diploweb.com La revue géopolitique
ISSN : 2111-4307

Thalassopolitique des fonds marins, théâtre d'une nouvelle conflictualité inter-étatique ?

dimanche 5 novembre 2023,par Florian MANET

Citer cet article / To cite this version :
Florian MANET, **Thalassopolitique des fonds marins, théâtre d'une nouvelle conflictualité inter-étatique ?**, *Diploweb.com : la revue géopolitique, 5 novembre 2023.*

Hum... Vous semblez apprécier le DIPLOWEB.COM. Nous vous en remercions et vous invitons à participer à sa construction.

Le DIPLOWEB.COM est LE media géopolitique indépendant en accès gratuit, fondé en l'an 2000. Nous vous proposons de participer concrètement à cette réalisation francophone de qualité, lu dans 190 pays. Comment faire ? Nous vous invitons à verser un "pourboire" (tip) à votre convenance via le site **https://fr.tipeee.com/diploweb** . Vous pouvez aussi rédiger un chèque à l'ordre du DIPLOWEB.COM et l'adresser à Diploweb.com, Pierre Verluise, 1 avenue Lamartine, 94300, Vincennes, France. Ou bien encore faire un virement bancaire en demandant un RIB à l'adresse expertise.geopolitique@gmail.com.

Avec 5 000€ par mois, nous pouvons couvrir nos principaux frais de fonctionnement et dégager le temps nécessaire à nos principaux responsables pour qu'ils continuent à travailler sur le DIPLOWEB.COM.
Avec 8 000€ par mois, nous pouvons lancer de nouveaux projets (contenus, événements), voire l'optimisation de la maquette du site web du DIPLOWEB.COM.

Matérialisée par le conflit russo-ukrainien et ré-affirmée au Proche-Orient depuis l'attaque par le Hamas d'Israël, la nouvelle donne stratégique a des incidences directes et immédiates sur les politiques de défense des États, contraints d'adapter la protection de leurs intérêts majeurs. La maritimisation des modes de vie conjuguées à la digitalisation des économies et aux objectifs de transition énergétique ont dessiné, notamment, une géopolitique énergétique et numérique qui est questionnée aujourd'hui. En effet, ces dynamiques reposent sur des réalisations industrielles à l'image des câbles sous-marins (énergie, télécommunication), des plates-formes d'extraction de matières premières (hydrocarbures, terres rares…) mais aussi les projets d'envergure des îles énergétiques artificielles. Ces infrastructures critiques sous-marines et maritimes sont devenues des centres de gravité stratégiques qui conditionnent la résilience des États. Transparentes pour l'usager, elles constituent, néanmoins, selon les points de vue, soit des vulnérabilités soit des cibles d'intérêt dans la perspective d'une guerre totale ou guerre d'attrition. Florian Manet se fait pédagogue pour expliquer les ressorts de ces nouveaux risques majeurs et met les États devant leurs responsabilités.
4 illustrations : deux photos et deux cartes.

LES ESPACES OCEANIQUES font, actuellement, l'objet d'une cristallisation des intérêts des nations. L'une des illustrations les plus criantes demeure le conflit russo-ukrainien et, notamment, les opérations militaires engendrées à la suite de l'invasion du Donbass le 24 février 2022. Le théâtre des opérations s'est, progressivement, dilué vers les espaces maritimes stratégiques encadrant le théâtre européen aéro-terrestre. L'attaque portée au Moskowa, vaisseau amiral de la flotte russe de la mer Noire, le 14 avril 2022, n'était que le premier épisode d'opérations aéronavales. Le contrôle de la navigation dans cette mer presque fermée, ce cul de sac maritime à la frontière de l'Europe et du Moyen-Orient, constitue l'un des enjeux majeurs au plan militaire comme économique. La pose de mines maritimes, les attaques répétées à base de navires autonomes comme le tir de missiles mer-mer, terre-mer et air-mer visant des installations portuaires comme les flottes de combat ont contraint à une réorganisation des chaines d'approvisionnement internationales. Ce volet d'opérations navales s'avère finalement tout à fait conventionnel dans la perspective d'un conflit armé inter-étatique de haute intensité.

Cependant, une révolution aux conséquences durables s'est jouée, simultanément, sur une mer adjacente au théâtre des opérations aéro-terrestres, la mer Baltique. Les actes de sabotage portés à quatre reprises sur les gazoducs Nord Stream 1 et 2 ont banni durablement la croyance universelle en l'inviolabilité des infrastructures flottantes ou posées au fond des océans dans un contexte de dépendance accrue aux espaces maritimes. Quand bien même fussent-elles situées hors des eaux territoriales.

De fait, alors que les acteurs étatiques se polarisent nettement et que les opérations militaires multi-champs et multi-milieux éprouvent la résilience des parties prenantes, **les infrastructures critiques maritimes constituent, plus que jamais, des centres de gravité des conflits inter-étatiques**. Des modes d'action qualifiés d'hybrides mettent, désormais, en risque la capacité d'opérateurs de services essentiels à assumer la fourniture de communication, d'énergie et de transport par voie maritime.

Ainsi, après avoir décrit les enjeux de l'« infrastructuration » des espaces océaniques (I), les menaces et des scénarii envisageables d'expression des conflits hybrides dans les espaces maritimes seront présentés (II). Enfin, cette nouvelle donne stratégique invite les États à développer une thalassopolitique conforme à leurs responsabilités et à la défense de leurs propres intérêts (III).

I. L'infrastructuration des espaces océaniques

Les espaces océaniques connaissent un mouvement universel d'exploitation de leurs potentialités ce qui se traduit par l'implantation d'installations artificielles *offshore* très variées. Cette dynamique est qualifiée par le néologisme d'« infrastructuration » (A). Néanmoins, le droit international a précédé, accompagné et s'est adapté à ces évolutions, s'efforçant de réguler les activités humaines en mer en combinant les principes de souveraineté des États et de protection de l'environnement naturel maritime (B).

A. Une variété et une complexité croissante d'installations posées ou flottantes

Le progrès technologique a accompagné la dynamique de mondialisation économique fondée sur un rapport de dépendance accru aux espaces maritimes. Pour décrire cette réalité irréfragable, on évoque alors le concept de « maritimisation » des économies et des modes de vie. Initiés au XIX ème siècle, ce mouvement de travaux maritimes a affecté initialement les télécommunications avec la pose du premier câble en Manche le 28 août 1850 [1]. Puis, à compter des années 1920, les pionniers de l'exploration pétrolière *offshore* ont exploité des nappes pétrolifères du golfe du Mexique, rendant possible *in fine* une production industrielle en 1947. Dès lors, ces infrastructures se développent et se multiplient, de plus en plus loin des côtes et de plus en plus profondément. L'*offshore* profond se développe entre 1 500 et 3 000 mètres de profondeur.

L'exploitation minière et pétrolière sous-marine

Recouvrant près de 64 % de la surface du globe, ces espaces singuliers regorgent, en effet, de matières premières. Le potentiel minier des fonds et grands fonds marins est très prometteur, notamment dans le contexte de production d'énergies alternatives sans émission de gaz à effet de serre. Les gisement de terres rares ou de modules polymétalliques [2] constituent des défis, certes, technologiques mais aussi économiques.

Par ailleurs, les fonds marins servent de support à des réseaux de tuyaux ou *pipe-line* [3] alimentant en gaz ou en hydrocarbures les économies énergivores depuis des plates-formes de forage *offshore*. L'Organisation Maritime Internationale [4] considère que le fret pétrolier, brut ou raffiné, représente un tiers du commerce maritime international. Le stockage comme la distribution des hydrocarbures nécessitent des installations dédiées de plus en plus souvent localisées *offshore*. Pour des gains de productivité, les navires citerne délivrent les hydrocarbures non plus à quai dans un port mais au large à partir de bouées d'amarrage *offshore* situées sur le plateau continental. Les bouées d'amarrage par point unique sont utilisées pour immobiliser les pétroliers navettes pendant les opérations de chargement et de déchargement. Attachée à une structure sous-marine à l'aide de tuyaux flexibles, la bouée est

maintenue en place par des ancres.

Enfin, se développent, pour des raisons d'autonomie stratégique et de sécurité énergétique, des solutions de stockage de gaz liquéfié. L'exemple lituanien est très illustratif. Il s'agissait, pour cet état balte, d'opter pour une alternative au gazoduc russe et de diversifier ses approvisionnements. Amarré à l'embouchure du port lituanien de Klaipéda, un navire-citerne, INDEPENDANCE, joue le rôle de terminal flottant de gaz naturel liquéfié (GNL).

Un navire-citerne opérant à une bouée d'amarrage par point unique
Copyright : Louis du Plessix/Diploweb.com
du Plessix/Diploweb.com

La mer, remède circonstanciel à la transition énergétique ?

De même, les enjeux environnementaux favorisant des productions d'énergies décarbonnées invitent à la conception et à la réalisation de parcs éoliens, soit posés, soit flottants ou encore à celle de plateformes produisant de l'énergie hydrolienne ou marémotrice promouvant ainsi des Énergies Marines Renouvelables (EMR).

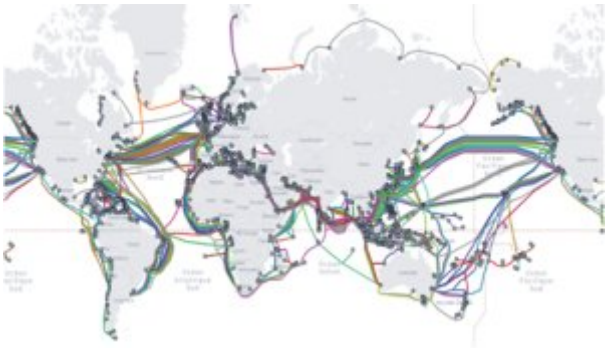
Témoignant, désormais, d'une réelle maturité, ce mouvement connaît actuellement des développements sans précédent comme le démontrent des projets scandinaves en mer du Nord. Il s'agit de la construction d'îles énergétiques [5] (« *energy island* ») situées au large des côtes qui fourniront de l'hydrogène et de l'électricité aux pays riverains dans une logique d'intégration européenne. Ainsi, un complexe d'envergure, Princess Elizabeth, est en cours de construction à 45 kilomètres des côtes belges, entre La Panne et Ostende. Dotée d'un port, d'un héliport et d'équipements haute tension (transformateur, sous-station), elle s'étendra sur 6 hectares et sera reliée à des parcs éoliens *offshore* et disposera d'une capacité totale de production de 3,5 gigawatts (GW). Elle alimentera en électricité la Belgique, le Danemark et le Royaume-Uni. Ce premier projet ouvre la voie à des réalisations encore plus importante comme le suggère l'appel d'offre lancé au Danemark pour une île de 20 à 40 hectares. Elle sera implantée à une centaine de kilomètres des côtes occidentales du Jutland, en mer du Nord. Réparties en 10 fermes, les installations composées de 670 turbines *offshore* seront ancrées à 30 mètres de profondeur. Lors de sa mise en service en 2030, elles produiront nominalement une puissance de 10 GW soit l'alimentation électrique de 10 millions de foyers ou encore la production de 6 réacteurs EPR. Cette île artificielle accueillera, aussi, une capacité de production d'hydrogène et de stockage d'énergie qui sera, ensuite, convoyée par un réseau de câbles d'alimentation à destination du continent. L'hydrogène apporte plus de souplesse dans

le stockage et le transport de l'électricité. Ce défi technologique réside aussi dans sa capacité d'intégration dans un environnement naturel particulièrement exigeant.

Les perspectives de transport par voie maritime d'énergie électrique produite *offshore* mais aussi *onshore* s'avèrent très dynamique à l'échelle internationale. L'Australie s'impose par une politique très volontariste de production d'énergie électrique au sein du Pacifique sud. Ainsi, le Japon est dépendant de l'énergie produite par l'Australie à hauteur de 15 % de ses importations totales. Une des sources principales provient des champs d'exploitation gazier *offshore* de IMPEX ICHTHYS [6] implantés sur la côte nord-ouest de l'Australie. De même, le projet sous-marin « Sun Cable » ambitionne de transporter l'électricité produite par des fermes solaires à proximité de Darwin à destination de Jakarta (Indonésie) et de la cité-État de Singapour. Cette géopolitique énergétique constitue l'un des volets conditionnant les relations internationales dans la zone Indo-Pacifique.

Vingt milles câbles sous les mers

Enfin, les espaces océaniques constituent des traits d'union entre les hommes, les peuples et les continents. Ainsi, dès le XIX ème siècle, des câbles de communication ont été déployés en Atlantique nord, reliant la France aux États-Unis d'Amérique. Dès lors, stimulés par la brutale numérisation des économies, les réseaux de câbles sous-marin se sont développés à tel point qu'il est estimé que 97 % des *data* échangées dans le monde empruntent les fonds marins selon de multiples combinaisons géographiques. Le montant global des transactions financières empruntant les câbles est estimé, en valeur, à 10 trillions de dollar US par jour. Ainsi, sous forme d'impulsions lumineuses circulant à très grande vitesse, ils véhiculent dans les fibres optiques, c'est-à-dire un long fil de verre de l'épaisseur d'un cheveu, des informations de toutes natures. Ordres de bourse, messageries personnelles comme professionnelles, renseignement militaire, etc.



Carte. Planisphère des réseaux de câbles sous-marins
Copyright : TeleGeography (Attribution-ShareAlike 4.0 International (CC BY-SA4.0)

Les câbles maillent les fonds marins. D'un continent à l'autre. D'un rivage à l'autre. Concentrés en leur point d'atterrissement (ou d'attérage), ils s'immergent en faisceau qui, au fur et à mesure, gagnent leurs destinations finales. En 2023, 485 systèmes opérationnels étaient dénombrés pour un réseau fort de 1,2 million de kilomètres. La France, métropolitaine ainsi que les outre-mers en dénombrent une cinquantaine. D'une longueur de 6800 kilomètres, le câble dénommé « Amitié » a été mis en service le 18 octobre 2023 : il relie Boston aux États-Unis d'Amérique à Porge (département de la Gironde) en France ainsi qu'à Bude (Cornouaille) au Royaume-Uni. De même, dans le cadre d'un programme de résilience numérique opéré en

Pacifique sud, deux câbles sous-marins transpacifiques « Honomoana » et « Tabua » seront prochainement exploités par Google. Ils visent à améliorer la connectivité et la fiabilité sur les routes transpacifiques entre les États-Unis, l'Australie, la Polynésie française et les Fidji. C'est un premier pas dans la construction de réseaux numériques alimentant et désenclavant les nombreuses îles et archipels du Sud-pacifique. C'est aussi une démarche, certes, technologique et économique Mais, cette démarche est aussi porteuse de conséquences géopolitiques dans une région à forts enjeux.

Or, chacun peut imaginer les difficultés et les obstacles qui compliquent l'entretien d'un tel réseau peu accessible et transparent aux yeux de nombre d'utilisateurs. Ces opérations de maintenance exigent des moyens considérables et un savoir-faire à haute valeur ajoutée maitrisé par peu d'acteurs.

L'une des spécificités majeure repose dans le statut juridique de ces infrastructures qui relève d'acteurs privés et, notamment, des champions de l'Internet. Résumés dans deux acronymes GAFAM (ou plus exactement GAMAM) et BATX [7], ils reflètent, à leur manière, une nouvelle réalité géopolitique d'un monde pivotant sur deux orbites culturelles concurrentielles. Ces partenaires économiques agissent de fait comme des acteurs géopolitiques de dimension internationale dotés d'un pouvoir qui, à bien des égards, égale voire surpasse celui des États tant leur raison sociale – permettre la communication – est déterminante.

B. Une exploitation des espaces maritimes régie par des conventions internationales

Cette exploitation des espaces océaniques s'inscrit effectivement dans le cadre juridique de la Convention des Nations Unies sur le Droit de la Mer (CNUDM) signé à Montégo Bay, en Jamaïque, en 10 décembre 1982. Suite à la ratification préalable par un nombre suffisant d'États, ce texte fondateur est entré en vigueur en 16 novembre 1994. Son apport est fondamental à de multiples titres.

Tout d'abord, cette « constitution de la mer » structure l'espace maritime selon une double perspective, sécuritaire et économique. Ainsi, l'espace de 12 milles nautiques courant depuis la laisse de basse mer vers le large est qualifiée de « mer territoriale ». C'est le prolongement maritime de l'État-côtier. En conséquence, ce dernier exerce, pleinement, des pouvoirs de police à la fois sur le milieu comme sur les vecteurs qui y évoluent librement. Cette garantie constitutionnelle contribue à l'expression pleine et entière de la souveraineté de l'État-côtier exercée sur ses approches maritimes. Ainsi, la pose d'installations (câble ou tuyaux) comme les opérations de recherche scientifique marine sont soumis à un régime d'autorisation préalable.

Par ailleurs, au-delà de cette ligne symbolique des 12 milles nautiques (soit 22 km), s'étend la Zone Économique Exclusive (ZEE) jusqu'aux 200 milles (soit 370 km). La CNUDM [8] attribue de fait à l'État-côtier le monopole de « *l'exploration et de conservation et de gestion des ressources naturelles, biologiques, et non biologiques des eaux surjacentes aux fonds marins, des fonds marins et de leur sous-sol, ainsi qu'en ce qui concerne d'autres activités tendant à l'exploration et à l'exploitation de la zone à des fins économiques , telles la production d'énergie électrique à partir de l'eau, des vents et des courants* [9] ». Il est, ainsi, libre de réguler les activités économiques telles la pêche maritime et la gestion des ressources halieutiques ou encore la construction d'îles artificielles, d'ouvrages et d'installations. Enfin les 64 % des espaces océaniques restants constituent la haute mer, patrimoine commun de

l'humanité. Selon la formulation latine "*res nullius, res communis*", la mer relève du patrimoine commun de l'humanité. Les autres puissances étatiques ont la possibilité de poser et d'entretenir des réseaux sous-marins immergés dans la ZEE relevant de la souveraineté de l'État côtier [10].

Enfin, l'État-côtier peut encore valoriser davantage les potentialités offertes par l'espace sous-marin en sollicitant l'extension de son propre plateau continental, auprès de la Commission des Limites du Plateau Continental, organe spécialisé des Nations unies. Déterminée par des conditions géophysiques, cette extension au sol et au sous-sol marin s'inscrit dans le prolongement naturel des terres émergées du rebord jusqu'à une distance de 350 milles nautiques. A la différence de la ZEE, l'État-côtier ne peut revendiquer des droits sur la colonne d'eau surjacente des fonds marins. Il s'agit, en effet, d'eaux à statut international. A titre d'illustration, le 10 juin 2020, la France [11] a obtenu une telle dérogation, notamment, dans l'océan Indien. Cette décision lui a permis d'étendre le domaine sous-marin français de 151 323 kilomètre carré au large de l'ile de la Réunion (58 121 Km2) et de Saint Paul et Amsterdam (93 202 Km2).

De fait, le bouillonnement actuel de projets d'implantation de parcs éoliens ou encore de pose de câbles s'inscrivent en parfaite cohérence avec les dispositions des normes internationales en vigueur. Ces projets d'envergure déployés en mer posent des défis non seulement technologiques mais aussi sécuritaires dont la perception a été renouvelée avec gravité depuis les événements du Nord Stream 1 et 2 en 2022. Les conventions internationales ont envisagé des événements affectant la sécurité des installations *offshore* à l'image de la convention MARPOL [12] et de ses différentes annexes.

La convention internationale mise en œuvre par l'Organisation Maritime Internationale (OMI) dite de Rome est dédiée à la suppression des actes illicites contre la sécurité de la navigation maritime [13] et des plates-formes situées sur le plateau continental. Elle envisage la commission d'actes de malveillance de nature terroriste ou en lien avec la prolifération de matières nucléaires mettant en péril la sécurité de la navigation maritime.

II. Les infrastructures critiques maritimes, nouveau champs de bataille ?

L'Union européenne définit les infrastructures critiques maritimes comme « des actifs ou un système qui est essentiel pour la maintenance des fonctions vitales de la société ». Elles incluent non seulement les réseaux d'énergie et de communication sous-marins mais encore les installations portuaires, les rails de navigation, les plates-formes *offshore* et les réseaux afférents. Elles jouent un rôle central dans les chaines d'approvisionnement globalisées et dans la souveraineté des États à l'image de la liberté de manœuvre des forces armées par exemple [14].

Ces infrastructures posées sur les fonds marins ou flottantes sont l'objet de menaces protéiformes qui retrouvent une acuité singulière au regard d'une polarisation croissante des relations internationales. Elles cristallisent, désormais, l'attention des États qui ont une parfaite conscience de l'importance de ces installations qualifiées, à juste titre, de critiques. Ces risques sont d'ordre accidentels (A) mais aussi volontaires et intentionnelles (B). Ainsi, il

convient de distinguer le concept de « sécurité » avec celui de « sûreté ». La sécurité ou *safety* désigne « *la prise en charge des risques d'origine naturelle ou provoqués par la navigation maritime* [15] ». Par différence, la sûreté maritime ou *security* est « *la combinaison des mesures préventives visant à protéger le transport maritime et les installations portuaires contre les menaces d'actions illicites conventionnelles [16]* ».

A. Les atteintes accidentelles aux infrastructures critiques maritimes

Les infrastructures maritimes sont exposées aux aléas d'un environnement naturel et industriel particulièrement exigeant.

Ainsi, la météorologie spécifique en mer peut se traduire par des tempêtes, raz de marée et courants susceptibles d'endommager les installations. Ainsi, des conflits d'usage entre les vecteurs maritimes et les infrastructures localisées en mer peuvent être provoqués par des éléments naturels conjugués à des problèmes d'ordre mécanique. Un cargo, le PETRA L [17], a heurté une turbine de la ferme éolienne *offshore* Gode Wind 1 situé en mer du Nord à environ 45 kilomètres des côtes allemandes et à 33 km au large des îles de Juist et de Norderney. Mettant hors service une turbine, cette perte de contrôle serait consécutive à une avarie dans une situation de forts vents.

Par ailleurs, le risque industriel encouru par l'exploitation *offshore* est une réalité omniprésente, notamment, au regard de la complexité d'infrastructures toujours plus sophistiquées. Ces plates-formes opérées en haute mer concentrent une multitude d'aléas liés à l'activité elle-même d'extraction à forte profondeur et au stockage d'un produit hautement inflammable ainsi qu'au milieu maritime particulièrement exigeant. Le contexte actuel est marqué par une recherche accrue de gisements. Aussi, les frontières du possible sont sans cesse repoussées : des forages toujours plus profonds exposent à des températures et des pressions de plus en plus fortes. Garantir un niveau élevé de sécurité est un enjeu fondamental pour l'industrie pétrolière. Le risque financier encouru est, aussi, susceptible de contribuer à la faillite de l'entrepreneur tant les coûts liés à la gestion d'une crise et les pénalités peuvent être importants.

Exemples non exhaustifs d'accidents majeurs depuis 30 ans

• **Ixtoc 1 (golfe du Mexique), 3 juin 1979**. La plateforme Ixtoc 1, exploitée par le pétrolier Perforaciones Marinas del Golfo, est soufflée par une éruption de pétrole. Neuf mois sont nécessaires pour stopper la marée noire de plus 500 000 tonnes de pétrole. Coût : 1,5 milliard de dollars US.

• **Piper Alpha (mer du Nord), 6 juillet 1988**. La plateforme Piper Alfa, opérée par Occidental Petroleum en mer du Nord britannique, explose. Faisant 167 morts, l'accident est celui qui a le plus profondément marqué l'industrie pétrolière en mer. Coût : 3,5 milliards de dollars US.

• **Deepwater Horizon (golfe du Mexique), 20 avril 2010.** La plateforme de forage Deepwater Horizon de Transocean, opérée par BP, explose, causant 11 morts. BP met trois mois à stopper la fuite à - 1 500 mètres sous l'eau. 4,9 millions de barils de brut se sont échappés. Coût : 40 milliards de dollars.

• **Elgin (mer du Nord), 25 mars 2012**. Une fuite de gaz de 200 000 m 3 par jour survient sur une plateforme exploitée par Total au large de l'Écosse. Malgré les efforts, les opérations engagées par le pétrolier français pourraient prendre jusqu'à six mois. Coût : 2,5 millions de dollars par jour.

En matière de réseaux de communication, les câbles posés sont vulnérables aux mouvements géologiques du sous-sol marin [18]. Ainsi, parmi les risques les plus fréquents, se trouvent les opérations de pêche et d'ancrage [19] de navire. Si elles sont fort heureusement rares, ces pannes engendrent des effets domino observés parfois très loin de leur centre de gravité au regard du degré d'interconnexion et d'inter-dépendance des économies aux réseaux. Plus récemment, le 8 octobre 2023, le gazoduc Balticconnector [20] et deux câbles de télécommunications ont été victimes de dommages liés à des opérations d'ancrage selon les premiers éléments communiqués par les autorités finlandaises. L'origine accidentelle comme intentionnelle n'est pas encore déterminée [21].

Dans notre perspective, ces atteintes à la sécurité sont à prendre en considération non pas pour elles-mêmes. Mais véritablement comme les conséquences possibles d'un acte de malveillance perpétré sur des infrastructures critiques. Notons que l'environnement maritime démultiplie l'impact d'une crise qui est sans commune mesure avec celle des autres milieux. La maritimisation contemporaine témoigne du gigantisme de la construction navale qui met en circulation des navires citerne longs de 400 mètres transportant plus de 300 000 tonnes de brut. La perte d'un navire génère des conséquences démultipliées dans l'espace maritime et côtier mais aussi dans le temps, car, tant que l'épave n'a pas rendu l'intégralité du fret transporté, du produit s'échappe inexorablement. D'autant plus que l'intervention humaine semble bien dérisoire au milieu des océans, quand les éléments se déchaînent.

Nord Stream 2 ou la révolution de l'évaluation de la malveillance maritime

La maritimisation s'est trouvée renforcée par la dépendance croissante des économies aux richesses des océans mais aussi par le rôle majeur joué par les vecteurs maritimes dans les approvisionnements stratégiques en matières premières. Stimulés par le croissance de l'industrie, les acteurs publics et privés ont massivement investi les océans pour implanter des infrastructures. Conjointement, la notion de risque a été atténuée par cet enthousiasme collectif.

Ces actes malveillants [22] nécessitent la conception d'une manœuvre particulièrement audacieuse visant à interrompre ou à détourner le flux de données transitant par ces tuyaux. Ils supposent **des modes opératoires hybrides produisant des effets asymétriques sur le camp adverse** : quelques milliers d'euros d'investissement pour l'acquisition, par exemple, d'un drone maritime peuvent causer des dommages de plusieurs millions d'euros. Observé en 1898, lors de la guerre américano-espagnole, les Américains coupèrent les fils télégraphiques entre l'Espagne et ses possessions transatlantiques. Autre scénario possible qui expose moins les auteurs : « écouter » le flux de données qui empruntent ce canal en installant des mouchards aux points clés du réseau. Reste, cependant, à déchiffrer et à exploiter cette masse considérable de données frauduleusement collectées. Enfin, nous assistons à une privatisation progressive de ces infrastructures vitales qui irriguent l'ensemble de nos vies. Jadis réseau étatique, les opérateurs comme les GAFAM en prennent progressivement le contrôle. Ce qui ne laisse pas d'interroger sur les enjeux de souveraineté attachés aux données et aux garanties apportées à la liberté d'expression.

Toutefois, **les actes de sabotage portés aux pipeline Nord Stream 1 et 2 ont matérialisé une menace pensée comme théorique**. Ce trait d'union maritime gazier reliant la Russie à l'Allemagne est victime d'un acte de malveillance constaté les 26 et 27 septembre 2022. A

cette occasion, la communauté internationale s'étonne d'un bouillonnement inhabituel à la surface de la mer Baltique et, ce, en deux endroits différents. Gisant dans les fonds de la Baltique, en Zone Économique Exclusive du Danemark et de la Finlande, le pipeline rallie Vyborg en Russie à Lubmin en Allemagne, soit une distance de 1224 kilomètres. Ce défi technologique permettait d'alimenter l'économie allemande en matières premières bon marché. Les différentes enquêtes sont encore actives afin d'élucider ces actes de malveillance et d'en établir les responsabilités. Néanmoins, il convient de souligner la grande complexité de la conception et de l'exécution d'une telle opération à haut risque. L'expédition sous-marine a été conduite par des plongeurs missionnés pour positionner à différentes reprises des charges explosives sur des installations posées au fond de la mer Baltique.

Cet acte de sabotage a généré un séisme au sein des sociétés hyperconnectées et tributaires de la mer pour l'équilibre de leurs chaines d'approvisionnement. Ces menaces hybrides sont issues d'une zone grise évoluant entre la criminalité organisée et les organisations para-étatiques voire étatiques. Elles s'inscrivent dans un cadre juridique indéterminé entre le régime normal de la paix et le droit des conflits armés. Cyberattaque, subversion politique, coercition économique, opération de déstabilisation, … . tels en sont les modes d'action privilégiés. L'immensité océanique, la multiplicité et la complexité des réseaux posées ou encore des infrastructures *offshore* constituent autant d'effets multiplicateurs impactant la résilience de sociétés interdépendantes. D'autant plus que ces infrastructures critiques sont véritablement transparentes aux yeux des citoyens peu au fait de ces réalités. Ce rapport distant aux choses de la mer rend souvent inaudible ces enjeux lointains et technologiques. Or, **le contexte géostratégique actuel est caractérisé par un recours décomplexé à la force armée comme outil de règlement des conflits**, la conception d'une guerre totale incluant les infrastructures critiques et les chaines d'approvisionnement ainsi que par la polarisation des acteurs étatiques. Cette guerre des fonds marins (« *seabed warefare* ») est devenue une réalité comme le souligne sans ambages les conclusions du Sommet de l'OTAN des 11-12 juillet 2023. : « *La menace qui pèse sur les infrastructures sous-marines critiques est réelle, et elle s'accroît. Nous sommes déterminés à déceler et à atténuer les vulnérabilités et dépendances stratégiques de nos infrastructures critiques, ainsi qu'à assurer la préparation, la dissuasion et la défense face à l'instrumentalisation de l'énergie et au recours à tout autre procédé hybride par des acteurs étatiques ou non étatiques à des fins coercitives. Toute attaque délibérée contre les infrastructures critiques de pays de l'Alliance se verra opposer une réponse unie et déterminée, et cela vaut aussi pour les infrastructures sous-marines critiques. La protection des infrastructures sous-marines critiques se trouvant sur le territoire des Alliés demeure une prérogative nationale et un engagement collectif [23]. ».*

L'émergence de technologies de rupture duales menace la résilience de nos sociétés interconnectées

Le conflit russo-ukrainien a démocratisé l'emploi des drones non seulement lors des opérations terrestres mais aussi maritimes. Facilement disponible et bon marché, le drone impose une stratégie du faible au fort démultiplié par l'immensité du domaine sous-marin. Il exerce, ainsi, une menace diffuse sur les infrastructures critiques sous-marines et les lignes de communication.

Les drones sous-marins sont des véhicules capables de fonctionner sans être humain à bord voire sans contrôle à distance ou opéré par un humain.

Plusieurs scénarii [24] de perturbation voire d'interruption d'activités humaines en mer peuvent être identifiés par l'emploi de ce moyen :

. **Attaque physique coordonnée de drone (s)** sur les infrastructures critiques et lignes de communication.

L'engin sous-marin effectuerait des poses de mines réelles ou fictives en surface, en sous-marin ou dans les ports. Il pourrait, en outre, véhiculer des charges explosives (notamment des charges nucléaires) ou disséminer des agents chimiques et / ou biologiques. Au vu du faible coût d'acquisition ou de conception, ce cas d'usage pourrait être mis en œuvre par des acteurs para-étatiques ou issus de la criminalité organisée en qualité de sous-traitant au bénéfice d'autres organisations hybrides. Ce scénario est évalué comme probable.

. **Cyber-attaque** ciblant les infrastructures critiques sous-marines, maritimes et portuaires.

Ce mode opératoire complexe chercherait à porter une atteinte à la disponibilité et à l'intégrité de la donnée, notamment, en lien avec les systèmes de sécurité maritime (positionnement géographique des navires, cartographie maritime, communication, etc..). Par ses capacités cybernétiques, il pourrait prendre part à des manœuvres élaborées visant à leurrer ou à dupliquer des communications maritimes et portuaires entre des vecteurs entre eux mais aussi entre des vecteurs et des infrastructures (dispositif de *Command and Control*, sous-stations électriques). Pour accroitre encore les effets sur un théâtre d'opération maritime ou sous-marin, une attaque massive et coordonnée pourrait être envisagée par le recours à un ou des essaim(s) de drones. Furtif par construction, il présente l'avantage d'être difficilement « attribuable » à son commanditaire. Nécessitant encore des développements technologiques important, ce scénario est perçu comme peu probable en 2023.

. **Menace physique portée à la sécurité des routes maritimes [25] et des ports**

Ce mode opératoire conçoit l'emploi des drones télé-opérés comme des sous-marins ou des navires de surface. Dans cette perspective, ces engins pourraient être dotés d'armes de bord conventionnelles, poser des mines sous-marines pré-programmées voire emporteraient des matières fissiles dans un cas très extrême. Quelle que soit la nature des équipements embarqués, un tel cas d'usage avéré exerce par lui-même une très forte menace psychologique à l'égard des gens de mer, qu'ils relèvent de la navigation marchande ou des flottes militaires. Ce scénario est perçu comme probable.

. **Ces technologies évolutives** connaissent actuellement des développements par le recours aux apports de l'Intelligence Artificielle ou encore du *Machine Learning*. Ils posent, néanmoins, de nombreuses questions majeures, notamment en terme d'éthique de la décision ultime. Est-ce que la décision d'emploi de telles armes peut être confiée à des algorithmes ? Cette « démocratisation » d'emploi des drones sous-marins à usage dual interroge aussi sur les perspectives de prolifération vers des acteurs hybrides, voire relevant de la criminalité organisée. Une telle extension d'usage des drones nécessitera, à l'avenir, des mesures de coordination internationale, susceptibles d'impacter les principes du droit maritime international.

Face à ces questions en suspens, ces engins télé-opérés doivent gagner en maturité. En l'état actuel de l'art, les drones connaissent des limitations en termes d'autonomie de navigation et

de liaisons entre le pilote et son véhicule sous-marin, notamment, Internet dont la portée se trouve ralentie en milieu marin.

La mer, pare-feu numérique des infrastructures énergétiques et informationnelles [26] ?

Les infrastructures maritimes constituent, bien souvent, des sites industriels complexes dont le principe de fonctionnement et, partant, l'efficacité reposent sur des connexions internes mais aussi externes établies avec des centres distants de *Command and Control* (C2). Ces interconnexions sont donc consubstantielles à la conception de ces systèmes. En plein développement, elles s'inscrivent graduellement dans le sillage de l'industrie du futur, l'industrie 4.0 [27], qui accélère l'ouverture numérique des ensembles industriels.

Cette menace s'est déjà exprimée récemment au travers un chantage par déni de service avec un opérateur énergétique. Ainsi, en octobre 2015, immergée dans le raz de Sein, l'hydrolienne opérée par l'entreprise finistérienne Sabella est victime d'un rançongiciel [28] infectant l'ordinateur de contrôle de la production. Encore en phase de test, cet incident se traduit, néanmoins, par un arrêt de la production durant 15 jours, privant ainsi l'île voisine d'Ouessant d'électricité. Cet exemple symbolique permet d'envisager l'impact socio-économique sur l'activité humaine en le transposant au cas des îles énergétiques. Ce bilan étant accru par l'insularité.

De plus, les vecteurs maritimes affichent aussi des vulnérabilités susceptibles d'être exploitées par des acteurs hybrides malveillants. La société israélienne a illustré l'acuité de cette menace cybernétique en organisant une cyberattaque visant un navire porte-conteneurs. En décembre 2017 [29], l'équipe d'ingénieurs de Naval Dome est parvenue à prendre le contrôle du ZIM GENOVA à la fois lors d'une escale que lors d'une navigation transatlantique, en compromettant le système de navigation, les radars comme la gestion de la salle des machines. Les effets de cette intrusion numérique opérée à distance démontrent les champs nouveaux d'une action hybride impactant le commerce international et la viabilité des routes maritimes. Au total, l'analyse des risques de la navigation peut se résumer de manière synthétique comme suit :

. usurpation et brouillage des systèmes de positionnement ou de communication ciblant le vecteur ou son environnement,

. dérèglements ou perte de disponibilité des systèmes cartographiques,

. diffusion de fausses informations de sécurité vers le navire,

. intrusion des systèmes industriels à bord,

. chiffrement des systèmes d'information en tout ou partie.

Ce panorama du risque permet d'identifier les modes opératoires hybrides susceptibles d'impacter les activités humaines en mer et, partant, la résilience des sociétés et des États.

Des plates-formes pétrolières sont ancrées au cœur des ZEE comme ici en Irak, au large de Bassorah

Copyright : Louis du Plessix/Diploweb.com

du Plessix/Diploweb.com

III. Le défi de la protection des infrastructures critiques maritimes dans le contexte de guerre haute intensité ou retour en force de la thalassopolitique ?

Le contexte géo-stratégique semble s'orienter durablement sur une polarisation des relations internationales, laissant peu d'espace à une troisième voie. De manière très concrète, cela se traduit par un recours à la force armée comme outil de résolution des conflit et une militarisation multi-champs, multi-domaines. A ce titre, et dans le contexte de maritimisation des économies, **les infrastructures critiques maritimes apparaissent comme des centres de gravité stratégiques qui conditionnent la résilience d'un État ou d'une alliance**. Elles font l'objet d'un regain d'intérêt des États comme en témoigne un foisonnement doctrinal inédit (A). De plus, cette situation nouvelle recentre l'État sur sa mission de protection de ses propres intérêts dans une thalassopolitique renouvelée, miroir de ses ambitions et de ses moyens (B).

A. Un foisonnement inédit de doctrines en lien avec les fonds marins et de développements technologiques

La période actuelle est fertile en multiples réflexions et propose de nombreuses mesures destinées à diminuer le risque d'atteintes aux infrastructures critiques maritimes. Des études et recherches scientifiques préparent des efforts doctrinaires et invitent au développement de technologies de rupture afin de sécuriser ces infrastructures, certes, difficiles d'accès mais, ô combien, vitales.

La Francea rendu public la stratégie ministérielle de maitrise des grands fonds marins [30] en février 2022, combinant une dimension militaire et économique. Cette stratégie se fonde sur un double constat :

. les activités étatiques et économiques se développent dans les fonds marins,

. la protection de nos intérêts stratégiques et la liberté d'action de nos forces pourraient être contestées.

Désireuse de consolider l'autonomie stratégique tout en saisissant les opportunités liées à cet espace de compétition, la France développe une feuille de route dont les éléments principaux sont énoncés ci-après :

. intégrer la maitrise des fonds dans la stratégie de défense au travers des Opérations de Maitrise des Fonds Marins (OMFM) [31],

. définir une gouvernance interministérielle basée sur un groupe de travail multidisciplinaire,

. préparer les capacités de maitrise des fonds marins en cohérence avec les programmes d'armement existants ou prévus [32],

. intégrer cette stratégie au sein d'une dynamique interministérielle portée par la Stratégie nationale d'exploration et d'exploitation des ressources minérales dans les grands fonds marins de 2020 et l'objectif 10 du plan d'investissement « France 2030 ».

Le Royaume-Uni renforce sa flotte hydrographique par la mise en service de deux frégates multi-rôles en janvier 2023 et par des projets d'acquisition de drones sous-marins. Les missions opérationnelles sont axées, principalement, sur la surveillance des infrastructures critiques sous-marines, scellant simultanément un partenariat stratégique avec la Norvège.

Par ailleurs, les États-Unis d'Amérique investissent massivement le champs de la recherche scientifique et du développement de technologies de rupture ou émergentes telles le positionnement géographique ainsi qu'un réseau de senseurs et de capteurs dédiés aux grandes profondeurs associés à une flotte de navires autonomes pilotée à base d'intelligence artificielle.

Les organisations internationales se sont aussi saisies des enjeux des infrastructures critiques.

Avant le sabotage des gazoducs Nord Stream 1 et 2, l'Union européenne s'est emparée de ce sujet au travers d'un rapport publié par le Parlement européen en juin 2022. Il est intitulé « Conséquences pour l'UE des atteintes à la sécurité des câbles de communication et infrastructures sous-marines [33] ». Ce document suggère une meilleure coordination dans la protection et la surveillance des réseaux immergés et le développement de solutions technologiques. En mars 2023, la Stratégie européenne de sûreté maritime [34] est réévaluée à la lumière des dernières attaques en mer Baltique. Des partenariats stratégiques [35] sont alors noués avec l'OTAN en matière de protection d'infrastructures critiques, sans se limiter exclusivement au domaine maritime.

De plus, l'OTAN a renforcé ses missions de surveillance des espaces maritimes de la mer du Nord et de la mer Baltique sans négliger la mer Méditerranée. La coordination générale est confiée au commandement maritime de l'OTAN ou MARCOM [36] basé à Northwood au Royaume-Uni. Un centre dédié à la sécurité des infrastructures critiques sous-marines a été, en outre, intégré à MARCOM à la suite du sommet l'OTAN organisé à Vilnius les 11 et 12 juillet 2023. Des nations alliées prêtent leur concours à l'image du Corps d'auto-défense japonais et de l'Australie qui ont pris part à l'opération de l'OTAN *Sea Guardian* en octobre 2022. De

même, l'OTAN encourage le partenariat public-privé en créant « un réseau rassemblant l'OTAN, les Alliés, le secteur privé et d'autres acteurs concernés qui permettra d'améliorer le partage de l'information et l'échange de bonnes pratiques » [37].

B. Les États recentrés sur la mission organique de protection des intérêts vitaux ?

Les infrastructures critiques maritimes délivrant des services essentiels relatifs aux communications, à l'énergie, à la fourniture de matières premières… relèvent d'acteurs privés qui assument *in fine* une mission de service public et concourent activement à la résilience de l'État et des populations. C'est précisément un point commun majeur qui les relient toutes entre elles. Cette situation singulière oblige l'État à assurer la protection de ces activités essentielles. Car ces dernières garantissent directement la défense de ses propres intérêts.

Cette tendance lourde semble irréversible tant la numérisation croissante de l'économie associée aux exigences de la transition climatique se traduisent par une exploitation accrue des potentialités offertes par les espaces maritimes. Néanmoins, au vue du contexte géo-stratégique actuel qui désigne ces infrastructures critiques comme des objectifs militaires, les projets de création de nouvelles connexions numériques sous-marines ou d'installations *offshore* produisant des énergies marines renouvelables sont susceptibles d'être réévalués. S'inscrivant sur des cycles de conception et de production supérieure à 25 ans, ces projets de grande envergure supposent des investissements conséquents, des autorisations préalables d'acteurs étatiques variés et des défis technologiques. Ainsi, l'exemple du projet Xlinks opéré par des acteurs privés britanniques est illustratif des enjeux. Il s'agit de fournir de l'électricité sûre, fiable et durable à 8 % des foyers britanniques. Conforme aux engagements du gouvernement en matière de développement durable, cette électricité verte sera produite au Maroc [38] à la fois mixant des énergies éoliennes comme solaires. Avant d'être distribuée, elle sera transportée par câbles sous-marins sur plus de 3800 kilomètres à travers l'océan Atlantique.

L'enjeu de protection et de surveillance de ce réseau de transport d'énergie posé connaît une acuité renouvelée depuis la relance le 24 février 2022 du conflit russo-ukrainien. Quels en seront les impacts ? Comment anticiper les évolutions géo-stratégiques dans un projet intercontinental à proximité de *chokepoints* internationaux ? Les investissements particulièrement conséquents sont très régulièrement assumés par des consortiums internationaux à l'image du câble « Amitié ». Celui-ci est constitué de Facebook, Microsoft, Aqua Comms et Vodaphone avec lequel Orange a signé un partenariat.

Carte des réseaux de câbles sous-marins dans l'espace Balte et ses abords
Copyright : TeleGeography (Attribution-ShareAlike 4.0 International (CC BY-SA4.0)

Pour ce faire, les organisations internationales comme les États émettent des normes, des obligations afin de sécuriser ces activités essentielles. Le maritime donne, à ce titre, une illustration concrète des efforts déployés. Véritable clé de voute, le code ISPS (*International Ship and Port Facility Security*) est l'instrument réglementaire en matière de sûreté maritime. Il dispose que « l'évaluation de la sûreté du navire devrait porter sur (…) les systèmes de radio et télécommunications, y compris les systèmes et réseaux informatiques ». Il impose, néanmoins, un plan de sûreté du navire comportant une cartographie logicielle et matérielle du navire, la définition des éléments sensibles et la gestion des vulnérabilités du système. En 2017, l'Organisation Maritime Internationale émet des directives [39] sur la gestion des cyber-risques maritimes dans le sens d'une meilleure protection du transport maritime. Elle impose sous échéance la mise en conformité des systèmes de gestion de la sécurité [40] aux cyber-menaces. Enfin, la directive européenne NIS [41] prévoit la mise en œuvre de mesures destinées à assurer un niveau élevé et commun de sécurité des réseaux et systèmes d'information au sein de l'UE. Transposée en 2018 en droit français, elle identifie comme Opérateur de Services Essentiels les compagnies de transports maritimes et les gestionnaires de ports soumis à des mesures techniques et organisationnelles contre les cyber-risques.

*

En conclusion, matérialisée par le conflit russo-ukrainien et ré-affirmée au Proche-Orient depuis l'attaque par le Hamas d'Israël, la nouvelle donne stratégique a des incidences directes et immédiates sur les politiques de défense des États, contraints d'adapter la protection de leurs intérêts majeurs. La maritimisation des modes de vie conjuguées à la digitalisation des économies et aux objectifs de transition énergétique ont dessiné, notamment, une géopolitique énergétique et numérique qui est questionnée aujourd'hui. En effet, ces dynamiques reposent sur des réalisations industrielles à l'image des câbles sous-marins (énergie, télécommunication), des plates-formes d'extraction de matières premières (hydrocarbures, terres rares…) mais aussi les projets d'envergure des îles énergétiques artificielles. Ces infrastructures critiques sous-marines et maritimes sont devenues des centres de gravité stratégiques qui conditionnent la résilience des États. Transparentes pour l'usager, elles constituent, néanmoins, selon les points de vue, soit des vulnérabilités soit des cibles d'intérêt dans la perspective d'une guerre totale ou guerre d'attrition.

Le sabotage de Nord Stream 1 et 2 a remis en cause l'ordre international existant. Parmi d'autres enseignements, il a placé au centre des débats notre organisation socio-économique et, singulièrement, notre rapport à la mer. En ce sens, **cet acte de sabotage renforce l'État dans sa fonction première de protection de ses intérêts vitaux et de disponibilité des fonctions et services essentiels**. Qui sont en très grande partie tributaires des espaces océaniques. **La thalassopolitique offre ainsi aux observateurs comme aux décideurs une opportunité d'adopter un point de vue fertile pour mieux appréhender la complexité du monde et des relations internationales**.

Copyright Novembre 2023-Manet/Diploweb.com

Plus

Dossier géopolitique : Mers et océans au coeur de la mondialisation

---

P.-S.

L'auteur s'exprime à titre personnel. Colonel de la gendarmerie nationale, expert en sûreté globale, chercheur associé à la Chaire de géopolitique de *Rennes School of Business*. Auteur de Florian Manet, "*Le crime en bleu. Essai de thalassopolitique*", préfaces du général d'armée Richard Lizurey et de l'amiral Christophe Prazuck, ed. Nuvis.

Notes

[1] John Watkins BRETT, à bord du remorqueur GOLIATH, pose le premier câble entre le cap Gris nez, en France, et la cap Southerland au Royaume-Uni. L'émission dura 11 minutes avant que le câble ne se rompt en divers endroits.

[2] La réalisation des batteries de stockage d'énergie réclame du magnésium, du cobalt ou encore du nickel. Ces matières sont présentes dans des enrochements. Ainsi, la zone de Clarion-Clipperton - allant du Mexique à Hawaï- regorgerait de 6 fois plus de cobalt et de trois fois plus de nickel que l'ensemble des réserves connues au monde.

[3] Le gazoduc Franpipe fonctionne depuis 1988. Long de 840 kilomètres, il relie la plate-forme de Draupner dans les eaux territoriales de la Suède au terminal gazier de Dunkerque.

[4] *Thalassocratie criminelle et sécurisation des approvisionnements stratégiques*, Florian MANET, in *Sécurisation des infrastructures vitales*, Mare et Martin, novembre 2020

[5] https://www.lesechos.fr/industrie-services/energie-environnement/en-mer-du-nord-des-iles-energetiques-pour-sauver-la-planete-1948932, consulté le 29/10/23

[6] Le FPSO (*Floating Production Storage and Offloding*) ICHTYS VENTURER est amarré à

250 mètres de profondeur et à plus de 220 kilomètres des côtes, dans la Zone Économique Exclusive australienne.
https://www.offshore-mag.com/field-development/article/16799853/ichthys-lng-fpso-in-place-offshore-australia

[7] Cet acronyme désigne les quatre grandes entreprises du web chinois, à savoir Baidu, Alibaba, Tencent et Xiaomi.

[8] Article 55 et suivants de la CNUDM

[9] Article 56 de la CNUDM

[10] Articles 58 et 112, CNUDM

[11] Voir décision de la Commission des limites du plateau continental, consulté le 23/10/24, 2020_03_04_COM_SUMREC_FRA2.pdf

[12] Cette convention est dédiée à la prévention et à la répression des rejets volontaires en mer par des navires ou des plates-formes offshore, que la cause soit accidentelle ou liée à l'exploitation. Elle a été adoptée en 1973 et enrichie de protocoles additionnels (en 1978 et 1997) ,
https://www.imo.org/fr/about/Conventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-(MARPOL).aspx

[13] Ou *Suppression of Unlawful Acts against the Safety of Navigation* (dite SUA). Elle a été signée le 10 mars 1988 et ratifiée le 1 er mars 1992. Elle fait suite à un acte de terrorisme commis à bord du navire à passagers ACHILLE LAURO 1985 au large d'Alexandrie. Ce navire a été détourné et un passager de nationalité américaine a été tué sur fonds du conflit israélo-palestinien. Elle a été enrichie par le protocole pour la répression d'actes illicites contre la sécurité des plates formes fixes situées sur le plateau continental.

[14] Protecting critical maritime infrastructure – the role of technology, 032 STC 23 E rev.2 fin – 7 octobre 2023

[15] POLÉRE, Pascal « Sûreté maritime : bilan et perspectives du code ISPS », *DMF*, 2006, p.66

[16] Règlement européen n° 725/2004 reprenant le Code ISPS

[17] .https://www.offshore-energy.biz/cargo-ship-strikes-orsteds-gode-wind-1-offshore-wind-farm-suffers-massive-damage_gl=1*7wn26z*_ga*OTA1ODIyMjM5LjE2OTg1ODk0MjY.*_ga_R07LJ1W79Y*MTY5ODU4OTQyOC4xLjAuMTY5ODU4OTQyOC42MC4wLjA

[18] Le 26 décembre 2006, un tremblement de terre de magnitude 7 sur l'échelle de Richter secoue Taïwan. L'épicentre est localisé dans le détroit de Luçon par lequel transitent l'ensemble du réseau de câbles qui relie l'île et une partie de l'Asie du Sud-Est avec le reste

du monde. L'ensemble des communications ont été très perturbés, 50 jours ayant été nécessaires pour rendre opérant cette infrastructure.

[19] En juillet 2017, la Somalie a été isolée du reste du monde après qu'un porte-conteneurs coupe l'*Eastern Africa Submarine System* (EASSy), unique câble du pays. Les pertes quotidiennes ont été évaluées à 9 millions d'euros par jour soit la moitié du PIB journalier de la Somalie.

[20] Ouvert le 11 décembre 2019, le gazoduc BALTICCONNECTOR approvisionne en gaz la Finlande depuis l'Estonie. Il permet à la Finlande d'accéder au stockage de gaz naturel d'Incukalns en Lettonie. Le gazoduc comprend trois tronçons : 22 km sur le sol finlandais, 80 km en mer et 50 km sur le sol estonien. Dans le même temps, un câble de communication a été endommagé entre la Suède et l'Estonie.

[21] Voir https://www.reuters.com/world/europe/finland-retrieves-anchor-seabed-near-broken-gas-pipeline-2023-10-24/, consulté le 23/10/23

[22] Voir *Security Threats to undersea communications cables and infrastructure-conséquences for the EU*, DG for External Policies, juin 2022,

[23] Communiqué du sommet de l'OTAN de VILNIUS, https://www.nato.int/cps/fr/natohq/official_texts_217320.htm, consulté le 26/10/23.

[24] Voir Australia's Trade and the Threat of Autonomous Uncrewed Underwater Vehicles, RMIT University, disponible https://www.rmit.edu.au/research/centres-collaborations/cyber-security-research-innovation/autonomous-uncrewed-underwater-vehicles, consulté le 26/10/2023

[25] Pourraient être visé en priorité les chokepoint. L'agence américaine pour l'énergie (EIA) définit ainsi le *chokepoint* : « *narrow channels along widely used global sea routes* ». Voir MANET, Florian, 17/09/21,https://www.diploweb.com/Pourquoi-le-detroit-d-Ormuz-est-il-un-symbole-des-enjeux-contemporains-de-la-maritimisation-de-nos.html

[26] *La marétique, un enjeu essentiel pour l'humanité ?* Florian MANET, in Cybercercle Collection, décembre 2020

[27] *Industrie 4.0, cheval de Troie de la cybersécurité intégrée au sein de l'aéronautique ? Une opportunité historique à saisir*, Florian MANET, in Cybercercle Collection, juillet 2022

[28] Technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement. https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/rancongiciel/

[29] Consultation du site de Naval Dome, http:// navaldome.com/

[30] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi2vaH_mZOCAxUrT6QEHfhjAnYQFnoECBkQAQ&url=https%253A%252F%252Fwww.defense.gouv.fr%252Fsites%252Fdefault%252Ffiles%252Fministere-armees%252F20220210_LANCEMENT%2525, consulté le 26/10/23

[31] Ces OMFM se définissent comme « l'ensemble des opérations conduites vers, depuis et sur les fonds marins et associant des systèmes pouvant opérer de manière autonome ou en réseau. Le spectre des OMFM s'étend des opérations hydro-océanograhiques à des opérations d'intervention et d'action sous la mer, en passant par des missions de surveillance.

[32] Comme les Capacités hydrographique et océaniques du Futur (CHOF), Système de Lutte Anti-mines du Futur (SLAMF) ou encore les premiers drones (AUV) et robots (ROV) pouvant opérer jusqu'à 6 000 mètres.

[33] BUEGER, Christian, LIEBTRAU, Tobias et FRANKEN, Jonas, http://europarl.europa.eu/Regdata/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

[34] http://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/maritime-security-strategy_en

[35] Une Task Force UE – OTAN dédiée à la résilience des infrastructures critiques est créée le 16 mars 2023.

[36] http://mc.nato.int/media-centre/news/2023/nato-maritime-assets-play-key-role-in-offshore-critical-infrastructure-security

[37] Communiqué du sommet de l'OTAN de VILNIUS, https://www.nato.int/cps/fr/natohq/official_texts_217320.htm, consulté le 26/10/23

[38] Les installations seront localisées dans la région de Guelmin Oued Noun au Maroc. La connexion au réseau britannique est envisagée dans le Devon à Alverdiscott. La production théorique est évaluée à 10,5 gigawatts dont 7 GW proviendraient de l'énergie solaire et 3,5 GW de l'énergie éolienne. Le Maroc apporte une prévisibilité et une constance dans la production d'énergie, contrairement à l'éolien britannique, instable et irrégulier. La première phase du projet sera opérationnelle en 2029, la deuxième phase étant prévue en 2031.

[39] MSC – FAL 1/Circ.3

[40] http://www.imo.org/fr/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC%2098-23-Add.1.pdf

[41] Ou *Network and Information System Security* n° 2016/ 1148