsi qu'en Amérique Centrale et Amérique du Sud, où le trafic de narcoleptiques est une industrie prospère.

La cyberpiraterie, autre danger menaçant la sécurité maritime, peut prendre des formes diverses, toujours plus insidieuses. Les cybercriminels possèdent des motivations différentes, qu'elles soient purement financières ou politiques. L'industrie maritime est une cible intéressante pour ces criminels, qui voient les entreprises comme des cibles intéressantes.

Les navires subissent leur retard technologique. La plupart possède des équipements informatiques datés et facilement piratable. Les OT présents à bord sont des cibles à risques pour la sécurité du navire et de son équipage. La corruption de leurs données pourrait menacer la vie des marins à bord en falsifiant les valeurs du GPS, AIS, ECDIS, HSMS ou du Radar.

Les compagnies souffrent également de la sensibilité de leurs IT. Les cybercriminels n'hésitent pas à exploiter les faiblesses des systèmes de sécurité des entreprises, comme lors de la cyberattaque de *Maersk*, ou encore lors de l'infection de scanners lors de l'incident *Zombie Zero*.

Ces cyberpirates travaillent également en étroite collaboration avec les autres secteurs criminels, comme celui du trafic de stupéfiants, lors de l'incident au port d'Anvers et même celui de la piraterie.

Le progrès technologique du secteur maritime amène également son lot d'enjeux concernant la cybersécurité, avec le futur développement de navires autonomes.

Un autre danger majeur des cyberattaques est la facilité d'accès aux équipements de piratage. N'importe quel individu en possession d'un ordinateur dispose de toutes les capacités nécessaires pour s'engager dans des actes cybercriminels.

Pour contrer ces risques grandissants, les organismes internationaux développent depuis quelques années des législations afin de créer une nouvelle génération de navires cyber résistants. On ne peut cependant affirmer l'efficacité de ces mesures pour le moment, l'industrie maritime étant très lente au changement. Cette dernière devra continuer ses efforts afin d'améliorer la cybersécurité au sein des entreprises et des navires et empêcher les cybercriminels de profiter de leurs activités.

Bibliographie

Abke, Tom. *Singapore counters pirates with new maritime flotilla.* 20 03 2021. https://ipdefenseforum.com/2021/03/singapore-counters-pirates-with-new-maritime-flotilla/ (accès le 04 17, 2022).

Ademefi Isumonah, V. «Armed Society in the Niger Delta.» 8 Juin 2012.

Agency Report. «Pirates' Attacks: Navy deploys 13 warships, 1,500 troops in Gulf of Guinea.» *Premium Times Ng*, 2021.

Akinbobola, Yemisi. «Le Nigeria n'a pas besoin de nouveaux puits de pétrole.» *Afrique Renouveau*, 2014.

AllAfrica. *Nigeria Records First Coronavirus Case.* 28 02 2020. https://allafrica.com/view/group/main/main/id/00072180.html (accès le Mai 2021, 13).

Allianz. «Safety and Shipping Review 2021.» 2021.

Amazon. *Instances P4d Amazon EC2.* 2021. https://aws.amazon.com/fr/ec2/instance-types/p4/ (accès le 04 07, 2022).

Andreone, G., G. Bevilacqua, G. Cataldi, et C. Cinelli. *INSECURITY AT SEA: PIRACY AND OTHER RISKS TO NAVIGATION.* GIANNINI, 2013.

Anele, Kalu Kingsley. *A study of the role of seafarers in combating piracy.* Etude, World Maritime University, 2015.

ANSA. «Sub al lavoro, recuperata 'scatola nera' plancia.» *ANSA.it*, 2012.

Anthony, (US Navy), interviewer par J. Reubrecht. *Interview personnelle* (07 04 2022).

Badot, Marion. «La sécurisation du détroit de Malacca : un défi pour l'Asie.» 2006.

Baraniuk, Chris. «How hackers are targeting the shipping industry.» *BBC*, 2017.

Barber, Charles Victor, et Vaughan R. Pratt. *Poison and Profits - Cyanide Fishing in the Indo-Pacific.* Noumea: Secretariat of the Pacific Community, 1999.

Bateman, S. «Safety and security in the Malacca and Singapore Straits.» Etude, 2006.

Belga. «Saisie de 4,5 tonnes de cocaïne à destination d'Anvers.» *7sur7*, 2021.

Bell, Curtis. *Pirates of the Gulf of Guinea: A Cost Analysis for Coastal States.* Rapport, Stable Seas, 2021.

Biju, Gopal, Prakash. *Cyber Attacks And Its Different Types.* Journal de recherche, Pattoor: IRJET, 2019.

BIMCO et al. «The Guidelines On Cyber Security On Board Ships V4.0.» Lignes directrices, 2021.

BlueVoyant. «Supply Chain Disruptions and Cyber Security in the Logistics Industry.» 2021.

BNP PARIBAS. *Nigéria : Le contexte économique.* Mai 2021. https://www.tradesolutions.bnpparibas.com/fr/explorer/nigeria/le-contexte-economique (accès le Mai 14, 2021).

Bockmann, Michelle Wiese, et Alan Katz. «Shooting to Kill Pirates Risks Blackwater Moment.» *Bloomberg* (Bloomberg), 2010.

BP Statistical Review. «Statistical Review of World Energy.» 2020.

Brume-Eruagbere, Omovigho Cynthia. *Maritime law enforcement in Nigeria: the challenges of combatting piracy and armed robbery at sea.* Malmo: World Maritime University, 2017.

C4ADS. «Above Us Only Stars.» 2019.

Carnegie, Paul J. *Human Insecurities in Southeast Asia.* Singapour: Springer, 2016.

CFR. «Jemaah Islamiyah (a.k.a. Jemaah Islamiah).» *Council on Foreign Relations*, 2009.

Chalk, Peter. *GREY-AREA PHENOMENA IN SOUTHEAST ASIA: PIRACY, DRUG TRAFFICKING AND POLITICAL TERRORISM.* Etude, Canberra: The Australian National University, 1997.

Chilaka, Edmund. *Piracy and Nigeria's National Security in the Early 21st Century.* Lagos: University of Lagos, 2015.

Christian. *Top 10 Richest Asian Countries 2022 (Per Capita).* 2022. https://www.webbspy.com/top-10-richest-asian-countries/ (accès le 05 17, 2022).

CIA. *Indonésie.* 2020. https://www.cia.gov/the-world-factbook/countries/indonesia/#people-and-society (accès le 02 17, 2022).

Cimpanu, Catalin. *All four of the world's largest shipping companies have now been hit by cyber-attacks.* 29 09 2020. https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/ (accès le 05 23, 2022).

Clapson, Colin. «Flemish port companies under cyberattack due to Ukraine's woes?» *vrt news*, 2022.

Computer Forensics World. *Can Malware Hide From Antivirus?* 18 03 2022. https://www.computerforensicsworld.com/can-malware-hide-from-antivirus/#2 (accès le 04 13, 2022).

Congressional Research Service. *Illegal Drug Trade in Africa: Trends and U.S. Policy.* CRS, 2009.

Congressional Research Service. *Latin America and the Caribbean: Illicit Drug Trafficking and U.S. Counterdrug Programs.* CRS, 2010.

CSO. *Global cybercrime dominated by 50 core groups, CrowdStrike report finds.* 23 01 2014. http://cdn.cso.com.au/article/536606/global_cybercrime_dominated_by_50_core_groups_crowdstrike_report_finds/ (accès le 04 12, 2022).

CVE Details. *Security Vulnerabilities.* 2021. https://www.cvedetails.com/vulnerability-list.php?vendor_id=26&product_id=739&version_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&ye (accès le 04 07, 2022).

CyberKeel. «Virtual pirates at large on the cyber seas.» Analyse, 2014.

Daniel. *20 Anti-Piracy Weapons Deployed In Ships To Fight Pirates.* 15 04 2021. https://www.maritimemanual.com/anti-piracy-weapons/ (accès le 04 24, 2022).

Data Journalism Team. *Cybersecurity hiring levels in the offshore industry rose in April 2022.* 16 05 2022. https://www.offshore-technology.com/analysis/cybersecurity-hiring-levels-in-the-offshore-industry-rose-in-april-2022/ (accès le 05 20, 2022).

Davis, Anthony. *Piracy in Southeast Asia shows signs of increased organisation.* 2004.

de La Grange, Arnaud. «Le Ponant : l'histoire secrète d'une libération.» *Le Figaro*, 2008.

defense.gouv.fr. *TF 150 : Opération commune de sécurité maritime.* 2012. https://www.defense.gouv.fr/marine/a-la-une/tf-150-operation-commune-de-securite-maritime (accès le 05 15, 2022).

Demeestere, Matthieu. «European oil port terminals hit by cyberattack.» *Tech Xplore*, 2022.

Diangituwka, Fweley. *Terrorisme et piraterie dans le golfe de Guinée : esquisses de solutions.* Yaoundé: Fondation Friedrich Ebert, 2010.

Dotselaere, Peter. *DP BASIC COURSE.* Cours, Antwerp: Antwerp Maritime Academy, 2022.

Dunt, John. *Marine Cargo Insurance.* Informa Law, 2009.

ENISA. «ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR.» Analyse, 2011.

Etevenard, Loïc, et Denis Bassompierre. «A l'abordage des pirates du Golfe de Guinée.» 2016.

EUROPOL. «EU Drug Markets Report.» La Haye, 2019.

EUROPOL. «European Union Cocaine Situation Report.» 2007.

Expatica. *Cocaine seized at key European port busts records.* 05 01 2021. https://www.expatica.com/be/uncategorized/cocaine-seized-at-key-european-port-busts-records-166146/ (accès le 04 14, 2022).

FORTINET. *Cyberglossary.* 2022. https://www.fortinet.com/resources/cyberglossary (accès le 03 30, 2022).

France Télévisions. «Complément d'enquête.» *Le Havre, coke en stock.* Paris, 25 10 2018.

FXCM. *CFDs sur Pétrole Brut (Brent).* 13 Mai 2021. https://fr.tradingview.com/chart/?symbol=FX%3AUKOIL.

Gallagher, Sean. «Hacked at sea: Researchers find ships' data recorders vulnerable to attack.» *ars Technica*, 2015.

Gesami, Brigid. *MARITIME SECURITY THREATS IN AFRICA.* Article, Academia Letters, 2021.

Gliha, Dino. «MARITIME CYBER CRIME - 21ST CENTURY PIRACY.» 2018.

Global Fire Power. *2022 Nigeria Military Strength.* 09 04 2022. https://www.globalfirepower.com/country-military-strength-detail.php?country_id=nigeria (accès le 04 24, 2022).

Graham, Luke. «Shipping industry vulnerable to cyber attacks and GPS jamming.» *CNBC*, 2017.

Gwin, Peter. *Dark Passage.* National Geographic, 2007.

Gwin, Peter, interviewer par Scott Simon. *Writer Tracks Modern-Day Pirates in Malaysia* (13 10 2007).

Harvey, Cynthia. *Top 8 Cyber Insurance Companies for 2020.* 09 11 2020. https://www.esecurityplanet.com/products/cyber-insurance-companies (accès le 04 10, 2022).

Have I Been Pwnd. *';--have i been pwned?* 2021. https://haveibeenpwned.com/ (accès le 04 07, 2022).

Herbert-Burns, R. *Compound piracy at sea in the early twenty-first century.* 2006.

Hive Systems. *Are Your Passwords in the Green?* 02 03 2022. https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=tabletext (accès le 04 07, 2022).

HyperSpike. *HS-18 RAHD.* 2022. https://www.ultra-hyperspike.com/product/hs-18-rahd/ (accès le 04 23, 2022).

IACS. «Recommendation on Cyber Resilience.» Recommendations, 2020.

ICC-IMB. «2007 Piracy and Armed Robbery Against Ships Annual Report.» Londres, 2008.

ICC-IMB. «2011 Annual Piracy Report.» 2012.

ICC-IMB. «2020 Annual Piracy Report.» London, 2021.

ICC-IMB. «2021 Annual IMB Piracy Report.» London, 2022.

ICS et al. *BMP WA.* 2020.

IMO. *Code of Practice for the Investigation of the Crimes of Piracy and Armed Robbery Against Ships.* Londres, 2001.

IMO. «Piracy in the Gulf of Guinea.» Londres, 2021.

INTERPOL. «PROJECT AGWE.» 2021.

—. *Project AGWE, West Africa.* 2020. https://www.interpol.int/en/Crimes/Maritime-crime/Project-AGWE-West-Africa (accès le Avril 12, 2021).

INTERTANKO. «Jamming and Spoofing of Global Navigation Satellite Systems (GNSS).» 2019.

ISC. «Piracy and Armed Robbery against Ships in Asia Annual Report.» Rapport, Singapour, 2022.

Jacq, Olivier. *Détection, analyse contextuelle et visualisation de cyber-attaques en temps réel : élaboration de la Cyber Situational Awareness du monde maritime.* Thèse de doctorat, Brest: HAL open science, 2021.

Janardhanan, Arun. «Lost voice data recorder may cost India Italian marines case.» *Times of India*, 2013.

Jeff. *10 Ways Sailors Use to Fight Pirates.* Hong Kong, 01 04 2022.

Joubert, Lydelle. *The State of Maritime Piracy 2019.* Rapport, Broomfield CO: One Earth Future, 2020.

Justers, Capitaine W., interviewer par Jorys Reubrecht. *Interview personnelle* (22 05 2022).

justice.gov. *MSC Gayane Crew Member Pleads Guilty to Cocaine Trafficking Stemming from One of the Largest Drug Seizures in U.S. History.* 15 06 2020. https://www.justice.gov/usao-edpa/pr/msc-gayane-crew-member-pleads-guilty-cocaine-trafficking-stemming-one-largest-drug (accès le 04 15, 2022).

Ross Kemp in the Search of Pirates. Réalisé par Ross Kemp. 2009.

Knox, Jodie. *Coast guard commandant on cyber in the maritime domain.* 2015. http://mariners.coastguard.dodlive.mil/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/ (accès le 04 08, 2022).

La Banque Mondiale. *Bénéfices tirés du pétrole (% du PIB) - Nigeria, Angola.* 13 Mai 2021. https://donnees.banquemondiale.org/indicator/NY.GDP.PETR.RT.ZS?end=2018&locations=NG-AO-CG&start=1971&view=chart (accès le Mai 13, 2021).

—. *Croissance du PIB par habitant (% annuel) - Nigeria, Angola.* 13 Mai 2021. https://donnees.banquemondiale.org/indicator/NY.GDP.PCAP.KD.ZG?end=2018&locations=NG-AO&start=1971&view=chart (accès le Mai 13, 2021).

Lagouvardou, Sotiria. *Maritime Cyber Security: concepts, problems and models.* Thèse de doctorat, Technical University of Denmark, 2018.

Lataire, Evert. *Propulsion (Part 2).* Anvers: Antwerp Maritime Academy, 2021.

Le Journal Du Dimanche. «Les secrets de l'opération Thalathine.» *JDD*, 2008.

Le Monde. «Le skipper du "Tanit" a bien été tué par une balle française.» *Le Monde*, 2010.

Le Point Afrique. «COVID-19 : Le Nigéria en récession accuse le coup.» *Le Point Afrique*, Novembre 2020.

Le Point. «L'histoire secrète du « Ponant ».» *Le Point*, 2008.

Libération. «La force et la réactivité des armées.» *Libération*, 2008.

Liss, Carolin. *The Challenges of Piracy in Southeast Asia and the Role of Australia.* Global Collaborative, 2007.

LMA. «War, Cyber War and Cyber Operation Exclusion.» London, 25 11 2021.

LMA, IUA. «Hull War, Piracy, Terrorism and Related Perils Listed Areas.» Londres, 2020.

Luntumbue, Michel. *Piraterie et insécurité dans le golfe de Guinée : défis et enjeux d'une gouvernance maritime régionale.* Brussels: Notes d'analyse du GRIP, 2011, 6.

Macro Trends. *Somalia Surface Area 1961-2022.* 2022. https://www.macrotrends.net/countries/SOM/somalia/surface-area-km (accès le 04 24, 2022).

Marine Traffic. *Callao Port.* 16 04 2022. https://www.marinetraffic.com/en/ais/details/ports/2739?name=CALLAO&country=Peru (accès le 04 16, 2022).

—. *LAGOS Port.* 23 04 2022. https://www.marinetraffic.com/en/ais/details/ports/802?name=LAGOS&country=Nigeria (accès le 04 23, 2022).

MarineTraffic. *Guayaquil Port.* 2022. https://www.marinetraffic.com/en/ais/details/ports/1488?name=GUAYAQUIL&country=Ecuador (accès le 02 18, 2022).

MDAT-GoG. «ReCAAP Brief.» 2018.

Menon, Malakiva. «Singapore navy takes part in exercise with 20 countries to boost regional maritime security against terrorism, piracy.» *The Straits Times*, 2021.

Mer et Marine. *Détournement du Ponant : Bateau au mouillage et contact établi avec les pirates.* 2008. https://www.meretmarine.com/article.cfm?id=107359 (accès le 05 15, 2022).

Ministère de l'Environnement, de l'Energie et de la Mer, ANSSI. «Guide des bonnes pratiques de sécurité informatique à bord des navires.» Paris, 2016.

Monnet, Bertrand. «Rencontre avec « Black Devil », le pirate du delta du Niger.» *Le Monde*, 2020.

Moreels, Stephan. *The insurability of maritime terrorism* . Master Thesis, Gand: Universiteit Gent, 2016.

MSC. *RECOMMENDED ACTION TO ADDRESS PIRACY AND ARMED ROBBERY IN THE GULF OF GUINEA.* Résolution, Londres: OMI, 2021.

Munro, Ken. «OSINT from ship satcoms.» 2017.

Murphy, Martin N. *Small boats, weak states, dirty money.* Londres: HURST Publishers Ltd, 2008.

National Bureau of Statistics. «National Gross Domestic Product Q4 2021.» 2021.

NATO Shipping Centre. «Piracy - Revised Guidance on the use of AIS in the High Risk Area off Somalia.» 2011.

Nigerian Navy. *Nigerian Navy Ships.* 16 Avril 2021. https://www.navy.mil.ng/ships/.

NVIDIA. *NVIDIA TITAN V.* 2022. https://www.nvidia.com/en-us/titan/titan-v/ (accès le 04 07, 2022).

offshore-technology.com. *Cybersecurity in Oil & Gas.* 2022. https://www.offshore-technology.com/cybersecurity-in-oil-gas/ (accès le 05 20, 2022).

OMI. «Code of Practice for the investigation of crimes of piracy and armed robbery against ships A.1025.» Résolution, Londres, 2010.

OMI. «Guidelines On Maritime Cyber Risk Management.» Circulaire, Londres, 2017.

OMI. *IMO Res A 917 (22)* . Résolution, Londres: OMI, 2001.

—. *ISPS Code.* Londres, 2003.

OMI. *MSC.1/Circ.1332* . Circulaire, Londres: OMI, 2009.

OMI. «Outcome Of The Regulatory Scoping Exercise For The Use Of Maritime Autonomous Surface Ships (MASS).» Circulaire, Londres, 2021.

OMI. *Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships.* Circulaire, Londres: OMI, 2009.

OMI. «SN/Cir.198.» Circulaire, Londres, 1998.

One Earth Future. «The Economic Cost of Somali Piracy 2012.» 2013.

One Earth Future. *The Human Cost of Somali Piracy 2011.* Bilan, ICC, 2012.

ONU. «Convention des Nations unies sur le droit de la mer.» Convention, Montego Bay, 1982.

—. *United Nations Convention on the Law of the Sea.* Montego Bay, 1982.

Onuoha, Freedom C. *Piracy and Maritime Security in the Gulf of Guinea: Trends, Concerns, and Propositions.* Publication, The Journal of the Middle East and Africa, 2013.

Operation Ocean Shield. «Operation Ocean Shield.» 2013.

Organisation Mondiale du Commerce. *La COVID-19 et le commerce mondial.* 2021. https://www.wto.org/french/tratop_f/covid19_f/covid19_f.htm (accès le Mai 12, 2021).

OSCE. «Latest from the OSCE Special Monitoring Mission to Ukraine (SMM), based on information received as of 19:30, 19 January 2017.» Kiev, 2017.

Permal, S. *Piracy and Sovereingty in the Strait of Malacca.* Centre for Maritime Security and Diplomacy, 2005.

Pertuet, S.J.P. *The challenges of criminalising piracy & armed robbery at sea under International Criminal Law.* Master Thesis, University of Groningen, 2021.

Pietsch, Marian, et Eric Pichon. *Piracy in the Gulf of Guinea.* Brussels: (c) European Union, 2020.

Placek, Martin. *The world's leading container ship operators as of March 31, 2022, based on number of owned and chartered ships.* 06 04 2022. https://www.statista.com/statistics/197643/total-number-of-ships-of-worldwide-leading-container-ship-operators-in-2011/#professional (accès le 04 08, 2022).

Pompeo, MICHAEL R. «Explosion in Beirut – Secretary Pompeo's Statement.» *Explosion in Beirut – Secretary Pompeo's Statement.* U.S. Embassy Beirut, 2020.

Ramachandran, Sudha. «Divisions over Terror Threat in Malacca Straits.» *Asia Times*, 2004.

Ramirez, Maria Fernanda. *Container Shipping: Cocaine Hide and Seek.* 09 02 2021. https://insightcrime.org/investigations/container-shipping-cocaine-hide-and-seek/ (accès le 04 15, 2022).

Raymond, Catherine Zara. «Piracy and Armed Robbery in the Malacca Strait.» 2009.

ReCAAP et al. «Regional Guide to Counter Piracy and Armed Robbery Against Ships in Asia.» Guide, 2016.

ReCAAP, IFC . *Tug Boats and Barges (TaB) Guide Against Piracy and Sea Robbery.* Guide, ReCAAP, 2013.

ReCAAP, IFC, RSIS. *Guide for Tankers Operating in Asia against Piracy and Armed Robbery Involving Oil Cargo Theft .* Guide, ReCAAP, 2015.

Reiff, Nathan. *10 Biggest Shipping Companies.* 11 09 2020. https://www.investopedia.com/10-biggest-shipping-companies-5077534 (accès le 04 08, 2022).

Reuters. «Indonesia says could also take China to court over South China Sea.» *Reuters*, 2015.

Séré, Ludovic. «En 1947, un cargo chargé de nitrate d'ammonium explosait à Brest.» *La Croix*, 2020.

«Somalian hostage taking - French commando.» *youtube.com.* 22 03 2010. https://www.youtube.com/watch?v=ZWkeymNjpsI (accès le 05 15, 2022).

Spiess, Robin. «Black Spots.» *South East Asia Globe.* 15 07 2019.

SplashData. *Les mots de passe les plus utilisés de 2018 : les vôtres y figurent-ils?* 18 12 2018. https://www.welivesecurity.com/fr/2018/12/18/mots-de-passe-2018-palmares/ (accès le 04 05, 2022).

Sun, Zhen. *Regulation of Shipping in the Straits of Malacca and Singapore.* Malmö: World Maritime University, 2017.

Terra Firma. «Risk Focus : Kidnap and Ransom.» Londres, 2016.

The Guardian. «Twenty-three tonnes of cocaine seized in Europe's biggest haul.» *The Guardian*, 2021.

The Maritime Executive. «One Crew Member Killed, Six Kidnapped in New Gulf of Guinea Incident .» *The Maritime Executive*, 2021.

The Maritime Executive. «Tests Show Ease of Hacking ECDIS, Radar and Machinery.» *The Maritime Executive*, 2017.

TIdy, Joe. «European oil facilities hit by cyber-attacks.» *BBC*, 2022.

Trading Economics. *Indonésie - PIB par habitant.* 2022. https://fr.tradingeconomics.com/indonesia/gdp-per-capita (accès le 05 17, 2022).

—. *Malaisie - PIB par habitant.* 2022. https://fr.tradingeconomics.com/malaysia/gdp-per-capita (accès le 05 17, 2022).

—. *Nigeria - Population.* 13 Mai 2021. https://fr.tradingeconomics.com/nigeria/population (accès le Mai 13, 2021).

—. *Nigeria - Taux de chômage des jeunes.* 14 Mai 2021. https://fr.tradingeconomics.com/nigeria/youth-unemployment-rate (accès le Mai 14, 2021).

—. *Nigeria Inflation Rate.* 13 Mai 2021. https://tradingeconomics.com/nigeria/inflation-cpi (accès le Mai 13, 2021).

—. *PIB PAR HABITANT - LISTE DES PAYS - ASIE.* 01 01 2022. https://fr.tradingeconomics.com/country-list/gdp-per-capita?continent=asia (accès le 02 17, 2022).

—. *Singapour - PIB par habitant.* 2022. https://fr.tradingeconomics.com/singapore/gdp-per-capita (accès le 05 17, 2022).

—. *Taux de chômage - Liste des pays.* 13 Mai 2021. https://fr.tradingeconomics.com/country-list/unemployment-rate (accès le Mai 13, 2021).

TrapX. *ANATOMY OF AN ATTACK Zombie Zero Weaponized Malware Targets ERP Systems.* Rapport, TrapX Research Labs, 2017.

Trend Micro. «Russian Underground 101.» 2012.

Tucker, Patrick. «DHS: Drug Traffickers Are Spoofing Border Drones.» *Defense One*, 2015.

UK War Risks. *War risks cover details.* 01 02 2022. https://www.ukwarrisks.com/cover/cover-details/ (accès le 05 13, 2022).

UKP&I. *Electronic Bills of Lading - An Update: Part II.* 01 04 2020. https://www.ukpandi.com/news-and-resources/legal-content/legal-articles/electronic-bills-of-lading---an-update-part-ii/ (accès le 04 10, 2022).

UNDP. «Human Development Report 2020.» New York, 2020.

UNODC. *Container Control.* 2021. https://www.unodc.org/unodc/en/urban-safety/container-control.html (accès le 04 14, 2022).

UNODC. *Transnational Organized Crime in Southeast Asia: Evolution, Growth and Impact.* UNODC, 2019.

UNSC. «Resolution 1816.» 2 June 2008.

—. «Resolution 2554.» 4 December 2020.

UT News. «UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea.» *UT News*, 2013.

Verizon. «Data Breach Digest, Scenarios from the field.» Rapport, 2016.

von Hoesslin, Karsten. «Lawless Oceans.» 2017.

Whiting, Kate. «Stuck at sea: How to save the world's seafarers and the supply systems they support.» *World Economic Forum*, 19 Juin 2020.

Wong, Lester. «Sea robbery attempt in Singapore Strait foiled by Singapore and Indonesian navies.» *The Straits Times*, 2020.

World Bank. «Somalia GDP per capita.» *Trading Economics.* 2022. https://tradingeconomics.com/somalia/gdp-per-capita (accès le 04 24, 2022).

Worldometer. *Total Coronavirus Cases in Nigeria.* 13 Mai 2021. https://www.worldometers.info/coronavirus/country/nigeria/ (accès le Mai 13, 2021).

Liste des annexes

Annexe 1 : Localisation des incidents réels et tentés entre Janvier 2017 et Décembre 2021
Source : ICC-IMB 2022

ICC- IMB Piracy and Armed Robbery Against Ships Report – 01 January – 31 December 2021

TABLE 1: Locations of ACTUAL and ATTEMPTED incidents, January – December 2017 – 2021

	Location	2017	2018	2019	2020	2021
S E ASIA	Indonesia	43	36	25	26	9
	Malacca Straits					1
	Malaysia	7	11	11	4	2
	Philippines	22	10	5	8	9
	Singapore Straits	4	3	12	23	35
	Thailand				1	
EAST ASIA	China	2	3	3		
	Vietnam	2	4	2	4	1
INDIAN SUB	Bangladesh	11	12		4	
CONTINENT	India	4	6	4	6	2
SOUTH AMERICA	Brazil		4	2	7	3
	Colombia	6	1	3	1	6
	Dominican Republic			1		
	Ecuador	2	4	3	5	4
	Guyana	1	2			
	Haiti	1	3	2	5	4
	Mexico			1	4	1
	Panama			1		
	Peru	2	4	10	8	18
	Venezuela	12	11	6		
AFRICA	Algeria			1		
	Angola	1			6	4
	Benin		5	3	11	2
	Cameroon		7	6		1
	Dem. Republic of Congo		1	1		1
	Dem. Rep. of Sao Tome & Principe	1		1	2	5
	Equatorial Guinea			2	3	2
	Gabon			1	2	4
	Ghana	1	10	3	9	5
	Guinea	2	3	2	5	3
	Gulf of Aden*	3	1			1
	Ivory Coast	1	1	1	3	
	Kenya	1		1		
	Liberia			2	2	1
	Morocco			2		
	Mozambique	2	2	3	4	1
	Nigeria	33	48	35	35	6
	Red Sea*	1				
	Senegal	1				
	Sierra Leone	4		1		
	Somalia*	5	2			
	The Congo	1	6	3	3	1
	Togo		1	3	3	
REST OF	Iraq				1	
WORLD	Oman	1				
	Yemen	3				
	Total at year end	**180**	**201**	**162**	**195**	**132**

All incidents with * above are attributed to Somali pirates