ANNUAIRE FRANÇAIS DE RELATIONS INTERNATIONALES

2019

Volume XX

PUBLICATION COURONNÉE PAR

L'ACADÉMIE DES SCIENCES MORALES ET POLITIQUES

(Prix de la Fondation Edouard Bonnefous, 2008)

Université Panthéon-Assas
Centre Thucydide

LA CYBERSÉCURITÉ EN MER

UN DÉFI INTERNATIONAL AU CONFLUENT DE DEUX ESPACES COMMUNS

PAR

HÉLÈNE TERROM (*)

Penser la cybersécurité dans l'espace maritime revient à envisager la vulnérabilité des flux de communication dans deux « *espaces communs* » (1), semblables (2) et complémentaires (3). La qualification même de cybersécurité prédispose l'analyste à une vision occidentale fondée sur la liberté de l'espace, opposée à une vision portée par la Chine et la Russie dans les cercles internationaux reposant sur l'affirmation souveraine des Etats. L'étymologie même du mot « cyber » – gouvernail – invite à la liberté des grandes traversées maritimes. Depuis les premières cyberattaques en mer touchant aussi bien des navires, des compagnies, des ports ou des infrastructures, les opérateurs maritimes ont tardé à intégrer la menace dans un secteur particulièrement vulnérable, puisque très informatisé. De surcroît, l'explosion des échanges et la constitution d'un monde en réseaux à partir de la seconde moitié du XX^{e} siècle ont fortement exposé le secteur maritime aux menaces sur les flux, décuplant ainsi le risque en parallèle de sa probabilité d'occurrence.

Dans le même temps, l'interconnexion Internet a entraîné une course à l'information et l'espérance, portée par le changement d'ère technique – perçu comme « *facteur décisif* » (4) de la nouvelle géopolitique mondiale –, de rapprocher les peuples. Ce bouleversement s'est traduit dans le discours politique des Etats qui ont cherché à réagir en accompagnant cette

(*) Maître de conférences à l'Université catholique de l'Ouest (France).

(1) Le terme « espaces communs » désigne les espaces – par opposition aux territoires – qui se situent hors emprise de la souveraineté d'un Etat.

(2) Certains auteurs discernent même des analogies entre emploi de la force informatique et guerre navale. Ainsi, les offensives informatiques sur des capacités adverses de cyber défense ou les actions défensive en matière cyber correspondraient aux manœuvres de la guerre d'escadre ; l'appui de la force informatique aux actions militaires physiques s'apparenterait à la guerre de côte ; enfin, l'action numérique des Etats éventuellement sous-traitée à des groupes criminels évoquerait la guerre de course. *Cf.* Arnaud SUDRES, « Cyberespace et dimension stratégique de la force informatique », *Stratégiques*, 2017/4, n°117, pp. 65-82.

(3) Arnaud COUSTILLIÈRE, « Le combat numérique au cœur des opérations : quels enjeux pour le monde maritime ? », *Revue Défense Nationale*, n°789, avr. 2016, pp. 44-48.

(4) Philippe MOREAU-DEFARGES, « Mondialisation économique et mondialisation politique depuis 1945 », *Relations internationales*, 2005/4, n°124, pp. 41-51.

« *transformation stratégique* » (5). Ces « *autoroutes de l'information* » (6) représentant alors « *les moyens techniques et économiques de rassembler toutes les communautés du monde* » (7), d'un monde maritimisé.

Dans ce contexte, cyberespace et espace maritime présentent de nombreuses similitudes. Les débats internationaux voudraient imposer dans ces espaces communs la vision d'une communauté internationale accomplie. Pourtant, les Etats s'y affrontent, fondant leurs actions stratégiques dans le cinquième milieu (8) sur des conceptions géopolitiques et juridiques distinctes, issues de leurs propres stratégies maritimes. A la liberté occidentale entraînant une domination américaine sur les échanges de flux dans les espaces maritimes et cyber, répond une affirmation de souveraineté de la part d'Etats continentaux qui se sécurisent en s'appropriant les ressources numériques indispensables au développement de l'industrie cybernétique. A ces oppositions conceptuelles entre Etats s'ajoute une difficulté supplémentaire : celle de l'intégration au schéma d'acteurs non étatiques, intégration facilitée par la dissimulation offerte par le cybermilieu et la difficulté subséquente d'identifier les auteurs de la cyberattaque. Les Etats y apportent des réponses tactiques – les nouveaux programmes de navires ou de ports autonomes en sont un exemple –, stratégiques et juridiques. Toutes ces réponses échouent à universaliser la lutte. Les visions géopolitiques trop éloignées annihilent en effet l'idée d'une communauté internationale prête à s'entendre dans les espaces communs. La cybercriminalité maritime représente donc une nouvelle donne géostratégique à prendre en compte dans les relations internationales, à laquelle les Etats cherchent à répondre tactiquement, stratégiquement et juridiquement par le développement d'une cybersécurité maritime dont le volet international reste embryonnaire.

La cybermenace en mer : une nouvelle donne géopolitique

Le cyber risque en mer est dorénavant une menace. Cette dernière traduit, par sa nouveauté et son utilisation stratégique, une continuité marquée de la géopolitique des espaces communs.

Caractère critique de la cybermenace maritime

On différencie généralement les cyberattaques selon trois objectifs distincts : l'espionnage, le déni d'accès et la destruction. Leur probabilité d'occurrence et la gravité de leurs répercussions éventuelles permettent

(5) Olivier Kempf, « Des différences entre la cybersécurité et la transformation digitale », *Stratégique,* 2017/4, n°117, pp. 59-64.

(6) Al Gore, Discours sur la National Information Infrastructure, 1991.

(7) Union internationale des télécommunications (1994).

(8) Livre blanc sur la défense et la sécurité nationale, DILA, 2013, 160 p.

de dégager le caractère critique de la cybermenace pesant sur le secteur maritime.

Probabilité d'occurrence d'une cyberattaque maritime

On ne peut plus sous-estimer la menace cybernétique en mer. Depuis 2011, aucune cible maritime n'a été épargnée (ports, navires, compagnies maritimes, infrastructures) par des Etats ou des acteurs non étatiques.

Le port d'Anvers, en 2011, est la cible de la première cyberattaque maritime médiatisée. Un cartel de drogue s'introduit dans le réseau informatique afin de dissimuler le trafic de conteneurs chargés de substances psychotropes. La même année, au large de la Somalie, des pirates s'emparent du pétrolier *Enrico Levolli* après l'avoir ciblé *via* son AIS (9). Ces deux premières attaques traduisent l'utilisation, par des groupes criminels, de l'outil cybernétique comme simple moyen au service d'une action illicite classique et caractérisée. A partir de 2013, on note pourtant une évolution majeure : l'emploi, par des acteurs non étatiques, d'une nouvelle criminalité, essentiellement informatique, le rançongiciel (*ransomware*) (10). A cette date, le groupe Moller-Maerks est atteint par le virus NotPetya, dont les conséquences s'étendent aux ports de New York (Etats-Unis), Rotterdam (Pays-Bas) et Jawaharlal Nehru (Inde). En 2017, la compagnie iranienne IRISL est victime d'une attaque effaçant l'ensemble des données sur les cargos qu'elle gère. L'année suivante, c'est au tour des autorités portuaires de Barcelone (Espagne) et de San Diego (Etats-Unis) de faire état d'une attaque sur leurs systèmes informatiques par un *ransomware* déjà détecté au port de Longbeach (Californie), puis dans le terminal portuaire de la China Ocean Shipping Company. Cette deuxième série d'attaques marque un palier dans la menace : les opérateurs maritimes deviennent des cibles à part entière de la criminalité numérique. D'autres attaques dispersées doivent tout autant alerter : une plate-forme pétrolière au large de l'Afrique ou une hydrolienne immergée au large d'Ouessant ont ainsi été victimes de cyber-intrusions. On assiste inexorablement à une montée en puissance de la menace cybernétique en mer et à une autonomisation de son outil qui rend plausible l'hypothèse d'une mutation de la menace et de ses auteurs dans l'espace maritime.

La déviation de l'outil numérique maritime n'est pourtant ni toujours le fait de criminels, ni même, *a priori*, celui d'acteurs non étatiques. Il peut toutefois servir, dans tous les cas, à détourner le droit international et les rapports de confiance internationaux. En 2013, un pétrolier en provenance du Pakistan a modifié volontairement son AIS afin de contourner l'embargo américain envers l'Iran en se faisant passer pour un chimiquier. De plus, l'internationalisation des marchés fragilise les Etats délocalisant leurs industries navales. Ainsi, le Sénat américain a accusé la Chine d'avoir

(9) Système d'identification automatique informatisé des navires.

(10) Il s'agit d'un logiciel malveillant infectant l'ordinateur et prenant en otage des données contre rançon.

compromis de multiples systèmes à bord d'un navire commercial assurant des liaisons logistiques au profit du commandement militaire américain des transports (11). Les Etats inscrivent également leur stratégie cybernétique dans une vision plus vaste, en soutien d'un jeu de puissances plus classique entre appropriation et domination.

Le secteur maritime fait ainsi l'objet, en termes de cybermenace, d'une pression avérée. Cependant, se contenter d'illustrer les menaces pesant sur le secteur maritime conventionnel ne rendrait pas compte de l'ensemble des enjeux de cybersécurité en mer. Les fonds marins accueillent en effet une part considérable de la couche physique (12) du cyberespace puisque 99% des transmissions numériques transitent par des câbles immergés. Ces derniers ont fait l'objet d'une série d'accidents à partir de l'an 2000 : un câble rompu à Singapour a entraîné la réduction à 30% des capacités de l'Internet australien durant quelques heures ; l'Algérie et la Somalie ont connu les mêmes désagréments en 2015 et 2017. Ces accidents ont poussé les autorités à communiquer aux opérateurs maritimes la carte du maillage câblier, précaution sécuritaire certes, mais qui entre en opposition directe avec les mesures minimales de sûreté qui devraient garantir la sécurité du réseau. D'autant qu'un navire câblier a déjà été pris pour cible en 2016 par des pirates somaliens.

Toutes ces attaques sont autant de signaux sporadiques qu'il faut relever afin de protéger un secteur maritime particulièrement stratégique dès lors qu'il représente le poumon de l'économie mondiale.

Gravité d'une cyberattaque dans le secteur maritime

60% de la population mondiale vit à moins de 150 kilomètres des côtes, plus de 90% des biens en volume transitent par la mer et la part du secteur maritime dans l'économie mondiale, qui représente aujourd'hui 1 500 milliards de dollars, est appelée à doubler d'ici 2030 selon les projections actuelles. Ces données suffisent à comprendre en quoi les ports sont qualifiés de poumons des *hinterlands* et pourquoi l'économie maritime est à ce point concurrentielle. La compétitivité du secteur peut partiellement expliquer la prise de conscience tardive de la gravité de la cybermenace en mer : afin de s'assurer une publicité positive, les opérateurs maritimes n'ont pas toujours déclaré les cyberattaques dont ils étaient l'objet, d'autant plus, qu'en France, les assureurs les excluent des risques couverts (13).

(11) *Inquiry into cyber intrusions affecting U.S. transportation command contractors*, Report of the Committee on Armed Services United States Senate, 2014, 34 p.

(12) Le cyberespace est communément partagé en trois couches : la couche physique (équipements physiques associés à une localisation géographique), la couche logique (applications et logiciels pour gérer les données) et la couche sémantique (structures sociales et politiques induites par les informations du réseau). Ces trois couches peuvent être réduites à deux : milieux informatique et informationnel. *Cf.* Arnaud Sudres, *op. cit.*

(13) Le coût financier de la cybercriminalité a pourtant été estimé en 2008 à 1 000 milliards de dollars, soit 1,64% du produit intérieur brut (PIB) mondial. Oriane Barat-Ginies, « Existe-t-il un droit international du cyberespace ? », *Hérodote*, 2014/1, n°152-153, pp. 201-220. Des réflexions sont en cours pour pallier la non-prise en compte par les assureurs en faisant notamment appel à la Caisse centrale de réassurance.

De surcroît, le secteur maritime, déjà très fortement informatisé, risque d'être confronté dans l'avenir à une amplification de sa vulnérabilité. La Convention SOLAS dont l'objet est de garantir la sécurité maritime impose en effet aux opérateurs maritimes la navigation électronique, mais l'expose ainsi davantage aux menaces humaines. Tous les navires ou infrastructures qui ne seraient pas protégés par des programmes de sécurité des systèmes d'informations (SSI) de haut niveau deviendraient des cibles faciles. On pourrait alors aisément brouiller leur AIS, leur transmettre de fausses informations ou encore des virus informatiques. Le développement de projets comme ceux des navires autonomes ou d'automatisation totale de gestion de certains parcs à conteneurs va encore augmenter le nombre de cibles potentielles (14) d'une cyberattaque sur la diversité desquelles alertent les organismes internationaux (15).

Ce renforcement des causes de vulnérabilité du secteur maritime risque d'entraîner un changement de perspective d'un droit de la mer fondé jusqu'à présent sur la liberté de navigation. En mettant en lumière la cybermenace sur les opérateurs maritimes et donc en cherchant des solutions efficientes, on risque de remettre en cause la liberté de la navigation maritime au profit d'une conception plus restrictive issue d'une projection, sur les espaces maritimes, de la souveraineté territoriale des Etats.

Complémentarité géostratégique : espaces communs et flux internationaux

Le cyberespace, virtuel, n'existe pourtant pas sans l'homme ni sa géographie. La géopolitique a façonné les rapports de forces internationaux et les lectures étatiques du monde ; elle ne saurait être étrangère à l'analyse des positions étatiques dans les espaces communs. De surcroît, l'industrie cybernétique repose sur des ressources physiques, situées sur des fonds marins stratégiques, dont découle une nouvelle course à l'or numérique.

Contrôle des communications et déni d'accès

La similitude des espaces maritime et cyber autorise à invoquer la réflexion géostratégique maritime pour éclairer les défis à venir. La puissance maritime a toujours été pensée comme allant de pair avec la maîtrise des communications (16), reconnaissant de fait une bipolarité dans la stratégie entre forces organisées et guerre de communications (17)

(14) Pour une approche synthétique, *cf.* Camille Valero / Paul Tourret, « 20 ans d'apports des technologies aux industries maritimes », Note de synthèse ISEMAR, n°191, juin 2017, disponible à l'adresse www.isemar.fr/wp-content/uploads/2017/06/note-de-synthèse-isemar-191.pdf.

(15) Organisation maritime internationale, MSC 96/4/2, 9 fév. 2016, Rapport présenté par le Canada, les Etats-Unis, les Iles Marshall, le Japon, le Liberia, le Norvège : il cible sept menaces (terrorisme ; criminalité organisée ; hacktivismes ; travailleurs en place mal intentionnés ; ou innocents ; clients, concurrents, partenaires ; défaillances techniques). ENISA (Agence européenne de cybersécurité), *ENISA Threat Landscape 2015*, Rapport sur les principales menaces.

(16) Sir Julian Stafford Corbett, Anglais, 1854-1922, *Some Principles of Maritime Strategy*, 1911.

(17) Amiral Raoul Castex, Français, 1878-1968, *Théories stratégiques*, 1929-1935.

pour déboucher sur la distinction entre maîtrise des mers (*sea control*) et interdiction des mers (*sea denial* (18))(19). La Convention des Nations Unies sur le droit de la mer (CNUDM) ne s'y est pas trompée lorsqu'elle souligne l'importance de mettre en place « *un ordre juridique sur les mers et les océans qui facilite les communications internationales* ». Si l'hégémonie dans l'espace maritime s'accompagne de la domination sur les flux et les communications, alors, Internet, en tant que « *nouvelle dimension transnationale d'échange* », apparaît comme « *la troisième expression historique de la puissance maritime et marchande anglo-saxonne* » (20). La confrontation actuelle entre les Etats en matière cybernétique peut donc être décryptée grâce aux enseignements maritimes et à la lumière d'une dialectique partageant les tenants de la liberté des espaces communs et ceux prônant leur captation souveraine.

Les Etats occidentaux, menés par les Etats-Unis, font de la liberté des communications et de l'accès au cyberespace le fondement du nouveau régime juridique de celui-ci. Cette liberté est pour autant contrainte, pour les autres Etats, par la domination américaine en la matière. Si 97% des flux transitent par le territoire américain, la gestion de la majeure partie des infrastructures est laissée aux acteurs privés anglo-saxons, à l'image de l'ICANN, société de droit privé californien en charge de la gestion des noms de domaines et donc de l'accès effectif au réseau. Malgré son affichage de neutralité (21) et sa tendance à la mondialisation, elle a déjà décidé de suspendre, en 2003, l'enregistrement de sites iraquiens et afghans (22) et inquiète, symboliquement (23), les opinions internationales. Dans cette configuration, les Etats eux-mêmes deviennent fébriles face à une vulnérabilité qu'ils pressentent chaque jour plus sérieuse, doublée d'une inquiétude liée à la territorialisation des espaces cyber et maritime.

Une autre vision se dessine nettement sur les traces ravivées du *Heartland* cher à Halford Mackinder. La Russie – cœur du monde – et la Chine – puissance technique – pourraient dominer le monde, voire, dans l'enjeu actuel, le cybermonde. Les deux Etats proposent en effet une perspective différente, fondée sur le concept de souveraineté informationnelle, à laquelle répondent les tentatives d'appropriation ou de déni d'accès dans leurs sphères d'influences maritimes. C'est ainsi que la

(18) Bernard Brodie, Américain, 1910-1978, *Sea Power in the Machine Age*, 1941, et *A Guide to Naval Strategy*, 1942.

(19) Hervé Coutau-Bégarie, « Les lignes directrices de la pensée navale au XX^e^ siècle », *Guerres mondiales et conflits contemporains,* 2004/1, n°213, pp .3-10.

(20) Pierre Bellanger, « De la souveraineté numérique », *Le Débat,* 2012/3, n°170, pp. 149-159.

(21) La Commission fédérale des communications (FCC) américaine a voté en juin 2018 la fin de la neutralité du Net qui garantissait un accès égal au réseau quels que soient l'utilisateur et le service auquel il se connecte.

(22) Elle a ainsi décidé de suspendre l'enregistrement des sites iraquiens et afghans en 2003. Emmanuel Meneut, « Le rêve chinois de la puissance est un défi global pour la sécurité internationale : le cas de la cybersécurité », *Monde chinois,* 2015/1, n°41, pp. 44-55.

(23) Bertrand de La Chapelle, « Souveraineté et juridiction dans le cyberespace », *Hérodote*, 2014/1, n°152-153, pp. 174-184.

Russie, détentrice du segment russophone de l'Internet *Runet* et deuxième langue sur le réseau, a développé un modèle économique d'exploitation des matières premières en Sibérie, couplé à un système de traitement et de conservation des données dont elle fait bénéficier la Chine, jusqu'à devenir un « *nouveau territoire stratégique du cyberespace* » (24) échappant au contrôle américain. De la même façon, sa politique maritime est orientée vers ce grand dessein de recouvrement de puissance par la recherche de contrôle sur son étranger proche, l'arme cybernétique devenant un moyen d'y parvenir. Perpétuellement à la recherche de l'accès aux mers chaudes, elle impose dans la région baltique une pression tant navale que cyber, en y déployant des « *systèmes* [de déni d'accès] *très sophistiqués* » (25) » et fait du port de Tartous, en Syrie, un élément fondamental de sa politique d'accès aux deux espaces communs. Ce « *Port Potemkine* » (26), ouvert sur la Méditerranée et lieu d'atterrissement de trois câbles sous-marins, est une pièce stratégique pour le contrôle de la connexion Internet incluant la surveillance de la Syrie et des Etats limitrophes, tout en ancrant la volonté de Moscou de réinvestir la haute mer comme le prouve son programme d'armement 2011-2020 (27).

Dans le même temps, la Chine démontre, sans ambiguïté, une stratégie de territorialisation des espaces maritime et cyber. Adepte de la souveraineté informationnelle, cette « *île géopolitique* » (28) de plus de 772 millions d'internautes (29) cherche à sortir de son enclavement tout en affirmant sa souveraineté sur son étranger proche. Le projet des « nouvelles routes de la soie » (30) vise à lui permettre d'étendre son influence dans ces deux espaces par une démarche parallèle et complémentaire, parmi d'autres visées stratégiques. Il s'agit pour Pékin, de renforcer ses capacités maritimes (infrastructures portuaires et pérennisation d'une marine hauturière) tout en promouvant le développement des infrastructures cyber. La souveraineté informationnelle chinoise s'accompagne aussi d'une tentative de territorialisation des espaces maritimes en mer de Chine méridionale et d'une campagne de déni d'accès ayant entraîné des affrontements épars dans les espaces aérien (2001), maritime (2009) et cyber (2010) entre Américains et Chinois.

(24) Frédérick Douzet *et al.*, « Les nouveaux territoires stratégiques du cyberespace : le cas de la Russie », *Stratégique,* 2017/4, n°117, pp. 169-186.

(25) Leçon inaugurale de la chaire « Grands enjeux stratégiques » donnée par le ministre de la Défense à l'université Panthéon-Sorbonne le 18 janvier 2016, citée par Académie de Marine, « Forces pré-positionnées et positionnement dynamique. Eclairages complémentaires au rapport d'études de 2014 », *Rapport d'études CEMM*, n°3, 2016, 10 p.

(26) Igor Delanoë, « Le partenariat stratégique russo-syrien : la clef du dispositif naval russe en Méditerranée », Fondation pour la recherche stratégique, Note n°06/13, 9 p.

(27) *Id*.

(28) Hugues Eudeline, « La nouvelle puissance maritime de la Chine et ses conséquences », *Stratégique*, 2015/2, n°109, pp. 169-196.

(29) Ce qui correspond à plus que la moitié de la population européenne.

(30) Alice Ekman (dir.), *La France face aux nouvelles routes de la soie*, Institut français de relations internationales, oct. 2018, 149 p.

Une troisième voie a été envisagée par l'Inde, le Brésil ou l'Afrique du Sud qui, par la Déclaration de Brasilia en 2003 (31), ont appelé de leurs vœux l'instauration d'un régime de collaboration au sein de la « société de l'information », afin de contrer l'hégémonie américaine sans pour autant l'affronter frontalement. On assiste donc encore plutôt à une confrontation entre puissances « maritimes » partisanes d'une liberté qui favorise la domination américaine sur le monde contre des puissances « continentales » qui cherchent à garantir leur souveraineté sur des espaces fluides par l'appropriation des ressources ou des données.

Géopolitique physique : les « profondeurs stratégiques »

Si le cyberespace est caractérisé par sa virtualité, il possède aussi une dimension physique que les Etats, voire les acteurs privés, ont la nécessité de protéger : câbles sous-marins et métaux rares font ainsi l'objet d'une nouvelle ruée vers l'or numérique.

Géopolitique des câbles sous-marins

Les fonds marins sont maillés de plus de 430 câbles sous-marins à fibre optique, qui représentent dans leur ensemble plusieurs milliers de kilomètres de circuit et assurent plus de 99% de la connectivité internationale. Malgré le caractère parfois anarchique des poses dû à la libéralisation du marché dans les années 1990, ces nouvelles routes suivent, tout en les prolongeant au gré des échanges internationaux, les anciennes routes du cuivre. Ainsi, trois routes principales (Europe–Etats-Unis ; Europe–Extrême-Orient ; Etats-Unis–Asie) alimentent les échanges numériques principaux et sont complétées par d'autres routes secondaires (Europe–Afrique ; Etats-Unis–Amérique du Sud) sans pour autant atténuer la domination américaine. Afin de s'en prémunir, les BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud) ont lancé un projet de câbles destinés à contourner les Etats-Unis et le Royaume-Uni (32). La Chine a confirmé, dans ce domaine, sa politique volontariste par le projet PEACE (33) qui lui offrira une voie d'accès à l'Afrique et à l'Europe, indépendante de l'Inde. Ces nouvelles routes matérialisées sous les mers sont des cibles potentielles : elles sont concentrées dans des espaces resserrés (Malacca, Luçon, Suez) et les stations d'atterrissement sont des infrastructures reconnaissables. En outre, on assiste à un net positionnement des groupes privés (Google, Apple, Facebook, Amazon, Microsoft) sur le marché alors que le droit de la mer laisse aux Etats la responsabilité de lutter contre les menaces et leurs conséquences. La France bénéficie d'atouts dans ces « *routes du fond*

(31) Hannes Ebert / Tim Maurer, « Revendications sur le cyberespace et puissances émergentes », *Hérodote*, 2014/1, n°152-153, pp. 276-295.

(32) Jean-Luc Vuillemin / Raynald Leconte, « Liberté, communication et câbles sous-marins », *Etudes marines*, n°14, juin 2018, pp. 36-43.

(33) Pakistan East Africa Cable Express.

des mers » (34). La société française Submarine Networks Solution détient 47% du marché des systèmes de transmission sous-marins et le quart de la flotte câblière mondiale (35). Elle est à la recherche d'un repreneur et, à l'heure où ces lignes sont écrites, une solution franco-française serait envisagée sous le regard bienveillant du ministère de l'Economie.

Géopolitique des terres rares

La révolution numérique passe par l'exploitation des métaux rares, dont une partie des réserves se situe en mer. Aujourd'hui, la Chine a organisé un vaste système d'exploitation et de sécurisation des approvisionnements miniers afin de se positionner comme *leader* dans le secteur des nouvelles technologies. Pourtant, la France, deuxième espace maritime au monde avec 11 millions de kilomètres carrés sous juridiction, « *géant minier en sommeil* » (36), pourrait un jour se réveiller. Les campagnes d'extension raisonnée des plateaux continentaux dans le cadre du programme EXTRAPLAC comme d'autres programmes d'exploitation coréen, russe, japonais, indien, brésilien (37) visent à l'appropriation des ressources stratégiques alors même que Pékin s'étend en mer de Chine méridionale et se dote de capacités navales importantes (38). La création en France en 2011 du Comité pour les métaux stratégiques (COMES) est d'ailleurs le fait d'une réaction stratégique au « *premier embargo de la transition énergétique et numérique* » (39). Une dispute territoriale entre la Chine et le Japon relative à la souveraineté des îles Senkaku en mer de Chine orientale avait en effet poussé la Chine à rompre ses approvisionnements en métaux stratégiques, faisant alors prendre conscience aux Etats de leur vulnérabilité. Car assurer la cybersécurité maritime, c'est aussi sécuriser le cyberespace par l'action de l'Etat dans son espace maritime.

La menace cybernétique en mer représente ainsi une nouvelle donne géopolitique puisqu'elle allie transformation de la nature de la menace en mer et nouvelle grille de lecture des rapports internationaux. Il reste toutefois possible de prendre appui sur la stratégie maritime pour penser les défis du cyberespace et les problématiques propres à ce milieu virtuel pourront ainsi être éclairées par la doctrine maritimiste.

(34) Florence Smits / Tristan Lecoq, « Les routes du fond des mers : la colonne vertébrale de la mondialisation », *Annuaire français de relations internationales*, vol. XVIII, 2017, pp. 671-686.

(35) Raynald Leconte, « Les nouveaux flux : les câbles sous-marins transocéaniques », communication au Colloque « Les réseaux maritimes de l'économie mondiale », Centre d'études stratégiques de la Marine, 30 mars 2012.

(36) « La guerre des métaux rares » – 3 questions à Guillaume Pitron, Institut de relations internationales et stratégiques, 26 juil. 2018.

(37) Pierre Cochonat, « Les ressources minérales et énergétiques sont-elles dans les grands fonds ? », communication au Colloque « Planète mer : un océan de richesses », Centre d'études stratégiques de la Marine, 26 janv. 2012.

(38) La Chine a ainsi lancé un programme de sous-marins pouvant atteindre 6 000 mètres de profondeur.

(39) Guillaume Pitron, *La Guerre des métaux rares. La face cachée de la transition énergétique et numérique* (préface d'Hubert Védrine), 2018, 295 p.

Face à une donne géopolitique profondément modifiée par l'apparition d'un espace virtuel, les schémas stratégiques doivent être repensés afin de protéger les populations et les territoires d'une menace diffuse mais néanmoins prégnante. La France a pris conscience de ces enjeux et décline une stratégie fondée sur l'anticipation stratégique qu'elle a tout intérêt à conforter dans la construction juridique internationale.

Bouleversements et anticipations stratégiques françaises

Les opérateurs maritimes contribuent à mener une réflexion à différents niveaux afin de garantir, à terme, l'autonomie stratégique du secteur maritime. L'Etat a quant à lui déjà mis en place des mesures de protection *via* la qualification de secteur d'activité d'importance vitale.

Vers l'autonomie stratégique ?

Des réflexions stratégiques sont menées en France – et dans le cadre européen – afin de protéger le secteur maritime d'une cyberattaque en adaptant parfois des concepts déjà existants. Des centres de recherches sont créés à l'image de la chaire cyber de l'Ecole navale consacrée à la marétique (40) et des projets ont vu le jour comme le programme DéAIS qui, en partenariat avec l'Université de La Rochelle, est centré sur la détection des signaux falsifiés (2014-2018). D'autres recherches se concentrent sur les besoins en matière de navires du futur, qu'ils soient autonomes ou conduits de terre (CDT). Ce dernier, en supprimant les équipages en mer, pourrait épargner au navire les attaques en *ransomware*, voire rendre inutile le recours à des gardes privés. Il faudrait toutefois faire du central de navigation une infrastructure critique (41).

En outre, des perspectives stratégiques sont ouvertes. Ainsi, la notion de « cyber flotte maritime stratégique » a émergé pour désigner une flotte à fort niveau d'exigence en matière de cybersécurité, permettant d'assurer les approvisionnements stratégiques. Un réexamen des catégories des navires stratégiques est déjà lancé par une commission tripartite, sous l'égide du Conseil supérieur de la marine marchande. On commence également à prendre conscience de la nécessité qu'il y a à envisager la production nationale de matériels et à les certifier afin de lutter contre des éléments potentiellement corrompus (42) afin de combler un retard majeur et d'éviter de se retrouver dans la situation américaine face à l'industrie

(40) Définie comme « *l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'automatisation des opérations relatives aux activités maritimes fluviales et portuaires* [reposant] *à 80% sur la technologie sans fil* » par Gersende Le Dimna, « Le navire objet d'une attaque cybernétique, étude du risque juridique », *in* Patrick Chaumette, *Economic Challenge and New Maritime Risks Management: What Blue Growth?*, GOMILEX, 2017, 480 p.

(41) Bernard Dujardin, « Le principe des organisations à haute fiabilité et sûreté appliqué au navire de commerce du futur conduit de terre », *in* Patrick Chaumette, *op. cit.*

(42) Jérôme de Lespinois, « Guerre et paix dans le cyberespace », *Stratégique,* 2017/4, n°117, pp. 155-168.

chinoise. Une telle démarche faciliterait évidemment les capacités de résilience de la flotte nationale. Dans cette optique, des actions concrètes visent à garantir une protection optimale des matériels. Ainsi, le second arrêt technique majeur du *Charles-de-Gaulle* achevé à l'automne 2018 lui a permis de renforcer ses capacités de défense en matière cybernétique.

De plus, la France s'est dotée d'un commandement cyber dont la déclinaison maritime est placée sous l'autorité d'un amiral – Alcyber – et d'un centre support à la cyberdéfense dont les plateformes d'entraînement sont basées à Toulon et Brest. L'Etat a également introduit, depuis 2011, la menace cybernétique dans les stratégies nationales de défense et de sécurité, à l'image de ses partenaires européens. Il l'a décliné sur différents supports jusqu'à aboutir à la rédaction de la Stratégie nationale de la cyberdéfense en juillet 2018.

Mesures réglementaires : les secteurs d'activités d'importance vitale

La gravité des conséquences éventuelles d'une attaque sur des infrastructures de transport (zone portuaire) ou de télécommunication (câbles sous-marins) permet de les qualifier de secteur d'activité d'importance vitale (SAIV) et de leur apporter un régime de protection renforcée et un cadre plus exigeant en matière de cybersécurité (43). Ces infrastructures sont en effet indispensables à la satisfaction des besoins essentiels de la nation et difficilement substituables ou remplaçables. En revanche, les navires, mobiles par nature, ne sont pas intégrés aux dispositions françaises. Le secteur maritime français est soumis aux recommandations générales de l'Agence européenne de cybersécurité (ENISA) et la France a transcrit en mai 2018 une directive relative à la Sécurité des réseaux et des systèmes d'information (*Network & Information Security-NIS*) de 2016. Pour autant, le droit européen reste assez discret sur les questions spécifiquement maritimes.

La France appartient donc à un vaste ensemble européen qui conditionne ses actions. Elle participe en réalité à un grand ensemble occidental qui cherche à gagner une bataille juridique contre des puissances en pleine affirmation, à l'image de la Chine qui a planifié son influence juridique dans sa nouvelle stratégie des routes de la soie.

Cyberopérations et droit international : la vision juridique comme pilier d'influence stratégique

L'émergence du cyberespace oblige à penser un nouveau système de régulation, dont les prémices actuelles traduisent les affrontements juridiques entre liberté et souveraineté. Espace commun, il devrait dans tous les cas être gouverné par le principe d'utilisation pacifique, à

(43) Décret 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale, et arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « transport maritime et fluvial ».

l'instar de celui qui s'applique à la haute mer ainsi qu'à l'espace extra-atmosphérique, ce qui ne fait pas obstacle à l'invocation de la légitime défense.

Influences occidentales en matière de cybersécurité maritime

Les perspectives nationales divergentes entre partisans de la liberté et partisans de la souveraineté se sont traduites par des approches juridiques contradictoires qui ont fini par faire échec au Groupe des experts gouvernementaux de l'ONU (UNGGE), réunis sur trois cycles entre 2012 et 2017. Composée selon le principe de répartition géographique équitable, cette enceinte n'a pas pu dépasser les clivages interétatiques, chaque Etat ayant voulu préserver son opacité dans le milieu informatique (44) tout en cherchant, dans la construction d'un nouvel espace juridique, à imposer sa vision stratégique. La Chine, la Russie et l'Arabie saoudite, avec quelques autres Etats, prônent un droit plus contraignant du cyber, avec une vision de la souveraineté informationnelle qui ne laisse qu'aux seuls Etats le soin de construire un environnement juridique efficace. A l'opposé, les Etats-Unis, les Etats européens ou le Japon, souhaitent une gouvernance multi-acteurs, liant gouvernements, sociétés civiles et secteur privé. Dans ces premières rencontres, l'UNGGE a toutefois reconnu l'applicabilité du droit international au cyberespace, notamment celui de la Charte des Nations Unies et des conflits armés. L'utilisation pacifique qui préside au régime juridique des espaces communs s'inscrit dans le droit onusien et ne saurait donc faire obstacle au recours à la force d'un Etat en réponse à une cyberattaque en mer, dans les conditions posées par le droit international. Pourtant, Chine et Russie rejettent l'invocation du droit de légitime défense au cyberespace et renforcent *de facto* le critère de l'agression armée tout en rééquilibrant leur pression par l'investissement dans la sphère informationnelle (45).

Sans consensus et dans l'impossibilité de recourir à un texte international contraignant, il faut se reporter au texte le plus abouti, le *Manuel de Tallinn*, proposé par des Etats membres de l'Organisation du Traité de l'Atlantique Nord (OTAN) sans être une émanation de cette dernière. Ce document prend parti pour l'applicabilité du droit international au cyberespace et pour la licéité de la légitime défense dans ledit espace. La France, qui n'était pas impliquée dans les travaux d'origine mais qui reconnaît la licéité de la légitime défense dans le cyberespace (46), a finalement pris acte de l'intérêt d'être associée à ces travaux pour promouvoir sa vision du droit

(44) Arnaud Sudres, *op. cit.*

(45) Stéphane Taillat, « L'impact du numérique sur les relations stratégiques internationales », *Stratégiques*, 2017/4, n°117, pp. 137-153.

(46) Stratégie nationale de cyberdéfense, 29 juin 2018, p. 103 : « *La France a également eu l'occasion, avec plusieurs de ses partenaires, d'affirmer sa position en faveur de la reconnaissance claire et univoque de la licéité des moyens de réponse à une cyberattaque, qu'ils impliquent un recours à la force (légitime défense) ou non (contre-mesures, mesures de rétorsion, etc.) et de l'applicabilité du droit international humanitaire aux cyberopérations conduites dans le cadre des conflits armés.* »

dans le cyberespace. Dans cet affrontement de puissances à la genèse d'un nouvel espace juridique, les Etats occidentaux ont tout intérêt à densifier leur position juridique afin d'assurer leur prééminence sur ce « cinquième domaine de la guerre », en assurant son applicabilité aux acteurs non étatiques, aidés en cela par les avancées doctrinales en matière de droit de la mer.

Réactions juridiques face aux cyberattaques maritimes

Une cyberattaque peut d'abord être le fait d'un groupe criminel combattu sur le fondement de la *lex specialis* applicable en mer. La Convention pour la répression d'actes illicites contre la sécurité de la navigation maritime (SUA), sans traiter spécifiquement de la cybermenace, incrimine le fait de détruire ou d'endommager gravement les installations ou service de navigation ou de communiquer une information qu'on sait fausse si ces actions compromettent la sécurité de la navigation maritime. Ces deux incriminations permettent de traiter, dans une certaine mesure, les cyberattaques destinées à détourner un navire (47), à détruire un terminal portuaire, voire un central de navigation d'un navire CDT.

Une cyberattaque en mer, en raison de son intensité, pourrait également atteindre le seuil requis pour être qualifiée d'agression armée et ainsi ouvrir à l'Etat victime une action en légitime défense. Si la cyberattaque en déni de service contre l'Estonie, attribuée à la Russie, n'a pas été reconnue comme ayant atteint le seuil de gravité requis, celle du virus Stuxnet contre le programme nucléaire iranien l'a été par les experts du *Manuel de Tallinn*. Par analogie, on pourrait donc imaginer qu'une cyberattaque à terre sur un *hub* maritime, voire dans un central de navigation d'envergure, puisse être qualifiée d'agression armée. Qu'en serait-il en mer ? Dans l'affaire des plates-formes pétrolières entre la République islamique d'Iran et les Etats-Unis, la Cour internationale de justice (CIJ) a reconnu que le minage d'un seul navire de guerre pouvait justifier le recours à la légitime défense (48). Pour les navires de commerce, la question est plus ambiguë. Sans les écarter explicitement, la CIJ a restreint son invocation à l'Etat du pavillon en refusant l'argumentation des Etats-Unis fondant leur droit de légitime défense sur l'agression armée à l'encontre de navires contrôlés par les intérêts américains mais ne battant pas leur pavillon. Cependant, le Conseil de sécurité (CSNU) a déjà assimilé les navires contrôlés par des intérêts yougoslaves à des navires battant pavillon yougoslave (49) afin de permettre aux navires tiers de faire respecter le blocus imposé en 1992.

(47) En modifiant l'article 224-6 du Code pénal, la France a levé l'obligation de présence à bord de l'auteur d'un détournement de navire, permettant ainsi d'appliquer sa compétence pénale face à une cyberattaque. *Cf.* à ce sujet Gersende Le Dimna, *op. cit*.

(48) *Plates-formes pétrolières (République islamique d'Iran c. Etats-Unis d'Amérique)*, arrêt, CIJ, Recueil 2003, p. 161.

(49) S/RES/1787 (1992), 16 nov. 1992, Bosnie-Herzégovine.

Rien n'empêcherait le CSNU de récidiver en cas de carence ou de refus (50) du pavillon national qui l'empêcherait d'exercer son droit de légitime défense contre une cyberattaque contraignant la liberté de navigation et la continuité des flux potentiellement stratégiques. Cela permettrait aussi de lutter plus aisément contre des attaques multiples.

La Stratégie nationale de sûreté des espaces maritimes (51) formule clairement le risque d'une attaque terroriste simultanée sur différentes cibles maritimes. Sont ainsi pris en compte le trouble particulièrement fort et la désorganisation des forces qui découleraient d'une telle attaque. La CIJ, toujours dans l'affaire des plates-formes pétrolières, n'a pas écarté la théorie de l'accumulation en mer sous la condition de considérer les attaques comme un seul et même fait continu, qui conjointement se prolonge le temps que dure la violation de l'obligation internationale. Il faut alors considérer le contexte et les conséquences de l'attaque, étant entendu que « *dans des zones qui ne sont soumises à aucune juridiction, on aura davantage tendance à qualifier l'acte de grave et à appliquer l'article 2§4 de la Charte* » (52). Les conséquences potentielles d'une cyberattaque ciblée en mer peuvent porter atteinte à la souveraineté de l'Etat puisque sa finalité serait de déstabiliser la société en désorganisant la vie économique, ce qui peut avoir , si la cyberattaque est poussée à son paroxysme, de graves répercussions, en bloquant les voies de communication. Ainsi, certains militent, pour éviter d'arriver à ce stade, en faveur d'une action préemptive (« *last window of opportunity* »), voire préventive. Si cette dernière est rejetée de façon continue par le droit international, le critère de la concomitance (53) de la réaction vis-à-vis de la réalisation de l'attaque pourrait être, selon une partie de la doctrine (54), assoupli en mer en raison de circonstances spéciales, notamment du temps nécessaire pour rejoindre la destination visée après l'avoir identifiée.

Une attaque réussie repose sur la surprise et la surprise repose sur l'invisibilité. Le cyberespace est l'espace par excellence de la surprise stratégique et la réaction est d'autant plus difficile à organiser que l'attribution n'est jamais certaine. Le défenseur lui-même ne dénonce pas toujours la cyberattaque, dans la crainte d'une escalade ou de « *coûts réputationnels* » (55) trop importants. Le droit international fait classiquement (56) de l'agression armée une agression étatique. Toutefois,

(50) Bien que, dans ce dernier cas, la présence de la République populaire de Chine et de la Fédération de Russie comme membres permanents au CSNU rendrait l'hypothèse fort théorique.

(51) Comité interministériel de la Mer, *Stratégie nationale de sûreté des espaces maritimes*, 2015, 51 p.

(52) Olivier Corten, Le Droit contre la guerre, Pédone, Paris, 2008, 932 p., p. 119.

(53) Directive interarmées n°805/DEF/EMA/EMP.1/NP, EMA division emploi 1, 25 juil. 2006, sur l'usage de la force en opération militaire se déroulant à l'extérieur du territoire national.

(54) Kiara Neri, *L'Emploi de la force en mer*, Bruylant, 628 p.

(55) Stéphane Taillat, *op. cit.*

(56) La résolution 3 314 de l'Assemblée générale des Nations Unies de 1974 fait de l'agression armée, l'agression d'un Etat contre un autre. Sont prises en compte les attaques contre les marines civile et militaire de l'Etat.

les cyber attaquants ne sont pas que des Etats agissant directement ou par l'intermédiaire de groupes sur lesquels ils exerceraient un contrôle effectif ou global (57). L'émergence de nombreux acteurs non étatiques altère la conception traditionnelle interétatique du droit de la Charte. Une fois de plus, espace maritime et cyberespace partagent des enjeux communs. Confronté à la question de la licéité de l'emploi de la force contre des acteurs non étatiques, l'Institut de droit international (IDI) a reconnu à dessein, en 2007, que « [s]*i une attaque armée par des acteurs non étatiques est lancée depuis un espace hors la juridiction de tout Etat, l'Etat visé peut exercer son droit de légitime défense dans cet espace contre des acteurs non étatiques* » (58). Le cyberespace comme l'espace maritime de haute mer sont des espaces hors juridiction par excellence. Hors souveraineté, hors juridiction, les Etats n'y ont qu'une obligation de *due diligence* quand ils ont connaissance de l'utilisation de leur territoire – couche physique – pour mener des cyberattaques visant, dans ces espaces communs, d'autres Etats. Si l'Etat victime peut lui attribuer le contrôle des acteurs non étatiques, il sera fondé à agir en légitime défense contre lui, *via* des cyberarmes (59) ou des armes conventionnelles. Dans le cas contraire, il pourrait, en vertu des conclusions de l'IDI et s'il respecte l'intégrité territoriale de l'Etat tiers, mener des cyberopérations en légitime défense.

* *
*

L'interétatisme marqué du droit international est aujourd'hui bousculé par de nouveaux acteurs, dans de nouveaux espaces, par de nouveaux défis. Dans les affrontements entre domination et appropriation, entre liberté et souveraineté, on peut redécouvrir, adaptés au cyberespace, des champs de réflexions géopolitiques et juridiques propres à l'espace maritime. Face à des rapports de forces en restructuration, les Etats doivent à la fois mener des programmes pragmatiques et imposer leurs conceptions juridiques. La France n'y fait pas exception. En tant que deuxième espace maritime au monde, elle a un rôle essentiel à jouer. Forte de sa conception occidentale des rapports internationaux, de sa doctrine et de ses ressources, elle doit pouvoir compter dans la conception du droit nouveau s'appliquant à ce nouvel espace. Puissance maritime qui s'ignore, c'est en s'assumant comme une puissance des mers et des outre-mer qu'elle pourra s'accomplir en tant qu'inspirateur juridique en vue de sécuriser ce nouvel espace commun : le cyberespace.

(57) « *Après quelques références embryonnaires, le droit international a été utilisé pour la première fois dans ce contexte par les Etats-Unis en 2015 dans le cadre de l'attribution à la Corée du Nord du piratage de Sony Picture Entertainment et de la prise de mesures de rétorsion contre cet Etat* ». *Cf.* François Delerue, « Cyberopérations et droit international. De l'opportunité de saisir la Commission du droit international des Nations Unies de la question du droit international applicable aux cyberopérations », Institut de recherches stratégiques de l'Ecole militaire, 17 juil. 2018.

(58) IDI, *Problèmes actuels du recours à la force en droit international*, Résolution, Santiago, 2007.

(59) Les cyberarmes et les armes numériques ont été citées dans la *Revue stratégique de cyberdéfens*e, fév. 2018.