RDN

Étude

Les nouvelles frontières de la défense
La mer, l'Espace et l'information

Une étude réalisée par les étudiants des Masters
« Armées, guerres et sécurité dans les sociétés » (Sorbonne Université)
« Dynamique des systèmes internationaux » (Sorbonne Université)
et « Relations internationales » (Paris II-Sorbonne Université)

Sous la direction de M. Tristan Lecoq
Inspecteur général de l'Éducation nationale
Professeur des universités associé (histoire militaire et maritime contemporaine)
Faculté des Lettres de Sorbonne Université

CENTRE THUCYDIDE
analyse et recherche
en relations internationales

LES JEUNES INTERNATIONALISTES

UNIVERSITÉ PARIS II PANTHÉON-ASSAS

Association loi 1901
fondée en 1939

Les Cahiers de la
Revue Défense Nationale

DEFENSE · MOBILITY · SYSTEMS

ARQUUS
e-xpo

NOUS VOUS INVITONS À VIVRE UNE NOUVELLE EXPÉRIENCE.
RENDEZ-VOUS À PARTIR DU 8 JUIN SUR ARQUUS-DEFENSE.COM

VÉHICULES BLINDÉS | GAMME CAMION | TOURELLEAUX HORNET | OFFRES SERVICES

ARQUUS

ARQUUS-DEFENSE.COM

MEMBER OF THE VOLVO GROUP

Les nouvelles frontières de la défense
La mer, l'Espace et l'information

Une étude réalisée par les étudiants des Masters
« Armées, guerres et sécurité dans les sociétés » (Sorbonne Université)
« Dynamique des systèmes internationaux » (Sorbonne Université)
et « Relations internationales » (Paris II-Sorbonne Université)

Sous la direction de M. Tristan LECOQ
Inspecteur général de l'Éducation nationale
Professeur des universités associé (histoire militaire et maritime contemporaine)
Faculté des Lettres de Sorbonne Université

Sorbonne Université et Panthéon-Assas (Paris II)

Sommaire

5 **Préface**
Maximilien ROQUETTE, Anne STOVEN et Marie-Amélie VIEU

7 **Introduction à l'étude**
Tristan LECOQ

13 **La mer, nouvelle frontière de la défense**
Lisa BLANC, Marie DE ROSNAY, Aya EL-ALAMI (rapporteur), Coline FONTAINE, Alban GIRAULT, Paul HAXEL, Erwan NAVARRE, Daoud NOËL MASSENAT, Anne STOVEN, Marie-Amélie VIEU et Constance WYBO

27 ❖ **Étude de cas : les câbles sous-marins**
Elisa HELLER, Lucie GUICHARD, Guillaume KOUKOUI et José ZAAROUR (rapporteur)

35 **L'Espace : entre dissolution et multiplication des frontières**

45 ❖ **Étude de cas : l'Espace comme domaine renouvelé de la défense française** ***De la militarisation à l'arsenalisation***
Marcello PUTORTI et Hawa-Léa SOUGOUNA (rapporteurs), Yanis AMAE BENABDALLAH, Théo BRUNET, Pierre-Marie BUJADOUX , Camille FAGHEL, Esteban FAGNIEZ, Yanis FEKRACHE, Robinson GOUHIER, Brahimi HADJER, Sarah HAMBEC, Louis LAFAURIE, Marcello PUTORTI, Sophie SCHÖNUBE, Pacôme SEBASTIEN, Tristan TELLIER et Pauline VERGER

53 **L'Information : vers une dématérialisation des frontières de la défense**
Ludovic BUCQUET, Izabela BUKOWSKA et Cécile MOUCHON (rapporteurs), Bob BAKOULA MAURIN, Denis BAVEREZ, Julien BETTON, Tessa BOURCIER, Dusan BOZALKA, Grégoire GASTON, Ulysse GUERIN, Said KEDDACHE, Constance PARPEX, Maximilien ROQUETTE et Jean-Victor TSE

68 ❖ **Étude de cas : la cyberdéfense française**
Matthieu BIBEN, Myriam BOUMBAR et Amélie FALTOT

75 **Postface – Extension du domaine de la stratégie ?**
Jean-Vincent HOLEINDRE

La *Revue Défense Nationale* est éditée par le Comité d'études de défense nationale
(association loi de 1901)
Adresse géographique : École militaire, 1 place Joffre, bâtiment 34, PARIS VII
Adresse postale : BP 8607, 75325 PARIS CEDEX 07
Fax : 01 44 42 31 89 - www.defnat.com - redac@defnat.com
Directeur de la publication : Thierry CASPAR-FILLE-LAMBIE - Tél. : 01 44 42 31 92
Rédacteur en chef : Jérôme PELLISTRANDI - Tél. : 01 44 42 31 90
Rédactrice en chef adjointe : Audrey HÉRISSON
Secrétaire général de rédaction : Pascal LECARDONNEL - Tél. : 01 44 42 43 69
Assistante de direction et secrétaire de rédaction : Marie-Hélène MOUNET - Tél. : 01 44 42 43 74
Secrétaires de rédaction : Jérôme DOLLÉ et Antoine AUBERT - Tél. : 01 44 42 43 69
Abonnements : Éliane LECARDONNEL - Tél. : 01 44 42 38 23
Chargés d'études : Laurent HENNINGER et Emmanuel DESCLÈVES - Tél. : 01 44 42 43 72
Comité de lecture : Didier CASTRES, Marie-Dominique CHARLIER-BAROU, André DUMOULIN,
Jean ESMEIN, Sabine DE MAUPEOU et Bernard NORLAIN
Régie publicitaire (ECPAD) : Karim BELGUEDOUR - Tél. : 01 49 60 59 47
DL 97614 - 2e trimestre 2020 - ISSN : 2105-7508 - CP n° 1019 G 85493 du 10 octobre 2019
Imprimée par BIALEC, 23 Allée des Grands Pâquis, 54180 HEILLECOURT

Photo de couverture © Tristan Lecoq

Préface

Pour la quatrième année consécutive, l'Inspecteur général Tristan Lecoq, Professeur des Universités associé à la Sorbonne a proposé aux étudiants de son séminaire de recherche « La France et sa défense à l'époque contemporaine. Histoire, actualité, enjeux » de travailler durant une année universitaire sur un sujet mêlant actualité, défense et sécurité, et de le faire publier par la *Revue Défense Nationale*. Ce séminaire de recherche rassemble des étudiants de deux masters d'histoire de la Faculté des Lettres de Sorbonne Université, « Armées, guerres et sécurité dans les sociétés » et « Dynamique des systèmes internationaux », respectivement dirigés par les Professeurs Olivier Chaline et Olivier Forcade, ainsi que d'un master de l'Université Paris II Panthéon-Assas, « Relations internationales », codirigé par les Professeurs Jean-Vincent Holeindre, Olivier Forcade et Roseline Letteron.

C'est au début du mois d'octobre 2019 que le Professeur Tristan Lecoq nous a proposé ce thème des nouvelles frontières de la défense. Nous avons décidé d'étudier chacune de ces trois thématiques sous le prisme d'un triptyque commun : les acteurs, les enjeux et les conflits. Parallèlement, pour chaque thématique, nous avons adjoint à cette étude générale une étude de cas que nous avons jugée représentative du phénomène général. C'est également au mois d'octobre que nous nous sommes répartis en groupes de travail, chacun sous la responsabilité d'un rapporteur – pour mener nos recherches et en rédiger les résultats – groupes de travail qui furent aussi bien le cadre du travail de recherche que de celui de rédaction :

Groupe 1 : Aya El Alami et José Zararour (coordinateurs), Lisa Blanc, Marie De Rosnay, Coline Fontaine, Alban Girault, Lucie Guichard, Paul Haxel, Elisa Heller, Guillaume Koukoui, Erwan Navarre, Daoud Noël Massenat, Anne Stoven, Marie-Amélie Vieu et Constance Wybo.

Groupe 2 : Marcello Putortì et Hawa-Léa Sougouna (coordinateurs), Yanis Amae Benabdallah, Théo Brunet, Pierre-Marie Bujadoux, Camille Faghel, Esteban Fagniez, Yanis Fekrache, Robinson Gouhier, Brahimi Hadjer, Sarah Hambec, Louis Lafaurie, Sophie Schönube, Pacôme Sebastien, Tristan Tellier et Pauline Verger

Groupe 3 : Ludovic Bucquet, Izabela Bukowska et Cécile Mouchon (coordinateurs), Bob Bakoula Maurin, Denis Baverez, Julien Betton, Matthieu Biben, Myriam Boumbar, Tessa Bourcier, Dusan Bozalka, Amélie Faltot, Grégoire Gaston, Ulysse Guerin, Said Keddache, Constance Parpex, Maximilien Roquette et Jean-Victor Tse

C'est donc la quatrième année consécutive que le Professeur Tristan Lecoq propose à ses étudiants la rédaction d'un *Cahier* de la *Revue Défense Nationale*. Réciproquement, c'est donc également la quatrième année consécutive que la *Revue Défense Nationale* accepte de nous ouvrir les pages de ses prestigieux cahiers. Bien peu de jeunes chercheurs de notre niveau d'études ont la chance de pouvoir publier un travail de recherche dans une revue d'une telle stature. Nous adressons nos remerciements au général Jérôme Pellistrandi, son rédacteur en chef, pour sa confiance renouvelée année après année, ainsi qu'à Jérôme Dollé et Antoine Aubert, pour leurs précieux conseils de relecture, qui ont permis cette année encore l'aboutissement de ce projet. Nous les remercions certes de nous avoir ainsi ouvert la voie à une première publication scientifique, mais aussi de préserver cette jonction qu'est devenu ce *Cahier*, désormais annuel, entre les mondes de l'Université et de la défense, jonctions de moins en moins rares aujourd'hui.

Nous adressons également nos remerciements au Professeur Jean-Vincent Holeindre, directeur du master « Relations internationales » dont sont issus nombre des rédacteurs de ce *Cahier*, pour en avoir rédigé la conclusion, incarnant une fois de plus cette fraternité universitaire dont nous savons faire preuve au-delà des rivalités le plus souvent amicales entre nos Facultés.

Enfin, superviser un travail d'une telle envergure ne saurait reposer sur nos seules épaules de rapporteurs. Si nous avons pu le mener à terme, c'est avant tout grâce à l'intuition du Professeur Tristan Lecoq de la pertinence et de l'actualité de ce sujet ; c'est ensuite grâce la confiance qu'il a accordée aux jeunes masterisants que nous sommes ; c'est enfin grâce à ses conseils et ses orientations tout au long de nos recherches. Nous lui exprimons toute notre reconnaissance pour avoir si bien mené cette aventure intellectuelle dont l'aboutissement est pour nous une fierté.

Maximilien ROQUETTE, Anne STOVEN et Marie-Amélie VIEU

Introduction à l'étude

Tristan LECOQ

Inspecteur général de l'Éducation nationale, Professeur des universités associé (histoire militaire et maritime contemporaine) à Sorbonne Université.

Dans sa thèse de doctorat publiée en 1983, *Guerre et agriculture dans la Grèce antique*, l'historien militaire américain Victor Davis Hanson analysait comment les guerres entre les cités-États grecques avaient certes pour enjeu la préservation de leurs terres cultivées, mais aussi – et surtout – l'appréhension politique du territoire de la cité, et donc le devoir civique d'inviolabilité de celui-ci [(1)]. Militarisation de l'agriculture, militarisation du territoire, militarisation même de la politique : cet exemple du VII^e^ siècle avant J.-C. montre l'ancienneté de la propension des sociétés humaines à « militariser » toutes les dimensions de leur environnement. Aussi n'est-il pas étonnant qu'aujourd'hui la mer, l'Espace et l'information soient l'objet d'un tel phénomène. À l'heure où les frontières physiques entre les États, premiers acteurs de la défense, s'estompent de plus en plus [(2)], les frontières conceptuelles entre ce qui relève du domaine de la défense et ce qui n'en relève pas s'estompent de même.

Selon les domaines que nous avons étudiés, la relation aux milieux – la mer, l'Espace, les domaines liés à l'information – de l'organisation de la défense et de la sécurité nationale n'est pas la même. Ainsi la marine est-elle l'expression de la puissance depuis l'Antiquité : les bateaux à vocation militaire sont aussi anciens que les bateaux *stricto sensu*, et la mer aurait pu être l'objet d'une étude similaire à celle de Victor Davis Hanson sous le titre de *Guerre et mer dans la Grèce antique*. L'apparition des grandes marines de guerre, dès le XIV^e^ siècle en Angleterre, au XVII^e^ siècle en France, montre bien l'importance des enjeux maritimes dans les relations entre États. La guerre sur mer, sous les mers, au-dessus des mers, au fond des mers… est devenue le symbole de la projection, sur les mers et les océans, des enjeux de puissance [(3)].

À l'inverse, ce phénomène peut être particulièrement récent à l'échelle de l'Histoire : comme l'étude consacrée à l'Espace le rappelle, nous ne sommes en mesure d'y envoyer des satellites que depuis 1957, le phénomène d'« arsenalisation » de l'Espace ne pouvait-il qu'être aussi récent. Là encore, l'existence des satellites à vocation militaire en est directement consécutive, puisque les premiers satellites espions,

(1) HANSON Victor Davis, *Guerre et agriculture dans la Grèce antique*, University of California Press, 1983.
(2) LECOQ Tristan, « France : de la défense des frontières à la défense sans frontières », *Questions internationales* n° 79-80 (« Le réveil des frontières »), La Documentation française, mai-août 2016
(3) LECOQ Tristan et SMITS Florence, « Les routes des fonds des mers. La colonne vertébrale de la mondialisation », *Annuaire français de relations internationales*, vol. XVIII, juillet 2017, La Documentation française/Université Panthéon-Assas Centre Thucydide.

conçus dans le cadre de la guerre froide, datent de 1959, soit seulement deux ans plus tard. Les questions liées à l'information ont, elles aussi, pris une importance croissante à la mesure des progrès scientifiques et technologiques. Il y a bien une constante : toute dimension contrôlée par l'homme, qu'elle soit matérielle (comme la mer ou l'Espace) ou immatérielle (comme l'information), devient un enjeu de défense et de sécurité nationale.

L'appréciation de ce phénomène n'est pas l'apanage des réflexions des seules sciences humaines ou des sciences politiques comme celle que nous avons menée, mais elle fait l'objet d'une institutionnalisation. Ainsi, l'apparition des concepts d'« intérêts vitaux » puis d'« infrastructures vitales » dans les *Livres blancs* successifs illustre bien que les enjeux de défense ne se résument pas à gagner des guerres : « Assurer la continuité de la vie nationale et élever le seuil de la sécurité des populations, à l'intérieur et à l'extérieur du territoire : c'est cela qui, désormais, donne un sens à la politique publique de sécurité nationale » [(4)].

Si ce phénomène n'est pas nouveau, les études lui étant consacrées ne le sont pas non plus, comme l'ampleur de la bibliographie mise à profit dans ce *Cahier* le démontre. Mais si le changement de nature des frontières de la défense à la mer a pu être étudié, si la militarisation de l'Espace a déjà fait l'objet de publications, si la dimension éminemment stratégique de l'information est comprise au moins depuis Sun Tzu, l'originalité que nous avons souhaité conférer à notre étude réside dans la mise en perspective des trois. Si ces phénomènes sont respectivement très intéressants à étudier, c'est l'appréhension d'un phénomène général de militarisation qui nous a paru l'être tout autant.

Du reste, la pandémie de Covid-19 démontre, au moins à deux titres, l'actualité de ce phénomène d'extension des frontières de la défense. C'est d'une part, la militarisation de la gestion de cette crise, au moins dans l'expression. L'emploi par le président de la République de la formule : « Nous sommes en guerre » [(5)] peut relever de l'ordre de l'élément de langage. Elle se traduit, très directement, par la mise à contribution de nos forces armées dans cette gestion de crise : c'est ainsi le déploiement en moins d'une semaine d'un « Élément militaire de réanimation » à Mulhouse par le Service de santé des armées [(6)], ou encore l'emploi du Porte-hélicoptères amphibie (PHA) *Tonnerre* pour transférer les malades de Corse vers les hôpitaux marseillais [(7)]. Il n'empêche : c'est d'un cadre bien plus vaste dont il s'agit, et c'est à une réflexion d'ensemble sur la défense et la sécurité nationale et son organisation que la crise sanitaire sans précédent devrait conduire.

---

(4) Lecoq Tristan, « Assurer la sécurité de la nation : la question de l'organisation de la défense nationale », *Revue Défense Nationale* n° 829, avril 2020.

(5) Pietralunga Cédric et Lemarié Alexandre, « "Nous sommes en guerre" : face au coronavirus, Emmanuel Macron sonne la "mobilisation générale" », *Le Monde*, 17 mars 2020.

(6) Direction centrale du Service de santé des armées, « La Direction des approvisionnements en produits de santé des armées (DAPSA) au cœur de la préparation et du déploiement de l'Élément militaire de réanimation (EMR-SSA) », 3 avril 2020 (www.defense.gouv.fr/).

(7) Direction centrale du SSA, « Lutte contre le COVID-19 : la Marine nationale et le SSA en soutien », 7 avril 2020 (www.defense.gouv.fr/sante/actualites/lutte-contre-le-covid-19-la-marine-nationale-et-le-ssa-en-soutien).

Ce sont, d'autre part, les nouveaux enjeux de défense que soulève cette pandémie : ainsi, dans les régions rendues déjà instables par les conflits ethniques ou religieux, le manque de développement économique, la pression démographique ou encore l'insuffisance de l'État, le facteur sanitaire est apparu comme un nouveau facteur d'instabilité. De nouvelles situations découlant de cette pandémie, par exemple la réduction de la mobilité, peuvent influer sur des conflits déjà existants, soit en les atténuant : la réduction de l'activité maritime, y compris militaire, en Méditerranée a engendré une cessation des combats dans la ville syrienne d'Idlib [8], soit au contraire en les accentuant : la marine turque a profité de cette même réduction d'activité maritime pour faire main basse sur des ZEE chypriotes [9]. Faut-il y voir une « militarisation de la santé » ? La Chine, *via* sa marine de guerre, profite, elle, de l'épidémie qui s'est déclenchée sur son sol pour étendre ses opérations en mer de Chine méridionale.

C'est ainsi que nous avons dû délimiter les enjeux liés à ces trois nouvelles frontières de la défense que nous jugions suffisamment représentatives pour articuler notre étude autour d'elles. Mais, le lecteur l'aura compris, ce phénomène est bien loin de s'y cantonner. Quant à ces autres dimensions pour lesquelles il serait applicable, comme la santé, le champ de la recherche reste ouvert.

Au sein de la défense, la mer est un des piliers de la puissance d'un État. Milieu caractérisé par son hypermobilité, la mer est à la fois une route économique, un puits de richesses et un théâtre de l'exercice de la puissance. D'un espace sans frontières, la mer devient un territoire, ou mieux un « merritoire », c'est-à-dire un territoire maritime où se révèlent des enjeux, où s'exerce le jeu des acteurs, où se nouent des conflits. Le général de Gaulle l'affirmait dès 1969 : « L'activité des hommes se tournera de plus en plus vers la recherche de l'exploitation de la mer. Et, naturellement, les ambitions des États chercheront à la dominer pour en contrôler les ressources » [10]. Un demi-siècle plus tard, cette déclaration se vérifie, la géopolitique des terres est un miroir d'une géopolitique des mers, par une approche partagée du *continuum* mer-terre.

Compte tenu des transformations globales intervenues dans le système international à la fin de la guerre froide, la question de la maîtrise des mers et des océans sous l'optique des nouvelles frontières maritimes dans un sens géographique, économique et diplomatique, occupe une place importante dans le débat stratégique actuel et, par conséquent, il en est de même des espaces marins dans les politiques de défense et de sécurité nationale des États.

Partant de ce constat, cette évolution a complètement affecté l'ensemble des priorités en matière de questions maritimes : projeter des forces navales – marqueur d'une certaine hégémonie –, répondre aux nouvelles menaces et envisager les nouveaux enjeux maritimes sont les préoccupations majeures auxquelles doivent faire face les

---

[8] Ausseur Pascal et Razoux Pierre, « Les conséquences stratégiques du Covid-19 dans le bassin méditerranéen », *Fondation méditerranéenne d'études stratégiques*, avril 2020.

[9] *Ibid*.

[10] Discours du général de Gaulle le 1er février 1969 à Brest, cité dans Commission des Affaires étrangères et des forces armées, « Maritimisation : la France face à la nouvelle géopolitique des océans » *Rapport d'information* n° 674, 17 juillet 2012, Sénat (www.senat.fr/notice-rapport/2011/r11-674-notice.html).

États ayant pour ambition de se positionner comme acteurs influents sur l'échiquier mondial. Projection des intérêts de puissance de la terre vers la mer, « territorialisation » des espaces maritimes, acteurs, enjeux et conflits sont la trace et la marque de cet univers complexe où s'exerce la liberté des hommes, ligne de vie et de mort en même temps [(11)].

L'Espace n'est pas simplement un nouveau milieu de confrontations et d'affrontements militaires, mais bien plus un nouveau champ normatif de la défense. Par sa géographie d'abord, l'Espace extra-atmosphérique n'est pas naturellement délimité par rapport à l'espace aérien, faisant de lui un milieu distinct de la défense. Par sa logique ensuite, l'Espace peut tantôt être considéré comme le lieu de confrontation en soi pour des ressources ou comme possession, ou encore pour l'emplacement stratégique dont il dispose, mais également comme point d'appui nécessaire au déroulement d'opérations terrestres et maritimes. Enfin, tant comme centre de l'attention que comme périphérie incontournable, l'Espace se fait donc à la fois moyen et finalité de l'attention militaire.

Les États – et pas tous – ne disposent d'un accès continu à l'Espace que depuis 63 ans, ce qui réduit considérablement la capacité de projection, autant que cela promet un immense potentiel de développement. Ces difficultés se superposent cependant à des tendances inhérentes à la défense. L'affaiblissement de l'État, l'apparition de nouveaux acteurs du domaine de la défense, la centralité croissante des enjeux industriels et plus largement économiques, dans les orientations stratégiques et enfin la recomposition accélérée des menaces, ne sont pas des phénomènes propres à l'Espace mais ils structurent directement le rapport de la défense à celui-ci. La question des alliances se pose dans ce cadre. Ainsi en est-il de la défense de l'Europe, de la défense européenne, de l'Europe de la défense [(12)].

L'Espace n'est donc pas seulement une nouvelle frontière de la défense, mais bien un nouveau phénomène de la défense, bouleversant celle-ci et absorbant ses altérations. L'objet de cette recherche est de saisir l'état et les dynamiques de cette interaction entre l'Espace et la défense, d'établir que ce nouveau milieu est en fait le terrain privilégié d'une poignée d'acteurs hégémoniques et de montrer que cet avantage des plus puissants n'est pas tant un principe conservateur, que l'expression parallèle d'une redéfinition du rôle étatique de la défense, qui doit relever le défi croissant de l'internalisation des enjeux économiques dans la pensée stratégique. Ce principe veut que l'Espace, plus que tout autre milieu, impose à la défense de se projeter au-delà de son domaine propre et implique également d'analyser les interactions entre une stratégie et un cadre juridique qui reste à définir. Enjeux, acteurs, conflits : la tripartition de la problématique retenue fonctionne à plein.

Le domaine de l'information a peu à peu investi toutes les sphères de la vie politique, sociale, idéologique avec l'apparition et le développement de médias aujourd'hui

(11) Tristan Lecoq et Smits Florence (dir.), *Enseigner la mer. Des espaces maritimes aux territoires de la mondialisation*, Canopé, 2016.
(12) « Défense de l'Europe, défense européenne, Europe de la défense », *Les Cahiers de la* RDN, avril 2019.

traditionnels. Les exemples au XX^e siècle sont nombreux, des totalitarismes hitlérien et stalinien à l'usage de l'information à des fins de propagande pendant la guerre froide. Avec l'avènement d'*Internet* puis des réseaux sociaux, n'importe quel individu peut aujourd'hui produire du contenu, informer et désinformer. Cette dynamique s'insère plus globalement dans le mouvement de la mondialisation qui voit la multiplication des acteurs sur la scène internationale – firmes multinationales, acteurs non étatiques, organisations non gouvernementales, comme autant de concurrents des États. Leurs stratégies de communication peuvent parfois s'opposer. Surtout, elles créent des flux sans précédent d'informations dont le contenu n'est pas directement contrôlable. De fait, la manipulation de l'information fait aujourd'hui l'objet d'une attention renouvelée de la part de l'ensemble des acteurs de la mondialisation, que ce soit pour l'encadrer ou pour en faire un usage stratégique.

L'importance de cette souveraineté numérique est mentionnée dans la *Revue stratégique de défense et de sécurité nationale* de 2017 : « Les armées françaises doivent être en mesure d'agir de façon autonome et durable dans les domaines (…) de l'espace numérique » (p. 79). Depuis plusieurs années, la hausse de la masse de données numériques est l'une des manifestations tangibles de cette nouvelle orientation de l'économie mondiale, des enjeux qu'elle comporte et des conflits qu'elle engendre entre les États. Trois types de protagonistes s'emploient aujourd'hui dans le monde à la collecte et au traitement d'informations « massif », suivant des logiques très différentes : les acteurs du renseignement et de la surveillance d'État, comme la *National Security Agency* (*NSA*) aux États-Unis et la Direction générale de la sécurité intérieure (DGSI) en France ; les « Gafam » pour Google, Apple, Facebook, Amazon, Microsoft ; les institutions patrimoniales et scientifiques, qui se consacrent à l'archivage d'informations pour les générations futures.

Les systèmes d'information, c'est la dématérialisation de la menace, la déterritorialisation de la défense, la négation même de la frontière. La prise de conscience de l'importance de ces sujets, au milieu de la décennie quatre-vingt-dix, s'est traduite d'abord par le renforcement de la sécurité des systèmes d'information et une réflexion d'ampleur a été engagée, au même moment, sur le rôle des États, en matière de protection et de permanence des infrastructures vitales en France, chez nos alliés, à l'étranger.

L'exemple de ces infrastructures que l'on qualifie en France de « vitales », aux États-Unis de « critiques », au Canada d'« essentielles » parce qu'elles sont un élément décisif des économies et des sociétés modernes : transports terrestres, maritimes et aériens, communication, réseaux matériels et immatériels, chaîne de la santé… montre à la fois la complexité des systèmes, l'interdépendance et la multiplication des acteurs, la difficulté pour la puissance publique de s'assurer de la permanence et de la disponibilité d'ensembles qui, aujourd'hui, conditionnent la continuité de la vie des Nations.

Ces enjeux font directement écho aux études qui suivent, à ces trois milieux que sont les mers et les océans, l'Espace, l'information, à ces trois « nouvelles frontières » de la défense. ◆

La mer, nouvelle frontière de la défense

Aya El Alami et José Zararour (coordinateurs), Lisa Blanc, Marie De Rosnay, Coline Fontaine, Alban Girault, Lucie Guichard, Paul Haxel, Elisa Heller, Guillaume Koukoui, Erwan Navarre, Daoud Noël Massenat, Anne Stoven, Marie-Amélie Vieu et Constance Wybo.

Au sein de la défense, la mer est un des piliers de la représentation de la puissance d'un État. Milieu caractérisé par son hypermobilité, la mer est à la fois une route économique, un puits de richesses et un théâtre de démonstration de puissance. Le monde de la défense se doit de prendre en compte les facettes multiples de ce milieu dans une stratégie de protection et d'organisation d'un territoire sans cesse en mouvement.

Le général de Gaulle l'affirmait dès 1969 : « L'activité des hommes se tournera de plus en plus vers la recherche de l'exploitation de la mer. Et, naturellement, les ambitions des États chercheront à la dominer pour en contrôler les ressources » [(1)]. Un demi-siècle plus tard, cette déclaration se vérifie, la géopolitique des terres est un miroir d'une géopolitique des mers, par une approche partagée du *continuum* mer-terre.

Compte tenu des transformations globales intervenues dans le système international à la fin de la guerre froide, la question de la maîtrise des mers et des océans sous l'optique des nouvelles frontières maritimes dans un sens géographique, économique et diplomatique, occupe une place importante dans le débat stratégique actuel et suscite une importance grandissante des espaces marins dans les politiques de défense des États.

Partant de ce constat, cette évolution a complètement impacté l'ensemble des priorités en matière de questions maritimes : projeter des forces navales – marqueur d'une certaine hégémonie –, répondre aux nouvelles menaces et envisager les nouveaux enjeux maritimes sont les préoccupations majeures auxquelles doivent faire face les États ayant pour ambition de se positionner comme acteurs influents sur l'échiquier mondial.

Afin de mieux appréhender la complexité de ce domaine, il est primordial d'identifier les principaux acteurs qui interagissent au sein de cet espace. Nous pouvons ainsi identifier un premier groupe de puissances maritimes qui tentent d'asseoir leur

(1) Discours du général de Gaulle, 1er février 1969, Brest cité dans Commission des affaires étrangères, de la défense et des forces armées, *Maritimisation : la France face à la nouvelle géopolitique des océans* (*Rapport d'information* n° 674), 17 juillet 2012, Sénat (www.senat.fr/notice-rapport/2011/r11-674-notice.html).

hégémonie historique face à un deuxième groupe constitué d'acteurs émergents. Enfin, nous verrons le rôle des groupes supranationaux sur les océans. Nous avons sélectionné arbitrairement les États et les organisations qui reviennent régulièrement dans nos exemples car ils sont, à notre sens, les acteurs qui jouent aujourd'hui un rôle crucial dans l'espace maritime de par leur présence, les ressources auxquelles ils disposent et leurs enjeux.

Les acteurs maritimes

Les grandes puissances maritimes

Les États-Unis, le thalassokrator

Le *thalassokrator* est le nom que le géographe grec Strabon (60-20 av J.-C) donnait à la puissance qui domine les mers, dans une idée que celui qui les domine, domine le monde. Possédant la ZEE la plus importante du monde (11 millions de km²), les États-Unis s'affirment comme le dominant des mers. Sa marine, l'*US Navy*, a un tonnage de 3 millions avec 299 bateaux en activité [(2)], dont 11 porte-avions, 52 sous-marins nucléaires d'attaque (SNA) et 9 porte-hélicoptères amphibie (PHA). Elle possède un budget de 194 milliards de dollars en 2019 [(3)] ainsi qu'une capacité technologique largement supérieure à celle de tous ses concurrents. Ainsi, elle s'assure une hégémonie incontestée dans le monde. Cependant la puissance américaine repose surtout sur l'immense réseau d'alliances étendu sur toute la surface du globe. Cette maîtrise des mers fait des États-Unis les garants du commerce maritime mondial représentant 80 % des échanges commerciaux planétaires [(4)] et 10 Md$ de marchandises chaque année [(5)], conférant à l'*US Navy* un poids résolument incomparable aux autres marines de ce monde.

La France, excellent challenger *aux moyens limités*

Possédant la deuxième ZEE la plus étendue au monde (11 millions de km²) grâce à ses 12 territoires ultramarins, la mer est un pôle majeur de l'emploi français, les activités liées à la mer employant 400 000 personnes [(6)] et représentant 270 Md d'euros de chiffre d'affaires ainsi que 14 % du PIB [(7)]. Ce dynamisme est la résultante d'une extraordinaire qualité des acteurs de ce milieu. La grande force de la puissance maritime française tient en son réseau d'entreprises de pointe tourné vers la maîtrise technologique, ainsi que par les chantiers navals français exportant 80 % de leur production de navires civils et 30 % des bâtiments militaires construits [(8)]. De plus, faisant preuve

(2) Données officielles de l'*US Navy* au 10 décembre 2019 (www.secnav.navy.mil/).
(3) *Ibid*.
(4) Bellot Ingrid, « Le commerce maritime mondial : infographie », *Arte*, 15 juillet 2015 (https://info.arte.tv/fr/l).
(5) De Jaeger Jean-Marc, « 5 chiffres incroyables sur le commerce maritime », *Les Échos*, 10 décembre 2015 (https://start.lesechos.fr/societe/culture-tendances/5-chiffres-incroyables-sur-le-commerce-maritime-3341.php).
(6) Pôle Emploi, *Semaine de l'emploi maritime*, février 2019 (www.pole-emploi.org/).
(7) *Ibid*.
(8) Pezard François, « La France maritime », *Conflits* n° 4, janvier-février-mars 2015, p. 64-65.

d'une réelle compétitivité, les compagnies maritimes françaises représentent une centaine d'entreprises et plus de 900 navires dont 600 sous pavillon français [9]. Le parapétrolier *offshore* est également l'un des moteurs de son économie maritime, avec Total, faisant partie des six *majors* mondiaux du secteur.

Néanmoins, si l'économie a tiré profit de son potentiel maritime, la puissance navale française, bien que reconnue, est freinée par le manque de moyens financiers qui limite son renouveau. La force maritime de notre pays repose sur une marine de guerre dotée de 144 bâtiments [10] détenant l'ensemble des *capital ships,* c'est-à-dire : porte-avions, SNA (5) et PHA (3). Le pays s'affirme comme puissance nucléaire par la détention de 4 sous-marins nucléaires lanceurs d'engins (SNLE) également perçus comme des *capital ships*. Le lancement du programme *Barracuda* en 2007 dont le tout dernier SNA *Suffren* livré cette année est le reflet d'une marine de pointe. Malgré cela, elle ne se positionne qu'au septième rang des marines de guerre avec un tonnage ne dépassant pas les 280 000 tonnes. Ce faible tonnage contraste avec l'étendue de sa ZEE comparable à celle du géant américain.

La Chine, un nouvel empire sur mer

La Chine est aujourd'hui un acteur de poids dans les relations diplomatiques, économiques et militaires internationales. Puissance navale établie, au deuxième rang mondial par le tonnage de sa flotte de guerre (1,5 M de tonnes), la Chine a tout à prouver à ses adversaires autant qu'à ses alliés, conformément à ses vues stratégiques multiples qu'elles soient en mer de Chine méridionale, de l'océan Indien jusqu'au continent africain mais également sur sa « nouvelle route de la soie » à destination de l'Europe. Ainsi 1,4 % du PIB chinois, représentant 7 à 8 % [11] du budget de l'État, est employé pour la défense du pays.

L'objectif du président Xi Jinping est d'assurer à la Chine une place de choix sur la scène internationale par la modernisation et l'accroissement de sa flotte. La marine de l'Armée populaire de libération (APL), perçue comme le point d'orgue de l'armée chinoise, possède près de 600 bâtiments dont 2 PA, 5 SNLE et 8 SNA. Son tonnage a crû de façon exponentielle durant la première décennie du XXIe siècle : de 920 000 t à plus de 1,5 millions entre 2012 et 2019 [12] ! Pékin est désormais en mesure d'affirmer ses velléités en mer de Chine méridionale, mais également faire face aux puissances occidentales. Néanmoins, la Chine reste dépendante des technologies étrangères mais entre dans une période de transition vers une autonomie stratégique et technologique par ses investissements dans la recherche et l'innovation militaire.

Si sa marine est en plein essor, son rayonnement sur les mers demeure un sujet de litiges diplomatiques du fait de la revendication expansionniste de sa ZEE. Cette

---

[9] *Ibid*.
[10] *Circulaire relative à la liste des navires de guerre en essais et en service dans la Marine nationale* au 13 mars 2019 (www.defense.gouv.fr/).
[11] « Hausse probable du budget chinois de la défense en 2019 », *French.China.org*, 13 février 2019 (http://french.china.org.cn/china/txt/2019-02/13/content_74461474.htm).
[12] Groizeleau Vincent, « La Chine consolide sa position de seconde flotte mondiale », *Mer et Marine*, 6 février 2019.

dernière d'une superficie de plus de 2 millions de km² est, aux yeux de la Chine, trop étroite. Elle revendique un espace de plus d'un million de km² appartenant à ses voisins, créant ainsi des conflits en mer de Chine.

Les acteurs revenants ou émergents

Le Japon, le renouveau de la force maritime de l'île du Levant

Classée au 5e rang mondial en termes de tonnage avec 400 000 t, la Force maritime d'autodéfense japonaise détient aujourd'hui 114 bâtiments, dont 46 *destroyers*, auxquels il faut ajouter 16 sous-marins en cours de renouvellement (classe « Soryu »). Ces bâtiments lui garantissent une place de choix sur le podium juste derrière la Chine, parmi les puissances asiatiques [13], et permettent à l'État nippon de protéger son archipel et sa considérable ZEE de 4,4 millions de km² [14], faisant d'elle la 9e plus grande au monde [15].

La reconstitution d'un arsenal maritime japonais s'est faite avec le soutien direct des États-Unis qui exerce, encore aujourd'hui, une influence forte sur les forces nippones. En effet, 90 % de l'équipement militaire japonais est américain [16]. Au sommet de ce renouveau maritime se trouve l'aéronaval. Clé de voûte de cette nouvelle marine, le Japon prévoit de transformer deux *destroyers* porte-hélicoptères de classe *Izumo* pour qu'ils puissent accueillir des avions de combat *F-35B* [17] ; Tokyo prévoit d'en acquérir quarante-deux dont dix-huit à l'horizon 2023.

Face à la montée en puissance de la Chine au budget militaire trois fois supérieur, le Japon cherche à maintenir l'équilibre géopolitique de la région. La défense des voies de liaison vers le Japon, qui importe ses matières premières en partie du Moyen-Orient, est un enjeu majeur face aux velléités chinoises en mer de Chine méridionale et à la piraterie qui fait rage aux alentours du détroit de Malacca [18]. Le Japon tend ainsi à passer d'une marine de protection à une marine de projection.

La Russie, puissance post-*soviétique*

Depuis les années 2000, le pays sort de sa longue convalescence *post*-soviétique et, par l'impulsion de son dirigeant Vladimir Poutine, donne un nouvel élan à la politique maritime de défense afin de s'assurer une place confortable à la table des grandes puissances et protéger sa ZEE (7,5 M de km²). Ainsi en 2013, ce dernier affirmait publiquement vouloir moderniser sa marine et investir environ 100 Md€ sur 7 ans

---

[13] « Les plus puissantes marines de guerre du monde d'après le National Interest », *Sputnik France*, 12 décembre 2019 (https://fr.sputniknews.com/photos/201912121042585661-plus-puissantes-marines-guerre-monde/).
[14] Terra Bellum, « Japon - Empire du Soleil levant ? », *Youtube*, 1er décembre 2018 (www.youtube.com/).
[15] VLIZ maritime boundaries geodatabase, 2016 et Division statistique des Nations unies, Demographic Yearbook, 2008 (pdf). 20 novembre 2019 (https://unstats.un.org/unsd/demographic/products/dyb/dyb2008/Table03.pdf).
[16] Lagneau Laurent, « Washington fait grimper ses exigences financières pour maintenir ses forces en Corée du Sud et au Japon », *Zone militaire, Opex 360.com,* 16 novembre 2019 (www.opex360.com/).
[17] Satge Vincent, « Japon et Allemagne : le retour des vaincus ? », *Conflictualités modernes et postures de défense*, 28 novembre 2018, republié sur *GeoStretegia* le 25 mars 2019 (www.geostrategia.fr/).
[18] Terra Bellum, *op. cit.*

pour optimiser ses capacités navales [19]. Ces mesures s'accompagnent d'une présence croissante sur ses espaces maritimes stratégiques (Méditerranée et mer Noire). Ce renouveau est avant tout un message adressé à l'Otan qui observe non sans crainte le pavillon russe sillonner les mers sur lesquelles ses membres revendiquent une certaine hégémonie. Néanmoins la flotte russe, malgré un tonnage avoisinant les 1,2 M de tonnes faisant d'elle la 3e du monde, marque encore un retard avec du matériel obsolète et un porte-avions à l'arrêt dû à un violent incendie à bord en décembre 2019. Le maintien de la puissance russe sur les mers dépendra donc de la capacité du pays à maintenir sa flotte à niveau avec les autres pays.

L'Inde, l'ambition maritime d'un pays tourné vers la terre

L'Inde, 6e puissance navale mondiale en tonnage avec ces 0,3 M de tonnes, fait depuis quelques années face à de nouveaux enjeux qui ont encouragé l'amélioration et la modernisation de sa flotte. Elle doit défendre sa ZEE qui, bien que limitée (1,6 M de km^2), recèle de nombreuses ressources énergétiques, stratégiques, mais également pour se protéger des multiples trafics illégaux particulièrement présents dans l'océan Indien. En effet, en plus de la piraterie, les trafics illicites règnent dans ces eaux où demeure une insécurité maritime. En parallèle, améliorer sa marine est un moyen pour l'Inde de rivaliser avec la puissance chinoise, en particulier dans l'océan Indien.

Selon *The National Interest*, l'Inde aura d'ici 2030 rattrapé tout retard technologique [20]. Elle devient progressivement un acteur incontournable du domaine militaire, notamment pour la Russie qui semble opérer progressivement un virage stratégique en s'intéressant de plus en plus à cette région [21].

Les organismes supranationaux

Toutes ces puissantes marines ont néanmoins besoin d'un cadre international afin de limiter les rapports de force dangereux pour la stabilité mondiale mais également pour établir des accords interétatiques à l'échelle régionale et planétaire, à la fois pour lutter contre un ennemi qui se veut commun ou encore pour accroître la force de frappe et l'hégémonie d'un groupe d'États. À l'échelle régionale, l'exemple de l'Organisation de coopération de Shanghai (OCS) est révélateur des stratégies d'alliances. Fondée en 2001, elle regroupe les principales puissances mondiales et régionales du continent asiatique sur les plans démographique, économique et militaire, menées par la Russie et la Chine. Ses prérogatives étaient initialement limitées au redressement économique et sécuritaire régional. Les objectifs déclarés dans la Charte de l'OCS sont centrés essentiellement autour de la lutte contre le terrorisme, les extrémismes et les séparatismes

---

[19] Cervello Manon, *Les nouvelles ambitions maritimes de la Russie du sud, de nouvelles préoccupations pour l'Otan*, FMES, 2016, 22 pages (http://fmes-france.org/wp-content/uploads/2016/09/article-Manon-Cervello.pdf).
[20] Farley Robert, « Ranked: 5 Most Powerful Armies on the planet (In 2030) », *The National interest*, 20 septembre 2017 (https://nationalinterest.org/blog/the-buzz/ranked-5-most-powerful-armies-the-planet-2030-22386).
[21] Vassil Karan, « Russie-Inde : visite du ministre de la Défense indien en Russie, une relance de la coopération militaro-industrielle entre les deux États » (https://nemrod-ecds.com/?p=4247).

dans la région [22]. Néanmoins, l'objectif implicite est de lutter contre l'unilatéralisme américain qui prend forme à leurs yeux par le biais de l'Otan, modèle d'un organisme planétaire qui régit les politiques communes de défense.

Forte de 29 pays membres, l'Otan a pour but de gérer les différends de manière pacifique tout en ayant une force de frappe nécessaire constituée des armées de chaque pays membres en cas de gestion de crise. Dans le domaine maritime, l'Otan s'assure une présence continue sur les mers avec les forces navales permanentes (*SNF*) [23] affirmant le statut de grandes puissances maritimes aux forces de l'Alliance qui la compose. Réparties en quatre groupes, elles se composent de bâtiments des pays membres.

Les enjeux maritimes

L'exploitation de la mer

Les espaces maritimes français : des atouts multiples

Depuis les années 1970, on peut évoquer une maritimisation [24] des échanges dans le cadre de l'essor de la mondialisation qui régit dorénavant l'économie mondiale. La France a su ainsi s'insérer dans ce système économique jusqu'à en devenir une des puissances principales. Grâce à ses littoraux métropolitains, ses départements, régions et collectivités d'outre-mer (Drom-Com) la France est présente sur toutes les mers du globe.

En 2018, le secteur maritime français représentait une valeur de 81 Md€ [25]. La France s'impose à l'échelle européenne et mondiale grâce à ses ports. En effet, elle possède les premiers ports européens céréalier (Rouen) et de pêche (Boulogne-sur-Mer). Ainsi, l'actuel Premier ministre Édouard Philippe énonçait deux enjeux majeurs pour la France dans les années à venir concernant les flux maritimes : « analyser, avec les acteurs privés, les évolutions des flux stratégiques », et « adapter notre dispositif à toute nouvelle menace sur les routes existantes ou futures » [26].

L'enjeu juridictionnel : le cas de la pêche

Les États à l'image de la France sont priés de se plier aux conventions internationales qu'ils ratifient afin de s'autoréguler et de limiter les conflits comme celle de Montego Bay, instrument juridique principal du droit maritime international sur lequel nous reviendrons plus tard. En parallèle, en tant que membre de l'UE, la France suit un nombre important d'autres lois supranationales supplémentaires. Cette législation

---

[22] Victor Jean-Christophe, « L'organisation de coopération de Shanghai », *Le Dessous des cartes*, 11 juin 2016 (www.youtube.com/watch?v=-LvsGhCABVQ&t=339s).
[23] Otan, « Les activités maritimes de l'Otan », 6 août 2019 (www.nato.int/cps/fr/natohq/topics_70759.htm).
[24] Cette notion, théorisée en 1979 par Alain Vigarié, désigne une augmentation des échanges par voie maritime.
[25] Philippe Édouard, « Stratégie nationale de sûreté des espaces maritimes », 10 décembre 2019 (www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2019/12/snsem_2019_finale.pdf)
[26] *Ibid*.

lui permet de défendre ses intérêts avec plus de légitimité, car la décision, lors d'un litige, est prise par une institution supérieure du niveau étatique.

Afin d'étayer notre propos, prenons le cas de la pêche que l'UE organise et légifère à l'échelle européenne. La Politique européenne commune de la pêche (PCC), mise en place dès 1983, reprenant le modèle général de la Politique agricole commune (PAC) introduit et développe dès 2013 la notion de « durabilité », favorisant l'accès aux eaux européennes à toutes les flottes communautaires et impose des quotas de pêches [27]. Les infractions font l'objet de sanctions par l'Europe allant jusqu'à la suspension du droit de pêche et l'immobilisation de la flotte.

La France est totalement tributaire de ce type de juridictions internationales. Si l'UE étend théoriquement sa juridiction à toute la ZEE française, elle n'a toutefois que peu de pouvoir face aux pays non-membres dont les habitants pratiquent la Pêche illicite, non déclarée et non réglementée (INN) dans les eaux françaises. Ainsi, une zone ultramarine comme celle du Pacifique Sud doit être protégée par des conventions avec les acteurs régionaux.

L'océan Arctique, futur eldorado minier et autoroute maritime ?

« Bien plus qu'un simple laboratoire de recherche, l'Arctique est aujourd'hui une zone hautement stratégique » affirmait l'actuelle ministre des Armées Florence Parly en 2019 [28]. En effet, si l'Arctique a tout d'abord fasciné les explorateurs et les scientifiques, le contexte actuel de réchauffement climatique captive les acteurs économiques mondiaux. Si les perspectives de nouvelles routes maritimes et d'exploitation d'une importante quantité de minerais suscitent l'intérêt planétaire, il demeure essentiel de nuancer ce discours.

L'Arctique est aujourd'hui au cœur des discussions politiques. L'observation d'images satellites permet de constater que la banquise estivale a perdu 50 % de sa superficie et 75 % de son volume depuis trente ans [29]. Cette fonte intéresse tout particulièrement les acteurs économiques qui voient dans ce phénomène une possibilité d'accroître les rendements du commerce maritime, puisque deux nouvelles routes apparaissent, celle du Nord-Ouest et celle du Nord-Est permettant de diminuer les distances. Néanmoins, cet espace stratégique est à nuancer à cause des contraintes pour la navigation. De fait, les chiffres sont encore très modestes : en 2017, 60 navires sont passés par la route maritime du Nord, contre 84 456 navires par le détroit de Malacca, 17 550 par le canal de Suez et 13 795 par celui de Panama [30]. Bien que les flux dans cette zone soient actuellement minoritaires, l'ouverture d'une route régulière de

---

[27] Ministère de l'agriculture et de l'alimentation, « Quotas de pêche : comment sont-ils fixés ? », 16 décembre 2019 (https://agriculture.gouv.fr/quotas-de-peche-comment-sont-ils-fixes).
[28] Direction générale des relations internationales et de la stratégie du ministère de la Défense (DGRIS), *La France et les nouveaux enjeux stratégiques en Arctique*, ministère des Armées, 2019 (www.defense.gouv.fr/).
[29] Escude-Joffres Camille, « Les régions de l'Arctique entre États et sociétés », *Géoconfluences*, 19 septembre 2019 (http://geoconfluences.ens-lyon.fr/).
[30] Lasserre Frédéric, « La course à l'appropriation des plateaux continentaux arctiques, un mythe à déconstruire », *Géoconfluences*, 18 septembre 2019 (http://geoconfluences.ens-lyon.fr/).

porte-conteneurs en 2025 par l'armateur chinois Cosco et l'initiative chinoise dite des « nouvelles routes de la soie » (*Belt and Road Initiative*) pourraient bien changer la donne.

Rendre la mer plus sûre

La présence continue des États de plus en plus nombreux en mer, c'est-à-dire sur un espace par nature fluide et hypermobile fait du monde maritime un terrain où se mesurent et se confrontent les Nations. La mer en tant que lieu de représentation de la puissance s'observe sur les *Livres blancs* des pays émergents où la mer prend une place de plus en plus forte. Le *Livre blanc* chinois de mai 2015 affirme que « L'idée traditionnelle selon laquelle les enjeux terrestres auraient plus de poids que les enjeux maritimes doit être abandonnée » [31]. Une autre preuve de ce phénomène est la hausse des dépenses militaires mondiales surtout dans le domaine maritime [32].

L'objectif général de l'appropriation de la mer pour les États est la liberté d'action en mer encadrée par un système juridique et une armée afin de protéger leurs flux commerciaux et leurs territoires. Le point spécifique de la revendication et du contrôle des espaces maritimes repose sur l'idée que la mer est un théâtre de projection et de dissuasion. Pour la projection, il y a une continuité entre la force navale et la force terrestre. En effet, avec la mobilité des bâtiments, la portée balistique et la concentration de l'activité humaine dans les zones côtières, 80 % des objectifs stratégiques sur l'ensemble des continents sont à portée d'une projection maritime [33].

Un exemple frappant montrant l'influence de la mer dans les politiques de défense est celui de la Chine [34]. Depuis quelques années, le pays revendique sa souveraineté en mer de Chine dont 80 % de la mer de Chine du Sud. On assiste à la construction d'infrastructures militaires et/ou aéroportuaires sur les îles, notamment les Spratleys, un message de puissance envoyé à ses rivaux. Les litiges liés aux revendications maritimes sont aujourd'hui monnaie courante, notamment en Arctique. En effet, comme nous l'avons vu, le réchauffement climatique a permis l'ouverture de nouvelles routes mais également de découvrir un potentiel de ressources halieutiques. Ce facteur pousse les États riverains de cette zone à savoir la Russie, le Canada, la Norvège, les États-Unis, le Danemark et dans une moindre mesure la Finlande et la Norvège à revendiquer leur souveraineté sur ce nouveau territoire aboutissant parfois à des conflits. De ce fait, le Canada et les États-Unis se disputent une zone maritime en mer de Beaufort, zone riche en hydrocarbures [35].

---

[31] « IV Building and Development of China's Armed Forces », *Chinese White Paper 2014* (http://eng.mod.gov.cn/)
[32] Tian Nan, Fleurant Aude, Kuimova Alexandra, Wezeman Pieter D., Wezeman Siemon T., « Trends in World military expenditure », *SIPRI Fact Sheet*, avril 2019, 11 pages (www.sipri.org/).
[33] *Ibid*.
[34] Letouze Axelle, « Pourquoi la France doit regarder vers la mer de Chine », *Asia Focus* n° 41, Iris, 9 pages (www.iris-france.org/wp-content/uploads/2017/09/Asia-focus-41.pdf).
[35] Loïzzo Clara et Tiano Camille, *L'Arctique, à l'épreuve de la mondialisation et du réchauffement climatique*, Armand Colin, 2019, p. 160.

Faire face aux changements climatiques : un enjeu de défense

La prise en compte du changement climatique dans les politiques de défense nationale est un enjeu des plus actuels. Depuis une quinzaine d'années, on voit émerger les réflexions sur le changement climatique au sein de certains ministères de la Défense. Ce constat à échelle mondiale ne concerne encore qu'une poignée de pays parmi les plus puissants et prospères comme les États-Unis, le Royaume-Uni, la France ou encore l'Australie. Ces réflexions portent sur des enjeux de protection des territoires, la mer étant intrinsèquement liée à certaines conséquences du changement climatique : la montée du niveau de la mer, ainsi que les perturbations atmosphériques (cyclones, ouragans) [36].

La question du changement climatique comme enjeu de défense nationale devient un thème capital, notamment aux États-Unis après l'ouragan Katrina de 2005, qui mit en lumière les vulnérabilités des espaces côtiers nationaux face aux catastrophes climatiques. Du côté de l'hexagone, l'Armée française a commencé plus tardivement à réfléchir sur ces questions, la recherche se structurant officiellement en 2017 avec la création par l'Iris (Institut de relations internationales et stratégiques), de l'Observatoire géopolitique des enjeux des changements climatiques en termes de sécurité et de défense, contrat réalisé pour le compte de la DGRIS.

Le dernier rapport scientifique international sur la « défense-climat » [37] identifie la mise en place d'une coopération internationale efficiente. Dans le cas du Pacifique Sud, on peut ainsi relever l'efficacité de l'accord FRANZ (France, Australie, Nouvelle-Zélande), qui assure la mise en place d'interventions humanitaires d'urgence en cas de catastrophes naturelles dans les États insulaires de la région, par une coordination trilatérale des moyens civils et militaires [38].

Les conflits

Droit de la mer et conflits maritimes

À l'image de ce que nous avons pu apercevoir ci-dessus, le territoire maritime demeure un lieu à forte concentration d'activités humaines avec, d'une part des échanges internationaux qui transitent par la mer, et d'autre part le potentiel des différentes ressources qui se trouvent dans les fonds marins. Toutefois, si la mer est une source d'opportunités elle est aussi une source de menaces avec le développement de la criminalité en mer et des trafics illicites, de la violence, mais surtout les risques de tensions, voire de conflits, liés à la volonté de croissance des États de s'approprier et de maîtriser les routes d'approvisionnements stratégiques.

---

[36] GIEC, *Rapport spécial sur les effets d'un réchauffement climatique de 1,5 °C* (SR15) (https://citoyenspourleclimat.org/).
[37] IMMCS, *The World Climate and Security Report 2020*, février 2020 (www.iris-france.org/).
[38] Groupe interparlementaire d'amitié, *Solidarité Pacifique, la France un partenaire actif* (*rapport* n° 80), 7 février 2008, Sénat (www.senat.fr/ga/ga80/ga8017.html).

La Convention des Nations unies sur le droit de la mer

Afin d'éviter que les États s'approprient des territoires maritimes pour exploiter des ressources, la Convention des Nations unies sur le droit de la mer (CDNUM), appelée aussi Convention de Montego Bay (Jamaïque), donne un cadre juridique international à la gouvernance mondiale de la mer et à l'exploitation des ressources naturelles maritimes. Ce droit international a pour vocation de réguler les conflits. Signée le 10 décembre 1982, elle n'entre en vigueur que le 16 novembre 1994, après ratification ou adhésion de 60 États. Aujourd'hui, 168 États, côtiers ou non, l'ont ratifié. Cette convention est fondée sur cinq principes : paix, souveraineté, liberté, coopération et partage. Ils sont énoncés, pour la plupart, dès le préambule [39]. En outre, la CDNUM a défini et a précisé plusieurs espaces : les eaux territoriales d'un État de 13 milles nautiques ; les ZEE d'une largeur maximale de 200 milles nautiques, où l'État côtier dispose de droits souverains pour l'exploration et l'exploitation du sol et du sous-sol, la gestion et la conservation des ressources ; et enfin, le plateau continental qui comprend les fonds marins et leurs sous-sols au-delà de la mer territoriale jusqu'à 200 nautiques.

La Partie XV [40] de la Convention concerne le règlement des litiges entre les États. Ainsi, elle oblige ces derniers à les résoudre par des moyens pacifiques (article 279) que ce soit les voies juridictionnelles (Cour internationale de Justice à La Haye ou Tribunal international du droit de la mer à Hambourg [41]), les voies non juridictionnelles, les voies contractuelles prisées ou bien par arrangements provisoires entre États. À titre d'exemple, le traité entre l'Australie et le Timor-Leste en 2002 est un arrangement provisoire : il s'agissait de régler la question des droits sur les revenus provenant des gisements gaziers et pétrolifères [42].

Le droit de la mer : source de conflits ?

Si la Convention de Montego Bay est un tournant dans la réglementation des litiges, elle peut, cependant, être difficile à appliquer si ce n'est qu'elle peut être « une nouvelle source de contentieux voire de conflits entre voisins » comme l'exprime Bernard Dujardin, vice-président de l'Institut français de la Mer [43]. En effet, de plus en plus d'États revendiquent une extension de leurs ZEE afin de profiter des ressources halieutiques mais aussi celles, stratégiques, issues du sous-sol. C'est le cas notamment

[39] Convention de Montego Bay, préambule : « Les États Parties à la Convention, […] reconnaissant qu'il est souhaitable d'établir, au moyen de la Convention, compte dûment tenu de la souveraineté de tous les États, un ordre juridique pour les mers et les océans qui facilite les communications internationales et favorise les utilisations pacifiques des mers et des océans, l'utilisation équitable et efficace de leurs ressources, la conservation de leurs ressources biologiques et l'étude, la protection et la préservation du milieu marin, […] » (www.admin.ch/).

[40] Des articles 279 à 299.

[41] Galletti Florence, « Le droit de la mer, régulateur des crises pour le contrôle des espaces et des ressources : quel poids pour des États en développement ? », *Mondes en développement*, n° 154, 2011 (www.cairn.info/).

[42] Cour internationale de Justice : *Affaire relative à des questions concernant la saisie et la détention de certains documents et données (Timor-Leste c. Australie) Mémoire déposé par la République démocratique du Timor-Leste*, vol. I, 28 avril 2014 p. 11 (www.icj-cij.org/files/case-related/156/18699.pdf).

[43] Dujardin Bernard, « Le contentieux de délimitation des droits territoriaux en mer », *La Revue Maritime*, n° 484, février 2009, p. 40-47 (http://ifm.free.fr/htmlpages/pdf/2009/484-4-contentieux-delimitation-en-mer.pdf).

en Extrême-Orient et plus précisément en mers de Chine de l'Est et de Chine méridionale où il y a une diversité des tensions qui concernent les délimitations maritimes, pour la plupart du temps en raison des ressources pétrolifères et gazières [44]. De plus, à la fin de l'année 2019, la Turquie et la Libye ont signé un accord de délimitation maritime le 27 novembre. Cet accord prévoit « que les deux pays se partagent leurs ZEE et les réserves que celles-ci contiennent, notamment en hydrocarbures » [45]. Mais, les ZEE concernées recouvrent en grande partie celle de la Grèce, qui avait commencé à exploiter les ressources en hydrocarbures. Cet accord est d'autant plus intéressant que la Turquie n'est pas membre de la Convention de Montego Bay et que la Libye n'est que signataire et non pas un « État Partie ». En conséquence, la Turquie applique une vision du droit international maritime « coutumier ». Ainsi, le droit de la mer présente des limites dans la mesure où certaines Nations ne sont pas des membres à part entière de la Convention.

La mer, un usage conflictuel entre États

« Celui qui commande sur mer possède un grand pouvoir sur terre ». Cette idée évoquée quatre siècles plus tôt par le cardinal de Richelieu pourrait aussi bien être exprimée par un grand nombre de dirigeants actuels. En effet, la mondialisation, dont l'essor est majoritairement dû aux flux maritimes, a accru l'importance stratégique du milieu maritime et l'a placé comme l'un des épicentres de l'équilibre géopolitique. Les États ayant pour ambition de figurer comme grandes puissances sur l'échelle mondiale perçoivent la mer comme une aire de démonstration de leur force effective et de leur influence, poussant ainsi certaines Nations, qui à l'aube du XX^{e} siècle, n'avaient que peu d'influence sur les mers à redonner une place de premier choix à leur marine au sein de leur politique extérieure.

Tel est le cas de la Russie qui, depuis l'arrivée au pouvoir de Vladimir Poutine, investit dans sa marine pour marquer le renouveau de sa puissance [46]. En parallèle, la marine russe fait son apparition sur des espaces maritimes largement dominés par l'Otan. On assiste, depuis 2016, à un renforcement stratégique en mer Baltique et en Méditerranée grâce à ses accords avec la Syrie et Chypre, leur ouvrant certains ports et lui permettant ainsi une projection navale. Cette présence est avant tout un message envoyé aux forces occidentales, notamment l'Otan, lui signifiant le renouveau de sa marine. La mer est un lieu d'expression de sa puissance qui a pour ambition de contrebalancer celles des forces occidentales et de s'affirmer comme puissance régionale. Cette dernière a pu s'exprimer, notamment en 2015, lorsque sa flotte a tiré des missiles afin de bombarder des bases de l'État islamique en Syrie depuis la mer Caspienne où l'Otan n'officie pas, laissant ainsi à la Russie le champ libre pour s'imposer comme puissance maritime régionale [47].

---

[44] Campagnola François, « Droit de la mer et conflits maritimes en Extrême-Orient [1/2] » (Tribune n° 1093), *RDN*, 4 juin 2019.
[45] Pouvreau Ana, « Les ressorts de l'engagement de la Turquie en Libye », Fondation méditerranéenne d'études stratégiques (FMES), 13 février 2020 (http://fmes-france.org/les-ressorts-de-lengagement-de-la-turquie-en-libye/).
[46] Cervello Manon, *op. cit.*
[47] *Ibid.*

Se confronter, tel est le *credo* des grandes puissances maritimes qui souhaitent asseoir leur position de pouvoir y compris sous l'égide d'organisations multinationales telle que l'Otan, qui par la *SNF* assure une stabilité géopolitique occidentale tout en affirmant le statut de grandes puissances maritimes aux forces de l'Alliance face aux autres États, entre autres, les États-Unis, le Royaume-Uni et la France. Ces trois dernières ont d'ailleurs été, en avril 2018, les acteurs de l'opération *Hamilton* [48]. Appuyée par l'Otan, cette opération aéromaritime avait pour but de frapper trois cibles syriennes où les armes chimiques du régime politique étaient stockées et produites, l'utilisation d'armes chimiques étant condamnée par la communauté internationale.

Les frontières sources de conflits

L'espace maritime est un lieu mobile qui ne peut donc être départagé comme un espace terrestre. Plus qu'un territoire définit en tant qu'« espace délimité, approprié par un individu ou une communauté, sur lequel peut s'exercer l'autorité d'un État ou d'une collectivité » [49], les réflexions actuelles sur le concept de frontières maritimes, suite aux mutations environnementales et les enjeux qui en découlent, mènent à la représentation de l'espace maritime comme « méritoire » [50]. Ce terme, proposé par la géographe Camille Parrain, présente les espaces maritimes comme des « portions d'espaces maritimes, y compris en haute mer, qui font l'objet de délimitation et d'appropriation, mais dont l'appropriation est profondément marquée par les caractéristiques particulières de l'océan dont la principale est l'hypermobilité » [51].

L'Arctique représente autant un enjeu qu'un conflit dans l'espace maritime international. En effet, les États-Unis ont inauguré en 2016 le *NORTHCOM*, un pôle militaire dédié à la défense polaire auquel s'ajoutent 160 sites de l'armée américaine en Alaska [52]. La Norvège a également choisi de faire converger ses forces militaires vers le nord tandis que la Russie demeure le seul pays y possédant une base navale. Le cas de l'Arctique est représentatif des tensions frontalières maritimes et fait écho à d'autres conflits actuels symbolisant la représentation de l'espace maritime au sein du système international économique.

Néanmoins, la remise en cause des frontières peut, dans certains cas, entraîner des guerres commerciales et limiter les échanges économiques et diplomatiques comme on a pu le voir en mer de Chine méridionale depuis 2014. Ainsi, les enjeux économiques et les volontés hégémoniques des grandes puissances face à un monde maritime en mouvement provoquent des conflits que la communauté internationale peine à régler.

---

[48] Madi Naël, « Syrie – Après les frappes contre le régime syrien », Nemrod, 2018 (https://nemrod-ecds.com/?p=1605).
[49] Loïzzo Clara et Tiano Camille, *op. cit*, p.°65.
[50] *Ibid*.
[51] Parrain Camille, « La haute mer, un espace aux frontières de la recherche géographique », *ÉchoGéo*, n° 19, janvier-mars 2012 (https://journals.openedition.org/echogeo/12929).
[52] *Ibid*.

La mer, théâtre de la lutte contre les activités illégales

Combattre le terrorisme et la piraterie, enjeux de la défense maritime

Le terrorisme se définit par une « préparation, un financement, une désinformation, des menaces ou des actes de violence destinés à déstabiliser durablement l'opinion publique pour contraindre un pouvoir et atteindre des objectifs politiques » [53]. Il a, depuis les années 1960, connu une augmentation et un perfectionnement de ses actions dans le milieu maritime. *Al-Qaïda* a ainsi pratiqué, au début des années 2000, du terrorisme stratégique en mer en s'attaquant à l'économie mondiale et plus précisément pétrolière. On peut noter, entre autres, l'attaque en 2002 du pétrolier français *Limburg* aux abords du Yémen qui doit être abandonné, faisant perdre ainsi à la compagnie environ 60 millions de dollars [54]. Les groupes terroristes tirent une partie de leurs financements des activités illégales en mer, tant humaines que matérielles (drogues et vente d'armes).

Si le terrorisme, mode d'action aux visées politiques, et la piraterie, marquée par la recherche d'un profit financier, rentrent parfois en collision, ils demeurent deux phénomènes distincts aux dynamiques propres. Les actes de piraterie ont connu un retour en force depuis les années 1990. Les pirates prolifèrent dans des régions instables économiquement et politiquement, et sont de ce fait principalement recrutés parmi une population côtière pauvre et sans perspective. Ils opèrent dans des zones à fort trafic maritime et notamment dans les approches portuaires et détroits [55].

La mer des Caraïbes fait face à une forte augmentation des actes de piraterie et de brigandage maritimes depuis 2015, avec 135 événements enregistrés au cours de l'année 2019. La lutte contre la piraterie revêt un caractère international et nécessite une approche globale du phénomène, et doit permettre d'instaurer un « *continuum* de sécurité terre-mer » [56].

Lutter contre les flux illicites

Flux logistiques par excellence, les routes maritimes sont utilisées par les acteurs de l'économie parallèle pour transporter des cargaisons illicites, notamment le trafic de drogue. D'après le *think tank* Center for International Maritime Security, 90 % de la cocaïne sud-américaine transite par voie maritime. La richesse de certains réseaux criminels est mesurable aux moyens qu'ils mettent en œuvre, et le cas des sous-marins artisanaux des cartels sud-américains est en ce sens frappant. Face à cette menace, la coopération internationale reste la réponse la plus efficace. Elle se matérialise par le partage de renseignement au sein de plateformes spécialisées tel que le Centre de

---

[53] Eudeline Hugues, « Le terrorisme maritime contemporain », *Stratégique*, 2012/2, n° 100-101, p. 269-304.
[54] Eudeline Hugues, « Terrorisme maritime et piraterie d'aujourd'hui : les risques d'une collusion contre-nature », *ÉchoGéo*, vol. 10/2009, septembre 2009 (https://journals.openedition.org/echogeo/11405).
[55] Carnimeo Nicolo et Guglielmo Matteo, « Qui sont les pirates somaliens ? », *Outre-Terre*, 2010/2-3, n° 25-26, p. 413-425.
[56] Ministère des Armées, « La sécurité des espaces maritimes dans le Golfe de Guinée », 15 février 2019, (www.defense.gouv.fr/).

coordination de la lutte antidrogue en Méditerranée (CECLAD-M, basé à Nanterre) ou encore Frontex pour surveiller les frontières extérieures de l'UE [57].

Le trafic d'armes est aussi l'un des plus lucratifs proliférant sur mer. La faillite des États, comme ceux de l'Union soviétique ou plus récemment la Libye, a mis sur le marché noir d'importants stocks d'armements classiques. Le poids politique de ce trafic pèse dans l'équilibre géopolitique puisqu'il est directement responsable de la déstabilisation de plusieurs régions du globe.

Enfin, la mer est le théâtre d'importants trafics d'êtres humains orchestrés par des réseaux criminels. Porte d'entrée vers l'Europe, la Méditerranée a acquis un regain d'intérêt en 2015 à la faveur de l'afflux de migrants issus des pays situés au Sud et à l'Est du bassin méditerranéen. Cette crise migratoire a ainsi imposé à l'Europe un important défi sécuritaire et humanitaire. Sur mer, l'action de l'UE s'est matérialisée par plusieurs opérations de sauvetage de migrants et de surveillance de l'activité des passeurs. Il en est ainsi des opérations *Triton* (2014-2018) et *Themis* (2018) menées par Frontex, ainsi que de l'opération *Sophia* (2015-2020) menée par la force navale européenne [58]. Cependant, depuis fin 2018, on observe sur tout le couloir de la Manche une augmentation des traversées par l'utilisation directe de moyens nautiques (*via* des passeurs ou des embarcations volées), obligeant les autorités franco-britanniques à multiplier les sauvetages [59].

⁂

La mer est ainsi un lieu d'alliance et de confrontation pour les États qui cherchent tous, à leur échelle, à s'intégrer dans le jeu des puissances maritimes. L'enjeu est important puisque la mer est centrale pour l'économie mondiale et demeure une source de richesse en expansion aux vues des bouleversements climatiques. Ces « méritoires » cristallisent donc des conflits que la communauté internationale s'efforce de résoudre par la défense et par le droit. Moteur de la mondialisation, la communauté internationale est dépendante de ce milieu puisqu'elle lui assure puissance et richesse, elle est également garante des échanges matériels mais aussi, comme le démontre notre étude de cas, immatériels à l'image de l'importance des câbles sous-marins.

[57] Premier ministre, *op. cit.*, voir note 24.
[58] « Saving life at sea and targeting criminal networks », *Consilium.europa*, 30 septembre 2019 (www.consilium.europa.eu/en/policies/migratory-pressures/sea-criminal-networks/).
[59] *AFP*, « 2 500 migrants secourus dans la Manche en 2019, soit quatre fois plus qu'en 2018 », *RTL*, 1er janvier 2020 (www.rtl.fr/).

Étude de cas : les câbles sous-marins

Les câbles sous-marins : de biens communs mondiaux à infrastructures critiques

Des vecteurs physiques de l'information

« L'épine dorsale de l'économie numérique »
(Camille Morel)

Les enjeux économiques soulevés par les câbles sous-marins, dans un monde où le numérique fait partie intégrante du quotidien, sont de première importance. Le transit des informations intercontinentales dépend à 90 % des câbles sous-marins. Ainsi, les pertes économiques en cas de dysfonctionnement ou de rupture de câbles peuvent être considérables. Cependant, la diversité des opérateurs permet à un État d'éviter une vulnérabilité en cas de rupture subite de son accès à *Internet*. L'Australie estime que les cinq câbles sous-marins qui la relient au réseau mondial sont un « enjeu vital » et que leur rupture provoquerait des pertes estimées à 152 millions de dollars par jour, d'après des estimations fournies par l'Asia Pacific Economic Cooperation (APEC). De même, le tremblement de terre de 2006 qui détériora plusieurs câbles dans le sud de Taïwan provoque un blocage temporaire de l'économie dans cette région et la coupure de 120 M de lignes téléphoniques. Ces exemples prouvent que les pertes occasionnées par une rupture, même brève, d'*Internet* peuvent être très importantes.

Aujourd'hui, les investissements demeurent polarisés par les pays développés (les Gafam [60]) mais de nouveaux acteurs chinois émergent (les BATX [61]). Les Gafam sont rapidement devenues des bailleurs de premier plan dans le secteur des câbles. En 2015, ils représentaient environ 5 % des parts de marché dans la zone de l'Atlantique Nord, où le trafic est le plus intense. Aujourd'hui, ils captent un tiers du marché des câbles et les projections établissent que, d'ici la décennie 2020, ils pourraient représenter jusqu'à 90 % des parts de marché [62] ! De même, la part des États dans les investissements demeure modérée, à 10 % environ depuis 2010. Le marché des câbles marque donc le lent retrait des États au profit d'acteurs privés, bien que ces derniers entretiennent des liens avec les autorités gouvernementales.

Du fait qu'ils aient acquis une importance économique et stratégique de premier plan, les câbles sous-marins soulèvent des enjeux de souveraineté et de gouvernance mondiale. Les acteurs chinois créent un nouveau sentiment d'incertitude dans

(60) Google, Amazon, Facebook, Apple, Microsoft.
(61) Baidu, Alibaba, Tencent, Xiaomi.
(62) Gradt Jean-Michel, « *Internet*, la lutte pour la suprématie se joue sous les océans », *Les Échos*, 8 avril 2019 (www.lesechos.fr/tech-medias/hightech/internet-la-lutte-pour-la-suprematie-se-joue-sous-les-oceans-1007151).

le secteur des câbles, qui reflète les tensions géopolitiques déjà existantes et les menaces d'espionnage ou de guerre hybride exacerbées. Le continent africain est le terrain d'un affrontement entre les entreprises occidentales et les nouvelles venues dans le marché des câbles sous-marins. En effet, les acteurs américains ou encore chinois déploient de très nombreux projets de câbles dans cette région longtemps mal desservie par *Internet*. Facebook a annoncé, en avril 2019, le projet du câble *Simba*, qui vise à encercler le continent avec un câble utilisant des points d'accès déjà existant sur les côtes Ouest, Est et Nord [63]. La société chinoise Hengtong, quant à elle, est partie prenante d'un projet de câble qui va relier, d'ici 2020, le Pakistan, Djibouti, le Kenya, l'Égypte et la France. Baptisé PEACE (Pakistan and East Africa Connecting Europe), ce câble doit fournir aux géants chinois d'*Internet* un moyen de commercialiser leurs services sur le Vieux Continent et en Afrique, et aussi de concurrencer leurs grands rivaux américains du Gafam. La croissance soutenue de ces nouveaux entrants s'explique par le coût moindre de leurs infrastructures par rapport à leurs concurrents occidentaux.

La concurrence des entreprises dans le secteur des câbles fait donc apparaître les tensions géopolitiques qui incitent les États à lancer un certain nombre de dispositifs pour se prémunir de l'hostilité d'acteurs étrangers pouvant mener des activités de renseignement. Le gouvernement japonais, *via* un fonds public-privé « Corporation for the Overseas Development of Japan's ICT and Postal Services » (JICT), tente d'endiguer la montée en puissance d'entreprises chinoises telles que Huawei Marine Networks, et met à disposition de grandes entreprises japonaises du secteur des télécommunications toute une série de mesures d'accompagnement afin de stimuler leurs exportations.

Par d'autres vecteurs, les États-Unis multiplient les initiatives afin de ralentir la progression des acteurs chinois du secteur, par exemple en s'appuyant sur une loi dans le droit chinois qui contraint les entreprises du secteur des télécommunications à transmettre leurs données directement auprès des instances gouvernementales (ce que les États-Unis font par ailleurs, voir *infra*). En 2013, l'Administration américaine empêche la construction d'un nouveau câble transatlantique reliant New York à Londres par l'entreprise Huawei [64].

Des enjeux de souveraineté et de gouvernance mondiale

La maîtrise de la chaîne de production des câbles par des entreprises nationales permet de disposer d'une capacité d'écoute des informations qui entrent et sortent de son territoire et donc de protéger ses intérêts économiques ou encore militaires. De même, des liaisons diversifiées lui permettent de ne pas faire transiter une trop grande part de son information vers un territoire pouvant mener des activités hostiles, comme des activités d'espionnage industriel. Les câbles revêtent donc des enjeux de souveraineté auxquels il est nécessaire d'apposer des institutions capables de réguler le secteur.

---

[63] FitzGerald Drew, « Facebook looks to build underwater ring around Africa », *The Wall Street Journal*, 7 avril 2019.
[64] Manière Pierre, « Câble sous-marins, Huawei jette l'éponge », *La Tribune*, 4 juin 2019 (www.latribune.fr/).

Politique française

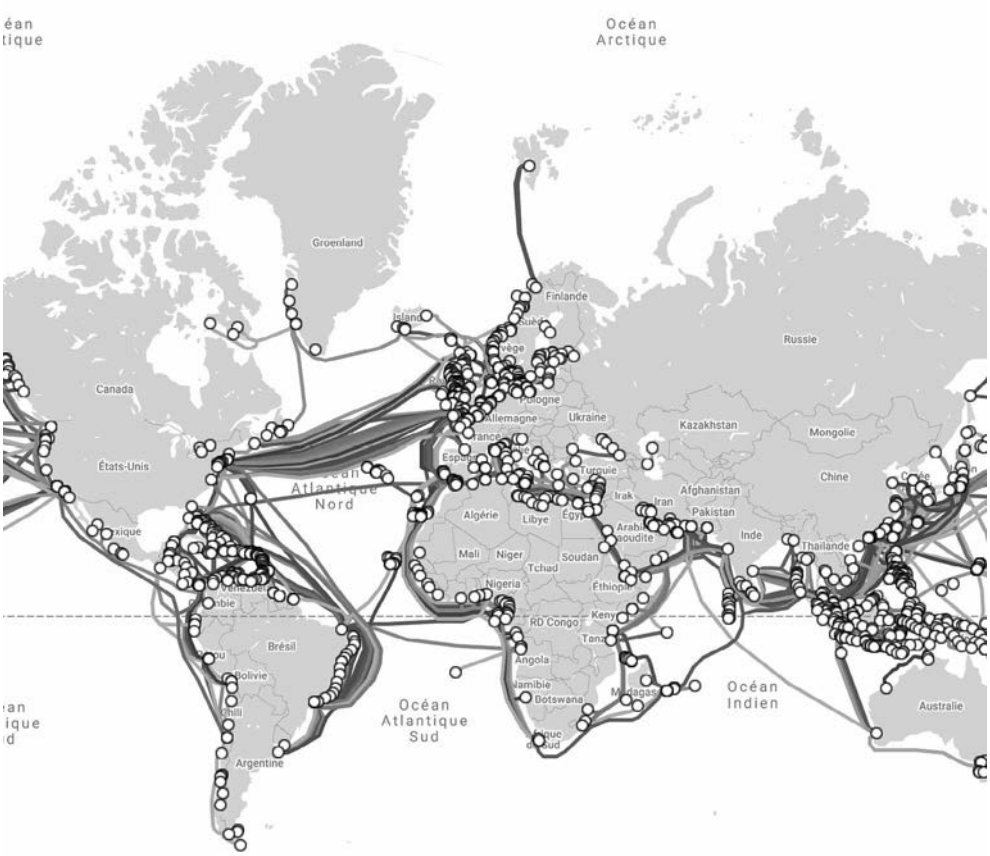
Dans le domaine des câbles, la France dispose de fleurons industriels dans la pose et la maintenance des câbles. Des entreprises opèrent très activement dans ce domaine, à commencer par Louis-Dreyfus Armateur, disposant d'une flotte de six navires câbliers et travaillant pour le compte de la société Alcatel, ou encore Orange Marine Networks, disposant, elle aussi, de six câbliers. Or, Alcatel Submarine Networks était jusqu'en 2015 une filiale d'Alcatel, géant français du secteur des télécommunications. Cependant, suite à son rachat par le finlandais Nokia en 2015, la filiale ASN est également absorbée par le groupe finlandais. Or par son importance et sa taille, ASN est considérée en tant qu'Opérateur d'importance vitale (OIV) au sens du Code français de la défense. Cela signifie qu'elle constitue une priorité pour les services de renseignements français, qui suivent attentivement, de concert avec Bercy, tout rachat d'ASN par un acteur étranger. Les autorités disposent d'un droit de regard si une autre proposition de rachat de la part d'un acteur étranger advenait.

En France, les câbles rentrent dans la catégorie des « points d'importance vitale » que le Secrétariat général de la défense et de la sécurité nationale (SGDSN) définit comme « des établissements, ouvrages ou installations qui fournissent les services et les biens indispensables à la vie de la Nation » [(65)]. Il revient au SGDSN de piloter la politique de sécurité et activités d'importance vitale (SAIV), de sorte à assurer la résilience de ces infrastructures critiques. La protection des câbles comme toute infrastructure critique, se fonde sur un dialogue permanent entre l'État et les opérateurs publics responsables de l'installation, de l'entretien et de la protection des infrastructures critiques. En vertu du Code de la défense [(66)], les opérateurs sont tenus de mettre en place des plans de protection approuvés par l'autorité administrative. Dans le cas des câbles sous-marins, ce sont les entreprises privées telles qu'Orange Marine et Alcatel Submarine Network qui assurent la surveillance des installations. En outre, l'État y participe directement par le biais de la Marine nationale. Ainsi, celle-ci garantit la protection des câbliers dans les eaux territoriales françaises et, sur ordre du préfet maritime, un contrôle des installations peut être effectué.

Politique américaine

Les États-Unis occupent une place centrale dans le domaine des câbles sous-marins lui permettant de surveiller en masse les communications et les échanges de données. Presque la totalité des câbles reliant le continent américain aux autres continents passent par les stations de contrôle situées sur le territoire américain : les câbles en direction de l'Asie du Sud-Est par l'océan Pacifique passent tous par des stations de contrôle de la côte ouest américaine ainsi que par Hawaï ; à l'Est, actuellement, il n'existe que deux câbles ne passant pas par le territoire américain reliant l'Amérique latine à l'Afrique. La *National Security Agency* (*NSA*) peut donc collecter des données

(65) *Sécurité & Défense Magazine*, « La sécurité des activités d'importance vitale », 26 juin 2017 (https://sd-magazine.com/).
(66) L. 1332-1 à L. 1332-7 : c'est-à-dire l'intégralité du Chapitre II (« Protection des installations d'importance vitale ») : « Section 1 : Dispositions générales », « Section 2 : Dispositions spécifiques à la sécurité des systèmes d'information » et « Section 3 : Dispositions pénales » (www.legifrance.gouv.fr/).



Carte des câbles sous-marins, source : TELEGEOGRAPHY, « Submarine Cable Map » (www.submarinecablemap.com/).

entrantes et sortantes du territoire américain et ce depuis le territoire national, lui permettant de travailler dans un cadre juridique validant ses actions sans devoir prendre les risques auxquels elle devrait faire face hors du territoire.

Les États-Unis disposent également de divers moyens leur permettant de s'assurer du contrôle des câbles. Premièrement, ils possèdent de grands groupes télécoms qui ont participé à la construction de certains câbles et qui peuvent donc peser dans les prises de décision internationales, même s'il existe depuis 2000 le *Regulation of Investigatory Powers Act* [67] qui oblige les entreprises du programme *Tempora* à collaborer avec les autorités britanniques. Les États-Unis bénéficient aussi des services de la *Team Telecom* composée de juristes dépendants du *Federal Bureau of Investigation* (*FBI*) et du *Department of Justice* (*DoJ*). Le but de cette équipe est d'empêcher la prise

[67] Regulation of Investigatory Powers Act 2000 (www.legislation.gov.uk/ukpga/2000/23/contents).

de contrôle des câbles par des grands groupes ou des gouvernements étrangers. Pour bien opérer, elle emploie deux outils :

– le *Network Security Agreement*, un accord contraignant les entreprises américaines à mettre en place un système qui permet aux agences de renseignement d'accéder aux données circulant sur les câbles lorsqu'ils le demandent.

– la *Federal Communications Commission* (*FCC*) qui doit accorder une licence validant le début de chaque projet, ce qui permet à la *Team Telecom* de profiter de ce temps pour mettre en place des accords de sécurité coercitifs avec les participants du projet. S'ils refusent, la *FCC* peut leur refuser à son tour la licence.

Les câbles sous-marins : de la dépendance à la vulnérabilité

Menaces étatiques : guerres hybrides (renseignement/espionnage et cyberattaque)

S'il existe des menaces naturelles ou accidentelles qui interfèrent dans le fonctionnement des câbles sous-marins (filets de pêches, ancres de navires, séismes, corrosion…) [68], d'autres types de menaces, cette fois intentionnelles, peuvent perturber l'activité des câbles en haute mer. Ainsi, le système câblier sous-marin est une cible privilégiée pour des actes de malveillance, physiques ou cyber, qui démontrent sa vulnérabilité. Cette dernière dévoile des rivalités entre les États concernant leur gestion (activité, maintenance, sécurité).

Les États ont, en effet, à l'origine, le monopole de la gestion des coupures ou ruptures de câbles, instrument de pouvoir majeur employé notamment en temps de guerre afin de paralyser l'ennemi. L'exemple canonique du « télégramme Zimmerman » [69] (1917) en témoigne. Par conséquent, les États cherchent à se prémunir des menaces des autres États à l'aide de pratiques qui relèvent de la guerre hybride, comme le renseignement ou les cyberattaques [70]. Ainsi, le virus *Stuxnet* [71], apparu en 2010, fut la cause d'un dysfonctionnement du programme nucléaire iranien : cette opération est suspectée d'être le fruit de la coopération entre la *NSA* et l'unité 8200 (unité de renseignement d'origine électromagnétique de *Thasal*, l'armée israélienne).

De plus, on observe un resserrement des liens entretenus entre acteurs privés et étatiques, et notamment dans le domaine du renseignement. Dans un contexte où l'intelligence économique a acquis une dimension fondamentale, les câbles sous-marins, en tant que vecteur de transmission des métadonnées mondiales, constituent des infrastructures capitales que les États emploient pour mener des activités d'espionnage ou de contre-espionnage. L'espionnage montre l'enjeu, longtemps sous-estimé, des

---

[68] Morel Camille, « Menace sous les mers : les vulnérabilités du système câblier mondial », *Hérodote*, vol. 163, n° 4, 2016, p. 33-43 (www.cairn.info/revue-herodote-2016-4-page-33.htm).

[69] L'interception par les câbles sous-marins du télégramme du ministre des Affaires étrangères allemandes à l'ambassadeur d'Allemagne au Mexique est un scandale majeur dont le message précipite la déclaration de guerre américaine.

[70] Becker Cyrille, « La sécurité physique menacée par les cyberattaques étatiques », *Les Échos*, 28 février 2019.

[71] Untersinger Martin, « *Stuxnet* : comment les États-Unis et Israël ont piraté le nucléaire iranien », *L'Obs* avec *Rue 89*, 17 novembre 2016 (www.nouvelobs.com/).

câbles sous-marins et en même temps leur vulnérabilité. En 2013, les révélations d'Edward Snowden (*CIA*) [72] sur la *NSA* dévoilent au monde la stratégie de surveillance massive par le renseignement américain, à commencer par l'espionnage des câbles sous-marins de télécommunications intercontinentales reliant les États-Unis à l'Europe (projet *Tempora*).

Aussi, la problématique du contrôle des données par les services de renseignement soulève la fragilité de la frontière entre intérêts publics (sécurité collective, protection des données, protection du territoire) et privé (confidentialité de données stratégiques ou sensibles par exemple). Le fait que de nombreux opérateurs téléphoniques soient liés directement ou indirectement avec des acteurs étatiques donne donc lieu à des accords intergouvernementaux de renseignement. Ce fait montre que la protection des données personnelles peut être mise en second plan au bénéfice de prérogatives régaliennes. Par exemple, l'*Australian Signals Directorate*, branche des services de renseignements australiens en matière de sécurité électronique, a signé un certain nombre d'accords avec des gouvernements étrangers tels que Singapour afin de contrôler les données qui transitent par câble.

Menaces non-étatiques : terrorisme et criminalité

L'augmentation croissante des activités industrielles en mer et la plus grande liberté d'y circuler ainsi que le développement des technologies simplifiant la navigation et des moyens de télécommunications en haute mer ont fait du milieu maritime une zone attractive pour y exercer des activités malveillantes. Le terrorisme a trouvé une cible stratégique dans les infrastructures maritimes qu'elles soient pétrolières ou de télécommunications : en voyant des complots d'*Al-Qaïda* ciblant l'*Internet* britannique en 2007 dans un local considérablement mieux protégé que de nombreux câbles sous-marins [73], il ne faudrait pas rejeter la possibilité d'attaques de tels groupes à ces câbles. Les câbles sous-marins sont particulièrement à risque puisqu'ils représentent 99 % des flux d'information [74]. D'autres menaces pèsent sur le milieu maritime, en particulier avec l'automatisation et l'informatisation croissante des systèmes à grande échelle, qui placent les câbles sous-marins dans la ligne de mire des cyberattaques. Les conséquences d'un tel acte pourraient être particulièrement fortes : sur la terre comme sur la mer, les câbles sont employés pour la transmission des télécommunications et au transfert de l'énergie. Le 23 décembre 2015, des *hackers* sont parvenus à pirater le réseau électrique ukrainien ce qui a eu pour conséquence de couper l'électricité d'une partie de l'Ukraine [75] : ce schéma pourrait parfaitement se reproduire si des pirates informatiques visaient l'infrastructure sous-marine.

---

[72] Greenwald Glenn, « L'affaire Snowden racontée par celui qui l'a révélée », *Le Monde*, 13 mai 2014 (www.lemonde.fr/).
[73] Leppard David, « Al Qaeda Plot to Bring down UK Internet », *The Sunday Times*, 16 mars 2010 (www.thetimes.co.uk/article/al-qaeda-plot-to-bring-down-uk-internet-b8vb32twcwt).
[74] Eudeline Hugues, « Le terrorisme maritime, une menace réelle pour la stabilité mondiale », *Hérodote*, vol. 163, n° 4, 2016, p. 9-31 (www.cairn.info/revue-herodote-2016-4-page-9.htm).
[75] Siboni Gabi et Magen Zvi, « The Cyber-Attack on The Ukrainian Electrical Infrastructure: Another Warning », *INSS Insight* (*The Institute for National Security Studies*) n° 798, 2016 (www.inss.org.il/).

Le milieu maritime possède cependant l'avantage d'avoir des barrières naturelles qui représentaient déjà des limites aux possibilités d'attaque, mais les câbles sous-marins représentent un cas particulier puisqu'ils relient la mer à la terre : les câbles sont installés sous l'eau dans les profondeurs mais doivent également être ramenés à la surface et rejoignent donc une station d'atterrissement. Ces stations sont bien plus accessibles que les câbles posés en profondeur, et peuvent donc subir différentes attaques : sabotages des équipements, explosifs, assaut sur le bâtiment, interruption du courant, piratage des systèmes informatiques… Un rapport de la *Protective Security Division of US* datant de 2004 [76] évoque les différents éléments expliquant pourquoi les stations d'atterrissement risquent une action terroriste : il y a, aux États-Unis, un manque de diversité de ces stations, ce qui conduit à une concentration importante des câbles au même endroit, dans un bâtiment qui présente une certaine facilité d'action. En plus d'être plus accessibles, les atteindre permettrait un résultat efficace et pluriel parce que cela toucherait tous les câbles présents dans la station.

Il y a également des endommagements sur les câbles causés non pas pour les atteindre directement mais plutôt pour en prélever certains éléments afin de les revendre : en 2007, des pêcheurs vietnamiens ont sectionné environ 500 kilomètres de câbles sous-marins afin d'y récupérer des matériaux composites pour les revendre illégalement. En conséquence, le Vietnam a perdu plus de 80 % de sa connectivité avec le reste du monde [77]. Il y a donc au final un large panel de menaces non-étatiques desquelles les infrastructures doivent être protégées : auparavant, les actions malveillantes recensées étaient plutôt d'origine étatique car opérer en milieu maritime profond nécessite de posséder des matériaux coûteux ; mais le progrès de la technologie avec de nouveaux moyens permettant de manipuler les fils de fibre optique à distance ainsi qu'une commercialisation croissante de ces outils ont ouvert de nouvelles voies aux activités illégales.

⁂

Les câbles sous-marins sont alors employés comme outils indispensables à l'évolution de la technologie de communication mais sont aussi instrumentalisés par des acteurs étatiques et non-étatiques pour des fins différentes que ce qui était prévu. Ces outils regroupent les intérêts des sphères du public et du privé, et relèvent alors de nouveaux défis.

* * * * *

Ainsi par ce travail de recherche, nous avons pu constater que les nouvelles frontières de la défense évoluent au fil du temps. La mer, comme nous l'avons vu, joue un

[76] US Department of Homeland Security, Prospective Security Division, *Potential Indicators of Terrorist Activity Infrastructure Category*: *Cable Landing Stations, Draft Version 1*, 30 janvier 2004, 19 pages (https://info.publicintelligence.net/DHS-UCL-PI.pdf).
[77] Morel Camille, *op. cit*.

rôle essentiel dans la stratégie de défense. Cependant, avec les avancées technologiques et l'apparition d'acteurs internationaux inédits sont survenues de nouvelles aires d'intérêts et de conflictualité dont l'Espace. Cette nouvelle sphère survient avec plusieurs avantages mais crée aussi de nouveaux enjeux : passant d'une ère où les attaques et défenses étaient majoritairement palpables à une période où les attaques sont moins proches et tangibles. L'avènement de l'Espace présente aussi une nouvelle opportunité pour chaque État afin d'y imposer son hégémonie ou du moins d'y étendre sa zone d'influence. ◆

L'Espace : entre dissolution et multiplication des frontières

Marcello Putortì et Hawa-Léa Sougouna (coordinateurs),
Yanis Amae Benabdallah, Théo Brunet, Pierre-Marie Bujadoux,
Camille Faghel, Esteban Fagniez, Yanis Fekrache, Robinson Gouhier,
Brahimi Hadjer, Sarah Hambec, Louis Lafaurie, Sophie Schönube,
Pacôme Sebastien, Tristan Tellier et Pauline Verger

Le rapport de la défense à l'Espace extra-atmosphérique est celui d'un phénomène social constamment altéré et réajusté par ses acteurs lui dictant en retour des enjeux nouveaux.

En ce sens, l'Espace n'est pas simplement un nouveau milieu de confrontations et d'affrontements militaires, mais bien plus un nouveau champ normatif de la défense. Par sa géographie d'abord, l'Espace extra-atmosphérique n'est pas naturellement délimité [(1)] par rapport à l'espace aérien, faisant de lui un milieu distinct de la défense. Par sa logique ensuite, l'Espace peut tantôt être considéré comme le lieu de confrontation en soi pour des ressources [(2)] ou comme possession [(3)], ou encore pour l'emplacement stratégique dont il dispose [(4)], mais également comme point d'appui nécessaire au déroulement d'opérations terrestres et maritimes [(5)]. Enfin, tant comme centre de l'attention que comme périphérie incontournable, l'Espace se fait donc à la fois moyen et finalité de l'attention militaire.

---

(1) Il est généralement estimé entre 80 et 100 km (ligne Karman) au-dessus du niveau de l'océan. Il n'existe aujourd'hui pas de consensus juridique pour la délimitation de l'Espace extra-atmosphérique. Pour les débats en cours se rapporter au « Projet de rapport du comité des utilisations pacifiques de l'Espace extra-atmosphérique de l'Assemblée générale des Nations unies », Vienne, 27 mars-7 avril 2017 (www.unoosa.org/).

(2) Malgré l'article 11 § 1 du Traité de l'Espace (www.unoosa.org/pdf/publications/STSPACE11F.pdf), régissant les activités des États sur la Lune et les autres corps célestes : « La Lune et ses ressources naturelles constituent le patrimoine commun de l'humanité, qui trouve son expression dans les dispositions pertinentes du présent accord, en particulier le § 5 du présent article. » La question de l'exploitation des ressources dans l'Espace est volontairement évacuée dans le § 5 du même article. « Les États parties au présent accord s'engagent à établir un régime international, y compris des procédures appropriées, régissant l'exploitation des ressources naturelles de la Lune lorsque cette exploitation sera sur le point de devenir possible. La disposition qui précède sera appliquée conformément à l'article 18 du présent accord. ». Les États-Unis, en 2015, puis le Duché du Luxembourg, en 2017, autorisèrent même explicitement par leurs législations respectives, l'exploitation à des fins commerciales des corps célestes.

(3) « L'univers est un océan, la Lune est comme les îles Diaoyu, Mars comme l'île d'Huangyan [îles qui font l'objet d'un conflit territorial dans la mer de Chine]. Si nous n'y allons pas maintenant, alors que nous en sommes capables, nos descendants nous le reprocheront. Si d'autres que nous y vont, ils vont s'en emparer et vous ne pourrez plus y aller, même si vous le voulez. C'est une raison suffisante. » Déclaration de Ye Pejian à un journaliste lors de la session plénière annuelle du Parti communiste chinois en 2017 (www.thedailybeast.com/chinas-looming-land-grab-in-outer-space?ref=scroll).

(4) Intérêt particulièrement mis en exergue dans l'étude de cas notamment en ce qui concerne l'analyse de l'affaire *Luch-Olymp*, de 2017.

(5) Zajec Olivier, « L'Espace extra-atmosphérique : l'enjeu de la surveillance spatiale », *Stratégique*, vol. 120, n° 3, 2018, p. 201-205.

Les balbutiements technologiques de l'humanité, qui ne dispose d'un accès continu à l'Espace que depuis 63 ans [6], réduisent considérablement la capacité de projection, autant qu'ils promettent un immense potentiel de développement. Seulement, ces difficultés se superposent à des tendances inhérentes à la défense. L'affaiblissement de l'État, l'apparition de nouveaux acteurs du domaine de la défense, la centralité croissante des enjeux industriels, et plus largement économiques, dans les orientations stratégiques et enfin la recomposition accélérée des menaces, ne sont pas des phénomènes propres à l'Espace mais ils structurent directement le rapport de la défense à celui-ci. L'Espace n'est pas seulement une nouvelle frontière de la défense, mais bien un nouveau phénomène de la défense, bouleversant celle-ci et absorbant ses altérations.

L'objet de cette recherche est de saisir l'état et les dynamiques de cette interaction entre l'Espace et la défense. Nous chercherons à établir que ce nouveau milieu est en fait le terrain privilégié d'une poignée d'acteurs hégémoniques. Mais cet avantage des puissants n'est pas tant un principe conservateur, que l'expression parallèle d'une redéfinition du rôle étatique de la défense, qui doit relever le défi croissant de l'internalisation des enjeux économiques dans la pensée stratégique. Ce principe veut que l'Espace, plus que tout autre milieu, impose à la défense de se projeter au-delà de son domaine propre et implique également d'analyser les interactions entre stratégie et régulation juridique des rapports, l'Espace ayant la spécificité d'être l'un des rares milieux dont le régime juridique reste à définir.

Des enjeux globaux saisis par une poignée d'acteurs à l'hégémonie contestée

Un Espace convoité par tous, à la portée de quelques-uns

L'Espace est un champ de confrontations et d'affrontements relativement nouveau. Comme tout autre champ revêtant d'intérêts stratégiques, les puissances capables de « jouer dans la cour des grands » [7], se distinguent de celles n'ayant pas acquis la technologie et les savoir-faire de projection et d'activité dans l'Espace.

L'Espace est donc un attribut symbolique de puissance [8], dont l'accès fut élargi progressivement, menaçant à chaque fois l'oligopole ou le « club » des puissances spatiales installées [9]. Cependant, si une poignée d'acteurs, toujours plus nombreux, se hissent au rang de puissance, les enjeux concernant la maîtrise extra-atmosphérique demeurent globaux [10]. Ainsi, le projet des constellations [11] vise à constituer des réseaux

---

[6] Le 4 octobre 1957, *Spoutnik* fut le premier engin artificiel envoyé en orbite autour de la Terre.

[7] Expression de Charles de Gaulle paraphrasée par le président du Centre national d'étude spatiale (Cnes) Jean-Yves Le Gall, *CNES-Mag*, n° 79, février 2019, p. 5 (https://fr.calameo.com/read/000015639bf4131d231dc).

[8] Liukkonen Juha-Matti, Sauzay Arthur et Straube Sebastian, « Espace : le réveil de l'Europe ? », *Note*, février 2020, Institut Montaigne, p. 9 (www.institutmontaigne.org/).

[9] Mauduit Jean-Christophe, *Collaboration around the International Space Station: science for diplomacy and its implication for US-Russia and China relations*, 2017, p. 2.

[10] L'anglicisme *global* tiré du substantif *globalization*, sera utilisé à dessein pour souligner l'étroit rapport des enjeux de l'Espace avec ceux de la mondialisation dépassant le seul cadre international au sens d'interétatique. Ces rapports constitueront particulièrement l'objet de la partie II, A.

de milliers de satellites afin de fournir des accès augmentés à *Internet* avec l'ambition de concurrencer les infrastructures terrestres [12]. L'accès *Internet* peut sembler anecdotique et essentiellement économique, cependant les effets de telles installations, en termes de compétitivité et d'usages militaires ultérieurs, quant aux informations drainées par ces réseaux, font de l'Espace le domaine, encore restreint, de quelques-uns alors qu'il concentre les intérêts de tous.

Cette asymétrie entre les intérêts et l'accès fonde le statut d'oligopole contesté de l'Espace. Seulement, l'horizontalisation de l'accès à l'Espace nécessite un rattrapage abyssal et des moyens colossaux pour les nouveaux venus, souhaitant s'y faire une place. À titre de comparaison, le Pentagone, la *National Aeronautics and Space Administration* (*NASA*) et l'*US Air Force*, comptent investir, ensemble, 60 milliards de dollars dans la politique spatiale en 2020, quand la France, bien que considérée comme grande puissance spatiale [13], ne consacre à elle seule que 1,3 Md d'euros pour cette année [14].

Pourtant des puissances, il y a quelques années encore absentes de l'Espace, montrent aujourd'hui d'ambitieux programmes spatiaux : l'Iran en 2009 et la République populaire démocratique de Corée (RPDC) en 2012 se sont montrés capables d'opérer des lancements et d'être ainsi présents dans le paysage extra-atmosphérique, stimulant des concurrents régionaux à faire de même ou à augmenter leur propre budget en la matière. De 2003 à 2013, le nombre de pays accordant des budgets compris entre 10 et 100 Md$ a triplé, croissant de 10 à 30. Cette tendance semble par ailleurs exponentielle, car ces pays seraient au nombre de 52 en 2014 [15].

Or, il est fondamental d'insister sur le caractère particulièrement prégnant de « l'incertitude de toutes les données » [16], en ce qui concerne le rapport de la défense à l'Espace. En effet, ces financements ne sont pas tous explicitement destinés à un usage militaire. Cependant, la porosité entre enjeux civils et militaires, et la facilité avec laquelle un outil peut basculer d'un usage à l'autre, fonde une corrélation entre accroissement de l'accès à l'Espace, y compris pour des usages civils, et accroissement des enjeux de défense dans l'Espace [17]. Cette ambiguïté peut être plus ou moins explicite : en novembre 2017, le Centre national d'études spatiales (Cnes) affirmait, par exemple,

---

[11] « Espace : le réveil de l'Europe ? », *op. cit.*, p. 11-12.

[12] « Cela dit, il est très possible qu'au moins certaines de ces constellations finissent par devenir des concurrents directs d'acteurs plus traditionnels du secteur des télécommunications, en particulier si elles décident, et réussissent, à cibler directement les consommateurs. », *ibid.*, p. 28.

[13] Bondiou-Clergerie Anne, « Les chiffres clés de l'industrie spatiale française », *Annales des mines – Réalités industrielles*, vol. 2019/2, mai 2019, p. 38.

[14] Guillemard Véronique, « La force spatiale européenne doit se réveiller face aux États-Unis », *Le Figaro*, 19 février 2020.

[15] Mauduit Jean-Christophe, *op. cit.*, p. 2

[16] Clausewitz (von) Carl, *De la Guerre*, Livre II, Chapitre 2, § 20 « Incertitude de toutes les données ». Le paragraphe est consacré à la part irréductible d'inconnu – le fameux brouillard (*nebel*) de la guerre – des données à disposition de la réflexion stratégique et surtout de la signification de ses données, quant à leur usage, une fois qu'elles se déploient effectivement dans l'engagement.

[17] « Sous couvert d'objectifs civils, des États peuvent financer ouvertement des technologies potentiellement antisatellites. Celles-ci permettraient la mise en service d'outils dont les actions seraient beaucoup plus difficiles à détecter, à suivre, à attribuer et à contrer que des actions exo-atmosphériques plus classiques (missiles, lasers, brouilleurs…). » *Revue stratégique de la défense et de la sécurité nationale*, 2017, p. 45-46 (www.defense.gouv.fr/).

que le système d'imagerie satellitaire marocain, développé à partir du modèle français *Pléiade NEO*, pouvait être utilisé à des fins militaires pour « servir à localiser les installations militaires de pays adverses afin de planifier une intervention armée » [18]. Les données sur l'Espace doivent donc être interprétées à l'aune de cette ambiguïté.

Une périphérie géographique, stratégiquement névralgique

La polyvalence de l'Espace brise un mythe profond de ce qu'il faut entendre par usage militaire de cet environnement ou plutôt complexifie et circonstancie cette signification. Le cadre juridique, pensé par le Traité de l'Espace de 1967, s'inscrivait dans la perspective d'un Espace comme champ de bataille [19] et l'enjeu était d'éviter des affrontements *dans* l'Espace ou *depuis* l'Espace. Or, il s'avère que l'usage militaire de l'Espace ne nécessite nullement une militarisation ou du moins pas exclusivement. C'est le principal enseignement qu'il nous faut tirer de l'appréciation de l'Espace, sous le prisme stratégique. Il se révèle sous forme de paradoxe : l'Espace est devenu un enjeu de puissance non parce que l'évolution technologique a permis d'y exporter la guerre [20], mais parce que cette évolution technologique a permis d'en faire une interface, un lieu de passage de l'information, comme déjà illustré par les enjeux de l'imagerie, d'*Internet* et des communications. Sans doute au XX^{e} siècle la représentation vulgarisée de l'usage de l'Espace se concrétisa dans le programme d'*Intrusion Detection System* (*IDS*) [21]. Ce programme, progressivement abandonné, comportait, par exemple, le développement de rayons X censés pouvoir détruire des missiles balistiques depuis l'Espace afin de, théoriquement, mettre sous cloche les États-Unis [22]. Cet usage de l'Espace est obsolète car à la fois trop peu modeste et ne rendant pas compte de la subtile intrication des enjeux spatiaux avec la défense. L'Espace est une périphérie géographique, stratégiquement névralgique. En effet, en 2015, 100 % des opérations terrestres, maritimes et aériennes menées par l'armée française ont mobilisé la technologie américaine du *Gobal Positioning System* (*GPS*) et 67 % des objectifs d'engagement furent localisés au travers du *GPS* [23].

Cela corrobore que l'Espace peut ne pas être le lieu de l'affrontement mais constituer une périphérie de celui-ci, radicalisant les asymétries sur Terre. Il est donc certes nécessaire de maîtriser l'Espace mais cela revêt d'une signification bien distincte de la maîtrise d'un territoire au sens classique, d'une occupation sans partage. Cependant cela ne doit pas éclipser les usages militaires de l'Espace, au sens classique combinant l'identité périphérique de l'Espace avec une appréciation de celui-ci comme

---

[18] Kadiri Ghalia, « Satellite marocain en orbite : un lancement secret qui inquiète », *Le Monde*, 19 novembre 2017 (www.lemonde.fr/).

[19] Traité de l'Espace, régissant les activités des États sur la Lune et les autres corps célestes, article IV, § 1 et 2.

[20] Voir à cet égard l'adaptation au cinéma du roman *Moonraker* de Ian Fleming par Lewis Gilbert en 1979. Il y est fantasmé une bataille dans l'Espace extra-atmosphérique, tel que probablement les contemporains s'imaginaient le futur des affrontements dans l'Espace même.

[21] Ce système fut annoncé lors de l'emblématique discours de Ronald Reagan du 23 mars 1983, dit du « *Star Wars Reagan's speech* » en référence à la saga éponyme dont le 3^{e} film sortit en salle deux mois plus tard, le 25 mai.

[22] C. Kumar N Patel. et Bloembergen N., « Strategic Defense and Directed-Energy Weapons », *Scientific American* vol. 257 n° 3, 1987, p. 39.

[23] Zajec Olivier, *op. cit.*, p. 202.

centre de l'affrontement, dont il s'agira comprendre la teneur dans l'étude de cas. La spatio-dépendance [24], à l'égard des technologies déployées dans ce champ, renvoie à un type de maîtrise qui dépasse le domaine militaire *stricto sensu*. Pour comprendre la logique de l'Espace sous le prisme de la défense, il faut en fait redescendre sur Terre, où s'articulent des bouleversements plus larges de la décision politique en matière de défense, avec les logiques de production industrielle, nécessaires à la projection spatiale.

Le défi croissant de l'internalisation des enjeux économiques pour penser la défense

L'intrication des secteurs privés et publics, exacerbée par les besoins technologiques de l'Espace

La production d'armement, et plus largement de matériels destinés à un usage militaire quelconque (logistique, ravitaillement, etc.), relève de la décision politique stratégique. Dans l'histoire de la guerre, la technologie joue un rôle croissant à mesure qu'elle se complexifie et détermine de plus en plus l'issue des conflits. Dans l'Espace, cette logique atteint son paroxysme dès lors que l'usage des technologies y constitue l'essentiel de la présence et de la maîtrise.

À ce titre, les stratégies de production industrielle ne sont pas des enjeux exclusivement économiques, mais s'invitent au centre de la réflexion stratégique de l'Espace. Sauf que les dynamiques économiques terrestres connaissent un affaiblissement de « l'État producteur » industriel au profit d'un « État régulateur » et incitatif [25]. Ce domaine est certes le champ des grandes puissances, mais cela par l'intermédiaire d'un appui croissant des acteurs privés, nécessaire pour s'y projeter en vue d'un usage militaire.

Le recours au secteur privé n'est pas une « réquisition », sur le mode de l'économie de guerre de la Première Guerre mondiale où l'appareil productif des entreprises privées et civiles fut reconverti pour la production de matériel militaire [26]. Rappelons que les technologies spatiales sont polyvalentes. Ainsi, tout développement de l'industrie spatiale privée, y compris pour des projets civils, relève, pour le pays d'où est développée cette technologie, d'un potentiel militaire. Cela implique de penser la relation des États – et leur puissance relative – avec les acteurs privés. L'intrication entre la production par des actifs spatiaux, aux mains des États, et la production issue d'acteurs privés, dépend des stratégies et des héritages industriels des pays ayant une prétention spatiale.

Ce découpage entre public et privé comprend en outre une structuration interne en écosystème [27]. En France, de grands groupes comme Airbus, Thales Alenia Space

---

[24] *Ibid*.
[25] Chevalier Jacques, « L'État régulateur », *Revue française d'administration publique*, vol. 2004/3, n° 111, p. 473-482 (www.cairn.info/revue-francaise-d-administration-publique-2004-3-page-473.htm).
[26] Antier Chantal, « 1915. La France en chantier », *Guerres mondiales et conflits contemporains*, vol. 2005/3, n° 219, p. 53-62 (www.cairn.info/revue-guerres-mondiales-et-conflits-contemporains-2005-3-page-53.htm).
[27] Bondiou-Clergerie Anne, *op. cit.*, p. 38.

et Ariane Group, ramifiés à un réseau de Petites et Moyennes Entreprises (PME) et de s*tart-up*, constituent une « *supply chain* spatiale française » [28]. L'enjeu est, à l'échelle nationale, d'être présent sur l'ensemble de la chaîne de valeur. Pour cela, l'État s'en remet en partie au secteur privé en tant que client stratégique [29]. Il organise l'écosystème et le stimule, il en est lui-même un maillon par les investissements qui y sont réalisés [30]. Cette intrication porte à considérer une évolution du rapport de l'État et du secteur privé dans l'Espace sous l'appellation « *New Space* » dont l'étude de cas nous donnera un aperçue quant au positionnement spécifique de la France en la matière.

Cette multiplication des acteurs et, surtout, la diversité de leur nature (privés et publics) interrogent la difficulté à faire converger les efforts selon des logiques communes au risque de voir des dynamiques s'affronter plutôt que de se compléter.

Une difficile ligne de crête à appréhender entre injonctions économiques et intérêts de défense

L'État se soumet par-là aux logiques du marché, profondément mondialisées, où se positionnent les entreprises des autres pays. Un adversaire potentiel est un réel partenaire économique, du moins par ses entreprises. La susmentionnée spatiodépendance de l'Armée française au système nord-américain *GPS* relève d'un avantage économique, car l'Armée se dote d'un outil performant sans en avoir supporté les coûts de conception et de production, mais contrevient au principe stratégique de rétention de l'information, les Américains ayant accès à celle-ci. À cet égard, les appels [31] se multiplient pour que la stratégie industrielle et économique recoupe les intérêts stratégiques de défense. Autrement dit, il s'avère de plus en plus urgent de développer une autonomie industrielle pour ne pas subordonner la stratégie militaire à la stratégie économique. Cette tension entre logiques économique et militaire se retrouve dans la politique de lancement des engins satellites. Un État peut décider de s'en remettre aux services d'un autre, ou d'une entreprise étrangère, pour effectuer les lancements de ses satellites, mais un tel calcul prive le demandeur d'une indépendance décisionnelle évidente [32]. Or, les dynamiques économiques poussent à la spécialisation et donc à la fragmentation des chaînes de production y compris à l'échelle internationale.

Pour concilier les intérêts de défense, tendant *a priori* à internaliser et centraliser les acteurs, avec les intérêts économiques, poussant *de facto* à fragmenter et spécialiser la production, il convient d'articuler l'écosystème industriel au réseau d'alliance le plus pérenne. C'est le choix de la France, dont nous ne pouvons apprécier la stratégie spatiale (économique et strictement militaire) hors de la perspective européenne. La régionalisation est la conséquence directe de cette tension entre défense et économie.

---

[28] *Ibid*.
[29] « Espace : le réveil de l'Europe ? », *op. cit.*, pp. 11-12.
[30] En ce qui concerne les États-Unis, par exemple, « le ministère américain de la Défense a exprimé son soutien à ces initiatives et a déjà attribué un contrat de 28 millions de dollars à Starlink [projet de constellation *Internet* de SpaceX] pour des tests de connectivité avec les avions de l'armée de l'air américaine ». *Ibid*, p. 12.
[31] *Le Monde*, « *Éditorial* - Les belles promesses de *Galileo*, le "*GPS* européen" », 16 décembre 2016 (www.lemonde.fr/).
[32] Gaillard-Sborowsky Florence, « Petits satellites, petits lanceurs : quelles opportunités pour de nouveaux entrants ? », *Annales des Mines-Réalités industrielles*, vol. 2019/2, mai 2019, p. 30-33 (www.annales.org/).

Ce processus permet, en effet, d'élargir ce qu'il conviendrait d'appeler l'« unité stratégique » d'acteurs supposés partager leurs enjeux défensifs.

Dans la continuité du problème attaché à l'usage des technologies et du système *GPS* américains, l'UE a investi 13 Md€ pour déployer le système de géolocalisation et de datation *Galileo*. Cette régionalisation des enjeux ne se limite pas aux seuls organismes de l'UE. L'*European Space Agency* (*ESA*) [33] n'est, par exemple, pas un organe rattaché à l'Union européenne, mais constitue l'institution garantissant aux Européens un accès propre aux lancements. La maîtrise collective des lancements concentre tous les enjeux de la complexification des rapports entre économie et défense. Car il s'agit d'articuler l'accès de l'Espace entre militaires et civils, et entre acteurs privés et publics, l'enjeu étant de contrôler le marché afin de ne pas subir les choix économiques ou stratégiques de tiers.

La difficile indépendance économique des acteurs est un gage de liberté décisionnel pour la stratégie de défense. Elle est le fruit de rapports de force militaires et économiques, mais ceux-ci s'insèrent eux-mêmes dans un cadre normatif, par-delà la simple confrontation des moyens. C'est le cas sur Terre pour les interactions commerciales et financières qui participent à la stratégie économique. C'est également le cas pour le droit de la guerre, qui délimite la pensée stratégique, en participant à l'endiguement d'une montée aux extrêmes de la violence. Or, l'Espace est également aux balbutiements du développement de son cadre juridique.

Peser sur la législation comme perspective de pacification et outil d'affirmation dans l'Espace

Puissance du droit, l'espoir de réguler les interactions dans l'Espace par la formation d'un régime juridique adapté

S'imposer dans l'Espace, notamment *via* des marchés économiques, soulève des enjeux plus subtils et structurels, ramassés dans la faculté, donnée aux acteurs prééminents, de légiférer sur l'Espace. Nous entendons par là que la présence dans l'Espace, dont nous avons décrit les conditions d'accès et de maîtrise, donne un poids différencié aux acteurs, pouvant dès lors orienter la législation qui poursuit les limites de l'activité des hommes dans de nouveaux milieux, posant de nouvelles questions juridiques. Cette influence résiduelle relève de la puissance immatérielle, et nous ramène au prestige qu'accompagne l'accès à l'Espace.

De plus, les enjeux juridiques de l'Espace peuvent aussi se concevoir comme créant des précédents dont les implications peuvent dépasser les seuls enjeux extra-atmosphériques. C'est la thèse que défend l'analyse juridique de Jean Klein, dans la foulée du Traité de l'Espace de 1967 et des espoirs que la détente alimente, depuis la crise de Cuba en 1962 : « Dès lors, il convient de s'interroger sur l'opportunité et les

[33] L'*ESA*, ou ASE en français, est une organisation internationale comportant 22 pays, tous géographiquement européens. Son budget était de 5,72 Md€ en 2019. « Espace : le réveil de l'Europe ? », *op. cit.*, p. 15.

chances d'une entreprise dont la visée serait, d'une part, de préciser la portée et d'étendre le champ d'application du traité de 1967, d'autre part, de tirer profit des possibilités qu'offre l'Espace pour mettre en œuvre un programme de désarmement général sur le globe terrestre » [34]. L'Espace n'est donc pas le seul réceptacle des logiques terrestre mais comme objet en soi, a pu stimuler, en 1971 par exemple, le rêve de peser, par sa législation particulière, sur le droit international en vigueur sur Terre.

Si donc les enjeux économiques ont un effet, que nous pourrions qualifier d'*ascendant*, faisant déborder leurs logiques terrestres dans l'Espace, le droit semble exercer un mouvement inverse. Le nouveau milieu, disposant de contraintes d'accès et de maîtrise nouvelles, engendre la possibilité, toute théorique, de faire déborder les normes qui lui sont spécifiques sur la Terre. Dans le *Nomos de la Terre*, Carl Schmitt conçoit la faculté d'un milieu spécifique à disposer de son propre régime normatif [35]. Selon lui, la maîtrise des océans fut la constitution d'un espace disposant de ses propres règles, distinctes de celles régissant les interactions sur la terre ferme. « *The firm land was divided into states, colonies, protectorates and spheres of influence. By contrast, the sea was free. It could be freely exploited by all states (for fishing, salt procurement, pearl fishing, etc.); it had no borders and was open* » [36]. Mais ce dualisme a connu une tension lorsque les gardiens hégémoniques de l'ordre maritime, les Britanniques au XIX^{e} siècle, puis les États-Unis, ont tenté de forger un ordre international fondé sur les mêmes libertés – théoriques – de circulation que permettait la mer. En d'autres termes, nous pouvons interpréter la tension de l'ordre international vers un système libéral, comme un débordement du régime juridique maritime sur le milieu terrestre.

Dans la lignée de Jean Klein, nous pouvons penser que le régime normatif de l'Espace, amené à se développer à mesure de son accès, produira un débordement *descendant* pour influencer les interactions terrestres. Seulement, pour suivre Carl Schmitt jusqu'au bout de sa pensée, ces débordements normatifs, loin d'être spontanés, sont le fruit de la puissance hégémonique profitant du cadre normatif de son milieu de prédilection pour s'imposer au-delà, comme le fit le Royaume-Uni à partir des océans.

Droits des puissants, l'enjeu de la maîtrise des règles pour s'imposer dans cet environnement

Le droit international étant le fruit des interactions entre sujets du droit international – les États, disposant d'intérêts propres –, la législation de ce champ relève de

[34] Klein Jean, « Le Traité de l'Espace et la réglementation des armements », *Politique étrangère*, vol. 36, n° 3, p. 272 (www.persee.fr/doc/polit_0032-342x_1971_num_36_3_1977).
[35] « *Land and sea were completely different orders. There was an international law of the land and a different international law of the sea. In international law, land war was distinguished completely from sea war. In land war, not the civil population, but only the adversarial army was the enemy. Land war was not conducted between peoples, but only between the armies of European states. The private property of civil populations was not booty according to international law. Sea war was trade war. In sea war, the enemy was any state with which the opponent had commercial dealings.* », Schmitt Carl, *The Nomos of the Earth in the International Law of the Jus Publicum Europeaum* (traduit et annoté par G.L. Ulmen), Telos Press, 2003, p. 353.
[36] *Ibid.*, p. 352.

dynamiques de puissances. La forme et le fond du droit sont le résultat d'interactions de puissances, qui aboutissent à une certaine *idéologie* [37] du droit correspondante. En somme, la maîtrise du droit est aussi un objet de puissance. Le droit de l'Espace est donc, à double titre, un enjeu indirect de la défense. D'une part, dans la mesure où il cadre les agissements des États dans ce milieu et conditionne leur puissance. Mais, d'autre part, le droit découle de cette même puissance qui fonde la prétention à participer à la législation de l'Espace [38].

Ces deux enjeux du droit de l'Espace se co-déterminent et doivent s'appréhender comme un pilier de la stratégie globale de l'Espace. Cela est particulièrement vrai pour les outils spatiaux dont l'évolution est rapide et le potentiel militaire encore à déterminer. C'est le cas des constellations dont la concurrence est non seulement économique, mais, en outre, géographique, à mesure que l'orbite géostationnaire se remplit. La législation en vigueur ne couvre pas ces enjeux de saturation du trafic et les problèmes qui en découlent indirectement, comme la gestion et responsabilités des déchets orbitaux, par exemple. En la matière, des standards *ad hoc* sont souvent constitués, sur la base de travaux d'experts et d'industriels, pour donner une ligne de conduite [39]. Ces « codes », ou « standards », pourront à terme constituer des normes de références et appuyer les positions des pays dont ils sont issus.

L'Espace connaîtra-t-il un *hegemon* tel que la Grande-Bretagne le fut pour les océans au XIX^{e} siècle ? Les États-Unis sont incontestablement la puissance prééminente de ce milieu, mais ils ne sont pas, pour autant, incontestés. Le droit de l'Espace s'organisera différemment si une puissance se fait l'arbitre de son orientation ou qu'un équilibre spatial s'organise pour élaborer un cadre juridique gelant ces rapports de force équivalents. En somme, malgré ces spécificités topographiques conséquentes, l'Espace reproduit un jeu de puissances traditionnel où la maîtrise des règles est l'enjeu primitif de celui qui veut jouer.

⁂

Notre réflexion a tenté de rendre compte d'un rapport complexe entre la défense et l'Espace, dont l'intrication porte à redéfinir les intérêts se rapportant à des enjeux différents, mais convergeant pourtant toujours sur une évaluation des puissances qui s'affrontent, en définitive, sur l'accès et la maîtrise de l'Espace. Les rapports de puissance entre pays, entre groupements régionaux, entre industries, entre influences juridiques, sont autant de confrontations proprement terrestres. Il est apparu pourtant que ces rapports s'appliquaient à l'Espace en tant que cadres des enjeux qui

[37] Scott Shrley V., « International Law as Ideology: Theorizing the Relationship between International Law and International Politics », *European Journal of International Law*, 1994, pp. 313-325 (www.ejil.org/pdfs/5/1/1245.pdf).
[38] « […] une éventuelle capacité européenne […] donnerait également à l'Europe un certain poids dans les futures négociations sur les réglementations et/ou normes internationales relatives à ces constellations, par exemple en ce qui concerne la gestion du trafic spatial », « Espace : le réveil de l'Europe ? », *op. cit.*, p. 29.
[39] « Après diverses éditions, d'un standard *EDMS* (*European Debris Mitigation Standard*), un code de bonne conduite européen, l'*ECOS* (*European Code of Conduct*), a été approuvé par les cinq chefs d'agence en juin 2004, donnant à l'Europe un document de référence unique, fort, et adoptable pat tous. ». Bonnal Christophe, *Pollution spatiale : l'état d'urgence*, Belin, 2016, p. 122.

s'y trament, mais aussi en tant que produit des activités proprement spatiales. Or, ces activités seront, à la vue de l'accroissement des investissements, vraisemblablement amenées à s'intensifier. Les signes de cette intensification se font ressentir dans les projets volontaristes des grandes puissances spatiales [40] ainsi que dans les projets scientifiques qui accompagnent ces rêves pour les faire basculer dans la réalité [41]. Une colonisation de l'Espace, par une présence permanente, au-delà de l'orbite de la Station spatiale internationale (*ISS*), réinterroge les vieux mythes de guerre froide sur l'affrontement dans et depuis l'Espace. S'il semble qu'une transposition des modes d'affrontement terrestre doit être écartée par les particularités du milieu que constitue l'Espace extra-atmosphérique, en revanche nous ne pouvons nous permettre d'évacuer la possibilité d'un accroissement des tensions au sein de l'Espace. Elles ne manqueraient pas d'accompagner la massification et la pérennisation de notre présence. Ces formes d'affrontement, dans ce nouveau milieu, interrogent l'arsenal dont disposent les puissances spatiales et les formes d'affrontement renouvelées pour lesquelles les puissances spatiales se préparent. Une étude de cas sera ainsi dédiée à une réflexion toute particulière sur la participation de la France à l'arsenalisation de l'Espace.

[40] Bezat Jean-Michel, « *Falcon Heavy* en route pour Mars, l'odyssée de l'Espace qui agace la Russie », *Le Monde*, 08 février 2018.

[41] En janvier 2020, l'*European Space Research and Technology Centre* (ESTEC), situé à Noordwijk (Pays-Bas), annonçait avoir pu simuler l'extraction d'oxygène respirable et utilisable pour les réacteurs de fusées, à partir de poussière lunaire. Ces recherches permettent d'espérer, à moyen terme, l'installation d'infrastructures permanentes sur la Lune. *ESA*, « ESA opens oxygen plant—making air out of moondust », 17 janvier 2020 (www.esa.int/).

Étude de cas : l'Espace comme domaine renouvelé de la défense française

De la militarisation à l'arsenalisation

« Si l'Espace a été une nouvelle frontière à franchir, c'est désormais un "nouveau front" que nous devons défendre » [42]. Comment articuler cette affirmation de Florence Parly, ministre des Armées, avec l'article IV du Traité de l'Espace de 1967 [43] dont la France fait partie ? Ce dernier dispose, par l'intermédiaire d'une approche libérale, à ce que les États s'engagent à une « utilisation de l'Espace extra-atmosphérique à des fins pacifiques », mais permet aussi une militarisation des orbites terrestres ainsi que leur arsenalisation, à l'exception des armes de destruction massive. Cependant, l'accord du 5 décembre 1979, dont la France est signataire depuis 1980 sans l'avoir ratifié, dispose que les corps célestes sont *res communis* (« chose commune ») et non *terra nullius* (« terre n'appartenant à personne ») et qu'ainsi « la Lune, les corps célestes et leurs orbites sont démilitarisés » [44]. De ce fait, comment s'articulent la militarisation croissante de l'Espace et son arsenalisation « rampante » [45] avec la défense nationale française ? En effet, même si la France adopte une politique, *a priori* stricte, contre toute arsenalisation comme le rappelle le président de l'Office national d'études et de recherches aérospatiales (Onéra) Bruno Sainjon [46], le développement des programmes étrangers appellent, quant à eux, à une redéfinition de la stratégie spatiale française.

La militarisation désigne « le placement sur orbite de satellites, non agressifs, à des fins militaires tels que les satellites de renseignement, de navigation, de télécommunications » [47]. L'arsenalisation désigne, quant à elle, « le placement sur orbite

---

[42] Discours de Florence Parly lors de la présentation de la stratégie spatiale de défense à Lyon le 25 juillet 2019 (www.defense.gouv.fr/).

[43] Traité de l'Espace régissant les activités des États sur la Lune et les autres corps célestes, article IV : « Les États parties au Traité s'engagent à ne mettre sur orbite autour de la Terre aucun objet porteur d'armes nucléaires ou de tout autre type d'armes de destruction massive, à ne pas installer de telles armes sur des corps célestes et à ne pas placer de telles armes, de toute autre manière, dans l'Espace extra-atmosphérique. »

[44] Accord sur la Lune, Article III : « Les États parties ne mettent sur orbite autour de la Lune, ni sur une autre trajectoire en direction ou autour de la Lune, aucun objet porteur d'armes nucléaires ou de tout autre type d'armes de destruction massive, ni ne placent ou n'utilisent de telles armes à la surface ou dans le sol de la Lune. »

[45] Discours de Florence Parly, 25 juillet 2019, *op. cit.*

[46] Fauvaud Stéphane, « Sécurité spatiale et militarisation : vers une arsenalisation de l'Espace ? », *RDN* n° 815, décembre 2018, pp. 94-99.

[47] Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE), *Concept exploratoire interarmées 3.3.13-ESPACE n°27/DEF/CICDE/DR* du 4 février 2014, ministère de la Défense.

de systèmes susceptibles d'atteindre des objectifs sur la Terre ou en orbite, et non plus de simples systèmes de soutien des opérations militaires » [48]. Le développement d'arme Terre-Espace, Espace-Terre ou Espace-Espace représente un enjeu, alors que le droit international ne pose que peu de limitations concernant la projection d'armes. *Quid* des armes de destruction [49]. La France ne considère pas qu'une révision des traités relatifs à l'Espace n'est de rigueur [50] malgré un changement de dynamique. Comment envisager alors l'incorporation de l'Espace dans la défense des intérêts nationaux alors qu'il s'agit d'un espace fluide au même titre que la mer, tel qu'il est défini par Laurent Henninger : un ensemble d'espaces « lisses, isomorphes et inhabitables par l'Homme » [51] nécessitant de s'appuyer sur de l'innovation technique afin de s'y projeter et *in fine* de s'y déployer. Dans quelle mesure les avancées techniques en matière d'armement impactent-elles la stratégie française ? Quelles conséquences aura une arsenalisation croissante de l'Espace par les puissances spatiales pour la sécurité nationale ? En quoi la « défense active » française s'inscrit-elle dans sa stratégie d'autoprotection et d'autonomisation stratégique ?

Alors que l'Espace, un milieu attractif, congestionné et contesté, est définit comme « la clé de voute de notre défense », il s'agit de revenir sur la maîtrise et la connaissance de l'Espace extra-atmosphérique dans toute sa complexité et ses capacités avant de s'interroger sur les modalités de projection dans ce théâtre d'opérations renouvelé tout en analysant la rhétorique française dans un environnement géopolitique en reconstruction.

La connaissance du milieu spatial, un atout pour saisir les menaces et vulnérabilités des infrastructures

Alors que l'arsenalisation occupe les états-majors des armées des principales puissances spatiales, la France n'envisage pas officiellement cette option, comme l'a rappelé Florence Parly en préambule de la stratégie publiée en 2019 mais plutôt de protéger les satellites et de défendre les intérêts français [52]. La priorité est mise sur un accroissement de la surveillance afin d'éviter des « confrontations majeures » en anticipant et prévoyant les manœuvres des autres acteurs, comme précisé dans l'*Ambition 2030*, présentée dans la Loi de programmation militaire (LPM) 2019-2025 [53]. Ainsi, la connaissance de l'Espace nécessite, entre autres, une discrimination entre satellites de surveillance, d'observation et d'écoute, et d'éventuels débris spatiaux ou satellites commerciaux et de communication civils. La France possède une avance considérable sur les autres pays grâce au système *Graves* (*Grand réseau adapté à la veille spatiale*).

---

[48] *Ibid*.
[49] Traité de l'Espace, *op. cit.*, Article IV.
[50] Ministère des Armées, *Stratégie spatiale de défense*, rapport du groupe de travail « Espace », 2019, p. 9 (www.defense.gouv.fr/).
[51] Henninger Laurent, « Espaces fluides et espaces solides : nouvelle réalité stratégique ? », *Revue Défense Nationale*, n° 753, octobre 2012, p. 6.
[52] *Stratégie spatiale de défense*, *op. cit.*, p. 27-28.
[53] Loi de programmation militaire 2019-2025, Rapport annexé, *Des conflits, plus durs et plus ambigus, étendus à de nouveaux espaces,* p. 8-17.

En service depuis décembre 2005 et utilisé par l'Armée de l'air, cet outil permet de recenser tous les objets en orbite basse [54]. De ce fait, ce radar permet à la France de se positionner comme acteur principal de la surveillance spatiale aux côtés de la Russie et des Etats-Unis, les deux seules autres puissances possédant cette technologie. Ce processus se voit compliqué par la multiplication d'infrastructures duales ayant des fonctionnalités à la fois civiles et militaires. La plus grande maîtrise de la surveillance et de la trajectographie, *via* le développement de radars conventionnels (*Space Situational Awarness*, *SSA*), et la modélisation des paramètres orbitaux appelée (*Space Surveillance and Tracking*, *SST*). Ces deux outils permettent d'avoir une meilleure conscience de l'environnement spatial et sont particulièrement développés par les grandes puissances actuelles telles que les États-Unis, la Russie, la Chine, l'Inde et la France. Néanmoins, les États-Unis restent la première puissance d'observation et détiennent le monopole de référence, constituant une entrave à l'indépendance stratégique française. Ainsi, la France voit son autonomie décisionnelle compromise par une dépendance au *GPS* américain, avec en 2015, 100 % des missions militaires nationales utilisant le *GPS* – le processus de conversion des systèmes d'exploitation vers la Géolocalisation et navigation par un système de satellites (GNSS) européen *Galileo* étant prévu pour 2023 [55].

La protection des infrastructures et des programmes est nécessaire au bon fonctionnement de l'aviation et des transports terrestres, qu'ils soient civils ou militaires. Au regard de la quantité de données, certes inférieures aux câbles sous-marins, ayant attrait aux communications transitant par les infrastructures satellitaires, les débats sont vifs et sont à l'intersection des questions de cybersécurité et du spatial [56]. Des infrastructures spatiales vulnérables pourraient avoir des conséquences graves sur les opérations militaires, mais, plus globalement, sur l'économie nationale. En effet, de nombreux systèmes garantissant l'efficacité et l'exactitude des transactions commerciales et financières passent par des infrastructures situées dans l'Espace. La menace d'une cyberattaque contre les infrastructures spatiales civiles et militaires français est planante. « Nous avons la certitude que les Russes, les Chinois et les Américains ont mis au point des systèmes destinés à aller observer et écouter au plus près les systèmes spatiaux d'autres pays, ce qui pose de graves questions en termes de sécurité » [57] commente le général Testé, ancien chef du Commandement interarmées de l'Espace (CIE). Face à cette menace, la France a réagi en publiant une *Revue stratégique de cyberdéfense* en 2018 *via* le SGDSN. Les satellites gouvernementaux disposent, par exemple, de codes de cryptages embarqués extrêmement difficiles à déchiffrer. Ainsi, Airbus se veut précurseur en matière de satellites, dits électroniques, répondant à des logiques de chiffrages différentes, réputées robustes. Il faut cependant envisager un futur proche où les ordinateurs quantiques seront en mesure de les décrypter. Pour y remédier, environ

---

[54] Onéra, *GRAVES, une surveillance spatiale française plus performante*, 12 décembre 2016 (www.vinci-energies.com/wp-content/uploads/2016/12/20161212-cp-graves-onera.pdf)

[55] European Defence Industrial Development Programme (EDIDP), *2019 calls for proposals, conditions for the calls and annex V. 1.1*, 22 juillet 2019, p. 42 (https://ec.europa.eu/).

[56] Livingston David et Lewis Patricia, *Space, the Final Frontier for Cybersecurity?*, Chatam House, septembre 2006, 44 pages (www.chathamhouse.org/).

[57] Lagneau Laurent, « Un satellite militaire français de télécommunication espionné par un engin "non identifié" », *Zone militaire–Opex360.com*, 31 mai 2016 (www.opex360.com/).

1 Md€ a été investi à l'échelle européenne afin de financer la recherche dans ce domaine. La France, de son côté, dispose d'un fond d'innovation pour financer l'industrie dont une partie est allouée à ces recherches. Néanmoins, comme le montre la stagnation des fonds reversés à l'Onéra ces deux dernières années [58], les moyens monétaires donnés à la défense limitent l'augmentation budgétaire.

L'Espace comme théâtre d'opérations renouvelé : vers des actions *in situ* ?

La surveillance permet de se prémunir contre d'éventuelles attaques terrestres impactant le domaine spatial. La spatio-dépendance implique des menaces et des vulnérabilités pour les éléments clés de la défense française. Quels sont alors les principaux défis et actions dans l'Espace (menaces cinétiques et cybernétiques) auxquels la France doit faire face dans le cadre d'une militarisation accrue ?

La question de la sécurisation des satellites se pose à cause des menaces cybernétiques. Les moyens utilisés pour ces menaces peuvent être les cyberattaques, les brouilleurs, l'éblouissement, l'interruption de transmissions (crucial notamment pendant les opérations), le *spoofing* (l'usurpation) ou encore le détournement des trajectoires des satellites et de leurs systèmes de navigation. Cela s'inscrit dans une guerre électronique (GE) touchant le spectre électromagnétique. Ce type d'action a la particularité d'être accessible aussi bien à des acteurs étatiques qu'à des acteurs non étatiques (par exemple les groupes subversifs). Face à cela, les autorités françaises s'organisent pour lutter contre ces menaces par le cryptage des systèmes informatiques des satellites et surtout l'anticipation et la meilleure connaissance de l'environnement. Les menaces cinétiques restent à l'heure actuelle compliquées à mettre en œuvre, et ce pour des raisons multiples : la perte de l'effet de surprise à cause du temps nécessaire à la réalisation des manœuvres (*quid* des *CubSats* [59], dont l'innovation permet justement de surmonter ces obstacles) ; les difficultés techniques liées à la précision des manœuvres nécessaires ; peu d'acteurs maîtrisent ces technologies ; ou encore les coûts de recherches et de développement non négligeables pour les économies fragilisées, facilitant encore la détermination de la source de la menace.

De plus, les programmes d'armes à énergie dirigée (tels que les lasers) restent embryonnaires et coûteux [60]. Néanmoins, la menace est réelle. En outre, la Chine aurait, selon le directeur du *National Reconnaissance Office* Donald Kerr, très vraisemblablement réussi à aveugler un des satellites américains, durant l'été 2016 [61] et à lancer un missile antisatellite (*ASAT*) pour détruire l'un de ses satellites météorologiques en fin de vie, le *Fengyun 1C*, le 11 janvier 2007 [62]. Les menaces cinétiques sont

[58] Commission des affaires étrangères, de la défense et des forces armées, *Projet de loi de finances pour 2020 : Environnement et prospectives de la politique de défense*, 21 novembre 2019 (www.senat.fr/rap/a19-142-5/a19-142-5.html)
[59] Nano-satellites discrets pouvant être intégrés à un satellite mère et être confondus avec d'éventuels débris : Basic NASA CubeSat Launch Initiative, *CubeSat101—Concepts and Processes for First-Time CubeSat Developers*, octobre 2017, 86 pages (www.nasa.gov/sites/default/files/atoms/files/nasa_csli_cubesat_101_508.pdf).
[60] Lewis James A, « La dynamique de l'arsenalisation de l'Espace », *Politique étrangère*, vol. 2007/2, été, p. 253-265 (www.cairn.info/revue-politique-etrangere-2007-2-page-253.htm).
[61] Pillsbury Michael, *An Assessment of China's Anti-Satellite and Space Warfare Programs, Policies and Doctrines*, U.S.-China Economic and Security Review Commission, 19 juillet 2007, 80 pages (www.uscc.gov/).

principalement liées aux programmes *ASAT* ou *Space to Earth Weapons* (*STEW*), dont l'objectif peut être de détruire des satellites sans placer d'armes en orbite et donc hors arsenalisation *in situ*. La France ne développe actuellement pas de tel programme à énergie cinétique, mais est considérée comme un acteur *ASAT* « clé en main », car elle possède les capacités technologiques nécessaires. Dès la guerre froide, la Russie [63] et les États-Unis [64] ont développé leurs programmes afin d'élargir leur puissance de dissuasion et plus récemment d'autres puissances comme le Japon, l'Inde [65] et la Chine [66]. Malgré les nombreux efforts afin d'améliorer la connaissance de l'environnement spatial, ce domaine reste difficile d'accès et restreint à l'observation, comme l'illustrent le rapprochement du satellite d'écoute russe *Lunch-Olymp* près du satellite dual français franco-italien *Athena-Fidus* en 2015 [67], la collusion américano-russe de février 2009 [68] ou encore la perte de véhicules spéciaux répétée.

Les progrès technologiques effectués au cours des vingt dernières années entraînent un renouvellement de la notion de champ de bataille classique en portant les affrontements dans un nouveau milieu. La France, par ses alliances (UE, Otan), participe à une réécriture des frontières de la défense et du *topos* de la bataille. L'Espace, en tant qu'élément de soutien aux opérations terre, air et mer, « facilitateur » stratégique, multiplicateur de puissance pour les forces armées, devient progressivement un théâtre d'opérations, passant du domaine de l'utilisation pratique (observation, écoute) à celui de milieu où il est possible de s'y déployer. En effet, alors que l'Espace extra-atmosphérique est tombé en désuétude à la fin de la guerre froide, il connaît aujourd'hui un regain d'intérêt, comme l'illustrent les budgets militaires des principales puissances spatiales alors que la militarisation et l'arsenalisation spatiales s'inscrivent de plus en plus dans les stratégies de défense des intérêts nationaux.

La réponse française : entre « défense active » et autoprotection

La France, première puissance spatiale européenne, est l'un des pays consacrant le plus de budget aux activités spatiales civiles derrière les États-Unis comme le souligne Nicolas Chamussy, président de la commission « Espace » du groupement des industries françaises aéronautiques et spatiales (Gifas) [69]. Elle s'est vue dans l'obligation de se

---

[62] Tellis Ashley J., « China's Military Space Strategy », *Survival*, vol. 49, n° 3, automne 2007 (www.tandfonline.com/doi/full/10.1080/00396330701564752).
[63] Missile de types *Nudol* (2016).
[64] Pic durant la guerre froide au *Ground-based Mid-course Defense* (*GMD*) aujourd'hui visant à intercepter les ogives entrant dans l'espace extra-atmosphérique, voir Grego Laura, « A History of Anti-Satellite Programs », *Union of Concerned Scientists*, janvier 2012 (www.ucsusa.org/).
[65] Mission *Shakti* développée par la *Defence Research and Development Organisation* (*DRDO*), l'agence gouvernementale indienne, permettant de placer le missile en *Low Earth Orbit* (*LEO*), voir Pubby Manu, « India tests first anti-satellite missile system, codenamed Mission Shakti », *The Economics Times*, 28 mars 2019 (https://economictimes.indiatimes.com/)
[66] Du projet 640 (1964-1980) au missile *SC-19*.
[67] Parly Florence (ministre des Armées), « Déclaration sur la défense spatiale » Toulouse, 7 septembre 2018 (www.vie-publique.fr/discours/206663-declaration-de-mme-florence-parly-ministre-des-armees-sur-la-defense-s)
[68] Collision entre un satellite russe et américain le 10 février 2009 à 800 km au-dessus de la Sibérie et ayant entraîné près de 550 débris. Ce fut le premier incident de ce type.
[69] Rapport d'information n° 1579, Commission de la défense nationale et des forces armées. 15/01/2019.

positionner face à l'émergence [70] d'autres acteurs en menant une politique active, voire agressive, dans l'Espace extra-atmosphérique à l'encontre des intérêts de ces autres acteurs. Cet espace renouvelé d'affrontement est marqué par des inégalités de projection non négligeables entre puissances, mais dont les attaques, notamment cyber, sont à la portée de groupes subversifs. Aujourd'hui, l'investissement dans ce domaine va au-delà de la politique de prestige, héritée de la guerre froide, car il participe à la préservation des intérêts stratégiques de la nation.

Pour pallier sa dépendance à la surveillance spatiale américaine, la France entend tirer profit des avantages comparatifs qu'apporte le *New Space* (contrairement à la Russie ou la Chine où le secteur privé est quasiment inexistant) au niveau du financement ou des innovations techniques. En effet, il s'agit de consolider l'industrie française afin de la rendre plus performante et compétitive (transversale – chaîne de production) afin de garantir l'indépendance française notamment en matière d'armement. En réponse au lanceur réutilisable *Falcon* développé par l'entreprise SpaceX, la France réaffirme son positionnement en développant, *via* l'*ESA*, le projet *Ariane 6*, prévu pour garantir une autonomie de lancement française et européenne. D'un point de vue européen, le Vieux Continent réclame un meilleur lien entre acteurs civils et militaires. Les résultats de cette convergence ne seront palpables qu'à la seule condition que les puissances privées reçoivent le soutien de puissances publiques, à l'image du modèle américain SpaceX.

Pour faire face à la menace que représente ce nouveau théâtre d'opérations, l'Administration américaine s'est aussi saisie du sujet. Le président américain Donald Trump a déclaré le 29 août 2019 vouloir entamer la course à la guerre spatiale lors d'une conférence à Washington : « C'est un moment historique, un jour historique, qui reconnaît que l'Espace est au centre de la sécurité nationale et de la défense de l'Amérique » [71]. Par cette déclaration, le président Trump répond à la menace que représentent la Chine et la Russie, y compris dans l'Espace. Il crée le « *Space Force-US Command* », un commandement militaire chargé d'assurer la domination des États-Unis sur ce nouveau terrain de guerre (*Space Dominance*).

La France se prépare à d'éventuelles opérations Espace-Espace *via* l'apparition des Opérations spatiales militaires (OSM) déclinées dans le rapport de 2019 [72]. Ces OSM s'articulent autour de quatre points clés : le soutien aux capacités spatiales, la connaissance de la situation spatiale (*SSA*), l'appui spatial aux opérations (le positionnement, la navigation et la synchronisation : *Positioning, Navigation and Timing*, *PNT*) et surtout les actions dans l'Espace. Il s'agit ici d'observer comment l'Espace est opérationnalisé. Ce dernier point se rapproche du discours pouvant entourer la politique française en haute mer ; soit la liberté de circulation et d'action, tout en dissuadant toutes actions inamicales. Néanmoins, les opérations tactiques dans l'Espace restent difficilement envisageables à court terme, du fait des difficultés techniques liées entre autres à la manœuvrabilité (changer d'orbite par exemple). Se pose alors la question

[70] Déclaration du 20 novembre 2019 à Bruxelles (www.nato.int/cps/en/natohq/opinions_171022.htm).
[71] *Le Monde* avec l'*AFP*, « Trump lance un commandement de l'Espace », *Le Monde*, 30 août 2019 (www.lemonde.fr/).
[72] *Stratégie spatiale de défense 2019*, *op. cit.*, p. 39.

du déploiement tactique : l'environnement spatial est hostile avec des variations de températures importantes ainsi que des rayonnements ionisants, pouvant mettre en danger les vies humaines et certains équipements techniques. Les lancements en forte augmentation ainsi que les accidents et destructions en orbite constituent des risques sérieux. Malgré les avancées américaines [73], les véhicules spatiaux manœuvrables restent à leurs balbutiements pour les autres puissances spatiales.

En tant qu'espace fluide, l'Espace, comme le cyber, pose des problématiques nouvelles pour la défense des intérêts français. Ainsi, comme nous l'avons précédemment détaillé, la question de la surveillance de l'Espace et donc de la connaissance de son environnement, toujours difficile, questionne la capacité de l'attribution des actions non amicales ou même hostiles, ce qui, face à une arsenalisation grandissante, soulève des problématiques juridiques et politiques. Ainsi, la politique de proportionnalité face à des actes difficilement attribuables, diffère d'un pays à l'autre. La France se réclame, quant à elle, de la Charte des Nations unies pour justifier de son droit de « légitime défense » (article 51), et se « réserve le droit de prendre des mesures de rétorsions » ou « contre-mesure » [74], sans pour autant préciser ces moyens de rétorsion. La notion de défense active [75], par son indéfinition juridique se prête donc bien à un accroissement de la militarisation de l'Espace basculant à mesure du développement des activités humaines dans une arsenalisation de plus en plus explicite.

⁂

Les enjeux de la défense spatiale sont parcourus de nombreuses tensions qui articulent des injonctions contradictoires entre stratégie économique et militaire, entre coordination publique et acteurs privés, entre principe de souveraineté et fragmentation des acteurs. Le nœud récurent de ces tensions revient au rôle central de l'information. L'information est dans l'Espace une ressource de passage convoité, mais elle intervient aussi sur Terre, dans les processus industriels et dans la conception technologique. L'information est donc à la fois protégée et partagée, surveillée et traquée. Au-delà de l'Espace, où elle est centrale, l'information constitue un enjeu de défense en soi, par l'accroissement de son rôle, mais aussi parce que les mutations fondamentales de ses supports questionnent le bouleversement des formes d'usage de l'information, pour la défense. Que les nouvelles frontières de la défense comportent des éléments virtuels, comme pour le concept même de frontière dont la ligne archétypique est une fiction juridique et géopolitique, est acquis à la réflexion de la défense. Cependant, la défense, comme domaine pratique et stratégique en soi, comporte aussi son extension et par là même sa frontière. Or, il semble que l'information constitue un domaine particulièrement dématérialisé de la défense, autrement dit, un nouveau type de frontière de celle-ci. ◆

---

[73] Développement du module sans pilote Boeing *X-37B*, au profit de l'*US Air Force*, en mai 2015 permettant de recueillir des informations dans l'Espace et dont les activités exactes restent inconnues.

[74] *Stratégie spatiale de défense*, *op. cit.*. pp. 28-29.

[75] Leclerc Thomas, « "Défense active" : quand la France fait de l'Espace la nouvelle frontière du droit international », Institut Open Diplomacy, 23 janvier 2020 (https://uploads.strikinglycdn.com/).

L'Information : vers une dématérialisation des frontières de la défense

Ludovic Bucquet, Izabela Bukowska et Cécile Mouchon (coordinateurs), Bob Bakoula Maurin, Denis Baverez, Julien Betton, Matthieu Biben, Myriam Boumbar, Tessa Bourcier, Dusan Bozalka, Amélie Faltot, Grégoire Gaston, Ulysse Guerin, Said Keddache, Constance Parpex, Maximilien Roquette et Jean-Victor Tse

Un jeu d'acteurs à plusieurs

Désinformation du fait des flux d'information

La manipulation de l'information n'est pas un phénomène nouveau. Depuis l'Antiquité, elle a été partie prenante des stratégies de guerre. Elle a peu à peu investi toutes les sphères de la vie sociale avec l'apparition et le développement des médias traditionnels. Les exemples au XX^{e} siècle sont nombreux, des totalitarismes hitlérien et stalinien à l'usage des médias à des fins de propagande pendant la guerre froide [(1)].

Avec l'avènement d'*Internet* puis des réseaux sociaux, n'importe quel individu peut produire du contenu, informer et désinformer. Cette dynamique n'est pas anodine, car elle s'insère plus globalement dans le mouvement de la mondialisation qui voit la multiplication des acteurs sur la scène internationale – firmes multinationales, acteurs non étatiques, organisations non gouvernementales (ONG) – autant de concurrents des États.

Leurs stratégies de communication peuvent parfois s'opposer. Surtout, elles créent des flux sans précédent d'informations dont le contenu n'est pas directement contrôlable. De fait, la manipulation de l'information fait aujourd'hui l'objet d'une attention renouvelée de la part de l'ensemble des acteurs de la mondialisation, que ce soit pour l'encadrer ou pour en faire un usage stratégique.

L'augmentation des flux d'informations pose de redoutables défis aux États. La loi sur la lutte contre la manipulation de l'information du 22 décembre 2018 [(2)] s'insère dans un axe majeur de la présidence d'Emmanuel Macron : la souveraineté numérique.

---

(1) Charlotte Lepri. « De l'usage des médias à des fins de propagande pendant la guerre froide », *Revue internationale et stratégique*, vol. 78, n° 2, 2010, pp. 111-118.
(2) « Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information » (www.legifrance.gouv.fr/).

L'importance de cette souveraineté numérique était déjà mentionnée dans la *Revue stratégique de défense et de sécurité nationale* de 2017 : « Les armées françaises doivent être en mesure d'agir de façon autonome et durable dans les domaines […] de l'espace numérique » [3]. Depuis plusieurs années, nous pouvons voir une hausse de la masse de données numériques (les *Big Data*). L'important accroissement des *data centers* est l'une des manifestations tangibles de cette nouvelle orientation de l'économie mondiale et des conflits que peuvent se mener les États. Trois types de protagonistes s'emploient aujourd'hui dans le monde à la collecte et au traitement d'informations « massif », suivant des logiques très différentes : les acteurs du renseignement et de la surveillance d'État comme la *NSA* (National Security Agency, aux États-Unis) et la Direction générale de la sécurité intérieure (DGSE) ; les GAFAM (pour Google, Apple, Facebook, Amazon, Microsoft) ; les institutions patrimoniales et scientifiques, qui se consacrent à l'archivage d'informations pour les générations futures.

L'Union européenne agit notamment selon le Règlement général sur la protection des données (RGPD) ou la proposition de « présence » et de taxation des géants du secteur. Cependant, dans d'autres champs, les États n'ont pas les capacités suffisantes pour refuser des possibilités « non souveraines ». Ainsi, en 2016, la Direction générale de la Sécurité intérieure (DGSI) a confié un marché de 10 millions d'euros à la société américaine Palantir, spécialiste des *Big Data*, qui travaille également pour les services de renseignement américain. Une situation qui pose un risque de confidentialité à la France et d'autres pays de l'UE [4].

La désinformation entre États

Les États peuvent manipuler l'information à l'encontre de leurs propres ressortissants. Moscou a mis en place une stratégie active de communication en ce sens. Pour lutter contre ce qu'elle estime être une domination occidentale de l'information, la Russie a recours à une intense propagande par différents canaux d'informations. Les Occidentaux *via* l'Organisation du Traité de l'Atlantique Nord (Otan) ont dénoncé l'intensification des campagnes de désinformation russes depuis l'annexion de la Crimée (2014), en particulier au travers des médias *Sputnik* et *Russia Today* (*RT*) financés en grande partie par le Kremlin.

La guerre de l'information se caractérise essentiellement par sa nature perpétuelle, ainsi que par la multiplication des supports et des approches, mais également par l'implantation à l'étranger et le recrutement de journalistes qualifiés [5]. *RT* et *Sputnik* disposent ainsi de plusieurs versions de leurs sites *Internet* et comptes secondaires [6], qu'on retrouve sur toutes les principales plateformes numériques (notamment

---

[3] *Revue stratégique de défense et de sécurité nationale*, octobre 2017, p. 79 (www.vie-publique.fr/).
[4] Laurent Lagneau, « La cyberdéfense française a des relations compliquées avec les géants américains de l'*Internet* », *Zone militaire-Opex360.com*, 15 mars 2018 (www.opex360.com/).
[5] Fedchenko Yevhen cité dans *Russian Information Campaign Against the Ukrainian State and Defence Forces*, NATO Strategic Communications Centre of Excellence, 2016, p. 68.
[6] *RT* dispose de versions anglaise, russe, espagnole, arabe, allemande et française de son site *Internet* tandis que *Sputnik* dispose d'exactement 31 versions de son site en différentes langues.

les réseaux sociaux), perçues comme un lieu privilégié pour « façonner l'opinion », en diffusant certaines valeurs contraires à celles des démocraties occidentales [7].

La stratégie d'influence russe s'inscrit dans un plan d'ensemble qui viserait à protéger le régime des menaces qui pèseraient sur lui en raison de la « guerre d'information » que les pays occidentaux lui livreraient [8]. Autrement dit, les manipulations de l'information russe s'insèreraient d'abord dans une stratégie défensive qui prendrait forme dans des actions offensives.

Anticipant le lancement de son Plan d'action contre la désinformation, l'UE s'est dotée en 2015 d'une *task force* de communication stratégique. En 2019, elle a créé un système d'alerte rapide (SAR) visant à faciliter la coopération avec des partenaires internationaux (G7, Otan) et les plateformes en ligne pour mieux détecter et prévenir les campagnes de désinformation [9].

En France, un débat doctrinal a opposé tenants (minoritaires) d'une contre-propagande, plus dirigée contre les actions djihadistes qu'étatiques, et tenants d'une riposte strictement défensive [10]. La majorité des théoriciens estime que la désinformation s'appuie sur deux propriétés de nos sociétés modernes : la défiance institutionnelle qui y règne et leur qualité démocratique. Or, une réponse trop appuyée de l'État ne pourrait qu'accentuer l'impact de la désinformation, visant à fracturer les sociétés et les populations plus qu'à y introduire une idéologie alternative, et entretiendrait la thèse complotiste selon laquelle l'État lui-même aurait quelque chose à cacher. En passant à son tour à l'offensive contre l'attaquant, il alimenterait le récit relativiste, à l'origine de toute désinformation, selon lequel la vérité objective est traversée par des vérités concurrentielles et équivalentes [11].

Le choix en France a été une réponse étatique modérée, conformément aux revendications de la plupart des experts cités, déclinée principalement en deux volets [12]. Le premier, légal : la loi contre la manipulation de l'information. Le second, technologique : il s'agit, pour l'État français, de soutenir la création d'outils permettant de contrer les campagnes de désinformation visant la population française comme le soutien à l'entreprise Storyzy dans la création d'un outil (VerDi) [13] capable de détecter les sites producteurs et relais de « fausses nouvelles ». La France a donc fait le choix d'une réponse défensive, cohérente avec ses institutions démocratiques.

---

[7] Secrétariat général de la défense et de la sécurité nationale, *Stratégie nationale pour la sécurité du numérique*, 2015.
[8] Marangé Céline, *Les stratégies et les pratiques d'influence de la Russie*, Études de l'IRSEM, n° 49, mars 2017, 55 pages.
[9] Union européenne, « Plan d'action contre la désinformation. Rapport sur l'état d'avancement », juin 2019 (https://ec.europa.eu/).
[10] Chauvancy François, « Armée française et contre-propagande : un débat doctrinal », *Theatrum Belli*, 2015 (https://theatrum-belli.com/armee-francaise-et-contre-propagande-un-debat-doctrinal/).
Voir aussi Jeangène Vilmer Jean-Baptiste, « La lutte contre la désinformation russe : contrer la propagande sans faire de contre-propagande ? », *Revue Défense Nationale*, juin 2017, pp. 93-105.
[11] Audinet Maxime, « Comment *RT* et *Sputnik* tissent la toile de Moscou à l'étranger », *La revue des médias*, juin 2019 (https://larevuedesmedias.ina.fr/).
[12] « *Hoax*, *fake news* et guerre informationnelle : technologies de la désinformation et outils de lutte contre l'intox », *Lettre trimestrielle de l'OMC* (Observatoire du monde cybernétique), mars 2018, pp. 2-11 (www.defense.gouv.fr/).
[13] Brunier Camille, « VerDi, la traque aux "*fake news*" », Dicod, ministère des Armées, 20 novembre 2018 (www.defense.gouv.fr/).

L'élection présidentielle de 2022, qui fera très probablement l'objet de campagnes de désinformation, agira sans doute comme un révélateur de l'efficacité de ces mesures.

Désinformation du fait d'actions subversives d'acteurs non étatiques

L'utilisation de l'information à des fins de propagande n'est pas une nouveauté induite par le développement des nouvelles technologies. Néanmoins, à l'heure de la mondialisation, la recherche de la maîtrise du narratif des événements n'est plus du seul fait des États, mais également d'acteurs non étatiques.

En 2015, le *Geneva Centre for Security Policy* [(14)] estimait à 18 000 le nombre de soldats étrangers (issus de 90 pays) recrutés par *Daech*, une preuve de l'ampleur et de l'efficacité informationnelles. Dans un rapport daté de 2018 [(15)], le Centre d'analyse, de prévision et de stratégie (CAPS) et l'Institut de recherche stratégique de l'École militaire (IRSEM) ont qualifié la propagande de *Daech* de multidimensionnelle, multivectorielle et ciblée. Multidimensionnelle, car basée sur un narratif complotiste et simpliste. Multivectorielle, car elle utilise de nombreux moyens, sites *Internet*, forums, revues en ligne ou réseaux sociaux, une diversité de moyens de diffusion qui se traduit par une diversité de formats, souvent de très bonne qualité (vidéos telles que les *deepfakes*, reportages, articles, etc.). Ciblée, enfin, car elle a vocation à toucher les plus démunis ou les plus fragiles d'une société. Avec le cas de *Daech*, nous comprenons que l'information n'est pas une variable neutre. Dans un contexte globalisé, tous les acteurs, y compris ceux non étatiques, sont en mesure de s'en emparer pour diffuser leur vision du monde.

Pour des groupes dont le rôle est la représentation et la valorisation d'intérêts communs (politiques, financiers ou autres), la diffusion de certaines informations ou à l'inverse l'occultation de celles-ci, selon qu'elles leur sont favorables ou non, deviennent un enjeu d'influence et de contre-influence contribuant à la désinformation à leur profit. Il peut s'agir de diffuser de fausses informations désavantageant l'image d'un concurrent : par exemple, en 2016, un faux communiqué de presse frauduleusement attribué à Vinci permit d'en faire chuter le cours de 19 % [(16)]. À l'inverse, il peut s'agir de diffuser de fausses infirmations avantageant sa propre image. En 2017, des documents découverts par *Le Monde* montrent comment Monsanto, le géant de l'agrochimie, a utilisé la technique du *ghostwriting* comme outil de désinformation sur le dossier controversé du glyphosate. Le géant de l'industrie biotechnologique agricole avait fait rédiger par ses propres employés des études prétendant démontrer la non-toxicité du glyphosate, mais avait laissé le chercheur Henry Miller s'en attribuer la paternité afin de leur donner une crédibilité scientifique [(17)].

---

(14) Schori Liang Christina, « Cyber Jihad : Understanding and Countering Islamic State Propaganda », *The Geneva Centre for Security Policy Policy Paper*, vol. 2015/2, février 2015 (www.files.ethz.ch/).
(15) Jeangène Vilmer Jean-Baptiste, Escorcia Alexandre, Guillaume Marine et Herrera Janaina, *Les Manipulations de l'information : un défi pour nos démocraties*, CAPS et IRSEM, août 2018, 210 pages.
(16) Jacqué Philippe, « Comment le groupe Vinci victime d'un "hoax" a chuté en Bourse », *Le Monde*, 23 novembre 2016 (https://www.lemonde.fr/economie-francaise/).
(17) Pouliquen Fabrice, « *Monsanto papers* ou comment les *lobbies* industriels manipulent la science », *20 Minutes*, 5 octobre 2017 (www.20minutes.fr/).

De leur côté, les ONG comptent parmi les acteurs clés de la fabrique de l'opinion publique internationale [18]. Elles y participent de trois manières. Elles jouent un rôle crucial au sein des mobilisations transnationales en lançant des « campagnes globalisées » ; elles se présentent comme leurs porte-voix et produisent des arguments participant à l'établissement de ces mobilisations en « opinion publique internationale » ; elles utilisent cette opinion publique qu'elles ont montée de toutes pièces pour faire pression sur les cibles des mobilisations, le plus souvent des États, des institutions financières internationales ou des entreprises multinationales [19]. De tels conflits asymétriques ont vu les acteurs se livrer à de véritables batailles informationnelles afin de rallier l'opinion publique à leur cause, conscients que son soutien ou sa réprobation pourrait infléchir le cours des événements et l'issue de l'affrontement [20].

Un État a donc un intérêt sécuritaire à contrôler sa couverture médiatique et à projeter une image positive, en particulier lors d'un conflit mettant en cause la légitimité de son régime, voire de son existence.

Citons en exemple la bataille informationnelle qui oppose l'État d'Israël à certains mouvements propalestiniens, comme la campagne *Boycott-Désinvestissement-Sanctions* (BDS), créée en 2005. Celle-ci appelle au *boycott* culturel, économique et académique d'Israël afin d'isoler le pays sur la scène internationale et de le contraindre à infléchir sa politique à l'égard des territoires occupés depuis la guerre des Six Jours de juin 1967. Elle milite également en faveur d'un « droit au retour » pour les réfugiés palestiniens et leurs descendants. En février 2010, le *think tank* Reut Institute a notamment appelé le gouvernement israélien à considérer la campagne comme une menace stratégique, ce qui a conduit à plusieurs mesures, notamment une loi de 2017 interdisant l'accès au territoire israélien aux personnes appelant au *boycott* de l'État. En mobilisant des moyens sécuritaires et politiques pour combattre une campagne visant à dégrader son image internationale, le gouvernement israélien illustre que l'information constitue bien une nouvelle frontière de la défense, dont l'importance est amenée à croître dans les années à venir.

Enfin, les technologies de l'information peuvent être utilisées par les réseaux criminels qui s'en servent pour l'escroquerie avec l'hameçonnage, visant à obtenir d'un internaute ses coordonnées bancaires ou ses identifiants de connexion à des services financiers [21], mais aussi pour faciliter leurs activités *via* le *Dark Web*. Les capacités des criminels sont du reste en constante évolution. Comme le dit le professeur Alain Bauer, « ce que les États font, les criminels ont toujours réussi à le faire. À quel moment est-ce que les organisations criminelles auront les moyens suffisants pour faire très exactement la même chose, mais à leur bénéfice, que ce que fait la NSA ? » [22].

---

[18] Debos Marielle et Goheneix Alice, « Les ONG et la fabrique de l'opinion publique internationale », *Raisons politiques*, vol. 2005/3, n° 19, pp. 63-80 (www.cairn.info/).
[19] *Ibid.*
[20] Nye Jr. Joseph S. et Owens William A., « America's Information Edge », *Foreign Affairs*, vol. 75, n° 2, mars-avril 1996.
[21] ANSSI, Attaque par hameçonnage (*phishing*) (www.ssi.gouv.fr/).
[22] Bauer Alain, « Dernières nouvelles du crime », MOOC du CNAM, janvier-février 2020 (http://foad.cnam.fr/).

Les enjeux de la maîtrise de l'information

La diversité des acteurs qui ont émergé sur la scène internationale est sans précédent. Les enjeux d'information et de désinformation étant bien réels au sein de la communauté internationale, ils obligent les acteurs à développer des mesures de protection et de coopération en creusant les divisions entre les secteurs public et privé.

L'enjeu de protection de l'information et du renseignement

Un secret de la défense nationale est défini par « les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès », selon l'article 413-9 du Code pénal. Depuis décembre 2019, il existe deux niveaux de classification selon la capacité de nuisance des informations en cas de divulgation : « Secret » et « Très Secret » [(23)]. Le système permet de protéger le secret de la défense nationale en limitant leur accès aux personnes habilitées. Toute compromission, soit la divulgation d'un secret de la défense nationale à une personne non habilitée ou n'ayant pas le besoin d'en connaître, est pénalement sanctionnée, et ce jusqu'à sept ans d'emprisonnement et 100 000 euros d'amende [(24)]. Cet enjeu de protection de l'information et du renseignement est assuré en France par la Direction du Renseignement et de la Sécurité de la Défense (DRSD), dont nous développerons les missions dans la partie consacrée aux acteurs de la lutte contre la soustraction d'information [(25)].

La contre-ingérence cyber est également un enjeu croissant pour la protection du renseignement. En novembre 2017, Strava Labs, réseau social dédié aux coureurs, a publié la *Global Heat Map*, relative aux parcours de courses empruntés par les utilisateurs. Conséquence imprévue, ces tracés *GPS* ont révélé l'emplacement de bases militaires confidentielles par reconstitution du parcours de courses de militaires. C'est le cas par exemple de Madama, base avancée française située dans le nord du Niger, dont la localisation a ainsi été dévoilée au grand jour, mettant en danger le personnel et les installations.

Malgré des systèmes de protection de plus en plus sophistiqués, il arrive que des documents intéressant la souveraineté de l'État soient compromis. Lanceurs d'alerte, *hackers* ou transfuges sont en quête de telles informations. En avril 2019, le média *Disclose* a révélé au grand jour le rapport « Yémen – situation sécuritaire » de la Direction du renseignement militaire (DRM). Classé « Confidentiel défense – spécial France », il dispose de la liste détaillée des armes françaises vendues aux armées saoudienne

(23) « Décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale » (www.legifrance.gouv.fr/).

(24) « Livre IV : Des crimes et délits contre la nation, l'État et la paix publique ; Titre I^{er} : Des atteintes aux intérêts fondamentaux de la nation ; Chapitre III : Des autres atteintes à la défense nationale ; Section 2 : Des atteintes au secret de la défense nationale » in *Code pénal*, articles 413-9 à 413-12 (https://www.legifrance.gouv.fr/).

(25) Voir *infra*, « La lutte contre la désinformation et la soustraction d'information. *Les renseignements et leur protection en France* ».

et émiratie dont celles impliquées dans la guerre au Yémen et supposément utilisées contre des civils.

Autre exemple, l'ONG Wikileaks, qui relaie des documents secrets à l'international et dont le slogan est « *We open governments* » (qu'on peut traduire par « Nous révélons le fonctionnement interne des gouvernements »). La plateforme est devenue mondialement connue en 2010 après avoir diffusé plus de 700 000 documents « Secret-défense » des États-Unis sur la guerre d'Afghanistan et d'Irak, révélant des crimes tels que les sévices infligés aux prisonniers de la prison d'Abou Ghraib à Bagdad. Son fondateur, Julian Assange, est actuellement emprisonné en Grande-Bretagne. Considéré comme un ennemi par de nombreux États, certains le voient au contraire comme un défenseur de la liberté d'expression.

Le multilatéralisme et l'échange d'information : un objectif réaliste ?

Le multilatéralisme dans sa définition se caractérise par des engagements réciproques entre groupes de trois pays ou plus. La coopération institutionnalisée en termes d'échanges d'informations à l'international s'opère notamment autour du Renseignement d'origine électromagnétique (ROEM). Il couvre une surveillance des signaux électromagnétiques utilisés dans la téléphonie, les télégrammes, les courriers électroniques et dans toute autre forme de communication *via* les ondes. Quelques moyens de récolte notables sont les satellites, les systèmes d'interception radio et les câbles subaquatiques. Il est possible de diviser le ROEM en deux catégories : *Communications Intelligence* (*COMINT*), entre les humains ; *Electronic Intelligence* (*ELINT*), qui concerne les signaux électroniques envoyés par les radars. Le ROEM comprend à la fois la collecte et l'analyse de ceux-ci.

Les principaux acteurs du ROEM à l'international sont fortement régionalisés. Un des premiers traités dans le domaine, le *United Kingdom – United States Communications Intelligence Agreement*, ou *UKUSA* [(26)], a été signé en 1946 entre le Royaume-Uni et les États-Unis, rapidement rejoints par l'Australie, le Canada et la Nouvelle-Zélande. Son existence n'a été rendue publique qu'à la fin des années 1990 après la révélation de l'existence d'*Echelon*, système mondial d'interception des signaux de communication appuyé par des satellites et bases d'écoute le plus puissant au monde, et mis en place par les signataires du traité. Les documents révélés par Edward Snowden en 2013 ont fourni les détails de la participation des partis tiers au traité, notamment la France, l'Allemagne, Israël et la Pologne. Le traité, qui avait pour cible initiale les enjeux de la guerre froide, s'est depuis diversifié et couvre des domaines au cœur des préoccupations internationales, tels le terrorisme, le trafic de stupéfiants et la prolifération des armes.

---

(26) Prin-Lombardo Julie, *Le renseignement à l'épreuve de l'Union européenne*, Nouveau monde éditions, 2019, 312 pages.

Le deuxième acteur majeur est l'Association des Nations de l'Asie du Sud-Est (ASEAN) [27]. Formée en 1967, elle coopère actuellement avec les États-Unis et les membres du UKUSA autour des questions du terrorisme et de la sécurité internationale. L'Organisation du Traité de l'Atlantique Nord, une alliance politico-militaire, constitue aussi un réseau de ROEM conséquent avec 29 pays membres. Cependant, la récolte des données provenant des services de renseignement nationaux constitue un frein non négligeable au partage d'information.

L'opposition des intérêts personnels aux intérêts collectifs se rencontre aussi dans les initiatives de l'Union européenne. En l'occurrence, l'EU INTCEN [28] (*European Union Intelligence and Situation Centre*), rattachée au Service européen pour l'action extérieure [29], est une structure ayant pour ambition la mise en place du renseignement à l'échelle européenne. L'organisme ne possède pas de définition légale. Il est décrit officiellement comme une « communauté de renseignement ». Cette notion démontre une démarche de fluidification de la coopération et de l'échange d'informations entre les agences nationales. Celle-ci est néanmoins compromise par les divergences des intérêts nationaux, au regard des enjeux politiques et économiques au sein même de l'UE, et par les manquements technologiques face aux capacités de récolte d'informations des groupes plus anciens comme le *UKUSA* [30]. En effet, il existe un monopole américain sur ces technologies héritées de la guerre froide. Aussi, le problème de confiance et de partage des données confidentielles relève du dilemme du prisonnier : deux États ont intérêt à échanger en matière de renseignement, mais un État qui donnerait à l'autre des informations sans réciprocité serait pénalisé, et ce raisonnement amène les deux pays à ne pas échanger.

Cependant, la prolifération des conflits asymétriques, le terrorisme et la mondialisation de menaces (trafics d'armes, d'êtres humains et de stupéfiants) exigent une coopération. Les *Fusion Centers* mis en place après les attentats du 11 septembre 2001 représentent un des modèles à suivre pour contourner ces enjeux. De tels échanges, effectués entre les représentants ou agents de liaison, assureraient une efficacité et une fluidité d'information, une coopération à l'échelle humaine et technologique, tout en préservant la confidentialité des sources et la maîtrise de l'information en elle-même. Bien que cela soit envisageable, l'échange d'informations ne semble attrayant qu'en cas de grandes crises menaçant la sécurité internationale.

Souveraineté numérique et jeux d'influence

La révolution numérique et ses acteurs peuvent porter atteinte à la souveraineté de certains États. L'influence toujours grandissante des GAFAM, qui concurrencent

---

[27] L'ASEAN rassemble les Philippines, l'Indonésie, la Malaisie, Singapour, la Thaïlande, le Brunei, le Vietnam, le Laos, la Birmanie et le Cambodge, ainsi que la Papouasie-Nouvelle-Guinée en tant que membre observateur.

[28] Nomikos John M., « European Union Intelligence Analysis Centre (INTCEN): Next stop to an Agency? », *Journal of Mediterranean and Balkan Intelligence*, vol. 4, n° 2, décembre 2014 (https://rieas.gr/).

[29] Bayet Hugues, « Le rôle du Centre de situation et du renseignement dans l'amélioration de l'échange de renseignements », 7 avril 2016 (www.europarl.europa.eu/).

[30] Magerson John C, « Cooperation Among Foreign Intelligence Services », *Contemporary Perspectives and Review*, 12 janvier 2007.

leurs prérogatives en échappant largement à leur imposition et à leur législation « tout en restant ouverts aux agences fédérales et au système judiciaire américains » [31], en est l'illustration.

À l'ère du numérique, la gestion des données collectées demande des ressources dont la plupart des pays ne disposent pas de manière souveraine. En effet, la capacité d'entreposer et de conserver des données de façon massive n'est détenue que par un nombre restreint d'entreprises, parmi lesquelles les grandes plateformes américaines dominent le marché. En 2019, Amazon Web Services s'est adjugé 32,3 % des parts du marché lié au *cloud*, Microsoft Azure 16,9 % et Google Cloud 5,8 % [32]. Recourir à ces solutions apparaît tentant pour les entreprises et administrations, en termes de performances comme en termes de coûts. Les alternatives n'existent pas forcément [33] et si l'essor de solutions souveraines apparaît nécessaire, il semble improbable.

Dans le même temps, faire appel à une entreprise étrangère pour stocker des données pose des questions de confidentialité, d'intégrité et de disponibilité. L'enjeu est de taille alors que l'affaire Snowden a révélé que les services de renseignement américains avaient déjà transformé les grandes plateformes américaines en instruments de collecte d'informations.

Le secteur des communications se révèle également extrêmement sensible, d'autant plus que l'information y transite, contrairement à la *data*. L'enjeu principal des communications pour un État est double et paradoxal : déchiffrer les communications de certains acteurs – suspects, criminels, terroristes, espions, industriels, etc. – et protéger celles des autres. Or, ici aussi, les acteurs du numérique défient « les États dans ce qu'ils ont de plus précieux, leur souveraineté » [34]. D'un côté, certaines communications sensibles sont trop vulnérables : Google, WhatsApp (racheté par Facebook) ou Telegram (créé par deux ressortissants russes) ont été respectivement sommés par le FBI et par le FSB (Service fédéral de sécurité de la Fédération de Russie) de remettre leurs clés de cryptage. De l'autre, certaines peuvent être jugées par les autorités comme trop intransigeantes sur cette invulnérabilité de leurs données. Ainsi, Apple refuse régulièrement de déverrouiller ses iPhones lors d'enquêtes judiciaires.

La problématique d'une souveraineté informationnelle émerge également de plus en plus alors que les GAFAM et réseaux sociaux sont devenus de véritables alternatives aux médias traditionnels. Ils sont aujourd'hui en mesure d'altérer le cours des évolutions politiques, telles que les élections, comme l'a illustré la campagne présidentielle américaine de 2016 pendant laquelle le Parti républicain s'est appuyé sur les réseaux sociaux comme moyen d'information alternative. Les ingérences qui émaillent désormais la vie politique des États constituent un défi de souveraineté d'une nouvelle ampleur.

---

[31] Observatoire du monde cybernétique, « Les données, nouvel enjeu géopolitique ? », *Lettre mensuelle de l'OMC*, n° 62, mai 2017, p. 9.
[32] Canalys, « Global cloud infrastructure market Q4 2019 and full year 2019 », 4 février 2020 (www.canalys.com/).
[33] Gomart Thomas, Nocetti Julien et Tonon Clément, *L'Europe : sujet ou objet de la géopolitique des données ?,* Études de l'Ifri, juillet 2018 (www.ifri.org/).
[34] « Les données, nouvel enjeu géopolitique ? », *op. cit.*, p. 9.

Enfin, sans que l'on puisse parler d'ingérence *stricto sensu*, les GAFAM participent à la diffusion d'un « message universaliste des États-Unis » [35]. Quand en 2011 Facebook censure *L'Origine du monde* de Gustave Courbet, nombreux sont les médias à y voir la manifestation du puritanisme américain [36].

À terme, de tels comportements ont des conséquences culturelles puis politiques, certains auteurs allant jusqu'à dénoncer un « colonialisme » [37] dans la façon dont les géants du *Web* participent à une standardisation mondiale des interfaces (la page de recherche de Google, le profil personnel sur Facebook, la suite bureautique Windows Office) et s'imposent comme « les relais du *soft power* américain » [38].

La lutte contre la désinformation et la soustraction d'information

Les enjeux d'information constituent en effet de nouvelles frontières de la défense nationale et internationale. On assiste à une émergence d'outils et de coopérations afin de mieux maîtriser, échanger et anticiper les manipulations des données.

Les renseignements et leur protection en France

En 2008, le *Livre blanc sur la défense et la sécurité nationale* a introduit au premier plan la question du renseignement et la place de ses services pour la défense de la France. L'administration centrale chargée d'assurer la défense des données stratégiques, voire vitales à la survie de l'État, est assurée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN), lui-même placé sous l'autorité du Premier ministre.

Parmi les principaux services spécialisés, deux d'entre eux assurent la protection des renseignements : la Direction du renseignement et de la sécurité de la défense (DRSD) et la Direction du renseignement militaire (DRM). Ces directions remplissent des tâches différentes, mais vitales pour la République.

Créée en 2016 dans la lignée de la section de contre-espionnage de l'État-major des Armées, puis de la DPSD datant respectivement de 1872 et 1981, la Direction du renseignement et de la sécurité de la défense (DRSD) est un organisme du premier cercle de la communauté nationale du renseignement relevant directement du ministère des Armées. Composée de militaires et de civils, elle est dédiée à la protection « du personnel, des informations, du matériel et des installations sensibles »,

---

[35] Bouée Charles-Édouard, « Les États et la tentation de l'extraterritorialité », *Huffington Post* (France), 17 décembre 2014 (www.huffingtonpost.fr/).

[36] Fedeli Elisa, « L'Origine du monde à nouveau censurée par Facebook », *Paris-Art*, 16 avril 2011 (www.paris-art.com/) ; Vincenot Pierre, « Excès de puritanisme sur Facebook : la fronde s'organise en France », *La Dépêche*, 22 mai 2015 (www.ladepeche.fr/) ; Nunez Laurent, « Sommes-nous devenus plus puritains que Facebook ? », *Marianne*, 12 février 2016 (www.marianne.net/).

[37] Dounès Gilles (propos recueillis par Thomas Gorriz), « Facebook ou le colonialisme 2.0 », *Atlantico*, 16 mai 2016 (www.atlantico.fr/).

[38] Bouée Charles-Édouard, *op. cit.*

selon les articles D.3126-5 à D.3126-9 du code de la Défense. Elle veille au respect du secret de la défense nationale par une action préventive en renseignant les vulnérabilités et les menaces des informations et en protégeant le secret de toute compromission. Ce service comprend la contre-ingérence des forces, la contre-ingérence économique et la contre-ingérence cyber. Aussi, le terme d'ingérence est utilisé lorsqu'une entité, organisation, gouvernement ou individu, commet un acte contre les intérêts fondamentaux à la défense nationale et au secret de la défense d'une Nation.

Selon le code de la Défense, « la direction du renseignement et de la sécurité de la défense est le service de renseignement dont dispose le ministre des Armées pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles » [39]. Les activités considérées comme menaçantes pour la défense de la France, que la DRSD est chargée d'anticiper, sont terrorisme, espionnage, sabotage matériel, subversion, vol de données sensibles d'intérêts nationales (« *hacking* ») et crime organisé.

La DRSD peut être mobilisée à l'étranger notamment dans le cadre de la protection du dispositif militaire. Par exemple, en 2013, elle avait mis en place un détachement contre-ingérence – *French counter intelligence cellule* – en Afghanistan. Cette mission de *mentoring* opérationnel assurait la sécurité de l'armée afghane par la vérification, au recrutement, d'absence de lien avec les insurgés.

La DRM, quant à elle, est un service purement militaire, chargé de recueillir, de traiter, de rassembler des renseignements de toute nature et de les transmettre aux hautes sphères décisionnelles, à la fois politiques et militaires. Ces deux services de renseignement doivent ainsi permettre aux autorités de commander des opérations militaires viables. Parmi leurs effectifs se trouve une grande diversité de techniciens spécialisés : linguistes, ingénieurs, cartographes ou encore juristes.

La collecte d'informations stratégiques par ces deux services dépend du Renseignement d'origine humaine (*HUMINT*) et de ROEM. L'objectif est de vérifier la fiabilité et la crédibilité des informations collectées. Dans le cas où la DRM récolte l'information qu'un acte terroriste se prépare sur le territoire national suite à une opération militaire de renseignement, cette information va être traduite et analysée par des linguistes et des spécialistes du décryptage si nécessaire. Par la suite, l'information est partagée entre les services compétents, et celle-ci doit pouvoir être exploitée de manière efficace afin d'agir en conséquence.

Néanmoins, ce processus de traitement et d'exploitation de l'information, ainsi que la collaboration entre les services sont parfois ceux où l'on rencontre le plus de difficultés. En effet, la vitesse de traitement d'une information est primordiale. De

[39] Article D3126-5 du code de la Défense (www.legifrance.gouv.fr/).

plus, les six services constituant la communauté française du renseignement [40] sont en compétition entre eux, rendant ainsi difficile une collaboration saine et constructive.

Coopération et partage d'information entre États et avec les acteurs non étatiques

La prépondérance économique et numérique des GAFAM a élevé ces géants du *Web* au rang d'acteurs indispensables. Leurs utilisateurs et leurs recettes alimentées par la revente de données collectées se comptant en milliards, ces protagonistes non étatiques rivalisent aujourd'hui avec la majorité des pays. En 2017, si les GAFAM avaient été un État, leurs chiffres d'affaires combinés (648,7 milliards $)[41] les auraient placés devant les PIB de pays comme l'Argentine ou la Suède. Néanmoins, au-delà de ces données il faut s'intéresser à l'un des enjeux les plus importants de la stratégie de demain : la désinformation. En effet, les plateformes de ces géants du secteur, destinées à l'utilisation de la population aux quatre coins du monde, représentent une zone grise de l'information numérique.

Dès lors, quelle peut être la stratégie des États face à une désinformation qui prolifère sur la Toile, domaine où leur souveraineté disparaît presque complètement et se retrouve en concurrence avec d'autres acteurs non étatiques ? Les membres de l'Otan ont formé en octobre 2018 le Centre des cyberopérations (*CyOC*). Ses buts consistent à fournir des informations nécessaires à la connaissance de la situation dans le cyberespace, à poursuivre la gestion centralisée des enjeux cyber ainsi que la collaboration autour des préoccupations opérationnelles liées au cyberespace.

Comme nous l'avons vu précédemment, l'information et la désinformation constituent des enjeux tant au niveau national qu'européen ; c'est donc en réponse logique à ces enjeux que la protection de l'information et la lutte contre la désinformation voient différentes mesures être prises à ces deux échelles.

De son côté, la Commission européenne a voté un « plan d'action contre la désinformation » [42] en décembre 2018 visant à accroître la coopération entre les États-membres de l'UE, mais aussi à mobiliser les GAFAM et les plateformes en ligne. Ceux-ci se sont engagés à respecter le Code de bonnes pratiques contre la désinformation en ligne [43], s'engageant notamment à « déployer des politiques et processus pour interrompre la publicité et les incitations à la monétisation pour les comportements en

---

[40] La Direction générale de la sécurité extérieure et la Direction du renseignement et de la sécurité de la défense (relevant du ministère des Armées), la Direction du renseignement militaire (relevant de l'état-major des Armées au sein du ministère), la Direction générale de la sécurité intérieure (ministère de l'Intérieur), ainsi que la Direction nationale du renseignement et des enquêtes douanières, et le service Traitement du renseignement et de l'action contre les circuits financiers clandestins (ministère de l'Économie).

[41] Perreau Charlie, « D'où viennent les revenus des Gafam ? », *Le Journal du net*, 19 mars 2018 (www.journaldunet.com/ebusiness/).

[42] Commission européenne, « Une Europe qui protège : l'UE renforce son action contre la désinformation », 5 décembre 2018 (https://ec.europa.eu/commission/presscorner/detail/fr/IP_18_6647).

[43] Commission européenne, « Code de bonnes pratiques contre la désinformation, un an après : les plateformes en ligne soumettent leurs rapports d'autoévaluation », 29 octobre 2019 (https://ec.europa.eu/commission/presscorner/detail/fr/statement_19_6166).

cause, comme la présentation erronée d'informations matérielles les concernant ou au sujet de la finalité de leurs propriétés » [44].

Outre ces projets inscrits dans le cadre des institutions européennes, la lutte contre la désinformation s'organise aussi au niveau national. En raison de certaines divergences d'approches, des pays décident de faire cavalier seul et instaurent une fermeté renforcée contre les actes de désinformation. Par exemple, le droit allemand permet depuis 2019 d'infliger une amende de plusieurs millions d'euros aux plateformes numériques si celles-ci ne suppriment pas les contenus haineux sous 24 heures [45].

De plus, la collaboration entre les GAFAM et les États révèle parfois le danger envers la souveraineté des seconds (du fait des réticences des GAFAM à coopérer) ainsi que de l'opinion publique (par la situation monopolistique des GAFAM en la matière) et pousse les gouvernements à adopter de nouvelles stratégies afin d'encadrer juridiquement leurs actions. Le rachat constant d'entreprises concurrentes donne lieu à la création de quasi-monopoles dans la distribution d'information, et certains acteurs politiques y répondent en promouvant leur démantèlement [46]. Le *Cloud Act* avait déjà constitué une autre forme de réponse de la justice américaine aux entreprises numériques peu enclines à communiquer les données personnelles de leurs utilisateurs. Cette loi, facilitant l'obtention par l'Administration américaine de données stockées ou transitant à l'étranger, affirme ainsi la pleine souveraineté numérique des États-Unis et même, en vertu de l'extraterritorialité du droit américain, sa pleine application au détriment de la souveraineté des autres États [47].

La Chine comme la Russie ont également développé des politiques dans ce sens. Le modèle chinois cherche à maintenir un contrôle complet sur son sol grâce aux rivaux chinois des GAFAM, les BATX (le moteur de recherche Baidu, le site de *e*-commerce Alibaba, l'entreprise Tencent dont la diversité d'activité numérique va de la messagerie instantanée au site d'enchères, et le fabricant de *smartphones* Xiaomi) [48], en interdisant aux entreprises étrangères de transférer leurs données électroniques vers leurs sièges nationaux et en utilisant les données de ses citoyens pour asseoir la domination du Parti communiste chinois *via* son projet de surveillance et de censure, appelé « bouclier doré »[49].

Ainsi, les GAFAM sont les acteurs clés de la lutte contre la désinformation. Leur domination numérique est perçue comme un danger tout en constituant un allié potentiel des États grâce à leur impact sociétal et leurs capacités informationnelles et financières.

---

[44] Commission européenne, *Code de bonnes pratiques contre la désinformation*, 28 juin 2018 (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59114).
[45] Orsini Alexis, « L'Allemagne instaure une amende record de 50 millions d'euros contre les propos haineux en ligne », in *Numerama*, 30 juin 2017 (www.numerama.com/politique).
[46] « Une sénatrice américaine veut démanteler les GAFAM pour restaurer la concurrence », *Next INpact*, 11 mars 2019 (www.nextinpact.com).
[47] Caprioli Éric, « *Cloud Act* et souveraineté numérique », *L'Usine Digitale*, 28 février 2019 (http://usine-digitale.fr/).
[48] Chelet Jonathan, « Baidu, Alibaba, Tencent et ces incroyables "GAFA" chinois », *Capital*, 17 juin 2016 (www.capital.fr).
[49] Philippone Dominique, « La Chine renforce son bouclier doré et perturbe des services VPN », *Le Monde Informatique*, 23 janvier 2015 (www.lemondeinformatique.fr/actualites/).

L'anticipation des crises et risques majeurs de la lutte contre la désinformation

Dès 2008, Nicolas Sarkozy, alors président de la République, affirmait à l'occasion d'un discours sur sa nouvelle politique de défense que « c'est en anticipant les crises que nous garantirons notre indépendance et la sécurité des Français » à propos de la priorité accordée à la fonction stratégique « connaissance et anticipation » [50].

Afin de lutter efficacement contre la désinformation, la France doit être capable de connaître et d'anticiper les risques et les menaces qui pèsent sur ses enjeux vitaux, ses intérêts de puissance et sa sécurité. Depuis le *Livre blanc sur la défense et la sécurité nationale* de 2013, la fonction « connaissance et anticipation » [51] du renseignement revêt un caractère tout particulier dans la capacité de l'État français à se défendre et à protéger son territoire et sa population. Développée au chapitre 6, cette fonction constitue un multiplicateur de forces, tant pour la sécurité de la population sur le territoire national que pour les interventions extérieures. Elle doit permettre « l'anticipation stratégique qui éclaire l'action ». « Une bonne connaissance de l'environnement stratégique et tactique est indispensable à la prévention des risques et des menaces », précise-t-on dans le *Livre blanc* [52].

Ainsi, celui-ci a érigé, pour la première fois, la fonction d'anticipation en fonction stratégique à part entière. Il y est précisé que « face aux incertitudes qui pèsent sur les quinze ans à venir, la fonction de connaissance et anticipation vient au premier plan. Le développement de la connaissance et des capacités d'anticipation est notre première ligne de défense ». En effet, les grandes incertitudes et l'imprévisibilité du système international actuel justifient la prise de mesures conséquentes pour anticiper ces risques et menaces.

En janvier 2017, Jean-Yves Le Drian, alors ministre de la Défense, déclarait à l'occasion de la clôture d'un colloque sur le renouveau de la recherche stratégique : « De l'anticipation d'une dynamique générale à la prévision des événements eux-mêmes, il y a une différence majeure. C'est justement ce qui distingue l'anticipation d'une tendance, que rendent possible la recherche prospective et la prévision d'un événement au sens strict du terme » [53].

L'anticipation ne peut donc être performante que si nous disposons des connaissances utiles avant que le besoin ne s'exprime, c'est-à-dire avant le déclenchement d'éventuelles crises. De plus, ces connaissances doivent être connues par les services de renseignement intéressés, supposant ainsi une réelle coopération. Le principe de

---

[50] « Déclaration de M. Nicolas Sarkozy, président de la République, sur la nouvelle politique de défense, notamment la réforme des armées et la réintégration de la France dans le commandement militaire de l'Otan à Paris le 17 juin 2008 » (www.elysee.fr/).

[51] Cette fonction ouvre cinq domaines : le renseignement (avec notamment création du CNR, le Conseil national du renseignement) ; la connaissance des zones d'opérations potentielles ; l'action diplomatique (favoriser l'échange d'informations et stratégie globale) ; la démarche prospective (anticiper risques et menaces) ; et la maîtrise de l'information (http://archives.livreblancdefenseetsecurite.gouv.fr).

[52] « Chapitre 6 – La mise en œuvre de la stratégie ; A. La connaissance et l'anticipation », *Livre blanc sur la défense et la sécurité nationale*, La Documentation française, 2013, pp. 70-74 (www.livreblancdefenseetsecurite.gouv.fr/).

[53] Le Drian Jean-Yves, « La surprise stratégique - de l'anticipation à la réponse », conférence de clôture du colloque *Le renouveau de la recherche stratégique*, École militaire, 25 janvier 2017 (www.defense.gouv.fr/).

mutualisation des moyens pour le renseignement apparaît donc essentiel afin d'anticiper les risques divers.

Comme le rappelle le Secrétariat général de la défense et de la sécurité nationale (SGDSN), en termes de lutte contre la cybercriminalité, « par le biais d'*Internet* et des réseaux sociaux, l'espace cyber est un vecteur de diffusion des messages haineux et de manipulation de l'information qui mérite un suivi du renseignement » [(54)]. Ainsi, tous les services de renseignement doivent impérativement disposer d'outils spécifiques d'analyse des sources multimédias et consentir au partage d'informations et de sources ouvertes entre eux, de même qu'au niveau ministériel et interministériel. Cette collaboration entre les services est désormais possible et effective grâce au SGDSN et à la mise en œuvre d'une « coordination des travaux de prospective ». En effet, le Secrétariat a pour mission primordiale de définir les priorités et les orientations stratégiques et d'assurer la coordination des travaux de prospective conduits dans les ministères concernés.

(54) Coordination nationale du renseignement et de la lutte contre le terrorisme, *La stratégie nationale du renseignement*, juillet 2019 (www.sgdsn.gouv.fr/).

Étude de cas : la cyberdéfense française

Dans quelle mesure les technologies de l'information représentent-elles un enjeu nouveau et majeur en matière de défense pour la France, à l'aune d'une multiplication des interactions conflictuelles dans un espace cyber affranchi de la plupart des contraintes légales du droit international public ?

La cyberdéfense, souveraineté et sécurité numérique : de nouveaux enjeux décisifs pour les États

L'affaire de la cyberattaque (probablement russe) en 2017 visant des membres de la campagne d'Emmanuel Macron, alors candidat à l'élection présidentielle, a révélé au grand jour la prégnance des enjeux pour la souveraineté nationale portés par la cyberdéfense [55].

En effet, au cours de la dernière décennie, la cyberdéfense a émergé comme une des principales préoccupations sécuritaires des États. Le gouvernement français a notamment désigné celle-ci comme « un enjeu majeur de sécurité nationale », selon le rapport d'information publié en 2012 et réalisé au nom de la Commission des affaires étrangères, de la défense et des forces armées du Sénat [56].

Le néologisme « cyberdéfense » est aujourd'hui communément admis dans le discours des États. L'émergence et la prolifération d'une numérisation massive ont conduit à une généralisation des systèmes informatiques. Cela a créé un nouveau champ de conflictualité potentielle qui échappe aux mécanismes conventionnels de défense, et bouleverse principalement trois variables : les acteurs, le temps et l'espace.

Dans son rapport paru en février 2011 [57] précisant les grands objectifs de la stratégie française en matière de cyberdéfense, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a défini le cyberespace comme « l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées ». L'agence définit les mesures à prendre en la matière, en assurant « la fonction d'autorité nationale de défense des systèmes d'information » [58].

---

[55] David Romain, « Une cyberattaque russe sur le second tour de la présidentielle ? "Tout est plausible, mais..." », *Europe 1*, 25 avril 2017 (www.europe1.fr/).

[56] Commission des Affaires étrangères, de la Défense et des Forces armées, « La cyberdéfense : un enjeu mondial, une priorité nationale » (rapport d'information n° 681), Sénat, 18 juillet 2012 (www.senat.fr/).

[57] Agence nationale de la sécurité des systèmes d'information, « Défense et sécurité des systèmes d'information – Stratégie de la France », février 2011, 22 pages (www.ssi.gouv.fr/).

[58] « Décret n° 2011-170 du 11 février 2011 modifiant le décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé "Agence nationale de la sécurité des systèmes d'information" » (www.legifrance.gouv.fr/).

Elle décide de ce que « l'État met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et elle coordonne l'action gouvernementale ». La création de l'ANSSI en juillet 2009 a traduit l'impératif de sécurité des systèmes d'information et les nouveaux enjeux liés aux stratégies sécuritaires des États.

L'identification des menaces est particulièrement mise à l'épreuve par l'hétérogénéité et la complexité des acteurs stratégiques concernés. Par ailleurs, le caractère protéiforme des menaces, qui vont de la cybercriminalité à la prise de contrôle à distance des systèmes informatisés, constitue un autre défi pour les organes sécuritaires et défensifs nationaux. Ceux-ci doivent réadapter leurs stratégies à un espace virtuel inédit, en réponse aux formes de conflictualité nouvelles telles que les cyberattaques.

Ainsi, l'enjeu principal de la cyberdéfense implique la souveraineté nationale et place l'appareil étatique comme acteur central dans la protection de données à caractère militaire, politique ou économique. Cependant, se pose aussi la question de l'adaptation des cadres juridiques et légaux. L'exercice de la souveraineté se trouve *de facto* mis au défi, dans la mesure où « les limites de juridictions et de souveraineté sont plus floues et entremêlées » [(59)] dans l'espace cyber. Un réseau globalisé efface les frontières et rend plus délicate l'appréhension des activités illégales et des attaques.

Les États ont d'ores et déjà pris en compte ce défi et ont engagé une réflexion quant à la dimension juridique relative aux conflits cybernétiques, comme en témoigne la création en 2013 du Manuel de Tallinn au sein de l'Otan, visant à définir comment transposer le droit international à l'espace cyber [(60)]. S'il est généralement admis par les pays que le droit international est applicable dans le cyberespace, reste à savoir comment l'adapter à cette problématique [(61)]. À ce titre, l'approche française semble mettre en avant une défense de cet ordre juridique international.

En France, un corpus juridique interne s'est progressivement constitué afin d'intégrer les principes internationaux et encadrer la stratégie de cyberdéfense française. Les articles du code de la Défense composant la Loi de programmation militaire de 2013 [(62)] incluent pleinement la cyberdéfense. De plus, les articles de loi relatifs à la loi de programmation militaire [(63)] pour la période 2019-2025 démontrent notamment une hausse de l'attribution de missions et de compétences à l'ANSSI, dans le but d'améliorer la détection des menaces cybernétiques [(64)].

[(59)] Douzet Frédérick, « Géopolitique du cyberespace : La cyberstratégie de l'administration Obama », *Bulletin de l'association de géographes français*, vol. 91 n° 2, 2014, pp. 138-149 (https://journals.openedition.org/bagf/1837).

[(60)] Barat-Ginies Oriane, « Existe-t-il un droit international du cyberespace ? », *Hérodote*, vol. 2014/1-2 n° 152-153, pp. 201-220 (www.cairn.info/revue-herodote-2014-1-page-201.htm).

[(61)] Delerue François, « Stratégie juridique pour la cyberdéfense », *Les Champs de Mars*, n° 2018/1, pp. 297-306.

[(62)] « Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale » (www.legifrance.gouv.fr/).

[(63)] « Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense » (www.legifrance.gouv.fr/).

[(64)] Selon l'article L. 33-14, « à la demande de l'Autorité nationale de Sécurité des systèmes d'information, lorsque celle-ci a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information, les opérateurs de communications électroniques ayant mis en œuvre les dispositifs prévus au premier alinéa procèdent, aux fins de prévenir la menace, à leur exploitation, en recourant, le cas échéant, à des marqueurs techniques que cette autorité leur fournit ».

De façon plus générale, la constitution d'un cadre légal implique également la sécurisation des données. Ainsi, le Référentiel général de sécurité (RGS) – relatif aux échanges électroniques des autorités administratives et des usagers – doit permettre de sensibiliser, généraliser et orienter la sécurisation des systèmes informatiques des autorités administratives de l'État afin de garantir la protection de la souveraineté nationale. Il fixe les règles liées à la protection des données ainsi que des niveaux de sécurité et un code de conduite dans la mise en place de systèmes de sécurisation des informations. Ce référentiel, d'abord mis en place par une ordonnance de 2005, a été suivi d'une seconde version proclamée par arrêté du Premier ministre le 13 juin 2014 [65].

La France et la lutte informatique : une politique publique en constante adaptation

Depuis la création d'une doctrine de Lutte informatique offensive (LIO) en 2018, venue compléter la défensive déjà existante (LID) [66], la politique de cyberdéfense nationale française se décline en deux pendants – défensif et offensif. Elle témoigne d'une reconfiguration complète de l'organisation étatique et militaire. Si une telle ligne de conduite est représentative des ajustements réalisés par d'autres États, la France se démarque par sa diplomatie en faveur d'une meilleure prise en compte internationale des questions de cyberdéfense.

Alors que les modèles anglo-saxons concentrent leurs opérations au sein de la communauté du renseignement, la France applique donc une doctrine de séparation de ses capacités offensive et défensive. Cette distinction assure non seulement une plus grande flexibilité de la part de ces deux pôles dans les différentes missions qui leur incombent, mais permet également à ceux-ci d'être mieux acceptés par les acteurs non étatiques avec lesquels ils coopèrent, notamment parce qu'une action purement défensive est davantage respectueuse de la vie privée, des droits humains et des libertés. L'État français cherche ainsi à identifier des opérateurs d'importance vitale et services essentiels à son bon fonctionnement : 249 d'entre eux ont été, en 2016, identifiés comme indispensables à la vie de la Nation [67]. Pour faire face à des attaques informatiques susceptibles de porter atteinte aux intérêts du pays, la France s'est dotée d'un dispositif permettant d'opposer une défense informatique robuste [68]. La protection des réseaux informatiques est le premier rempart dans la lutte informatique défensive.

Du côté offensif, l'État français a reconnu en 2015 de manière officielle l'utilisation armée de certains outils cyber [69]. Considérée aujourd'hui comme une arme de supériorité opérationnelle au même titre que les armes conventionnelles, la LIO vise à produire des effets à l'encontre d'un système adverse pour altérer la disponibilité ou la

[65] Cf. Article L2321-1 de la loi n° 2013-1168 du 18 décembre 2013 (www.legifrance.gouv.fr/).
[66] Parly Florence, « Cyberdéfense : la France passe à l'offensive », 18 janvier 2018 (www.defense.gouv.fr/).
[67] Secrétariat général de la défense et de la sécurité nationale, *La sécurité des activités d'importance vitale*, communication externe, 18 mars 2016 (www.sgdsn.gouv.fr/).
[68] Ministère des Armées, *Politique ministérielle de lutte informatique défensive*, 2019 (www.defense.gouv.fr/).
[69] Cabirol Michel, « "La lutte informatique offensive n'est pas un tabou" (Jean-Yves Le Drian) », *La Tribune*, 28 septembre 2015 (www.latribune.fr/).

confidentialité des données [70]. Si elle a pour but de se substituer à d'autres modes d'action (sur l'ensemble du spectre de l'engagement militaire : renseigner, défendre, agir), de les préparer ou de les compléter, elle est néanmoins nécessairement soumise au droit international [71].

Le développement du cyber a entraîné une profonde restructuration de l'appareil militaire. La cyberdéfense française – s'articulant entre l'ANSSI et les services du ministère des Armées coordonnés depuis peu par le Commandement de cyberdéfense (Comcyber), créé en 2017 – est directement placée sous le commandement du chef d'État-major des armées (Céma).

Par ailleurs, l'enjeu critique des technologies liées à la cyberdéfense explique non seulement la volonté très marquée des États d'investir massivement dans ce domaine, mais aussi la nécessité d'une meilleure coordination internationale afin de réguler la production et l'exportation des armements et des activités offensives cyber. La France tend à se positionner comme un fer de lance pour un meilleur encadrement par le droit international. Le gouvernement et les services de défense, en faveur d'une plus grande régulation d'*Internet*, ont ainsi appelé à l'adoption de « mesures bienveillantes » par les géants du numérique, notamment lors de l'Appel de Paris lancé par Emmanuel Macron le 12 novembre 2018 à l'occasion du Forum de gouvernance de l'*Internet* [72], ou encore lors du sommet *Tech for Good* rassemblant le 15 mai 2019 plus de 80 acteurs du numérique [73].

Le discours français se fait aussi entendre au sein des organisations internationales, telles que l'UE et l'Otan, avec des prises de position marquées, comme la volonté affichée de mutualiser les moyens de cyberdéfense afin d'opposer une réponse commune lors d'attaques, et permettre la protection des alliés en difficulté. Ainsi, dès 2014, le plan baptisé « Pacte Défense Cyber » mentionnait l'idée de « bâtir des coopérations pour échanger des informations et éventuellement coordonner ses actions dans le cyberespace », citant l'UE et l'Otan, et même de « mutualiser au niveau européen la R&D qui peut l'être, par exemple dans le domaine de la sécurité des systèmes industriels », proposant comme cadre l'Agence de Défense européenne [74].

La France œuvre également à la reconnaissance de l'universalisation de plusieurs normes de droit international pénal et public applicables dans le cyberespace, notamment en ce qui concerne les contours du concept de souveraineté dans le cyberespace, le seuil du recours à la force ou d'une agression armée, l'interdiction de faire

---

[70] Ministère des Armées, « Éléments publics de doctrine militaire de lutte informatique offensive », 2019, 11 pages.
[71] Notamment en matière de déclenchement ou d'adoption de telles mesures, du recours à la force et de légitime défense.
[72] Ministère de l'Europe et des Affaires étrangères, « Cybersécurité : Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans le cyberespace », 2018 (www.diplomatie.gouv.fr).
[73] Piquard Alexandre et Chaffin Zeliha, « Tech for Good : une édition 2019 un peu plus tricolore », *Le Monde*, 17 mai 2019 (www.lemonde.fr/).
[74] Ministère de la défense, *Pacte Défense Cyber. 50 mesures pour changer d'échelle*, février 2014, 22 pages (www.defense.gouv.fr/).

usage du droit de légitime défense en réaction à la violation par un État du principe de diligence due, ou la définition de l'attaque en contexte de conflit armé [75].

Le traitement de l'information, une nouvelle frontière de la défense

Aujourd'hui, l'information existe dans un vaste espace numérisé et interconnecté. Elle se déploie dans des systèmes de communications mis en relation à l'échelle mondiale par des moyens divers, câbles sous-marins et satellites principalement. Elle est accessible grâce à des médias omniprésents dans la vie des individus. L'information est au cœur d'un monde électronique globalisant marqué par la superposition de l'information et du réseau.

Le traitement de l'information et sa transmission sont aujourd'hui les deux faces d'une même pièce ; l'avènement de la connexion informatique a ainsi marqué le début de stockages dans des *clouds*, la transmission systématique des informations traitées et la mise en réseau des appareils propres à une ou plusieurs institutions. Dès lors, l'espionnage par le biais de ces réseaux d'information est d'autant plus facilité que ces derniers, autrefois locaux et clos sur eux-mêmes, sont désormais reliés à l'*Internet* et sont donc largement ouverts au réseau global et « public ».

L'enjeu principal de leur sécurisation réside dans l'équilibre idéal entre la garantie de la disponibilité de l'information, la protection de son intégrité et sa confidentialité. Les protocoles de communication sont certes souvent protégés par la cryptographie [76], mais malgré leur complexité, leur caractère standardisé les expose à des attaques brutales et extrêmement contagieuses alors qu'une faille est susceptible d'impacter l'ensemble des systèmes et des appareils.

L'information apparaît donc particulièrement exposée dans le monde cyber. Son milieu, l'informatique, constitue un monde numérique fragile, accessible par des voies multiples et poreuses [77].

Alors que l'espionnage avait traditionnellement une cible définie, les moyens informatiques actuellement mis en place n'ont plus de visée spécifique. Ils se transforment en panoptique numérique, passant au crible de ses dictionnaires de mots-clés une grande partie du trafic des communications électroniques et mettant en place un espace où règne l'omniprésence d'un potentiel espionnage. Les principales actions relatives à l'information sont celles qui visent à déstabiliser des acteurs publics ou privés par l'exfiltration puis la divulgation massive de données sensibles. La cyberattaque se veut alors la plus insidieuse possible, afin que l'acteur visé puisse être mis en observation pour un temps indéfini dans le but d'avoir accès à ses projets stratégiques.

---

[75] Ministère des Armées, *Droit international appliqué aux opérations dans le cyberespace*, septembre 2019, 18 pages (www.defense.gouv.fr/).
[76] Définition du Larousse : Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données.
[77] Dejean Philippe et Sartre Patrice, « La cyber-vulnérabilité », *Études*, vol. 2015/7, pp. 21-31 (www.cairn.info/).

Par ailleurs, la cyberattaque à objectif idéologique peut apparaître comme un autre *modus operandi*. Elle prend la forme d'une action de vandalisme terroriste. Elle peut alors être associée à une tentative d'extorsion, à du parasitage contestataire d'un site *Web*, à la diffusion d'un message activiste, ou encore au vol et à la destruction de données ou de systèmes d'information, au nom d'une cause religieuse, politique ou idéologique [78].

Ainsi, l'information apparaît bien comme un enjeu majeur de la cyberdéfense et la multiplication de ses acteurs représente un véritable défi à relever pour les États. Parmi les technologies dont la maîtrise est nécessaire à l'exercice de leur souveraineté numérique, citons le chiffrement des communications, la fabrication d'outils de détection et d'attaque, ou encore la mise en œuvre de radios mobiles professionnelles de nouvelle génération avec l'essor de la 5G [79]. Pour être capable de se protéger contre les attaques informatiques, à les détecter et à en identifier les auteurs, l'État doit soutenir des compétences scientifiques et technologiques performantes.

La menace cyber appelle donc à repenser radicalement la stratégie militaire et défensive autour de l'information, car celle-ci engage l'intégrité de l'État, sa souveraineté, ainsi qu'une certaine compréhension et définition du droit. Dans ce cadre, c'est la nature même du cyber qui pose question : s'agit-il d'une rupture technologique ou, de manière plus décisive, d'une modification de la grammaire de la guerre [80] ?

Sur le plan technique, l'importance de l'espace cyber appelle le développement accru d'outils de prévention et de protection des données. Sur le plan politique, il implique de repenser la notion même d'ennemi. En effet, dans le cadre d'un monde surconnecté où un individu marginal peut causer des dégâts exponentiels, la menace peut potentiellement devenir multiforme et généralisée.

Dans ce contexte, l'univers du cyber appelle le politique à percevoir le monde comme un espace hostile où les menaces seraient devenues protéiformes et émaneraient d'une multitude d'acteurs, un espace où il n'y aurait plus d'ennemi défini et clairement désigné, mais plutôt empli d'ennemis potentiels. La discrimination ami/ennemi disparaîtrait au profit d'un monde gouverné par la potentialité de l'hostilité. La défense de l'information se ferait donc au sein d'un univers dont l'horizon serait toujours celui de la conflictualité. Le cyberespace rendrait manifeste la nouvelle nature post-hobbesienne du monde, celle de la lutte de tous contre tous [81].

Ainsi, la menace cyber modéliserait un espace hostile témoignant de la généralisation de la menace et des nouvelles frontières de la défense des États. Prendre conscience de cette réalité semble aujourd'hui nécessaire pour comprendre des enjeux bien plus vastes comme le terrorisme ou les guerres hybrides.

---

[78] Lehu Jean-Marc, « Cyberattaque : la gestion du risque est-elle encore possible ? Analyse et enseignements du cas Sony Pictures », *La Revue des Sciences de Gestion*, vol. 2018/3-4, n° 291-292, pp. 41-50.
[79] Gautier Louis, « Cyber : les enjeux pour la défense et la sécurité des Français » *Politique étrangère*, vol. 2018/2, Institut français des relations internationales (Ifri), pp. 29-42.
[80] Clausewitz (von) Carl, *De la guerre*, 1832, Livre I, Chapitre 1. La guerre serait le produit d'une histoire et d'une logique politique, la guerre étant considérée comme la « *poursuite de la politique par d'autres moyens* ».
[81] Kempf Olivier, « Cyber et surprise stratégique », *Stratégique* vol. 2014/2, Institut de stratégie comparée (ISC), p. 111-123.

Conclusion

Dans ce *Cahier de la RDN* sur les nouvelles frontières de la défense, nous avons donc analysé trois domaines – maritime, spatial et cyber – qui, s'ils peuvent paraître séparés au premier abord, sont en réalité extrêmement liés. Pour chacune de ces thématiques, les États ne représentent plus les seuls acteurs ; ils doivent composer avec des entreprises privées, des ONG, mais aussi des organisations criminelles ou terroristes. Les nouvelles technologies permettent à ces différents protagonistes non étatiques d'obtenir des pouvoirs équivalents à ceux des pays. Dans le seul domaine des infrastructures, les câbles sous-marins, les satellites et les réseaux sont gérés par des entreprises privées dont les moyens n'ont (pour les plus importantes d'entre elles) pas grand-chose à envier aux grandes puissances.

Cette importance accrue des acteurs non étatiques oblige dans certains cas des délégations de compétences qui sont plus importantes dans les secteurs (le cyber par exemple) où les coûts sont réduits. Quand les coûts augmentent, les États redeviennent quasi hégémoniques (comme le montre le domaine de l'Espace). On retrouve ainsi une forme de compétition entre ces acteurs, étatiques ou non, qui travaillent ensemble et s'affrontent, parfois les deux en même temps, dans un cadre où les règles ne semblent pas vraiment établies.

On peut tirer trois conclusions de cette analyse :

– Tout d'abord, la place dominante des États-Unis, qui restent la première puissance mondiale, et ce, dans tous les domaines malgré le rattrapage impressionnant effectué par la Chine ces dernières années. À côté des efforts déployés par les deux superpuissances, ceux de la France peuvent paraître moins importants. Pourtant, il faut noter qu'ils touchent eux aussi tous les domaines, prouvant que ce pays reste une grande puissance avec laquelle il faut compter.

– Ensuite, l'émergence de nouveaux acteurs et de nouvelles menaces impliquent une adaptation rapide des stratégies de défense. Face à l'évolution des technologies, les États doivent mettre en place de nouvelles lois et doctrines, ainsi que de nouveaux équipements. Ils ont aussi l'obligation de s'allier à d'autres acteurs.

– Enfin, les trois sujets pointent l'importance du secteur privé sur lequel les États s'appuient afin de déployer leur puissance, et l'importance de l'indépendance d'une stratégie industrielle nationale permettant de ne pas dépendre d'autres acteurs.

Ce dernier point nous ramène à l'actualité avec la crise du coronavirus (Covid-19) durant laquelle la France se retrouve menacée d'une pénurie de médicaments [(82)], de gels hydroalcooliques et de masques [(83)]. Il est frappant de noter les similitudes entre cette crise et les sujets abordés jusque dans le vocabulaire utilisé, le président Macron ayant déclaré le 16 mars 2020 : « Nous sommes en guerre ». ◆

[(82)] « Coronavirus. La menace d'une pénurie de médicaments plane sur l'Europe », *Ouest-France*, 7 avril 2020 (www.ouest-france.fr/).
[(83)] BAUDAIS Pierrick, « Coronavirus. Pénurie de masques : comment en est-on arrivé là ? », *Ouest-France*, 20 mars 2020 (www.ouest-france.fr/).

Postface
Extension du domaine de la stratégie ?

Jean-Vincent HOLEINDRE

Professeur de science politique à l'Université Panthéon-Assas. Directeur scientifique de l'IRSEM.

C'est un plaisir de conclure, par cette postface, le *Cahier de la RDN* qui expose les travaux menés par les étudiants suivant le cours de mon collègue et ami le professeur Tristan Lecoq, donné en Sorbonne et consacré aux questions de défense. Je les remercie vivement de me proposer de contribuer à ce beau volume accueilli par la *RDN*, revue centrale du débat stratégique français dirigée par le général Jérôme Pellistrandi, rédacteur en chef, dont il faut ici saluer le travail. Ce projet réunissant les étudiants et leur enseignant est renouvelé d'année en année, pour le meilleur. Il matérialise la collaboration fructueuse entre Sorbonne Université et l'Université Panthéon-Assas, qui portent ensemble le Master Relations internationales, dont une partie des contributeurs est issue.

« Les nouvelles frontières de la défense : la mer, l'Espace, l'information » : la perspective et les thèmes choisis cette année sont particulièrement pertinents. Ils mettent en lumière des évolutions stratégiques majeures qui sont le quotidien de celles et ceux qui pensent et font la guerre aujourd'hui. Trois de ces évolutions peuvent ici être relevées, qui redéfinissent au concret les frontières de la défense : premièrement, la diversification des acteurs qui composent la scène internationale ; deuxièmement, le développement de nouveaux domaines ou champs de bataille où se déroule le combat ; troisièmement, la combinaison croissante entre formes cinétiques et non cinétiques de la guerre, qui conduit au développement – sans doute excessif – de la notion d'hybridité.

Tout d'abord, la diversification des acteurs internationaux a des implications stratégiques fortes. Comme le montrent bien les pages qui précèdent, les États voient leur action perturbée ou influencée par les acteurs non étatiques. Les groupes djihadistes (*Al-Qaïda*, *Daech*, *Boko Haram*…), qui usent d'un mode d'action terroriste, restent l'une des menaces majeures à la sécurité nationale des États, notamment les démocraties occidentales désignées comme ennemies sur le plan idéologique par ces groupes.

Sur le plan économique, le succès des GAFAM (Google, Apple, Facebook, Amazon, Microsoft) illustre certes la résilience de la puissance américaine, capable de faire naître ces géants de l'innovation numérique. Elle montre aussi la capacité d'influence et parfois de nuisance des acteurs privés sur la scène internationale, à l'image de Strava,

application de course à pied qui, en publiant les tracés de coureurs (dont de nombreux militaires), a dévoilé à son corps défendant la localisation de bases militaires secrètes.

Enfin, à l'échelle des sociétés, l'actualité internationale fait ressortir la capacité croissante des individus à se mobiliser face aux États ainsi que leur volonté de peser sur la décision politique. La publication par *Wikileaks* de documents diplomatiques confidentiels américains en 2010 et 2011 constitue l'un des témoignages de cette injonction sociale à la transparence dans un domaine de l'action politique, la politique étrangère, où le secret est, et reste encore, la règle. Ces révélations ont fortement ébranlé les diplomaties, et ont conduit les États à développer leur « stratcom », stratégie de communication.

De manière générale, bien que les États restent les acteurs centraux et déterminants du système international, l'affirmation d'acteurs non étatiques à l'échelle mondiale constitue une entrave, qui les oblige à s'adapter et à absorber les compétences acquises au sein des sociétés civiles (comme on le voit avec les *hackers*).

Le deuxième point que ce volume souligne avec brio, est l'émergence de nouveaux domaines d'action militaire, à l'image du spatial ou du cyber, qui font l'objet de deux études de cas bien documentées. Ces « nouveaux » domaines s'ajoutent aux trois « classiques » que sont le terrestre, le maritime et l'aérien. Sur les trois parties que comporte ce numéro, deux sont consacrées à l'espace et l'information qui sont aujourd'hui au centre de l'attention, comme en témoigne, dans le cas français, la rédaction de documents de doctrine tels que la *Revue stratégique de cyberdéfense* en 2018 (produite par le SGDSN) ou la *Stratégie spatiale de défense* en 2019.

Ces nouveaux domaines ne viennent aucunement se substituer aux formes « classiques » de l'action militaire (terrestre, maritime ou aérien). Au contraire, ils complexifient et densifient la scène guerrière. Un bon exemple est celui des câbles sous-marins, qui représentent, par leur contenant et leur contenu, un enjeu essentiel des stratégies maritimes et informationnelles. La sécurisation des câbles sous-marins, qui font transiter par les mers et les océans les données numériques, suppose en effet la maîtrise de l'espace maritime. La gestion de ce réseau mondialisé suscite d'un côté des tensions géopolitiques et territoriales, mais elle justifie de l'autre le renforcement des régulations et des coopérations fonctionnelles, dans un contexte où la privatisation des câbles par les GAFAM s'amplifie ; plus de 50 % du marché sur l'Atlantique aujourd'hui est détenu par les GAFAM contre 5 % il y a quatre ans. Sur ce sujet, il convient également de relever les disparités entre les États : si la Chine et la Russie se sont organisées pour ne pas être économiquement dépendantes des câbles sous-marins, il n'en est pas de même de l'Europe dont le trafic dépend essentiellement des États-Unis et des GAFAM. Ce faisant, le caractère stratégique de ces câbles, comme du reste des satellites, rappelle que la dématérialisation du monde, incarnée par les nouveaux usages numériques, est toute relative. Les câbles sous-marins, comme les satellites, apparaissent donc comme un révélateur de la dualité des conflits actuels : dualité au sens où la compétition économique, qui peut se muer en « guerre commerciale », redouble les rivalités politiques et les clivages idéologiques (entre la Chine et la Russie d'une part, et les puissances occidentales d'autre part) ; dualité aussi, dans ces conflits technologiques,

commerciaux et politiques, au sens où les intérêts publics s'entrelacent aux intérêts privés ; dualité enfin puisque l'ancien se mêle au moderne, les puissances qui maîtrisent les « nouveaux » flux immatériels de l'économie de la connaissance étant précisément celles qui dominent les territoires et les mers (États-Unis, Chine, Russie, Grande-Bretagne et dans une moindre mesure la France).

L'articulation des différents domaines d'action militaire, par ces stratégies « multidomaines » ou « multidimensionnelles », constitue donc un enjeu stratégique majeur, notamment sur le plan organisationnel. Les armées distinguent ainsi ces nouveaux domaines d'action, la France créant par exemple des commandements propres au cyber et à l'espace. Ces structures doivent cependant être adossées à une vision globale de la guerre – ce qui suppose de fournir un effort majeur d'anticipation et de prospective. Toute innovation technologique constitue, en effet, le miroir de pratiques sociales, économiques et politiques. En ce sens, elle ne revêt pas seulement une portée technologique et a besoin, pour être comprise, des sciences humaines et sociales.

La troisième tendance identifiée dans les différents textes du volume, est le développement de « l'hybridité ». Le terme suscite débats et controverses, mais il désigne commodément une tendance stratégique qui n'est pas nouvelle : la scène guerrière combine des actions militaires dites « conventionnelles » (envoi et usage de troupes au sol, par exemple) et « non-conventionnelles » (cyberattaques, intoxications…). Le conflit en Ukraine a mis en évidence la manière dont les États, la Russie en tête, peuvent, outre le fait d'envoyer des troupes, user de stratégies informationnelles visant à affaiblir leurs adversaires, en usant de la propagande médiatique ou en agissant plus spécifiquement sur les processus électoraux. Dans le cas russe, cette stratégie « indirecte » s'inscrit dans une longue tradition d'art opératif remontant aux années 1920 et 1930, par lequel les stratèges soviétiques pensaient la guerre au-delà de la guerre. L'idée essentielle est que le conflit armé ne s'arrête pas au champ de bataille, celui-ci prenant des formes multiples, qui ne relèvent pas seulement de l'action militaire « directe ». Cette tendance n'est pas propre à la Russie et elle concerne, à vrai dire, l'ensemble des acteurs stratégiques, étatiques ou non. On l'observe en Chine, qui investit tous azimuts s'appuyant, pour l'élaboration de sa doctrine, sur une longue tradition stratégique promouvant l'hybridité. On l'observe aussi chez les groupes djihadistes usant de propagande pour attirer les volontaires de la mort en leur sein ou développant des techniques très proches des services de renseignement étatiques. Elle est utilisée enfin par les États démocratiques, aussi bien sur le plan offensif que défensif, considérant que ces « guerres informationnelles » reflètent avant tout un conflit de normes et de valeurs (ce qui suppose, de la part des démocraties, de savoir se prémunir des menaces ainsi que Raymond Aron l'avait déjà souligné, à l'aube de la guerre, dans sa conférence à la Société française de philosophie en 1939, « États démocratiques et États totalitaires »).

Ces trois tendances dessinent un questionnement plus général quant au périmètre de la stratégie. Peut-on considérer que ce périmètre s'étend, justifiant qu'on substitue la « sécurité globale » à la stratégie militaire ? Clausewitz s'interrogeait déjà sur ce point considérant, d'une part, que toute guerre est un conflit armé et « sanglant » entre deux entités politiques et, d'autre part, que cet affrontement n'est pas seulement

physique, mais aussi moral et surtout politique. Si l'on suit Clausewitz, la guerre est par nature bifide, militaire et politique, matérielle et immatérielle, physique et morale. Accélérée par la révolution nucléaire combinée à celle des nouvelles technologies, « l'extension du domaine de la stratégie » (pour paraphraser le titre du roman de Michel Houellebecq, *Extension du domaine de la lutte*) est à l'œuvre. Par cette expression, on désigne l'intégration, dans la pensée et l'action militaire, de facteurs qui lui sont extérieurs. Ce phénomène ne constitue pas une rupture récente liée aux nouvelles technologies de l'information et de la communication, elle constitue en réalité une donnée essentielle de la réflexion stratégique qui se nourrit toujours de facteurs externes, qu'ils soient économiques, culturels, technologiques ou politiques. La guerre est donc « hybride » par nature, de même que la stratégie, à l'image de la pensée, se nourrit du « dehors ». La stratégie n'est jamais à elle-même sa propre fin, à l'instar de la guerre qui n'est jamais qu'un moyen dont il faut user à bon escient. ◆

RDN

La revue du débat stratégique

10 numéros par an

N° 831 - Juin 2020

www.defnat.com

Suivez l'actualité stratégique dans la Tribune de la RDN en ligne

Revue Défense Nationale

École militaire, 1 place Joffre, Case 64, 75700 Paris SP 07

Étude

Les nouvelles frontières de la défense
La mer, l'Espace et l'information

Depuis 2017, les étudiants des masters « Armées, guerres et sécurité » et « Dynamique des systèmes internationaux » de l'Université de la Sorbonne et « Relations internationales » des universités Paris II et de la Sorbonne participent activement à une réflexion à partir de l'enseignement qui leur est délivré, dans le contexte politique dans lequel ils vivent et étudient, avec un recul naissant et fondé sur le monde qui les entoure et où ils serviront.

En 2017, ils ont réalisé une étude sur « La défense et la sécurité dans les programmes présidentiels ». En 2018, ils ont analysé « La défense et la sécurité nationale. Un an après » et en 2019, année des élections européennes, leur travail portait sur « Défense de l'Europe, défense européenne, Europe de la défense ».

En 2020, leur étude est toute aussi actuelle : « Les nouvelles frontières de la défense. La mer, l'Espace et l'information », dans le contexte d'une projection des intérêts de puissance vers les espaces maritimes, de l'Espace comme milieu d'affrontement de nouvelles armes, des risques liés aux systèmes d'information et d'une dématérialisation des menaces, qui sont la trace et la marque des problématiques de défense et de sécurité nationale de la France, de ses alliés, de ses voisins et du reste du monde, comme autant de témoins du passage d'une défense aux frontières à la défense sans frontières.

Comme leurs prédécesseurs, les étudiants de cette belle promotion sont engagés, décidés, travailleurs. Leur Professeur leur doit parmi ses plus belles années d'enseignement.

Tristan LECOQ

SORBONNE UNIVERSITÉ — CENTRE THUCYDIDE — analyse et recherche en relations internationales — LES JEUNES INTERNATIONALISTES — UNIVERSITÉ PARIS II PANTHÉON-ASSAS

Lancée en 1939 par le Comité d'études de défense nationale (Association loi 1901), la Revue Défense Nationale assure depuis lors la diffusion d'idées nouvelles sur les grandes questions nationales et internationales qu'elle aborde sous l'angle de la sécurité et de la défense. Son indépendance éditoriale lui permet de participer activement au renouvellement du débat stratégique. La Revue Défense Nationale permet de garder le contact avec le monde de la défense et apporte, grâce à ses analyses, la réflexion à l'homme d'action.

www.defnat.com