MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

Lycée(s) | **Général** | Technologique | Professionnel

Niveau(x) | CAP | Seconde | Première | **Terminale**

Enseignement(s) | Commun | **De spécialité** | Optionnel

Histoire-géographie, géopolitique et sciences politiques

L'enjeu de la connaissance (26-28 heures)

Sommaire

Programme

Ce thème a un double objectif : mettre en avant les conditions nationales et internationales de la construction de la connaissance, en particulier de la connaissance scientifique, et expliquer la manière dont les États favorisent ou contrôlent, entre coopérations et conflits, la production ou la diffusion de celle-ci.

- Le premier axe souligne l'importance de l'alphabétisation des sociétés pour accroître le nombre de personnes susceptibles de produire, de recevoir et de diffuser de la connaissance, et examine le fonctionnement d'une communauté savante à partir de l'exemple des recherches sur la radioactivité au XX^{e} siècle.
- Le second axe montre comment des États se sont saisis de l'enjeu de la connaissance dans leurs affrontements, comme lors de la guerre froide, ou dans leur souci de favoriser leur développement économique, restreignant ou favorisant la circulation des connaissances scientifiques et technologiques.

<table>
<tr><td colspan="2">Introduction
La notion de « société de la connaissance » (Peter Drucker, 1969), portée et débats.
La notion de communauté savante, communauté scientifique en histoire des sciences.
Les acteurs et les modalités de la circulation de la connaissance.</td></tr>
<tr><td>Axe 1
Produire et diffuser des connaissances</td><td>Jalons
• Donner accès à la connaissance : grandes étapes de l'alphabétisation des femmes dans le monde, du XVI^{e} siècle à nos jours.
• Produire de la connaissance scientifique : recherche et échanges des hommes et des femmes de science sur la question de la radioactivité de 1896 aux années 1950.</td></tr>
<tr><td>Axe 2
La connaissance, enjeu politique et géopolitique</td><td>Jalons
• Le renseignement au service des États : les services secrets soviétiques et américains durant la guerre froide.
• Circulation et formation des étudiants, transferts de technologie et puissance économique : l'exemple de l'Inde.</td></tr>
<tr><td>Objet de travail conclusif
Le cyberespace : conflictualité et coopération entre les acteurs</td><td>Jalons
• Le cyberespace, entre réseaux et territoires (infrastructures, acteurs, liberté ou contrôle des données…).
• Cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français.</td></tr>
</table>

Sens général du thème en classe de terminale

Le professeur peut envisager un traitement du thème en **26 à 28 heures** (évaluation comprise).

Explication du préambule du thème

La géopolitique, qui est au cœur de l'enseignement de spécialité, met en lumière les conflits et les coopérations entre entités politiques. Ces conflits et ces coopérations s'inscrivent dans les évolutions multiples des sociétés et dans de grandes tendances parfois cumulatives. Il en est ainsi de l'accroissement des connaissances et des progrès de la circulation de l'information. Sociétés, États et organisations internationales sont semblablement concernés par la question de la connaissance, de sa production, de sa circulation, de son contrôle éventuel.

Il y a un lien fort entre ce thème abordé en terminale et le thème 4 du programme de première. Ce dernier concernait l'information, et il est important que le rapport entre information et connaissance soit clairement perçu par les élèves. L'information est plus ponctuelle, la connaissance, telle qu'elle est envisagée ici, l'englobe et la dépasse, en particulier dans l'expression de « société de la connaissance » telle que développée plus loin. Elle englobe en particulier les sciences et la technologie.

L'idée générale de ce thème est bien de saisir toutes les dimensions de cet enjeu de la connaissance, qui est rarement présent directement dans les programmes scolaires, bien qu'il soit très présent au fil du cursus des élèves. Ces derniers ont bien conscience de vivre dans un monde où les évolutions technologiques sont rapides et où l'interpénétration entre science et technologie structure leur quotidien. Ils sont également très au fait de l'importance de l'information, et ont eu à plusieurs reprises, non seulement dans le programme de spécialité de première, mais aussi dans celui d'enseignement moral et civique (EMC) et dans le cadre de l'éducation aux médias et à l'information (EMI), l'occasion de saisir les enjeux citoyens de la diffusion de connaissances inexactes ou tronquées, en particulier dans le cadre des réseaux sociaux. À titre d'exemple, les polémiques concernant la vaccination ou des phénomènes comme le « platisme » auront pu les alerter sur ce point.

Explication de la structure générale du thème

Les deux axes « Produire et diffuser de la connaissance » et « La connaissance, enjeu politique et géopolitique » sont des guides pour aborder, à partir d'angles d'attaques et d'exemples précis, une matière par nature profuse, car toutes les activités humaines ont une dimension cognitive. Ces deux axes ne sont pas absolument étanches, et il ne faudra pas hésiter à mettre en avant la cohérence de l'approche en montrant comment chaque jalon s'inscrit dans l'ensemble du thème.

Ainsi, l'enseignement est présent dans les deux axes, aussi bien dans la question de l'alphabétisation des femmes depuis le XVIe siècle (enseignement primaire) que dans celle de la circulation internationale des étudiants indiens (enseignement supérieur). De même, les enjeux de rivalité internationale traversent les deux axes : les recherches sur la radioactivité débouchent entre autres sur le projet Manhattan, et les questions militaires liées à l'arme nucléaire sont très présentes dans l'activité des services secrets soviétiques et américains durant la guerre froide.

La structure du thème indique également à quel point la production et la diffusion croissante des connaissances sont un des aspects du phénomène global que nous désignons sous le nom de mondialisation. Comme très souvent dans l'enseignement de spécialité HGGSP, l'aspect dialectique du phénomène est central : les connaissances sont de plus en plus diffusées, reçues et produites sur le plan international, ce qui ouvre la perspective d'une unification croissante de l'humanité, mais dans le même temps, ce domaine en extension est aussi le théâtre de rivalités, ce qui explique l'utilisation fréquente dans cet enseignement du couple conflit/coopération. Cela s'applique de manière particulièrement frappante dans l'objet de travail conclusif sur le cyberespace.

Ce thème conduit donc à s'intéresser aux systèmes éducatifs (pour l'alphabétisation des filles comme pour la circulation des étudiants indiens), à la communication et aux débats à l'intérieur d'une communauté scientifique (pour les échanges sur la question de la radioactivité), mais aussi, dans une optique géopolitique, au rôle des États et à l'évolution de la technologie, ce qui structure la réflexion dans le thème conclusif.

Problématique générale du thème

Dans quelle mesure des conditions politiques et géopolitiques favorisent-elles la construction et la diffusion de la connaissance ? Pourquoi la connaissance est-elle un enjeu politique majeur ?

Orientations pour la mise en œuvre de l'introduction du thème

Articulation et sens général

L'introduction de ce thème est consacrée à la mise en place de notions fondamentales qui seront mobilisées tout au long de son traitement. Il incombe au professeur de veiller à l'articulation entre les éléments présentés dans la mise en œuvre de l'introduction et les éléments développés dans les axes et l'objet de travail conclusif.

Éléments fondamentaux. Notions et points de connaissance

La notion de « société de la connaissance » (Peter Drucker, 1969), portée et débats

La notion de « société de la connaissance » est due à Peter Drucker dans un ouvrage de 1969, intitulé *The Age of Discontinuity. Guidelines to Our Changing Society* (New York, Harper and Row, 1969). Cet ouvrage a été rapidement traduit en français sous le titre *La grande mutation : vers une nouvelle société* (trad. Philippe Quoniam de Schompré, Paris, Les Éditions d'organisation, 1970). Peter Drucker, universitaire et éditorialiste, est l'un des fondateurs de la réflexion managériale. L'idée maîtresse de son ouvrage est que la connaissance, capacité à mettre en œuvre de l'information, devient la principale ressource du développement économique. Cette idée est reprise par les organisations

internationales, en particulier par l'Unesco et par l'Union européenne, en mettant l'accent sur la diffusion de compétences, qui seraient fondamentales à la fois pour le bon fonctionnement de la société et pour celui de l'économie. L'un des critiques de cette notion, Alain Mounier, en a donné une bonne définition, qui rend compte à la fois de sa première élaboration et de ses développements ultérieurs : « La société de savoir ou de la connaissance serait ce stade de développement où l'éducation, la science, les innovations technologiques et l'information occuperaient une place prépondérante comme vecteur de la croissance économique et de la justice sociale[1] ».

La notion « d'économie de la connaissance » est tout aussi répandue et correspond à un lien établi entre la prospérité et l'accroissement non seulement du volume d'informations, mais également d'une capacité à innover. Cela a conduit l'Unesco et l'Union européenne (avec le « Protocole de Lisbonne » en mars 2000) à promouvoir une approche par compétences dans le domaine de l'éducation.

Comme toute notion générale, les notions de « société de la connaissance » et « d'économie de la connaissance » ont été très discutées. On leur reproche globalement leur optimisme, leur insuffisante prise en compte des aspects financiers du capitalisme, des conflits sociaux et des inégalités, du poids des cultures d'origine des différents pays où les politiques visant à l'accroissement des compétences de la population se développent, la surestimation de la dimension « post-industrielle » de l'économie contemporaine et la sous-estimation des inégalités territoriales et sociales engendrées par le poids accru de la connaissance dans la vie économique. Le développement des technologies de l'information et de la communication (TIC) comme ceux plus récents de l'intelligence artificielle suscitent par ailleurs à la fois enthousiasme et angoisses.

Cependant, on emploiera ici la notion pour ce qu'elle affirme de plus incontestable : le rôle moteur de la connaissance et de l'éducation dans la vie sociale, économique et politique contemporaine.

La notion de communauté savante, communauté scientifique en histoire des sciences

L'histoire des sciences est rarement abordée en tant que telle dans les programmes d'histoire de tronc commun. Ainsi, en classe de 4e, le « développement de l'esprit scientifique » au XVIIIe siècle est étudié dans l'optique de la remise en cause des fondements politiques, sociaux et religieux des sociétés modernes. Toutefois, en classe de seconde générale et technologique, le « développement des sciences » est abordé, notamment au travers de figures historiques (Galilée, Newcomen, Émilie du Châtelet). L'un des enjeux et des apports de l'histoire (et de la sociologie) des sciences est précisément d'avoir mis à distance la représentation commune du travail scientifique comme œuvre solitaire[2].

La notion de communauté scientifique est issue des travaux du sociologue Robert K. Merton dans les années 1940. Devenue un classique de l'épistémologie et de l'histoire des sciences, elle met l'accent de manière décisive sur la dimension collective de la démarche scientifique. La communauté scientifique (qui se distingue

1. Alain Mounier, « Critique de la société de la connaissance : les paradoxes de la réforme éducative en Thaïlande », *in* M. Carton, J.-B. Meyer (dir.), *La société des savoirs : trompe-l'œil ou perspectives ?*, Paris (L'Harmattan), 2006, p. 233-261. Disponible en ligne.
2. Pour une présentation synthétique de l'histoire des sciences comme discipline, voir Laurent-Henri Vignaud, « Sciences et techniques : histoire d'un champ disciplinaire », *Histoire des sciences et des techniques*, Paris (Armand Colin), 2020, p. 11-52.

de la communauté savante par la professionnalisation de ses membres) organise la discussion des travaux de ses membres, la vérification de leur méthode et de leurs conclusions, et valide celles-ci. Elle repose sur un éthos scientifique, un ensemble de valeurs et de normes intégrées par les scientifiques : universalisme, communalisme, désintéressement, scepticisme organisé. En effet, comme l'avait établi le philosophe Karl F. Popper dans un ouvrage publié en 1934, *La Logique de la découverte scientifique*, un énoncé scientifique doit être « falsifiable », c'est-à-dire qu'on doit pouvoir le vérifier et montrer sa fausseté éventuelle. La science est constituée par ce qui a été déjà validé par des communautés savantes constituées en disciplines scientifiques. Mais la démarche scientifique consiste à formuler et vérifier des hypothèses, qui peuvent éventuellement remettre en question le consensus précédent sur tel ou tel sujet. Il est fondamental d'expliquer cela aux élèves, qui peuvent être confrontés à des discours anti-scientifiques. Il est normal qu'il y ait des débats entre scientifiques, mais ceux-ci sont tranchés par l'examen collectif de leurs méthodes et de leurs conclusions. L'existence d'une communauté scientifique est donc une condition *sine qua non* du progrès des sciences.

Les acteurs et les modalités de la circulation de la connaissance

Si l'histoire des sciences a pu montrer combien production et circulation des connaissances sont intimement liées[3], ce dernier point introductif doit permettre une première réflexion spécifiquement orientée sur la circulation de la connaissance. Dans la suite du modèle de Peter Drucker, les différents modèles économiques de circulation de la connaissance, notamment scientifique, peuvent être interrogés.

Après avoir réactivé les éléments de la révolution technique de l'information abordés en classe de première dans le cadre du thème « S'informer », on peut schématiquement opposer un modèle d'accès gratuit et collaboratif, incarné par Wikipédia, et un modèle payant fondé sur l'expertise. Il s'agit ensuite de montrer que les politiques d'accès ouvert ou accès libre (*open access*) permettent de concilier circulation (ou en tout cas mise à disposition) gratuite de la connaissance et validation experte (par les pairs). Cela suppose toutefois un financement des chercheurs ou scientifiques (financement public ou privé). L'enjeu de la monétisation et de l'accès aux publications scientifiques peut également être abordé[4].

Enfin, on peut aborder l'enjeu de la vulgarisation et de la médiatisation scientifiques, y compris dans le processus de décision politique (lien possible avec les travaux du GIEC, évoqués dans le thème « Environnement »).

Pistes pédagogiques

Il est possible de travailler avec les élèves la capacité « **Analyser, interroger, adopter une démarche réflexive** » à propos de la notion de « société de la connaissance » en confrontant les thèses de Peter Drucker à certaines de ses critiques. Des extraits de différents ouvrages de Peter Drucker lui-même peuvent également être confrontés à des documents statistiques ou cartographiques mettant en évidence l'inégale contribution des États à la « société de la connaissance » (par exemple en comparant le nombre de brevets déposés).

3. René Sigrist, « Les communautés savantes européennes à la fin du siècle des Lumières », *M@ppemonde*, vol. 2, no 110, 2013, accessible en ligne.
4. Une vidéo de la série « Data gueule », produite par France Télévisions, et intitulée « Privés de savoir ? », revient sur ces enjeux.

On peut également réfléchir à l'Internet comme modalité de circulation de la connaissance, en envisageant à la fois les bénéfices et les risques d'un tel outil pour fonder une société de la connaissance.

La capacité « **Se documenter** » peut également être travaillée dans une optique réflexive : l'ouvrage majeur de Peter Drucker, *The Age of Discontinuity*, n'est pas gratuitement accessible en ligne, mais de nombreux comptes rendus publiés dans des articles à comité de lecture, sont disponibles en ligne. C'est aussi l'occasion de réfléchir aux enjeux de la langue (et de la traduction) dans les modalités de circulation de la connaissance.

Orientations pour la mise en œuvre de l'axe 1 du thème : « Produire et diffuser des connaissances »

Articulation et sens général

Articulation de l'axe avec le thème

Après une introduction posant les grandes notions de société de la connaissance et de communauté scientifique avec les élèves, selon une démarche propre à la spécialité HGGSP, l'axe 1 amorce la réflexion sur les enjeux essentiels que sont la diffusion et la production des connaissances pour l'affirmation des États. Il convient d'être attentif au double objectif précisé dans l'en-tête du thème : « mettre en avant les conditions nationales et internationales de la construction de la connaissance, en particulier de la connaissance scientifique, et expliquer la manière dont les États favorisent ou contrôlent, entre coopération et conflits, la production et la diffusion de celle-ci ». Ainsi, l'unité profonde du thème est structurée autour d'un paradoxe apparent : si pour un État, encourager la production et la diffusion d'un savoir constitue une manière d'asseoir sa puissance, d'assurer son développement et son rayonnement, cela représente également un risque d'en être dépossédé. Loin d'aller de soi, la diffusion des connaissances et leurs modalités de production représentent un enjeu à la fois politique, social, économique et géopolitique.

Il s'agit de donner à voir aux élèves l'étroite intrication entre savoir et pouvoir, interrogée par les philosophes de Platon à Foucault, et leurs rapports complexes dans nos sociétés. Le savoir institutionnalisé, formel, dominant, est la résultante d'un processus actif de production et de diffusion de connaissances plus ou moins encadré par l'État, qui peut générer des rivalités et des tensions à toutes les échelles. Cette mise en tension, qui doit servir de fil d'Ariane tout au long du thème, permet aux élèves de mettre en perspective le rôle de l'enseignement et de la transmission des connaissances dans une approche transdisciplinaire : histoire, géographie, géopolitique et sciences politiques offrent en effet des clés de lecture et de compréhension complémentaires pour développer un recul critique sur la construction des savoirs.

Dans ce cadre de réflexion, le premier axe vise à montrer les enjeux et les conditions de la production et de la diffusion des connaissances, à travers les politiques nationales de promotion de l'alphabétisation[5], mais également le développement de réseaux

5. Le premier jalon peut également intégrer l'action supranationale en faveur de l'alphabétisation des femmes (Unesco, organisations non gouvernementales).

internationaux tel que les communautés scientifiques. Il doit être traité dans la perspective de celui qui suit : en effet, cette réflexion permet d'établir des liens avec l'axe 2, qui aborde plus directement la manière dont les États se saisissent des enjeux de la connaissance pour s'inscrire dans la compétition mondiale et asseoir leur puissance. Elle est également nécessaire pour appréhender le thème conclusif, qui traite plus spécifiquement des enjeux de la maîtrise des données dans le cyberespace.

Sens général de l'axe

Le traitement de l'axe est centré sur deux aspects différents, sous-tendus par son libellé « **Produire et diffuser des connaissances** », qui suggère une grille de lecture centrée sur les acteurs, notamment le rôle des États et des hommes et femmes de science.

Le premier jalon interroge les grandes étapes de l'alphabétisation des femmes dans le monde, du XVIe siècle à nos jours. Ce large empan chronologique donne au sujet une profondeur historique et l'inscrit dans le contexte de la construction progressive des États modernes. Cela permet aux élèves d'interroger les causes et les enjeux politiques et sociaux de la lente alphabétisation des femmes du XVIe siècle à nos jours. Il importe de ne pas tomber dans le piège d'un propos centré exclusivement sur la France, mais de varier les espaces considérés : par exemple, la question de l'instruction des femmes a été au cœur des politiques coloniales, comme en témoigne l'historiographie récente[6].

Le second jalon, en revanche, resserre l'étude sur une période de l'histoire contemporaine en analysant l'émergence et le fonctionnement d'une communauté scientifique internationale sur la question de la radioactivité. Ce jalon permet d'interroger les modalités de production de la connaissance, en mettant moins l'accent sur de grandes figures de scientifiques prises isolément que sur la notion de réseau, de travail collectif et collaboratif permettant l'émergence d'innovations. Les recherches sur la radioactivité de 1896 aux années 1950 dépassent largement le cadre des frontières nationales et sont influencées par les relations entre les États, dans un contexte de tension géopolitique entre les grandes puissances. Structuré par une dialectique coopération-rivalités et selon un emboîtement d'échelles autour de l'enjeu de la connaissance, il permet de faire naturellement la transition avec l'axe 2 du thème.

Problématique de l'axe

Dans quelle mesure la production et la diffusion des connaissances constituent-elles des enjeux majeurs pour les États et les sociétés ?

6. Pour le cas de l'Afrique subsaharienne, voir Catherine Coquery-Vidrovitch, « Les femmes et l'école », *Les Africaines. Histoire des femmes d'Afrique subsaharienne du XIXe au XXe siècle*, Paris (La Découverte), 2013, p. 225-252. Voir également : Pascale Barthélémy, « Instruction ou éducation ? », *Cahiers d'études africaines*, n°169-170 (2003), p. 371-388.

Éléments fondamentaux. Notions et points de connaissance

Donner accès à la connaissance : grandes étapes de l'alphabétisation des femmes dans le monde, du XVIe siècle à nos jours

La difficulté de ce jalon réside dans son envergure spatio-temporelle. Or, l'alphabétisation des femmes a connu un rythme très différent selon les pays et dépend étroitement des dynamiques internes complexes (développement et construction de l'État, contextes religieux et culturels, etc.), ce qui rend difficile toute analyse comparative : l'enjeu est donc d'éviter l'écueil de généralisations hâtives ou de catalogues d'exemples sans cohérence d'ensemble. En outre, sur le plan historiographique, l'insuffisance des sources a conduit les chercheurs à se focaliser sur les élites, les enfances populaires n'ayant laissé que peu de traces, notamment sous l'Ancien Régime. Enfin, il convient d'interroger la notion d'alphabétisation, dont le sens a évolué sur la période considérée. Elle est certes considérée aujourd'hui comme un facteur majeur de développement, mais en a-t-il toujours été ainsi ?

En Occident, l'alphabétisation a longtemps été réservée au clergé ainsi qu'à une élite lettrée[7]. Alphabétisation et scolarisation ne sont pas toujours allées de pair : ainsi, la société d'Ancien Régime se caractérise par une fragmentation des savoirs et une « alphabétisation en miettes[8] ». Les premiers pas dans l'alphabétisation sont souvent délégués hors du système scolaire institutionnel, et les apprentissages des mécanismes de la lecture sont très rudimentaires. Dans les familles d'origine moyenne et populaire, les enfants sont orientés vers des formes d'instruction non officielle : les « petites écoles » font fonction de lieu d'instruction, mais aussi de garderie et d'entraînement aux travaux manuels pour les enfants des deux sexes.

Dans le contexte du développement de l'imprimé et des réformes, l'enseignement devient majoritairement une affaire relevant de l'Église et les institutions religieuses d'éducation se multiplient en Europe. Cela dit, leur répartition géographique est inégale, et leur accès reste limité par des enjeux de classe et de sexe. Si, à partir du XVIIe siècle, de nombreux textes sont publiés sur les questions d'éducation et d'instruction des femmes, les conclusions convergent sur l'idée que celles-ci doivent accéder à un savoir spécifique, fondé sur la moralité et la vertu, dans le but d'acquérir une discipline comportementale et mentale dont elles feront bénéficier époux et enfants[9]. Pour former de bonnes mères, d'obéissantes épouses et de dévotes catholiques, il convient de réguler l'accès aux livres et d'orienter la formation des filles vers le terrain du savoir-faire et du travail manuel ; l'apprentissage de l'écriture a peu de valeur voire représente un danger potentiel. Ainsi, en 1686, madame de Maintenon fonde un établissement à Saint-Cyr pour les jeunes filles de la noblesse pauvre âgées de sept à douze ans : la Maison royale de Saint-Louis est le seul établissement à proposer un enseignement long analogue à celui des collèges masculins mais il comporte des spécificités liées au sexe des élèves : peu de latin, activités ménagères et « arts d'agrément » comme le dessin ou la musique.

7. Pour un aperçu des questions que pose l'alphabétisation des femmes dans l'Antiquité, voir Sophie Mano, « En toutes lettres. Femmes sur les murs de Pompéi », *Clio*, 24 | 2006, p. 9-25 (accessible en ligne).
8. Marina Roggero, « L'alphabétisation en Italie : une conquête féminine ? », *Annales. Histoire, Sciences Sociales*, 2001/4-5 (56e année), p. 903-925.
9. Fénelon, *De l'Éducation des filles*, 1687 : « La science des femmes, comme celle des hommes, doit se borner à s'instruire par rapport à leurs fonctions ; [...] elles peuvent se passer de certaines connaissances étendues ». Rousseau, *Émile ou de l'éducation*, 1762 : « Toute l'éducation des filles doit être relative aux hommes. Leur plaire, se faire aimer et honorer d'eux, les élever jeunes, les soigner grands, les conseiller, les consoler, leur rendre la vie agréable et douce : voilà les devoirs des femmes dans tous les temps, et ce qu'on doit leur apprendre dès leur enfance ».

La dépendance juridique, le rôle subalterne dans les fonctions sociales et l'exclusion formelle de l'école et de la culture latine sont alors des contraintes partagées par la plupart des femmes européennes, ce qui explique le grand écart dans les taux d'alphabétisation des deux sexes. En France, l'enquête de Maggiolo sur l'alphabétisation de 1686 à 1820 a montré le retard de l'alphabétisation des femmes au XVIIIe siècle. Le siècle des Lumières a peu innové sur la question de l'instruction et, s'il existe des exceptions dans les catégories élevées de la société (les salonnières et femmes de lettres, bien souvent des autodidactes bénéficiant de la bienveillance de leur père ou de leur mari), les femmes restent mises à l'écart de l'accès aux connaissances.

Durant la Révolution française, la nécessité d'une instruction élémentaire est affirmée pour l'un et l'autre sexe, avec la maîtrise de savoirs fondamentaux identiques : lire, écrire, compter ; la connaissance de la Déclaration des droits de l'homme et du citoyen ainsi qu'une instruction élémentaire sur la morale républicaine. Si l'école devient une arme républicaine, les hésitations des révolutionnaires[10] révèlent une continuité dans les représentations : la fonction de la femme restant d'assurer la reproduction biologique de la nation, l'entreprise politique doit s'orienter davantage vers leur moralisation que vers leur instruction. Napoléon, qui amorce pourtant l'organisation d'un enseignement public d'État, n'a pas innové davantage[11].

Le XIXe siècle marque le début d'un enseignement public d'État pour les filles : en 1836, la loi Guizot sur l'école primaire est étendue aux filles, sans étendre l'obligation aux communes d'ouvrir une école pour elles, ce qui, en pratique, favorise les congrégations religieuses. Cette obligation sera effective à partir de la loi Falloux en 1850. Au début de la IIIe République, le taux de scolarisation des deux sexes dans les écoles primaires est à peu près équivalent. Cela dit, l'enseignement est principalement laïque pour les garçons et religieux pour les filles. En 1881-1882, les lois Ferry rendent l'école gratuite, laïque et obligatoire de 6 à 13 ans : dans un contexte de rivalité avec l'Église, l'enseignement primaire devient un instrument de conquête républicaine et la scolarisation des filles une nécessité[12]. L'action menée pour l'enseignement primaire est complétée par la création de l'enseignement secondaire : la loi Camille Sée crée des lycées de filles, aux contenus spécifiques et ne conduisant pas au baccalauréat. Du fait de la généralisation de leur scolarisation, de l'école maternelle à l'université en passant par le lycée, l'enseignement technique et certaines écoles d'ingénieurs, la présence des femmes dans les institutions considérées comme légitimes progresse. Cependant, elles suivent souvent des cursus spécifiques ou des filières séparées dans les facultés de bon nombre de pays européens, car la mixité est réputée menaçante pour l'ordre social et les bonnes mœurs.

10. Les révolutionnaires défendent des idées contradictoires sur l'instruction des filles : si Talleyrand propose que les filles ne soient admises dans les écoles primaires que jusqu'à l'âge de 8 ans, Condorcet milite pour une éducation commune aux hommes et aux femmes.
11. Dans une lettre adressée aux maisons d'éducation tenues par des religieuses qui accueillent, à partir de 1805, les filles des récipiendaires de la Légion d'honneur, Napoléon recommande : « Élevez-nous des croyantes et non des raisonneuses. La faiblesse du cerveau des femmes [...], leur destination dans l'ordre social, la nécessité d'une constante et perpétuelle résignation et d'une sorte de charité indulgente et facile, tout cela ne peut s'obtenir que par la religion, par une religion charitable et douce ».
12. « L'égalité d'éducation, c'est l'unité reconstituée dans la famille. [...] les évêques le savent bien : celui qui tient la femme, celui-là tient tout, d'abord parce qu'il tient l'enfant, ensuite parce qu'il tient le mari [...]. Il faut que la démocratie choisisse, sous peine de mort [...] ; il faut que la femme appartienne à la Science ou qu'elle appartienne à l'Église ». Jules Ferry, discours du 10 avril 1870, « Sur l'égalité d'éducation », *Discours et opinions de Jules Ferry (Le Second Empire, la guerre et la Commune)*, publiés avec commentaires et notes, par Paul Robiquet, p. 304-305 (disponible en ligne).

Dans les sociétés coloniales, la fin du XIXe siècle voit également un plus grand investissement des États dans l'enseignement. Dans les premiers temps de la colonisation, celui-ci est resté l'apanage des missionnaires, considérés par les administrations coloniales comme des acteurs essentiels de la colonisation des esprits et de la « mission civilisatrice ». Les besoins administratifs et économiques des colonies conduisent cependant à encourager la formation d'une main-d'œuvre plus qualifiée et d'une classe moyenne éduquée de fonctionnaires, à travers des systèmes d'enseignement différenciés. Dans l'Afrique occidentale française (AOF), les écoles rurales primaires délivrent un maigre savoir technique en limitant l'apprentissage du français, et très rares sont les établissements offrant une formation dépassant celle d'institutrice ou de sage-femme[13]. Les filles ont accès à une scolarisation longtemps tournée vers l'éducation pratique et domestique, visant à former des jeunes femmes susceptibles de diffuser dans leur foyer un mode de vie à l'européenne. Tout comme les fondateurs de l'école républicaine en France, les administrateurs ont considéré les femmes comme des vecteurs d'adhésion à de nouvelles normes et des instruments de « mise en valeur ».

Ainsi, le modèle d'un processus d'alphabétisation graduelle sur la longue durée caractérise de nombreux pays occidentaux. Les XIXe et XXe siècles voient l'émergence d'un autre modèle, dans le contexte des révolutions et des mouvements de décolonisation : celui de l'alphabétisation rapide des populations par décision politique. C'est le cas au Japon dès 1870 (avec le mot d'ordre « Instruisez-vous »), en URSS à partir de 1919 ou encore dans la Turquie kémaliste de 1928.

Au cours du second XXe siècle, le nombre de filles scolarisées progresse très rapidement dans tous les pays industrialisés. Ainsi, dans le secondaire, la parité scolaire est atteinte au seuil des années 1970 en Norvège et en France. À l'échelle mondiale, le besoin d'une définition conventionnelle de l'alphabétisation se manifeste après le second conflit mondial, dans le contexte de l'émergence d'une coopération internationale. L'Organisation des Nations Unies pour l'éducation, les sciences et la culture (Unesco) est créée en 1946 et fait de l'alphabétisation un enjeu majeur d'émancipation individuelle et de développement économique et social. L'éducation est d'ailleurs inscrite au rang des droits fondamentaux dans la Déclaration universelle des droits de l'homme (1948). Au fil de l'évolution des définitions de l'alphabétisation[14] et de la publication des rapports, l'institution pointe du doigt des écarts persistants liés au sexe d'un pays à l'autre. L'alphabétisme des femmes est toujours loin de celui des hommes : 90 % des hommes adultes (plus de 15 ans) savaient lire et écrire en 2020, contre 83 % des femmes adultes[15]. L'alphabétisation des femmes est encore aujourd'hui un enjeu de développement dans les pays des Suds : elle fait partie des cibles de l'objectif de développement durable n° 4 (Assurer l'accès de tous à une éducation de qualité) défini par l'ONU et mis en œuvre par l'Unesco.

13. Pascale Barthélémy a retracé dans sa thèse les parcours de ces femmes venues de toute l'AOF et passées par l'école de Rufisque, créée en 1938 pour former des institutrices, ou par l'école de médecine de Dakar, incluant une section sage-femme. Voir également l'article cité *supra*.
14. La définition la plus récente de l'UNESCO (2015) s'éloigne de l'approche fonctionnelle et stipule que l'alphabétisation « inclut l'aptitude à lire et écrire, identifier, comprendre, interpréter, créer, communiquer et calculer à l'aide de supports imprimés et manuscrits, mais aussi l'aptitude à résoudre des problèmes dans un environnement de plus en plus riche en technologie et en information ».
15. Données de la Banque mondiale accessibles en ligne.

Produire de la connaissance scientifique : recherche et échanges des hommes et des femmes de science sur la question de la radioactivité de 1896 aux années 1950

Le titre de ce jalon suggère à nouveau de s'interroger sur la production et la diffusion des connaissances à travers l'exemple de la radioactivité. L'expression « des hommes et des femmes » souligne l'importance d'analyser la place des femmes dans la structuration de cette communauté scientifique, dans un contexte où la recherche est nettement masculine. Le sujet commence en 1896, avec la découverte d'Henri Becquerel, et s'arrête aux années 1950, marquées par l'engagement de plusieurs scientifiques dans des mouvements pacifistes luttant pour le contrôle international des armes atomiques. Cette étude de cas est particulièrement fructueuse pour analyser la production et la diffusion de connaissances par une communauté de recherche internationale qui se structure autour d'un nouveau champ de la physique, la physique nucléaire.

Il importe d'éviter d'aborder ce jalon sous la forme d'un catalogue de dates correspondant aux principales innovations dans le domaine de la physique nucléaire, mais plutôt d'analyser le processus d'émergence d'une communauté de recherche internationale ainsi que son fonctionnement en réseau, entre coopération et concurrence. Cette communauté savante est le théâtre de l'évolution du statut social et politique de la connaissance scientifique[16]. En effet, le rôle des États et des sociétés comme acteurs de la construction de ce groupe et de ses activités doit également être mis en valeur : le projet Manhattan lancé aux États-Unis en 1942 est le premier grand programme scientifique et technologique ; il amorce l'ère des politiques scientifiques. Par ailleurs, le largage d'une bombe atomique sur Hiroshima puis sur Nagasaki entraîne un déplacement de la place de la science dans les représentations : la puissance de la physique, en particulier, s'impose à tous et influe sur la transformation du métier de scientifique.

La radioactivité est le phénomène physique par lequel des noyaux atomiques instables émettent spontanément un rayonnement et peuvent se scinder en d'autres atomes. Elle est découverte presque par hasard par le physicien français Henri Becquerel en 1896, qui constate l'impression d'une plaque photographique par des rayons émis par du sel d'uranium : ces « rayons uraniques » représentent une révolution dans la connaissance de la nature de la matière. Cela dit, peu de scientifiques se saisissent alors de ce nouveau sujet. Marie Curie, jeune agrégée d'origine polonaise, conduit sa thèse de doctorat sur ce sujet en tandem avec son mari Pierre : ils découvrent que le polonium puis le radium émettent également des rayons et aboutissent à la conclusion que ceux-ci sont une propriété de la structure de l'atome, baptisée « radioactivité ». La figure du couple de savants permet une première réflexion sur la co-construction du savoir scientifique. En effet, les résultats de Marie et Pierre Curie sont rapidement reconnus internationalement : ils obtiennent tous deux le prix Nobel de physique en 1903 (en même temps qu'Henri Becquerel, pour leurs recherches sur les radiations)[17] et Marie Curie le prix Nobel de chimie en 1911 (pour ses travaux sur le polonium et le radium). La question de la radioactivité intéresse rapidement d'autres scientifiques, comme le Britannique Ernest Rutherford, qui découvre expérimentalement le noyau atomique.

16. Voir l'ouvrage de Pierre Verschueren, *Des savants aux chercheurs. Les sciences physiques comme métier* (1945-1968), Paris (ENS Éditions), 2024 [en ligne]. Pierre Verschueren, « Produire de la connaissance scientifique : recherche et échanges des hommes et des femmes de science sur la question de la radioactivité de 1896 aux années 1950 », Encyclopédie d'histoire numérique de l'Europe [en ligne].
17. Le discours de Pierre Curie, prononcé à Stockholm en 1905, illustre notamment le caractère collectif de la recherche en nommant très rapidement les chercheurs « radioactivistes ».

À la veille de la Première Guerre mondiale, cette communauté scientifique en est encore à ses débuts et ne concerne que quelques dizaines de chercheurs : l'étude de la radioactivité n'existe réellement que dans quelques villes occidentales, comme Paris, Vienne, Berlin, Londres, Manchester, Madrid ou Montréal. Les principaux laboratoires sont le Laboratoire du radium de Marie Curie à Paris, devenu en 1914 l'Institut du radium, le laboratoire Cavendish à Cambridge, l'Institut für Radiumforschung de Vienne et l'institut Kaiser Wilhelm de chimie à Berlin. Ils nourrissent de fortes singularités mais aussi d'intenses liens de correspondance et des congrès réguliers à partir de 1910. Ce nouveau domaine est également une occasion pour certaines femmes de construire une carrière scientifique, dans un monde presque entièrement masculin : Ellen Gleditsch à Oslo, Lise Meitner à Berlin, Jarmilla Petrova à Prague, Berta Karlik à Vienne ou Marie Curie à Paris. Cette dernière est la première femme élue professeure dans une faculté de sciences en France; elle dirige entre 1906 et 1934 les travaux de 45 femmes, dont sa fille, Irène Joliot-Curie. Deux instituts se singularisent par la proportion élevée de femmes en leur sein : l'Institut du radium à Paris (25 % à 30 % de femmes entre 1906 et 1934) et l'Institut für Radiumforschung à Vienne. Ce dernier devient la plaque tournante de la circulation d'échantillons, du fait que la mine de pechblende de Saint-Joachimsthal, en Bohème, est alors le seul gisement de radium connu. La découverte d'autres gisements dans le Katanga, au Congo belge, en 1913 puis dans l'Utah et le Colorado en 1922 rend la concurrence possible.

De ces travaux découle la possibilité d'une recherche sur la structure même des atomes : c'est le début de la physique nucléaire, qui se développe progressivement après la Première Guerre mondiale. En outre, l'intérêt pour la radioactivité émerge dans d'autres disciplines scientifiques, comme la biologie et la médecine : ainsi, en 1901, des applications du radium à des fins thérapeutiques sont tentées à l'hôpital Saint-Louis et débouchent sur la « curiethérapie », efficace contre certains cancers. La radioactivité entraîne également l'émergence d'une véritable industrie dont les applications vont des peintures au radium à la crème rajeunissante (marque Tho-Radia).

Au fur et à mesure de la structuration de ce nouveau champ de recherche, celle-ci s'internationalise et devient de plus en plus compétitive dans l'entre-deux-guerres : les laboratoires se dotent de dispositifs de plus en plus coûteux, comme des accélérateurs de particules. La découverte du neutron prend des allures de course de vitesse entre les Allemands, les Britanniques et les Français. Irène et Frédéric Joliot-Curie découvrent le phénomène de radioactivité artificielle (c'est-à-dire la possibilité de rendre n'importe quel élément radioactif) en 1934 ; quatre ans plus tard, plusieurs physiciens allemands observent la fission nucléaire, et les Joliot-Curie démontrent la même année la possibilité de réactions de fission en chaîne, produisant une quantité considérable d'énergie. À « l'âge de l'innocence[18] » des premiers temps de la recherche succède alors l'entrée dans l'ère nucléaire.

Avec le début du second conflit mondial, les polarités de la communauté scientifique sur la radioactivité se déplacent d'Europe vers les États-Unis, du fait de l'émigration massive de scientifiques venus d'Europe de l'Est.

18. Roger H. Stuewer, *The Age of Innocence : Nuclear Physics between the First and the Second World War*, Oxford, Oxford University Press, 2018.

Pistes pédagogiques

Ces deux jalons se recoupent et peuvent être rapprochés par l'enseignant à travers les parcours de femmes scientifiques ou encore l'évolution de communautés scientifiques, des salons du XVIIIe aux laboratoires. En effet, c'est la possibilité d'accéder aux études supérieures qui détermine en partie l'émergence de figures de femmes scientifiques, qui parviennent à conquérir des positions d'ingénieures, laborantines, chimistes, assistantes, techniciennes, dans des sphères socialement conçues comme « naturellement » masculines. Ainsi, au début du XXe siècle, plusieurs femmes travaillent dans les laboratoires les plus prestigieux de leur époque et étudient les propriétés chimiques, physiques et biologiques des matières radioactives. Certaines voix sont cependant encore réticentes à la présence des femmes dans la production scientifique. Ainsi, en 1910, lorsque Marie Curie, alors prix Nobel de physique, présente sa candidature à l'Académie des sciences, la presse s'insurge, comme ici *Le Figaro* : « Nous avons déjà plus de femmes de lettres qu'un pays civilisé ne peut en supporter. Que les dieux favorables nous épargnent une génération de femmes de sciences[19] ! »

Au court du second XXe siècle, dans l'ensemble des pays occidentaux, l'activité scientifique des femmes progresse mais les inégalités demeurent considérables dans les sciences et les domaines de l'ingénierie. En effet, si les filles réussissent mieux à l'école, l'institution scolaire reproduit les stéréotypes sexuels et les pressions sociales : longtemps quasiment exclues du monde des sciences et des techniques, les femmes sont encore rares aujourd'hui dans les instances scientifiques de haut niveau. Par ailleurs, la minimisation voire le déni du rôle des femmes dans les avancées scientifiques a été mise en lumière en 1993 par l'historienne américaine des sciences Margaret W. Rossiter, sous le nom d'« effet Matilda[20] ». Celle-ci s'appuie notamment sur le cas de Lise Meitner, dont les recherches ont porté sur la radioactivité.

Après avoir pris en note ce contexte, les élèves peuvent s'intéresser au parcours de certaines figures de femmes de sciences, en insistant sur l'origine sociale, le parcours de formation ainsi que les difficultés rencontrées. Ils mettront également l'accent sur leurs réseaux et leur intégration dans la communauté scientifique.

- **Émilie du Châtelet**, physicienne, mathématicienne, moraliste, traductrice, musicienne, a joué un rôle dans la diffusion des idées de Newton et Leibniz.
- **Laura Bassi**, mathématicienne et physicienne italienne, contribue à introduire les idées de Newton en Italie.
- **Sophie Germain**, l'une des premières femmes mathématiciennes, correspond avec les grands mathématiciens de son temps, notamment Lagrange, sous un pseudonyme masculin, connue pour sa théorie des nombres premiers, reçoit le grand prix de l'Académie des sciences de Paris en 1816.
- **Ada Lovelace**, fille de lord Byron, écrit le premier programme informatique pour machine analytique.
- **Clémence Royer**, conférencière et écrivaine, ouvre à Lausanne un « cours complet de philosophie de la nature » réservé aux femmes (1859-1860). En 1862, première traduction française de *L'origine des espèces* de Darwin. Première femme à voir ses travaux récompensés par la Légion d'honneur, en 1901.
- **Marie Curie**, découvre des éléments radioactifs jusqu'alors inconnus, le polonium et le radium. Première femme à obtenir le prix Nobel de physique en 1903.

19. Cité par Pierre Merle, *La démocratisation de l'enseignement*, Paris (La Découverte), 2017, p. 48.
20. L'article original en anglais a fait l'objet d'une traduction en français, disponible en ligne : Margaret W. Rossiter, « L'effet ~~Matthieu~~ Mathilda en sciences », *Les cahiers du CEDREF*, 11 | 2003, p. 21-39.

- **Mileva Maric**, physicienne, seule femme élève à l'institut polytechnique de Zurich, épouse et étroite collaboratrice d'Albert Einstein.
- **Lise Meitner**, physicienne, collabore dans le « projet uranium » et découvre le principe de la fission nucléaire. Elle n'obtiendra jamais le prix Nobel pour ses travaux.
- **Ellen Gleditsch**, chimiste et universitaire norvégienne, travaille dans le laboratoire de Marie Curie puis fonde un groupe de recherche sur la radioactivité à l'université d'Oslo. Elle s'engage auprès de l'Unesco dans la lutte contre l'analphabétisme. En 1962, elle est la première femme à obtenir un doctorat *honoris causa* de la Sorbonne.
- **Irène Joliot-Curie**, chimiste, physicienne et femme politique. Fille de Pierre et Marie Curie, prix Nobel de Chimie, engagée contre le fascisme, membre du gouvernement Blum en 1936.
- **Berta Karlik**, physicienne autrichienne, travaille à l'institut du radium de Vienne, dont elle devient directrice en 1947. Première femme professeur titulaire à l'université de Vienne puis première femme membre de l'Académie des sciences autrichienne.
- **Maria Goeppert Mayer**, physicienne et chimiste, rejoint le projet Manhattan visant au développement de la bombe atomique. La découverte de la coquille nucléaire du noyau atomique lui vaut le prix Nobel en 1963.
- **Chien-Shiung Wu**, physicienne, participe au projet Manhattan, où elle développe un processus pour enrichir l'uranium utilisé pour l'énergie nucléaire.
- **Katherine Johnson**, mathématicienne embauchée par la NASA, a calculé la trajectoire d'Apollo 11.
- **Rosalind Elsie Franklin**, biophysicienne britannique, invente une machine permettant d'exposer l'ADN aux rayons X, en fait plusieurs radiographies dont la « photo 51 » qui permet la découverte de la structure à hélice.
- **Lilli Hornig**, scientifique tchéco-américaine, a travaillé sur le projet Manhattan.

Orientations pour la mise en œuvre de l'axe 2 du thème : « La connaissance, enjeu politique et géopolitique »

Articulation et sens général

Articulation de l'axe avec le thème

Après un premier axe consacré à la production et à la diffusion des connaissances, mettant en avant le rôle des États parmi d'autres institutions, le second axe vise à mettre en évidence diverses modalités par lesquelles ces mêmes États tirent profit de la connaissance, que ce soit dans le cadre géopolitique d'un affrontement ou dans le cadre d'une politique nationale de développement économique.

On peut rappeler à titre de contextualisation que les États modernes se sont construits en développant leur capacité d'information et de connaissance (de leur population, de leurs ressources, etc.). Ce développement est marqué par la création de services ou d'administrations (statistiques notamment), chargés de mieux connaître le pays. La connaissance est alors constituée en enjeu politique (de gouvernement), à tel point que l'on a pu parler de gouvernement des experts ou de technocratie (souvent en mauvaise part). L'action publique est alors assimilée à une science, reposant sur des connaissances, précises et techniques.

Sens général de l'axe

Les deux jalons de cet axe ont pour point commun de mettre en avant directement l'action de certains États, qu'il s'agisse de conflit (dans le cas de la guerre froide) ou de développement économique (dans le cas de l'Inde) autour de l'enjeu de la connaissance comme ressource. Cet axe entretient des liens avec le thème 1 de terminale puisqu'il touche aux enjeux de la conquête spatiale, ainsi qu'avec le thème 4 de la classe de première, et remobilise la différence entre l'information, qui est une donnée placée dans un contexte, et la connaissance, qui introduit une dimension réflexive à partir des informations recueillies. Il importe tout particulièrement dans le traitement de cet axe de montrer comment la connaissance est saisie comme enjeu par différents États (l'URSS, les États-Unis et l'Inde), dans deux contextes différents ; celui de la guerre froide de 1947 (nous reviendrons sur cette borne chronologique) à 1991, et celui de l'émergence d'une nouvelle puissance économique.

Problématique de l'axe

Dans quelle mesure la connaissance est-elle un enjeu de concurrence et d'affrontement entre les États ? Quel rôle joue-t-elle dans leur développement économique ?

Éléments fondamentaux. Notions et points de connaissance

Le renseignement au service des États : les services secrets soviétiques et américains durant la guerre froide

Le temps présent abonde en exemples du rôle crucial du renseignement dans les affrontements entre États : si l'exemple de la seconde guerre du Golfe, où les services de renseignement français et britanniques savaient qu'il n'y avait pas d'armes de destructions massives en Irak, peut être bien lointain pour nos élèves, le rôle du renseignement dans le déroulement de la guerre actuelle en Ukraine a été largement souligné par les commentateurs[21].

Le renseignement est « produit par le recueil et le traitement des informations » (Olivier Forcade) et doit donner aux décideurs politiques une connaissance utilisable. L'expression de « services secrets » peut désigner les services de renseignement comme les polices politiques ; elle doit être prise ici dans la première acception.

Les organismes de renseignements qui sont le plus caractéristiques de la période sont la *Central Intelligence Agency* (CIA), fondée en 1947, et le Comité pour la sécurité de l'État (KGB), fondé en 1954. Cependant, ils ne sont pas les seules institutions de renseignement : le GRU, direction générale du renseignement militaire soviétique, a des liens avec le KGB mais ne se confond pas avec lui ; la *National Security Agency* (NSA), à l'origine spécialisée dans la cryptologie, est créée aux États-Unis en 1952. Leurs rôles, similaires, ne sont pas tout à fait superposables : si le renseignement intérieur confié au KGB est aux États-Unis l'apanage de la CIA, le rôle central du KGB

21. Yann Lledo-Ferrer, « Les mutations du renseignement à la lumière de la guerre en Ukraine », *Brève stratégique de l'IRSEM*, n° 57, 21 mars 2023. Une autre brève revient sur l'usage du renseignement dans la lutte informationnelle : Damien Van Puyvelde, « Médiatisation du renseignement et guerre en Ukraine », *Brève stratégique de l'IRSEM*, n° 37, 30 mars 2022.

dans la politique soviétique déborde très largement celui qu'a pu jouer la CIA dans la politique étasunienne. Par ailleurs, la manière dont le renseignement trouve à se déployer pendant la guerre froide n'est pas nouvelle : l'héritage des années 1930 et de la Seconde Guerre mondiale est fondamental.

Cela renvoie à une question récurrente et classique, celle de la datation du début de la guerre froide. Si l'année 1947 est retenue par commodité, plusieurs historiens, comme Georges-Henri Soutou, insistent sur les tensions déjà très perceptibles dès 1943 entre les États-Unis et l'URSS. De plus, l'espionnage est une réalité très ancienne, au moins autant que celle des ambassades fixes auprès desquelles il s'est d'abord organisé, et dès les années 1930 l'URSS a cherché à se gagner des informateurs et des soutiens parmi les élites des pays occidentaux (par exemple en constituant des réseaux à Cambridge et Oxford, où se forment les milieux dirigeants britanniques).

La Seconde Guerre mondiale met en lumière (à la suite de la Première) toute l'importance des services de renseignement et le besoin d'une structuration solide de ceux-ci autour de plusieurs missions, qui mettent en tension dans les pays occidentaux le renseignement intérieur et le renseignement extérieur (par exemple au Royaume-Uni le MI5 et MI6[22]) :

- la collecte et le traitement d'informations sur les projets stratégiques (le désastre de *Pearl Harbor* est le fruit d'une « magistrale lacune » (Alexis Débat) en matière de renseignement, et cela sera décisif pour faire accepter la naissance de la CIA par le personnel politique des États-Unis) ;
- la collecte et le traitement d'informations sur les innovations technologiques (en particulier sur tout ce qui concerne l'élaboration progressive de l'arme nucléaire) ;
- la volonté de désinformer l'adversaire et de protéger ses propres informations, qui constitue l'enjeu du contre-espionnage ;
- l'action clandestine et le soutien d'opérations de déstabilisation à l'étranger, moins centrale pour la question du renseignement.

Le contexte de guerre froide joue un rôle important en ce sens qu'il inscrit l'enjeu du renseignement dans un contexte plus large qui le dramatise et lui donne une importance vitale : du côté soviétique, le projet d'expansion lié à l'idée de révolution mondiale n'est jamais abandonné ; du côté étasunien, l'objectif est celui de l'endiguement de cette expansion. Ces lignes peuvent subir des inflexions, mais elles ne sont jamais abandonnées. Chaque camp identifie ses objectifs avec l'extension de sa puissance et de son influence, quand bien même il peut y avoir des accords plus ou moins tacites sur le périmètre de celles-ci. De plus, toute une série d'affaires (l'affaire Rosenberg, « les cinq de Cambridge », la trahison de George Blake, le passage à l'Ouest d'espions soviétiques, etc.) jette un jour nouveau et public sur le monde du renseignement, et l'émotion que suscite la révélation de cet aspect clandestin et fascinant des relations internationales nourrit les thèses complotistes qui se déploieront à l'ère d'Internet : l'existence de services secrets est bien plus déstabilisante dans une démocratie que dans un régime totalitaire.

Le monde du renseignement est à la fois un monde de relations humaines complexes et ambiguës (que l'on retrouve dans les romans de John Le Carré) et un monde où la technologie (militaire ou civile) est simultanément un enjeu et un puissant facteur d'évolution interne. Le renseignement se constitue soit à partir d'informations d'origine humaine (*human intelligence – humint*), soit à partir d'informations sous forme de

22. MI5 et MI6 sont des abréviations pour *Military Intelligence*, sections 5 (*Security Service*) et 6 (*Secret Intelligence Service*).

signaux (*signals intelligence* – *sigint*)[23]. Le *Sigint* a évolué au fur et à mesure de l'évolution des techniques de communication : transmission radar, signaux électroniques, acoustiques, imagerie, aujourd'hui *Osint* (*open source intelligence*), etc. « Il est certain que le coût croissant des matériels ainsi que la course technologique en matière des moyens de transmission ont profondément modifié le visage des centrales de renseignement après 1945 » (Olivier Forcade et Sébastien Laurent). Cependant, on se tromperait en pensant que le *Sigint* a été voué purement et simplement à remplacer le *Humint*. « Certes, les agences recueillent la part majeure en volume de leur renseignement par le *Sigint*, mais l'on ne doit pas oublier que la qualité du *Humint* est souvent supérieure. Tout au long de la guerre froide, les transfuges ou défecteurs des pays de l'Est ont fourni des renseignements souvent plus importants que l'action de surveillance des avions-espions ou des premiers systèmes d'écoute. » (Olivier Forcade et Sébastien Laurent).

L'échec de « l'opération Gold » dans les années 1950 illustre l'imbrication du *Sigint* et du *Humint*. Le projet initial relève du *Sigint* et est mené conjointement par la CIA et le MI6. Les Britanniques disposaient d'une avance certaine dans le fonctionnement des services secrets, et ils ont formé les agents de la CIA, d'où de nombreux contacts et de nombreuses collaborations. « L'opération Gold » est lancée en 1954, à Berlin, et consiste à creuser un tunnel sous la zone d'occupation soviétique, afin de parvenir à intercepter des communications sous forme téléphonique ou sous forme de télex. Du printemps 1955 au printemps 1956, ce système d'espionnage fonctionne. Mais il s'agit en fait d'un trompe-l'œil. Un agent du prestigieux MI6, George Blake, a informé les Soviétiques dès 1954. Ces derniers laissent d'abord fonctionner le dispositif afin de ne pas trahir la couverture de George Blake, qui par ailleurs leur fournit des informations précieuses : ils organisent ensuite une fausse découverte par un service d'entretien en avril 1956. Le *Humint* a ici mis en échec le *Sigint*. Ajoutons que George Blake fut lui-même démasqué quelques années plus tard par une « taupe » des services secrets polonais travaillant avec le KGB, Michal Goleniewski, passée à l'Ouest en 1961.

L'affaire de Cuba met en jeu tous les aspects du renseignement et souligne l'importance de ces différents aspects dans les années 1960. Le désastre du débarquement de la Baie des cochons, en avril 1961, coûte sa place à Allen Dulles, le chef de la CIA : la connaissance de l'opinion publique cubaine est spectaculairement insuffisante, la préparation de l'opération n'a pas été assez secrète et l'action clandestine n'a pas été à la hauteur. En outre, un nouveau plan d'invasion est très vite connu du KGB. Inversement, avec une meilleure coordination de tous les services de renseignement, et en bénéficiant du résultat de programmes lancés par Eisenhower et auxquels Dulles a participé, le renseignement va beaucoup aider les États-Unis pendant la crise d'octobre 1962 : les avions de reconnaissance U2-Lockheed qui prennent des clichés photographiques sont en service régulier depuis 1957, et le programme Corona de photographie par satellite est opérationnel depuis 1960. Tout au long de la crise, le président étasunien et son équipe sont informés grâce à ces multiples canaux.

Enfin l'affaire Farewell, dans la dernière phase de la guerre froide, témoigne mieux que tout autre de l'interpénétration des différents aspects du renseignement et de son importance[24]. L'officier du KGB Vladimir Vetrov décide en 1980 de livrer des renseignements à la France, qui seront rapidement transmis à la CIA. Il a travaillé à Paris de 1965 à 1970, sous la couverture d'attaché au développement du commerce

23. En français, ROEM pour renseignement d'origine électromagnétique et ROHUM pour renseignement d'origine humaine.
24. Voir la notice consacrée à Vladimir Vetrov par Jessica Coffi dans le *Dictionnaire du renseignement* (dir. Hugues Moutouh, Jérôme Poirot), Paris (Perrin), 2018.

soviétique avec la France. Il est alors entré en contact amical avec Jacques Prévost, haut cadre de Thomson-CSP, qui est lui-même en relation avec la direction de la surveillance du territoire (DST), chargée du contre-espionnage en France. Déçu par sa carrière, désillusionné par le système soviétique, Vetrov reprend contact avec Jacques Prévost pour lui proposer de faire passer à la France des documents. L'offre est d'autant plus intéressante qu'il travaille à la « division T » du KGB, qui centralise les résultats de l'espionnage technologique des pays occidentaux.

La DST décide de lui attribuer un nom de code, « Farewell », qui orienterait le contre-espionnage soviétique vers la CIA en cas de découverte de son rôle. La DST étant chargée du contre-espionnage et n'opérant théoriquement pas à l'étranger, le transfert d'information se fait d'abord par un ingénieur de Thomson-CSP, Xavier Ameil, puis par un attaché militaire à l'ambassade, Patrick Ferrant, aidé par sa femme Madeleine. La CIA, prévenue par le président François Mitterrand nouvellement élu, fournit un appareil photo qui aide au microfilmage sur place des documents. Environ 3000 pièces sont ainsi transmises entre 1981 et 1982, avant que Farewell ne soit arrêté pour avoir tenté d'assassiner sa maîtresse et collègue (qui avait compris ce qu'il faisait) et tué un milicien en civil qui s'était interposé. Démasqué en 1983, alors qu'il est déjà détenu, il est exécuté en 1985.

Les documents révèlent l'ampleur des réseaux d'espions du KGB (on estime alors le nombre de personnes travaillant pour le KGB à 700 000, contre 20 000 pour la CIA) à l'Ouest pour guetter et utiliser tous les progrès de la technologie militaire, et permettent de démasquer de nombreux agents soviétiques et agents doubles. La CIA utilisera en outre cette nouvelle connaissance des réseaux d'espionnage pour faire passer des procédés techniques soigneusement déformés. C'est incontestablement le plus rude coup porté à l'espionnage soviétique, dans un contexte de confrontation décisive avec les États-Unis.

Circulation et formation des étudiants, transferts de technologie et puissance économique : l'exemple de l'Inde

Bien que la dimension historique ne soit pas essentielle dans le traitement de l'axe 2, on peut rappeler que, dans le cas indien, la question de la circulation et de la formation des étudiants, tout comme la question des transferts de technologie, se sont d'abord inscrites dans le contexte de la colonisation britannique. Ainsi le transfert de technologies a-t-il pu être utilisé par les colons britanniques comme un instrument favorisant l'adhésion à la domination de la couronne britannique sur les Indes[25]. La circulation étudiante est également un phénomène ancien, comme en atteste le parcours de Gandhi, formé au droit à Londres. Avant la Seconde Guerre mondiale, les étudiants indiens à l'étranger s'inscrivent prioritairement au Royaume-Uni (un à deux mille personnes par année académique) tandis qu'ils sont très peu nombreux à se rendre aux États-Unis (208 au maximum pour une année universitaire). À partir de 1944, le gouvernement britannique indien (*British Indian government*) aide financièrement des étudiants suivant leurs études aux États-Unis. Pour l'année universitaire 1949-1950, 1680 Indiens sont inscrits dans les universités du pays, contre seulement moins de 700 dans les universités britanniques.

25. Voir Ian J. KERR, « Technologie et transfert de technologie dans l'Empire britannique en Inde », *Revue d'histoire du XIXe siècle*, 56 | 2018, p. 134-137. L'auteur rappelle notamment les controverses historiographiques sur la place et le rôle de la supériorité technologique européenne dans la domination coloniale.

La période qui s'ouvre avec l'accession à l'indépendance et la guerre froide permet d'illustrer la dimension géopolitique de l'enjeu de la connaissance pour l'Inde. Ainsi, dans son étude sur l'*Indian Institute of Technology* (IIT) de Kanpur, Ross Bassett insiste bien sur la manière dont la « paix froide » entre les États-Unis et l'Inde a pu s'accompagner de coopérations scientifiques et universitaires fondées sur des relations interpersonnelles et l'engagement des institutions académiques. Ainsi, l'IIT de Kanpur a été mis en œuvre en 1960, alors que les négociations indo-américaines entamées en 1958 n'avaient pas encore abouti : en 1961, un accord est finalement trouvé en associant 9 universités américaines (dont le MIT) et, en 1963, le premier ordinateur IBM 1620 est exporté et installé à Kanpur, avec l'aide d'ingénieurs américains[26].
Les premiers professeurs recrutés sont des Indiens ayant effectué leur formation (masters et doctorats) dans des universités américaines, où ils ont également débuté leurs carrières d'enseignant-chercheur. Ces professeurs, qui proposent rapidement des formations en informatique, ont par ailleurs bénéficié d'une formation sur l'informatique académique (*academic computing*) dans des universités américaines, dans le cadre de l'accord de 1961. Cet exemple illustre bien la façon dont les mobilités étudiantes peuvent favoriser des transferts de technologie.

Si les enjeux liés à la circulation et à la formation des étudiants ne sont donc pas sans incidence sur les transferts de technologie et la puissance économique de l'Inde, il semble plus simple de traiter successivement les deux points.

Circulation et formation des étudiants

En Inde, l'enjeu de la connaissance s'inscrit dans un pays au poids démographique gigantesque, avec une population plutôt jeune. Dans un contexte de croissance économique importante (en 2018, l'Inde est devenue la cinquième puissance économique mondiale en termes de PIB ; elle connaît une croissance annuelle de près de 6 % sur la décennie 2011-2021, malgré un épisode de récession lié au Covid-19 en 2020), les inégalités et la pauvreté restent un défi : le PNUD estime à 230 millions le nombre d'Indiens pauvres en 2022[27]. Lors de l'accession à l'indépendance, l'État indien adopte une politique développementaliste, marquée par la stratégie de substitution aux importations, nécessitant un développement de la science et de la technologie[28].

Cette stratégie suppose en effet que l'État forme des étudiants en Inde (création des *Indian Institutes of Technology*[29], universités), mais encourage également la mobilité, notamment dans les domaines des NTIC, de la finance, des biotechnologies. L'Inde compte aujourd'hui plus de 500 000 étudiants dans 86 pays, le plus souvent riches et développés. Issus pour l'essentiel des milieux sociaux les plus favorisés et des classes moyennes urbaines émergentes (« *shining India* »), ils accèdent aux formations les plus prestigieuses.

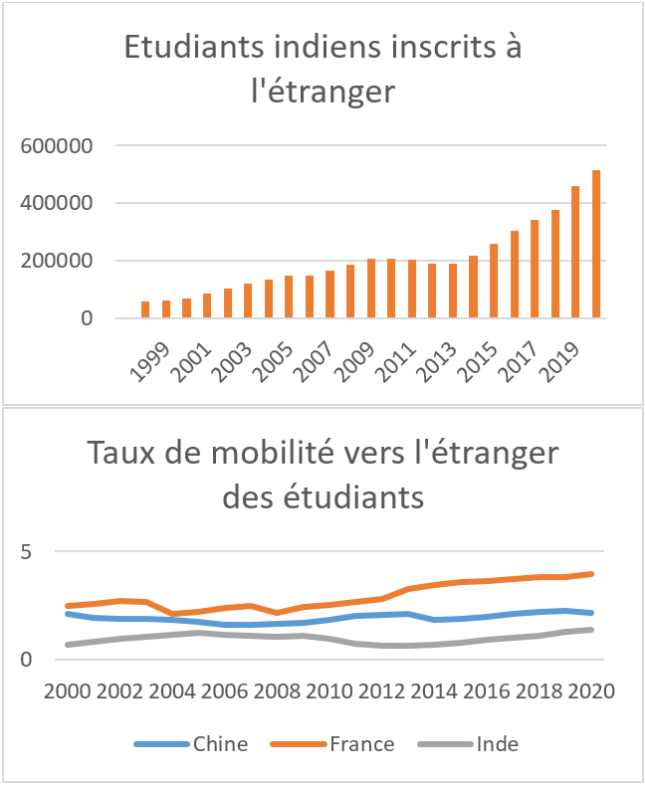
26. Ross BASSETT, « Aligning India in the Cold War Era: Indian Technical Elites, the Indian Institute of Technology at Kanpur, and Computing in India and the United States », *Technology and Culture*, vol. 50, n° 4 (octobre 2009), p. 783-810.
27. Le chiffre provient de la publication du PNUD sur l'indice de pauvreté multidimensionnelle (2022). Le PNUD estime que, sur les quinze dernières années, 415 millions d'Indiens sont sortis de la pauvreté multidimensionnelle. Sur la difficulté à mesurer la pauvreté en Inde, voir Christophe Jaffrelot, « La pauvreté en Inde - une bombe à retardement ? » *in* Durand Marie-Françoise, Lequesne Christian, *Ceriscope Pauvreté*, Sciences Po - CERI, 2012, p.1-12.
28. Cette stratégie, porteuse de croissance économique, a aussi suscité des tensions en Inde, notamment dans les domaines agricole et médical (confrontation de traditions de savoirs différentes, ne reposant pas sur les mêmes principes). Voir Schiv Visnavathan, « Sciences et savoirs dans l'État développementiste », in Dominique Pestre (dir.), *Histoire des sciences et des savoirs, t. 3 Le siècle des technosciences*, Paris (Seuil), 2015.
29. Créés à partir de 1951, les IIT sont aujourd'hui au nombre de 18. Leur concours de recrutement est très sélectif (5 % d'admis, pour 400 à 500 000 candidats).

L'encouragement à la mobilité a pu poser la question d'un possible *brain drain* : certains universitaires indiens dénoncent par ce terme la fuite à l'étranger des personnes formées sur le territoire national qui auraient pu contribuer au développement de l'Inde. D'autres universitaires préfèrent mettre en avant la notion de *brain gain*, la mobilité des « cerveaux » étant bénéfique pour le pays d'origine. L'ancienneté de la discussion dans les cercles d'économistes mérite d'être mentionnée : dès 1967, Rajendra Kumar dénonce, dans le cas de l'Inde, la notion de « *brain drain* » utilisée auparavant par K. Vikas pour lui substituer celle de « *brain gain*[30] ». On constate en effet que la mobilité des étudiants peut être bénéfique de deux manières. D'une part, une partie de ces étudiants reviennent s'installer en Inde : on estime ainsi que près de la moitié des médecins indiens formés à l'étranger rentrent exercer en Inde[31] ; à Bangalore, se met en place une « Silicon Valley à l'indienne[32] » qui attire les étudiants indiens formés dans l'ingénierie informatique. D'autre part, la diaspora aboutit à une influence indienne en dehors de l'Inde. Sundar Pichai (Google/Alphabet) et Satya Nadella (Microsoft) illustrent la place des Indiens dans les entreprises NTIC : après une formation supérieure initiale en Inde, ils partent aux États-Unis compléter leur cursus et entament une carrière brillante dans les GAFAM[33].

L'Inde cherche également à attirer des étudiants étrangers : en 2017, le gouvernement indien lance un label « *Institutes of Eminence* » visant à obtenir la reconnaissance internationale pour les meilleures écoles du pays, comme l'*Indian Institute of Science* de Bangalore, ou les IIT de Mumbai et New Delhi. Dans le même temps, les partenariats se multiplient avec de grandes écoles qui installent des campus dans les métropoles indiennes : c'est le cas des universités américaines de Virginia Tech, de Duke ou de l'École centrale de Paris. Par ailleurs, les institutions universitaires indiennes peuvent être attractives pour des étudiants issus de pays en développement, notamment d'Afrique, comme le souligne Pooja Jain-Grégoire : « l'Inde est prisée par les étudiants africains recherchant une éducation anglophone à juste prix. Le taux de change entre la plupart des devises africaines et la roupie indienne favorise l'attractivité financière du secteur de l'éducation en Inde. Cet élan a été renforcé par les annonces d'augmentation des bourses pour les étudiants africains par le gouvernement indien. D'après les chiffres les plus récents publiés par ICCR, 900 bourses sont accordées aux pays africains[34]. »

Pour une approche statistique du phénomène des circulations et formations des étudiants indiens, on peut s'appuyer sur les bases de données publiées par l'Unesco, ainsi que sur celles de l'*Institute for International Education* (IIE), concernant les États-Unis, disponibles en ligne[35].

30. Rajendra KUMAR, "Brain Drain or Brain Gain?", *Economic and Political Weekly*, vol. 2, n° 47, 1967, p. 2079.
31. Virginie CHASLES, « Les flux internationaux de personnel de santé, une illustration des inégalités de développement », *Géoconfluences*, juin 2012.
32. Clarisse DIDELON, « Bangalore, ville des nouvelles technologies », *Mappemonde* 70, 2003/2, p. 35-40. Sur la question spécifique des mobilités de retour à Bangalore, voir la thèse d'Aurélie Varrel : « 'Back to Bangalore': étude géographique de la migration de retour des Indiens très qualifiés à Bangalore (Inde) », thèse de doctorat en géographie, Université de Poitiers, 2008, disponible en ligne.
33. Le cas de Rajeev Suri (dirigeant de Nokia jusqu'en juillet 2020) est différent, puisqu'il n'a été formé qu'en Inde, notamment au *Manipal Institute of Technology*, également fréquenté par Satya Nadella.
34. Pooja JAIN-GREGOIRE, « La singularité de la géopolitique indienne en Afrique », *Hérodote*, vol. 173, n° 2, 2019, p. 49-65.
35. Pour l'Unesco : http://data.uis.unesco.org. Pour l'IIE : https://www.iie.org/research-initiatives/open-doors/



Source : UIS, Unesco.

Des transferts de technologie décisifs

Les transferts de technologie sont notamment développés dans le cadre d'activités stratégiques. Ainsi, le secteur de la défense est l'un des principaux concernés : 3e armée mondiale, l'Inde est également l'un des principaux importateurs mondiaux. Guillem Monsonis explique que, pour réduire sa dépendance aux importations militaires, le gouvernement de Narendra Modi a lancé un programme visant à favoriser la conception et la production locales d'armement, par le biais notamment de transferts de technologie[36]. Cette politique peine cependant à produire des résultats et se heurte à l'urgence et l'amplitude des besoins des forces : « Outre les achats purs et simples "sur étagère" (avions de transport tactiques C-130J achetés aux États-Unis, porte-avions Vikramaditya acheté d'occasion à la Russie), les programmes "nationaux" n'ont souvent consisté qu'en un simple assemblage local sous licence, sans réels transferts de technologie ou de savoir-faire. C'est le cas, depuis les années 1950, avec l'assemblage sous licence d'avions occidentaux (Vampire britanniques, Douglas C-47 américains ou MiG-21 soviétiques) sur lesquels la BITD [base industrielle et technologique de défense] indienne n'est que peu parvenue à capitaliser sur le plan technologique. La dépendance est également forte dans les programmes de conception et de fabrication locales, pour lesquels l'Inde est contrainte d'importer les systèmes critiques à haute valeur ajoutée, comme le radar ou la suite de guerre électronique du chasseur LCA[37]. »

Les transferts de technologie ont aussi concerné d'autres secteurs stratégiques pour la souveraineté nationale de l'Inde. C'est le cas notamment de l'agriculture : la Révolution

36. Guillem Monsonis, « Puissance et dépendance : l'Inde et les importations d'armement », *Hérodote*, vol. 173, n° 2, 2019, p. 173-193.
37. Guillem Monsonis, *op. cit.*, p. 176.

verte des années 1960 a reposé sur la coopération de chercheurs agronomes indiens et étrangers[38], et un nouveau partenariat initié avec les États-Unis en 2005 a été dénommé *Knowledge Initiative on Agriculture*. Ce partenariat vise « à développer les transferts de technologie (en particulier pour les OGM) et à harmoniser les normes dans l'agro-alimentaire pour engendrer une "seconde révolution verte[39]". »

L'Inde a par ailleurs choisi depuis le début des années 2000 de développer son industrie nationale en favorisant l'implantation de firmes étrangères ou en négociant des contrats incluant des transferts de technologie (*offset agreement*) : en général, un tiers du contrat doit être réinvesti en Inde. La création de plus de 200 zones économiques spéciales, en périphérie des grandes métropoles comme Chennai, Bangalore ou Hyderabad, offre aux firmes transnationales (FTN) des avantages fiscaux, des exemptions de droits de douane et l'accès à des infrastructures de qualité. Cette politique est particulièrement encouragée dans le domaine des NTIC ; les secteurs de la défense et de l'aérospatiale y sont les mieux représentés. L'Inde a par exemple profité des transferts de technologie imposés lors de la signature de contrats pour l'acquisition des avions militaires français Rafale, afin d'initier, en collaboration avec les entreprises françaises, la fabrication de son premier moteur d'avion de chasse. Dans un contexte de conflit gelé avec son voisin pakistanais et de tensions avec la Chine, New Delhi compte ainsi développer un appareil militaro-industriel national qui profite des dépenses croissantes du pays en matière de défense et d'armement.

Depuis 2014, les recours aux transferts de technologie sont relayés par le projet « *Make in India* » (« fabriquer en Inde »). Initié par le Premier ministre Narendra Modi, il vise à développer par l'innovation 25 secteurs industriels, en encourageant les entreprises étrangères à fabriquer leurs produits en Inde, et en investissant massivement dans la production industrielle nationale. L'Inde figure désormais au rang des destinations préférées pour les investissements directs à l'étranger (IDE) entrants. Il existe cependant des limites à cette stratégie de développement : l'Inde pâtit toujours de certains problèmes (infrastructures insuffisantes, économie souterraine/informelle, corruption). La croissance, par ailleurs, ne profite pas à tous : les catégories les plus pauvres ou les ruraux sont largement exclus de ses bénéfices. Ce sont aussi ces mêmes populations qui subissent les effets négatifs de l'arrivée d'entreprises étrangères : expropriations brutales, déstructuration du tissu économique, pollutions. Enfin, la montée du nationalisme hindou a pour conséquence des tensions intercommunautaires qui peuvent déboucher sur des violences comme en février 2020 à New Delhi.

Pistes pédagogiques

L'approche par « zooms » permet de travailler avec les élèves la compétence « se documenter », qui est centrale en HGGSP : la figure de James Angleton, l'opération Gold ou l'affaire des missiles de Cuba ont été largement médiatisées et sont l'objet de nombreuses productions qui permettent des investigations.

Après avoir posé les éléments de contextualisation, le second jalon peut être mis en œuvre par l'étude de parcours individuels de personnalités indiennes ayant accompli tout ou partie de leur cursus dans les institutions universitaires à l'étranger. À cet égard, le cas des dirigeants des grandes entreprises des nouvelles technologies peut être tout à fait pertinent (par exemple Sundar Pichai), mais l'on peut également s'appuyer

38. Voir l'entrée « Révolution verte » du glossaire Géonfluences.
39. Frédéric Landy, Aurélie Varrel, *L'Inde. Du développement à l'émergence*, Paris (Armand Colin), 2015, p. 129.

sur la carrière du prix Nobel d'économie Abhijit Banerjee (d'origine indienne mais de nationalité américaine depuis 2017). En exerçant la compétence « Se documenter », les élèves sont invités à retracer le parcours biographique et, au-delà, à mettre en évidence les cadres politique (via la législation, les investissements publics) et diplomatique (via des accords de partenariat entre États ou des conventions entre établissements d'enseignement et de recherche) dans lesquels ont pu s'effectuer ces parcours de formation.

Il est également possible d'articuler ou compléter cette approche à échelle individuelle avec un travail statistique, voire de mise en forme infographique ou cartographique de données statistiques. Les données fournies par l'Unesco peuvent fournir un support intéressant, notamment pour mettre en évidence la part très restreinte des jeunes Indiens qui entament des études universitaires, et la part encore plus réduite de ceux qui se forment à l'étranger. L'élaboration d'une carte des différents États d'accueil permet de réfléchir aux différents facteurs du choix de mobilité : facteur historique, linguistique, diplomatique, etc.

Enfin, la question des transferts de technologie peut être adossée à une étude spécifique, par exemple sur le contrat des Rafale : l'objectif est de mettre en évidence la façon dont les négociations diplomatiques prennent en compte la question des transferts des technologies, mais aussi de s'intéresser à la mise en œuvre concrète des engagements bilatéraux. C'est aussi l'occasion de réfléchir à la place particulière de certaines FTN dans la politique étrangère d'un État.

Orientations pour la mise en œuvre de l'objet conclusif : « Le cyberespace : conflictualités et coopérations entre les acteurs »

Articulation et sens général

Articulation de l'objet de travail conclusif avec le thème

Ce thème conclusif amène à s'appuyer sur les notions qui ont été construites à la fois dans l'introduction et dans les axes 1 et 2. En effet, en envisageant le cyberespace sous l'angle de la conflictualité et de la coopération entre acteurs, il est possible de mettre en évidence les points suivants :

- le cyberespace comme lieu d'élaboration, de circulation et d'accumulation de données, qui sont autant de connaissances potentielles, selon les cas et les acteurs impliqués dans leur circulation (mises à disposition des usagers, mises à profit pour orienter leurs comportements et agir sur les sociétés, ou encore en gêner le fonctionnement) ;
- le cyberespace comme lieu de coopération et de confrontation d'acteurs publics et privés, aux objectifs divers. La place de ces acteurs dans le cyberespace et leurs interactions interrogent les formes d'élaboration, de diffusion ou de protection de la connaissance ;
- le cyberespace comme lieu interrogeant la réalité de la souveraineté des États quant à leur capacité à maîtriser les flux de données et à protéger leurs populations et leurs intérêts.

Sens général de l'objet de travail conclusif

Cet objet de travail conclusif amène à s'interroger sur les différents acteurs impliqués dans le fonctionnement du cyberespace et, partant, sur sa caractérisation. Le cyberespace a pu être initialement perçu et conceptualisé par nombre de ses promoteurs comme un espace de pleine liberté de communication et de construction de réseaux dépassant les cadres traditionnels des États et des territoires. Mais l'affirmation rapide de quelques très grands acteurs privés au sein du cyberespace, dont la connaissance est aussi celle des identités et comportements des utilisateurs, l'existence de menaces nouvelles susceptibles de peser sur les usagers, leurs activités et, au-delà, celles existant sur un territoire, ont rapidement questionné cette vision. Espace de réseaux multiples, lieu de partage de la connaissance, le cyberespace est aussi un espace où se multiplient les formes d'influence à travers l'analyse réalisée par quelques acteurs des comportements des usagers mais aussi des formes variées de subversion, d'espionnage et de perturbations de la circulation des données.

Face au foisonnement des données au sein du cyberespace, les acteurs habituels de la géopolitique, à commencer par les États, se retrouvent dans une situation paradoxale. Ils peuvent tout à la fois trouver un champ nouveau d'affirmation de leur influence, et être démunis et affaiblis, peinant à réguler les communications en son sein, à protéger les usagers et à maintenir leurs fonctions et monopoles traditionnels sur les hommes et les choses. Selon les cas s'affirment des formes de régulation ou des tentatives de contrôle du cyberespace susceptibles de questionner l'idée de réseau planétaire au profit de formes nouvelles de territorialisation des données et des activités. L'enjeu est rien moins ici que de conserver la maîtrise de la connaissance des usages et usagers du cyberespace ou d'empêcher que certains acteurs aient un accès incontrôlé à celle-ci.

Pour autant, ces régulations sont-elles toujours possibles au regard du poids acquis par les géants du cyberespace, de leurs capacités d'investissement et de maîtrise des techniques et des données qu'ils ont pu accumuler ? La réflexion sur ce que peut être la cyberdéfense à l'échelle d'un État comme la France amène ainsi à envisager différents niveaux d'appropriation, réappropriation ou sécurisation des données circulant dans le cyberespace, en fonction de leur intérêt plus ou moins vital pour la nation, sans que la maîtrise de leur globalité soit envisageable.

Cet objet de travail amène à réinvestir certaines réflexions engagées en classe de première en spécialité HGGSP ou en terminale dans le cadre du programme de tronc commun de géographie et plus particulièrement :

- La puissance des géants du numérique venant, selon les situations, concurrencer, contester ou épauler la puissance des États (thème 2 sur la puissance en première HGGSP) ;
- La question de la circulation d'informations ou de fausses informations à l'heure d'Internet, susceptibles de subvertir les États, dans leur fonctionnement comme dans la défense de leurs valeurs (thème 4 sur l'information et les sources de communication en première HGGSP) ;
- L'importance de la circulation d'informations à travers les réseaux de câbles sous-marins (thème 1 sur « mers et océans au cœur de la mondialisation » en géographie en classe terminale).

Problématique de l'objet conclusif

Dans quelle mesure la structuration du cyberespace parvient-elle à combiner la quasi-infinité d'usagers et de réseaux et la domination ou le contrôle de celui-ci par quelques acteurs en nombre limité ? Comment les interactions entre acteurs de natures et de capacités d'influences très différentes peuvent-elles faire évoluer les relations et les rapports de force entre territoires ? Comment, pour un État, mettre en œuvre des politiques de défense prenant pleinement en compte le cyberespace et permettant de préserver les personnes, les activités ainsi que les fondements et les valeurs d'une société ?

Éléments fondamentaux. Notions et points de connaissance

Le cyberespace, entre réseaux et territoires (acteurs, enjeux, liberté ou contrôle des données…)

Le cyberespace peut être défini, en reprenant les termes de l'Agence nationale pour la sécurité des systèmes informatiques (ANSSI), comme un « espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques ». Il s'est constitué progressivement à partir des premières expériences d'échanges de données entre ordinateurs (naissance en 1969 du réseau Arpanet aux États-Unis), des progrès de la microinformatique, et d'un contexte géopolitique nouveau né avec la fin de la guerre froide (ouverture du réseau Internet au public en 1993). Il a pu apparaître aux yeux de nombre de ses promoteurs comme un espace où s'affirment des réseaux susceptibles de se jouer des gouvernements, des frontières. La « déclaration d'indépendance du cyberespace » de John Perry Barlow de 1996, affirmant que celui-ci « est un acte de nature », nullement borné par les frontières des États, amenant à « cré(er) un monde où tous peuvent entrer, sans privilège, ni préjugé dicté par la race, le pouvoir économique, la puissance militaire ou le lieu de naissance », inscrit ainsi le développement des réseaux l'animant dans un rapport, à tout le moins d'ignorance, sinon d'opposition aux territoires[40]. Avec l'affirmation d'acteurs animant les réseaux, souhaitant les contrôler ou en protéger les usagers, cette vision initiale du cyberespace peut cependant sembler désuète. À bien des égards, le cyberespace est aujourd'hui aussi un théâtre de conflictualité entrant pleinement en compte dans les tensions et alliances existant entre territoires.

On pourrait dès lors proposer la problématique suivante :

> Comment le cyberespace, pensé par nombre de ses promoteurs comme un lieu d'échanges ouvert et sans frontières, a-t-il pu devenir un espace de luttes d'influences, de rivalités, et parfois de cloisonnements ? En quoi les interventions des différents acteurs aux objectifs et aux poids très différents dans le cyberespace participent-elles à la définition des rapports de force et de pouvoir entre territoires susceptibles de générer des formes de conflictualité ?

40. Le texte de cette déclaration est reproduit dans Olivier Blondeau (éd.), *Libres enfants du savoir numérique*, Paris (éditions de l'Éclat), 2000, p.47-54 [en ligne].

La structuration des réseaux au sein du cyberespace

Il peut être utile d'envisager schématiquement le fonctionnement du cyberespace comme une superposition de différentes « couches », interagissant les unes avec les autres et le rendant opérationnel :

- La couche infrastructurelle : cette couche englobe l'ensemble des éléments matériels propres au cyberespace : terminaux d'accès (ordinateurs, smartphones, etc.), serveurs, *data-centers*, routeurs, câbles (et en particulier les câbles sous-marins).
- La couche logicielle : cette couche est celle qui permet aux machines de communiquer entre elles. Elle comporte les éléments de routage des informations (avec différents « protocoles », comme les plus connus d'entre eux, les protocoles TCP/IP *Transmission Control Protocol/Internet Protocole*, qui permettent pour le second à deux ordinateurs de se reconnaitre par leur adresse, pour le premier de vérifier la bonne transmission de données), ainsi que les programmes et applications dont la compatibilité entre machines permet d'assurer les échanges numériques. Cette couche logicielle fait l'objet des attaques informatiques les plus fréquentes.
- La couche cognitive ou informationnelle : cette couche comprend l'ensemble des éléments de contenus. Il s'agit donc de la couche des données proprement dites circulant dans le cyberespace.

Les possibilités d'échanges et de traitement d'informations et de données sont au cœur du cyberespace, les données pouvant être définies comme « la transcription d'un phénomène en un certain nombre de chiffres qui vont pouvoir être organisés et analysés » (A. Cataruzza). Le processus de mise en données du réel est quant à lui appelé « datafication ». L'ampleur de l'accumulation de données aujourd'hui amène à employer l'expression de mégadonnées (*big data*). Le traitement des données est facilité par le développement de systèmes de gestion de ces dernières sous des formes et des tailles variées. Le développement de données contribue largement au développement de la connaissance des sociétés, non sans que celles-ci soient parfois victimes d'une illusion de la connaissance à travers les données strictement quantitatives. Pour autant, elles constituent des apports indéniables et leur multiplication avec le numérique peut constituer un formidable atout. Leur production peut ainsi permettre de connaître certains aspects d'une population, d'un phénomène de façon exhaustive et non plus seulement à travers des procédés d'échantillonnage. L'accumulation et le traitement de ces masses de données, partagées par un ensemble de professionnels ou de chercheurs, peuvent avoir des applications extrêmement fructueuses dans de nombreux domaines, comme les recherches sur les évolutions du climat, les pandémies et les moyens de lutter contre elles. Dans d'autres domaines, elles peuvent aussi aboutir à une surveillance renforcée sur les sociétés. Il convient, de façon générale, de ne pas oublier que l'élaboration des données, le fait d'en retenir certaines plutôt que d'autres ou de privilégier telle mise en relation plutôt qu'une autre dans la perspective de développer une connaissance, relève de choix des observateurs et analystes. Une donnée ne s'impose pas en soi, mais s'inscrit toujours dans un contexte et au regard des objectifs que veut lui donner celui qui la produit et l'utilise. Cela est vrai *a fortiori* pour les métadonnées c'est-à-dire les données sur la donnée (par exemple, les éléments associés à une image comme le format, la résolution, le moment et le lieu de la prise de vue, etc.). Certains auteurs proposent à ce titre de remplacer le terme *data* par celui de *capta* traduisant ainsi le fait que les données retenues et exploitées à des fins multiples sont le résultat d'un processus de sélection, de capture[41].

41. Voir notamment : Rob Kitchin, *The Data Revolution*, Los Angeles (Sage), 2014.

Il apparaît aujourd'hui une véritable « territorialisation des données » (A. Cataruzza), quand bien même celles-ci sont ou semblent accessibles en tous temps et tous lieux. Elle traduit combien réseaux et territoires sont aujourd'hui articulés au sein du cyberespace. Cette réalité est bien visible avec l'émergence de pôles de centralisation de données, les *data centers*, allant de pair avec la dépossession des usagers du stockage physique des données. Le développement du *cloud computing* ou informatique en nuage, accélère d'ailleurs le processus. Si les États-Unis dominent, et de loin, en termes d'offre de *data centers* avec 38 % des *data centers* et 71 % de l'offre commerciale à l'échelle mondiale en 2021, il n'en demeure pas moins qu'il y a une territorialisation de ces centres bien réelle. Le développement de *data centers* en Russie, plus particulièrement en Sibérie où ces centres bénéficient de conditions favorables tant en matière d'alimentation électrique, du fait des infrastructures hydroélectriques héritées de l'ère soviétique, que de refroidissement, en est une illustration marquante. Leur développement s'inscrit à la fois dans le cadre légal fixé par les autorités russes depuis 2014 de voir toutes les données concernant des citoyens de ce pays stockées sur leur territoire, et dans la perspective de relations renforcées avec la Chine.

Cette territorialisation des données apparaît également dans les interrogations sur le « routage » de ces dernières et les mesures mises en œuvre en la matière. Il ne s'agit rien moins que de limiter voire empêcher que des données issues d'un territoire puissent transiter par un autre s'il n'y en a pas la nécessité. Si des pays comme la Chine ou l'Iran ont mis en place ce type de routage les isolant de fait du reste de la planète, d'autres pays ont engagé des dynamiques comparables : Malaisie, Brésil, Australie, Corée du Sud notamment. Le cyberespace laisse ainsi voir des jeux d'acteurs complexes articulant échanges en réseaux et (ré)affirmation de certains territoires.

Des acteurs aux rôles et poids inégaux, des acteurs en tensions

Différentes catégories d'acteurs interviennent au sein du cyberspace, avec des rôles et une maîtrise de celui-ci très différents. Ils peuvent être schématiquement présentés en trois grands ensembles dont les cloisons sont loin d'être étanches.

Les acteurs individuels ou collectifs, usagers du cyberespace, constituent un premier ensemble. Du fait des informations qu'il reçoit mais qu'il peut aussi produire et diffuser, chaque usager est en effet un acteur du cyberespace. Existent également des acteurs collectifs comme les Anonymous. Les *hackers* – pirates informatiques –, les cybercriminels comptent également parmi ces acteurs. S'il a existé jusqu'aux années 2000 l'idée que les hackers agissaient de façon assez solitaire, tel n'est plus le cas aujourd'hui. Des groupes structurés s'affirment, désignés sous l'acronyme APT (*Advanced Persistent Threat*) qui peuvent être des groupes agissant pour leur compte mais aussi en lien étroit avec un État. Certains de ces groupes peuvent être publics et renvoient de ce fait au rôle des États dans le cyberespace.

Les entreprises, et notamment les « super-plateformes » numériques, à commencer par les plus grandes d'entre elles comme les GAFAM étasuniens et les BATX chinois, ont acquis un rôle majeur au sein du cyberespace en quelques années seulement. Ces géants sont des entreprises jeunes (Microsoft, la plus ancienne des GAFAM, est née en 1975), qui ont acquis un nombre d'utilisateurs/clients qu'aucune autre entreprise n'avait jamais connu auparavant. Ainsi, Facebook comptait 2,7 milliards d'usagers en 2021, tandis que les trois super-plateformes de Google, Android, YouTube et Gmail, en comptaient respectivement la même année 3 milliards, 2,3 milliards, et 1,8 milliard.

Les GAFAM fondent leur puissance sur de gigantesques budgets de recherche et développement (passés de 16 à 127 milliards de dollars en 10 ans) et leur capacité à s'approprier l'innovation en acquérant les startups les plus prometteuses. Ces entreprises ont aujourd'hui une place majeure dans la circulation et l'accumulation de données numériques. En termes de circulation d'information, leur rôle de support des « réseaux sociaux » leur donne une place particulière dans la formation ou dé(sin)formation des opinions publiques, ou dans la segmentation de celles-ci en communautés plus ou moins isolées. De plus, ces super-plateformes disposent aujourd'hui des principaux *data centers* dans le monde. Aucun acteur public ne peut rivaliser avec elles en la matière, ce qui pose aujourd'hui de lourdes questions sur les usages et le contrôle de ces données. Leurs investissements se portent en outre aujourd'hui sur les câbles sous-marins. Si leur contrôle reste encore modeste en la matière, la tendance est bien au renforcement de celui-ci, venant ainsi concurrencer les opérateurs de téléphonie plus traditionnels et des États.

La place des États dans le cyberespace est assez particulière. Leurs fonctions régaliennes peuvent sembler remises en question au sein du cyberespace. Au regard de l'accumulation de données réalisée par différents acteurs privés, le monopole d'identification des personnes des États semble ainsi concurrencé. Il en va de même du monopole de la violence légitime dès lors que certains États (mais pas la France) autorisent des acteurs privés à riposter à des attaques au sein du cyberespace (*hack back* : action agressive en réponse à une attaque informatique). En termes de sécurité intérieure, il peut aussi y avoir un affaiblissement des outils régaliens, par exemple à travers la dépendance vis-à-vis de solutions techniques étrangères ou de leurs capacités bien moindres que celles des entreprises géantes du secteur à agir pour développer les outils et innovations nécessaires afin de rester compétitifs en terme technologique.

Pour autant, les États voient aussi leur influence s'affirmer à travers celle de différents acteurs du cyberespace. Ainsi les GAFAM « sont objectivement au service de la puissance américaine (même si) subjectivement ces derniers se conçoivent et agissent dans leur seul intérêt, à leur seul bénéfice et à celui de leurs actionnaires[42]. » Ainsi les États-Unis voient-ils leur capacité d'influence accrue par l'intermédiaire des GAFAM, à travers par exemple la diffusion des systèmes d'exploitation des outils numériques ou, sur un autre plan, les conditions générales d'utilisation (CGU) auxquelles adhèrent les usagers et qui sont de droit étasunien.

Réaffirmation des marqueurs territoriaux et difficile gouvernance du cyberespace

Cette place des États laisse voir aussi combien le cyberespace reste un lieu de régulations à construire. En la matière, différentes logiques s'opposent qui sont autant de manières différentes d'envisager la relation nouée entre réseaux et territoires dans le cyberespace. Outre l'idéal d'un cyberespace, tel qu'envisagé dans les années 1990, au sein duquel les échanges de données seraient totalement libres, apparaissent deux autres conceptions.

À l'inverse d'une lecture ouverte du cyberespace, ou du moins du réseau Internet, certains États développent une vision et des pratiques visant à leur assurer un étroit contrôle des flux d'information et des entreprises de ce dernier. Tel est le

42. Serge Sur, « De quoi les GAFAM sont-ils le nom ? », *Questions internationales* n° 109, septembre-octobre 2021 (dossier : Les GAFAM, une histoire américaine), p. 4-12.

cas de la Russie et plus encore de la Chine. Ce pays a développé une vision de sa souveraineté numérique aux antipodes d'échanges libres dans le cyberespace, chaque gouvernement devant, aux yeux des autorités chinoises, « être en mesure de décider seul comment règlementer son propre cyberespace[43] ». La construction de cette souveraineté passe par une stratégie de développement des technologies numériques autonomes très volontariste, avec un lien très étroit entre l'État et les grandes entreprises du numérique (développement des infrastructures en interne, acquisition des capacités technologiques clés pour sortir de la dépendance étasunienne avec un soutien appuyé à la recherche, par exemple dans le domaine de l'intelligence artificielle). L'attitude chinoise, passant par exemple par le souhait de pouvoir accéder à des données étrangères pour assurer le développement de l'intelligence artificielle, ne va au demeurant pas sans contradiction avec la fermeture instaurée vis-à-vis de l'étranger pour accéder aux données chinoises. En la matière est ainsi apparue la Grande muraille pare-feu de la Chine (*Great Firewall of China*), qui peut bloquer les sites de médias internationaux et les grandes plateformes numériques (Facebook et Twitter sont interdits en Chine depuis 2009, Google depuis 2010)[44].

La position d'États comme ceux de l'Union européenne ou les États-Unis laisse quant à elle apparaître le cyberespace comme un espace ouvert, de liberté, mais au sein duquel l'État peut engager des actions de protection des usagers et protéger ses intérêts. Ainsi, à partir de 2001 et l'adoption du *Patriot Act* consécutif aux attentats du 11 septembre, les entreprises installées aux États-Unis étaient tenues de permettre aux administrations l'accès aux données stockées sur des serveurs situés sur le territoire des États-Unis, que ces données concernent des citoyens étasuniens ou étrangers. Pour les entreprises de droit américain, les administrations avaient également la possibilité d'accéder à des données hébergées en Europe dans le cadre d'enquêtes sur des personnes suspectées de terrorisme ou d'espionnage, non sans susciter l'opposition des entreprises stockant les données, craignant de perdre la confiance de leurs clients. Si le *Patriot Act* a été remplacé par le *Freedom Act* en 2015, limitant les possibilités d'écoute directe par les administrations étasuniennes et notamment la NSA, les prérogatives en termes d'accès aux données stockées sur le sol américain demeurent. Le *Cloud Act* de 2018 (*Clarifying Lawful Overseas Use of Data Act*) facilite de son côté les procédures pour permettre aux administrations d'accéder aux données qu'elles souhaitent, sans passer par la justice, que leur stockage soit réalisé ou non sur le sol étasunien. C'est en partie pour répondre à ces possibilités d'intrusion américaines et notamment à la suite des révélations d'Edward Snowden que l'Union européenne a renforcé les règles de protection des données personnelles (voir jalon 2). Sur un terrain tout aussi fondamental, l'Union européenne se pose aujourd'hui en défenseur de la « neutralité du net », c'est-à-dire d'un accès égal aux contenus et services pour tous les usagers, là où cette neutralité a disparu depuis 2018 aux États-Unis, les fournisseurs d'accès pouvant octroyer un débit plus ou moins important aux usagers selon l'offre commerciale choisie (même si certains États fédérés contestent cette règle et peuvent maintenir cette neutralité).

Ces conceptions opposées du cyberespace entre différents États rendent délicate sa régulation à l'échelle mondiale, comme l'illustrent les débats autour de la gouvernance d'Internet. Si celle-ci amène à distinguer la dimension technique nécessaire au fonctionnement des réseaux et la régulation des comportements, elle pose clairement aujourd'hui la question du rôle des acteurs à l'œuvre dans celle-

43. Rogier Creemers, « Comment la Chine projette de devenir une cyber-puissance », *Hérodote* 2020/2-3 (n° 177-178), p. 297-311.
44. Ce contrôle n'est pas sans effet sur les recherches scientifiques conduites en Chine : Dennis Normile, « Science suffers as China's internet censors plug holes in Great Firewall », *Science* [en ligne], 30 aout 2017.

ci. L'opposition se joue entre tenants d'une gouvernance intégrant les acteurs non étatiques et ceux privilégiant une gouvernance multilatérale relevant des seuls États. C'est le cas aujourd'hui au sujet de l'ICANN (*Internet Corporation for Assigned Names and Numbers*). Son rôle est stratégique puisqu'elle doit à la fois assurer l'adressage et l'attribution de noms de domaines. Société de droit étasunien, ses membres ayant pouvoir de décision sont des acteurs non étatiques, les représentants des États n'ayant qu'un rôle consultatif. La plupart des pays en développement, mais aussi la Russie et la Chine s'opposent à cette gouvernance. Ils souhaiteraient une gouvernance étatique multilatérale du cyberespace, qui relèverait de l'Union internationale des télécommunications.

La question de la régulation est aussi celle des comportements et touche au respect de la vie privée, des droits de l'Homme, de la lutte contre la cybercriminalité, et de la souveraineté des États. Elle est plus complexe et avance lentement. Cependant depuis 2013 sous l'égide de l'ONU, les États se sont engagés à faire respecter la Charte des Nations unies et les droits de l'Homme au sein du cyberespace. Les États mais aussi différents acteurs privés souhaitent également une réelle sécurisation du cyberespace. Ainsi en 2017, le président de Microsoft a été à l'origine d'un appel pour une « convention de Genève du numérique », visant à protéger les personnes et les infrastructures d'attaques informatiques en temps de paix. En 2018, l'Appel de Paris « pour la confiance et la sécurité dans le cyberespace » fait clairement appel à une approche « multi acteurs » pour la sécurisation du cyberespace. Signé notamment par l'Union européenne et les États-Unis, mais aussi de nombreuses entreprises, il reste en revanche ignoré par de nombreux États[45]. Ces initiatives, qui ne sont pas les seules, suscitent des oppositions d'États soucieux de maintenir leurs prérogatives afin qu'il y ait une gouvernance multilatérale uniquement étatique.

Cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français

Définie par l'ANSSI comme « l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels », la cyberdéfense ne doit pas être confondue avec la cybercriminalité, laquelle correspond à l'ensemble des crimes et délits perpétrés sur les réseaux numériques, ni avec la cybersécurité[46]. La cyberdéfense est ainsi à envisager pour un État comme visant à défendre ses intérêts stratégiques, à permettre le maintien de sa « souveraineté numérique », c'est-à-dire, selon les termes employés par Claire Landais, la « capacité à rester maîtres de nos choix, de nos décisions et de nos valeurs dans une société numérisée[47] ». Dans un espace ouvert, même avec les limites vues plus haut, où le poids de certains acteurs privés non nationaux est tel qu'un État ne peut guère rivaliser sur ce terrain-là pour se doter en propre des outils lui permettant d'exercer sa capacité d'influence comme il le ferait en d'autres domaines, la possibilité d'assumer sa cyberdéfense ne va pas de soi. L'enjeu est pourtant majeur au regard de la multiplication des menaces cyber touchant aujourd'hui à tous les domaines de la vie

45. Voir le site Internet de l'Appel de Paris.
46. L'ANSSI définit la cybersécurité comme « l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. » (Glossaire ANSSI).
47. Définition proposée par Claire Landais, secrétaire générale de la Défense et de la sécurité nationale, lors d'une audition au Sénat le 23 mai 2019, dans le cadre des travaux de la commission d'enquête sur le devoir de souveraineté numérique. Le compte rendu est accessible en ligne.

d'une société.

Cela pourrait donner la problématique suivante :

> Comment penser la souveraineté d'un État dans un cyberespace ouvert et avec des outils techniques largement dépendants d'acteurs non nationaux ? Comment est-il possible d'agir avec certains partenaires de confiance, ainsi les pays de l'Union européenne pour la France, afin de gagner en autonomie d'action ? Pourquoi, malgré les risques d'escalade, est-il nécessaire d'envisager des actions offensives en matière de cyberdéfense allant au-delà de la protection des personnes et des systèmes ?

Multiplication des menaces : vers une nécessaire cyberdéfense

La circulation d'informations et le fonctionnement du cyberespace peuvent connaître des perturbations liées à des attaques portant sur les différentes couches de ce dernier.

Différents types de cyberattaques en fonction des couches du cyberespace[48]

Couche cyber	Attaques et menaces potentielles
Couche physique	Coupure de câbles sous-marins, destruction de satellites, bombardements de bâtiments accueillant des serveurs, des infrastructures de communication, etc.
Couche logicielle	Attaque par codes, *hacking*, logiciels malveillants (virus, cheval de Troie), déni de service, etc.
Couche cognitive	Modification de l'affichage des ordinateurs, modification de la présentation d'un site web (défacement de site), vols ou destructions d'informations ou de données, introduction de messages modifiant les perceptions, opérations de propagande, etc.

Si les attaques de la couche physique peuvent exister, celles qui concernent les deux autres tendent à se multiplier. Elles sont perpétrées à distance et l'identification de leurs auteurs réels est difficile à réaliser tant pour des raisons techniques – avec des possibilités de dissimulation de données et métadonnées relatives à l'émetteur d'une attaque – qu'au regard du rôle « écran » joué par des groupes de hackers ou cybercriminels pour le compte d'un acteur inamical.

Ces attaques peuvent être regroupées en trois catégories principales :

- **Le sabotage :** L'objectif est ici de provoquer des dommages chez l'adversaire, en touchant plus particulièrement la couche logicielle. Les conséquences peuvent être lourdes puisque des activités peuvent être paralysées. Les attaques, probablement d'origine russe, dont furent victimes certains sites gouvernementaux, administrations et banques d'Estonie en 2007, leurs serveurs étant rendus temporairement inaccessibles, ont alors sonné comme une alerte amenant à une prise en compte nouvelle des enjeux de cyberdéfense[49]. En 2010, le virus Stuxnet, virus fruit d'une

48. D'après Amaël Cattaruzza, *Géopolitique des données numériques. Pouvoirs et conflits à l'heure du Big Data*, Paris (le cavalier bleu), 2019, et Daniel Ventre, « Le cyberespace : définitions, représentations », *Revue de Défense Nationale*, n°751, 2012, p. 33-38.
49. L'imputation de l'attaque à la Russie s'explique notamment par le contexte : elle intervient au lendemain d'émeutes opposant des nationalistes estoniens à des factions pro-russes, après que le gouvernement a autorisé le déplacement de la statue représentant un soldat soviétique et symbolisant la victoire de l'Armée rouge durant la Seconde Guerre mondiale. Voir : Philippe Boulanger, *Géopolitique des médias*, Paris (Armand Colin), 2014.

coopération entre les États-Unis et Israël ayant principalement attaqué les systèmes informatiques des installations nucléaires iraniennes, a constitué un autre exemple d'attaque aux conséquences notables (même si ce virus fut transmis par clé USB). Les « rançongiciels », logiciels bloquant le fonctionnement d'un système informatique jusqu'à ce que la victime s'acquitte d'une rançon, participent de ce type d'attaques. Ce fut le cas du virus Wannacry en 2017, ayant touché au moins 300 000 ordinateurs dans le monde, et notamment ceux de certains hôpitaux britanniques. Un des risques majeurs en matière de sabotage concerne aujourd'hui les systèmes électroniques embarqués, dans les domaines automobile, aéronautique ou maritime. Des actions de sabotage sont en effet susceptibles de perturber le fonctionnement des appareils concernés, les systèmes d'aide à la navigation, etc.

- **L'espionnage :** Passant inaperçue sur le moment, l'activité d'espionnage vise à récupérer des données dans les systèmes informatiques d'un tiers ou à travers des échanges électroniques, dans des buts divers. Le cyber-espionnage industriel est une réalité aujourd'hui présente dans nombre de secteurs d'activités (aéronautique, automobile, constructions navales de pointe, etc.). Sur un autre plan, les révélations d'Edward Snowden faites à partir de 2013 ont montré l'ampleur de l'espionnage réalisé par la *National Security Agency* étasunienne en explorant les communications électroniques, y compris de dirigeants de puissances alliées et non sans relation avec différentes entreprises œuvrant dans le cyberespace.
  Les finalités de ces activités d'espionnage sont diverses. Selon les cas, l'objectif est de s'approprier dans la plus grande discrétion des données pour les exploiter à des fins commerciales, ou dans une perspective de connaître et anticiper les actions d'un adversaire ou partenaire, ou de pouvoir au contraire diffuser de façon massive ces données, dans un but de subversion. Tel fut le cas par exemple des « Macron Leaks » en 2017, piratage de plusieurs milliers de courriels de l'équipe de campagne d'Emmanuel Macron, rendus publics quelques jours seulement avant le second tour de l'élection présidentielle.
- **La subversion :** Si la liberté de circulation des informations dans le cyberespace comporte des vertus démocratiques indéniables (c'est le cas avec des lanceurs d'alerte, par exemple à travers le rôle des réseaux sociaux dans les « printemps arabes » de 2011), celle-ci peut également être à la source d'opérations visant à déstabiliser tout ou partie d'une population et à l'influencer à travers la diffusion de contenus idéologiquement orientés, de *fake news*. L'exemple de l'influence russe sur la campagne présidentielle étasunienne de 2016 est ici notable. C'est au sein de communautés existant sur les réseaux sociaux que s'est développée la pratique du « *trolling* », c'est-à-dire l'usurpation d'identité de l'un des participants de la communauté par un « troll », ce dernier diffusant ensuite des messages et informations subversifs en s'appuyant sur les inquiétudes de la communauté. Ces trolls professionnels ont agi en tant que membres d'une agence de propagande russe, l'*Internet Rechearch Agency* (IRA), et dans le cadre d'une vision du cyberespace largement développée en Russie, voyant les États-Unis comme une puissance développant une « guerre informationnelle » servant leurs intérêts[50].

Les menaces dont le cyberespace est potentiellement porteur sont multiples. Lorsqu'elles se muent en attaques, celles-ci peuvent déstabiliser en profondeur les États et les sociétés qui en sont les victimes. De plus, au regard des modalités d'actions mises en œuvre, il est toujours plus facile de porter une attaque au sein du cyberespace qu'il n'est aisé de s'en défendre. Il s'avère en effet parfois très difficile

50. Sur les « usines à trolls » russes, voir Colin Gérard, « "Usines à trolls" russes : de l'association patriotique locale à l'entreprise globale », *La revue des médias* [en ligne], 20 juin 2019.

d'identifier précisément l'origine d'une attaque et la riposte à celle-ci peut de ce fait manquer son but. En outre, au regard de la possibilité de prolifération des éléments susceptibles de nuire au fonctionnement des systèmes, la parade à une attaque peut avoir des conséquences non maîtrisées. Lorsqu'il élabore une stratégie de cyberdéfense, un État doit dès lors s'efforcer de prendre pleinement en compte ces différents aspects.

L'enjeu de l'autonomie stratégique : la France, l'Union européenne et leur cyberdéfense

La multiplication de ces menaces a amené la France et les États européens à engager progressivement une réflexion sur leur cyberdéfense en questionnant leur maîtrise des trois couches du cyberespace, et leur possibilité de les sécuriser. A ainsi été posée la question de la souveraineté ou de l'autonomie stratégique des États européens. Certains acteurs ont pu développer en la matière une vision de la souveraineté numérique relativement fermée, fondée sur « la représentation par les acteurs politiques d'une perte de souveraineté de l'État dans l'espace numérique et d'une volonté de réappropriation du cyberespace perçu comme un territoire à conquérir[51] ». Or, dans un espace ouvert comme peut l'être le cyberespace, une telle vision de la souveraineté paraît peu opérante. Et c'est bien plutôt à travers une autonomie stratégique, laquelle permet à l'État d'agir dans l'espace numérique « en y conservant une capacité autonome d'appréciation, de décision et d'action » que peut s'exercer la souveraineté[52]. C'est dans cette perspective que peuvent être articulées les échelles française et européenne en matière de cyberdéfense.

L'échelle européenne permet de porter une action défendant un ensemble de valeurs pour la défense des citoyens, susceptible d'avoir un réel impact en matière de protection des données personnelles. L'action de l'Union européenne en ce domaine s'est traduite par la mise en place du règlement général sur la protection des données (RGPD), adopté en 2016 et entré en vigueur en 2018. Cette règlementation rend les administrations et entreprises responsables de la sécurité et de la confidentialité des données qu'elles détiennent. En outre, ces données ne peuvent être collectées que dans un but précis et légal, être pertinentes au regard de ce but et être conservées pour une durée limitée. L'Union européenne a également été largement partie prenante de différentes actions diplomatiques, en particulier l'Appel de Paris pour la confiance et la sécurité dans le cyberespace de 2018 (voir premier jalon).

La volonté d'avoir une maîtrise de ses actions dans le cyberespace est aussi allée de pair avec le souhait de voir émerger des entreprises compétitives susceptibles d'intervenir dans celui-ci ou tout au moins de garantir la sécurité des États européens. Cependant, les expériences française ou européennes récentes ont eu des résultats assez mitigés, du fait de financements limités comparés aux budgets de recherche dont disposent les entreprises américaines du secteur, ou de stratégies entrepreneuriales mal étudiées. L'échec du projet Quaero visant à développer des technologies de recherches de données européennes ou les difficultés du développement d'un « *cloud* souverain » français, technologie visant à assurer disponibilité, fiabilité et sécurité des données à ses usagers, sont assez révélateurs de ces fragilités. De façon générale, en matière de technologies critiques dans le cyberespace, apparaît aujourd'hui un duopole sino-américain et l'émergence d'un nouvel acteur européen paraît

51. Didier Danet, Alix Desforges, « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques », *Hérodote*, vol. 177-178, n° 2-3, 2020, p. 179-195.
52. La citation est tirée de la *Revue stratégique de cyberdéfense* publiée en 2018, qui tient lieu de livre blanc de la cyberdéfense française.

difficilement envisageable[53].

Pour autant, une réelle autonomie stratégique européenne peut exister. Elle repose d'une part sur la capacité à intégrer des acteurs économiques réellement spécialistes des technologies à l'œuvre dans le cyberespace, d'autre part sur une identification fine des enjeux de sécurité dans l'usage d'une technologie. Ces éléments sont aujourd'hui présents dans la stratégie de cybersécurité de l'Union européenne formulée pour la première fois en 2017 et revue en 2020[54]. Celle-ci vise à développer un ensemble de règles de sécurité numérique afin d'élever les capacités de résilience face à des cyberattaques d'un certain nombre d'entités considérées comme vitales pour les sociétés concernées (hôpitaux, réseaux énergétiques, centres de données, etc.). Elle cherche également à favoriser le développement des outils de détection et de lutte contre des cyberattaques et à favoriser la coopération entre États européens de façon renforcée sur ce terrain-là. Dans cette optique, elle peut mobiliser une partie du Fonds européen de la défense, mais aussi appuyer le développement d'un certain nombre d'entreprises innovantes dans des « pôles d'innovation numérique ».

Ces évolutions à l'échelle européenne se retrouvent dans le cas de projets français ayant une importance notable en matière de cyberdéfense. La stratégie de développement des usages du *cloud computing* en France est extrêmement révélatrice à cet égard et laisse voir aussi les interpénétrations entre échelles européenne et nationale. La volonté de développer « l'informatique en nuage » en France est apparue au début des années 2010. Le projet initial envisagé par le gouvernement avec des entreprises de taille internationale des secteurs de la défense et/ou des télécommunications allait cependant échouer faute de maîtrise de cette technologie par ces dernières. Dans un second temps, à partir de 2014, ce sont des entreprises ayant une expertise en la matière qui sont impliquées dans le projet de *cloud computing* tandis qu'est également envisagée la création d'un label européen de sécurité. C'est cet aspect sécuritaire qui en vient à devenir dominant dans la *Revue stratégique de cyberdéfense* de 2018 et qui oriente la stratégie de l'État en termes de développement du *cloud* pour les administrations. Selon les niveaux de sécurité requis, variables selon les activités, plusieurs types de *cloud* peuvent être proposés, allant d'un *cloud* privé, à un *cloud* externe, hébergé par un fournisseur de services, accessible par le réseau Internet.

Rendre opérationnelle la cyberdéfense française : luttes informatiques défensive et offensive

Si les logiques à l'œuvre au sein de l'UE en matière de cyberdéfense se retrouvent dans les différents pays la composant, la prise en compte de ces enjeux en France conserve cependant des marqueurs propres, liés notamment à la manière de la mettre en œuvre.

La prise en compte des risques liés au cyberespace s'est faite de façon progressive en France, alors qu'apparaissaient de nouvelles menaces, que ces dernières la concernent directement ou pas. Le *Livre blanc sur la défense et la sécurité nationale* de 2008 est le premier document stratégique de cette importance à faire état de risques d'attaques majeures contre les systèmes d'information. Depuis les différents documents visant à définir de façon globale la stratégie de défense française (*Livre blanc sur la défense et la sécurité nationale* de 2013, *Revue stratégique de défense et de sécurité nationale* de 2017

53. Didier Danet, Alix Desforges, *op. cit.*
54. Présentée dans un communiqué de presse de la Commission européenne.

et *Actualisation stratégique* de 2021) ont systématiquement comporté un volet relatif à la cyberdéfense. En outre, différents documents spécifiques à la cyberdéfense et ses enjeux ont été réalisés entre ces dates, *Défense et sécurité des systèmes d'information. Stratégie de la France*, en 2011, *Stratégie nationale pour la sécurité du numérique*, 2015, *Revue stratégique de cyberdéfense* de 2018, témoignant de l'importance progressive prise par les questions de cyberdéfense.

Ces différents textes ont contribué à faire émerger le cyberespace comme un lieu vulnérable à des menaces majeures. C'est notamment le cas avec le Livre blanc de 2013, qui a positionné les cyberattaques au troisième rang des menaces susceptibles d'affecter la vie de la nation (les deux premières étant les agressions d'un autre État sur le territoire et les menaces terroristes). Ils ont également permis de distinguer les menaces n'attentant pas à la sécurité nationale (ainsi les usurpations d'identité dans le cyberespace), de celles en relevant : espionnage, atteinte aux « opérateurs d'importance vitale[55] ». Dans cette optique, c'est à partir de ces textes, et notamment les deux Livres blancs, que la cyberdéfense française s'est structurée autour de deux champs d'action séparés qui en font la spécificité : « missions et moyens dédiés à la cyber protection » d'un côté ; « renseignement et actions offensives » de l'autre, selon les termes de la *Revue stratégique de cyberdéfense* de 2018.

Dans sa dimension opérationnelle, la cyberdéfense en France est schématiquement structurée autour des pôles suivants :

- L'Agence nationale pour la sécurité des systèmes informatiques (ANSSI) est un organisme dépendant du Secrétariat général de la Défense et de la sécurité nationale (SGDSN), qui assure la coordination des travaux et actions de l'ensemble des ministères en matière de défense des systèmes d'information. Elle prescrit des règles de sécurité préventives et suit leur application. Elle peut également intervenir afin de stopper une attaque. Cela a par exemple été le cas en 2015 lorsque la chaîne de télévision TV5 Monde a subi une attaque l'amenant à interrompre la diffusion de ses programmes.
- Le commandement de la Cyberdéfense (COMCYBER) est responsable de la cyberdéfense pour le ministère des Armées. Il vise à détecter les attaques que peut subir le ministère des Armées et est amené à partager ses informations avec l'ANSSI pour plus d'efficacité. Il a également une dimension opérationnelle offensive. Le COMCYBER connaît une montée en puissance de ses effectifs, avec 3400 cyber-combattants en 2020 et plus d'un millier de plus d'ici 2025, dans le cadre de la loi de programmation militaire 2019-2025.
- Les services de renseignement extérieur et intérieur (Direction générale de la sécurité extérieure et Direction générale de la sécurité intérieure) participent dans leurs champs d'action à la détection de la menace.

Depuis 2021, le SGDSN dispose également d'un service technique opérationnel dédié à la vigilance et à la protection contre les ingérences numériques étrangères, VIGINUM[56].

Le modèle français distingue clairement les acteurs menant la lutte informatique défensive (LID) de ceux engagés dans des opérations plus offensives, elles-mêmes subdivisées entre lutte informatique offensive (LIO) et lutte informatique d'influence (L2I). Il est assez spécifique et diffère en tous les cas des pays anglo-saxons, où la cyberdéfense relève essentiellement du champ d'action des acteurs du renseignement.

55. Ces opérateurs d'importance vitale sont désignés par les ministères coordonnateurs du secteur. Voir la plaquette de présentation réalisée en 2016 par le SGDSN.
56. Le service VIGINUM est présenté sur une page dédiée du SGSDN, et ses publications sont accessibles en ligne.

La LID est à la fois civile et militaire. Elle est axée sur le développement de comportements vigilants, le renseignement quant à de possibles actes malveillants, ainsi que la protection et la restauration des systèmes et ressources numériques. La LIO n'a été pleinement assumée que récemment, à partir de 2019. Compte tenu des spécificités des auteurs de possibles cyberattaques et notamment de la difficulté à les identifier, la LIO reste en France du ressort de l'État (conformément à l'un des engagements de l'Appel de Paris de 2018) et est envisagée dans le cadre d'opérations militaires extérieures. L'État peut d'une part mobiliser ses capacités de renseignement avant d'engager une action offensive, d'autre part en mesurer davantage les risques, qui sont différents de ceux d'opérations conventionnelles. La réponse à une attaque est toujours envisagée comme devant rester proportionnée à celle-ci. L'usage de moyens d'action visant à neutraliser les capacités opérationnelles adverses peut en effet entraîner une propagation non désirée des moyens utilisés du fait de la multitude de connexions réseaux. Ceux-ci peuvent aussi être copiés et volés, etc. Ces éléments expliquent aussi que les opérations de LIO sont envisagées comme devant, initialement au moins, rester secrètes. La L2I, qui à la différence de la LID et de la LIO touche exclusivement la couche cognitive du cyberespace, s'inscrit dans une logique de guerre informationnelle et vise à déstabiliser l'adversaire. Son cadre d'application reste lui aussi limité au regard des risques d'effets retours. Elle ne peut en effet être développée que dans le cadre d'opérations militaires hors du territoire national.

Pistes pédagogiques – Une proposition sur la cyberdéfense dans le cas français

La proposition de piste pédagogique présentée ci-dessous vise à aider le professeur dans la mise en œuvre d'un des deux jalons. Elle n'exclut évidemment pas d'autres manières de mettre en œuvre ce jalon et ne signifie pas que la mise en œuvre de l'objet de travail conclusif peut se contenter de ne traiter qu'un seul des jalons au programme.

Il peut être intéressant, afin d'envisager la conception et la mise en œuvre de la cyberdéfense française, d'analyser un élément marquant une inflexion dans celle-ci. Compte tenu du caractère assez récent de la cyberdéfense française, le fait de pouvoir noter des inflexions sur une courte période traduit la nécessité d'adaptations rapides, et l'existence de pratiques non stabilisées. Les enjeux majeurs propres à ce jalon, tenant à la nécessité de prendre en compte des menaces très évolutives et croissantes, mais aussi à la difficulté de définir ce que peut être l'exercice de la souveraineté d'un État comme la France dans le cyberespace, peuvent être posés.

Le discours de la ministre des Armées, Florence Parly, du 18 janvier 2019 (ou des extraits de celui-ci)[57] constitue une entrée intéressante sur ce jalon en même temps que son étude permet de travailler l'étude critique de document. Ce discours, prononcé devant différents élus et hauts responsables militaires a été relayé par la presse et les médias nationaux – il est ainsi présenté dans *Le Point* comme « un discours majeur[58] » – traduisant sa portée. Il s'inscrit dans une logique de présentation d'une stratégie militaire, qui n'est pas uniquement destinée à des spécialistes. Ce discours vise à affirmer la volonté française de se doter d'une composante offensive

57. Déclaration de Florence Parly, ministre des Armées, sur le volet de la cyberdéfense des armées, à Paris le 18 janvier 2019 [en ligne].
58. Guerric Poncet, « Florence Parly : "La guerre cyber a commencé" », *Le Point* [en ligne], 18 janvier 2019.

dans sa cyberdéfense. S'il ne constitue pas une rupture au regard, par exemple, des perspectives tracées dans la *Revue stratégique de cyberdéfense* de 2018, il marque cependant une inflexion. Il amène, par la voix de la ministre des Armées, à donner officiellement corps à cette dimension de la cyberdéfense, à en définir les contours et à en évoquer les outils et moyens. Ainsi, à travers les arguments avancés pour justifier le déploiement d'une cyberdéfense offensive, ce discours permet au professeur d'aborder les différents enjeux propres à ce jalon. La structure aisément repérable de ce discours peut permettre, selon les choix du professeur, d'en faire une lecture visant à repérer les grands enjeux propres à ce jalon, ou bien d'en envisager une analyse approfondie, en conduisant les élèves à aborder, en lien avec le texte et pour le contextualiser ou le mettre en perspective, plusieurs aspects majeurs du jalon. C'est cette seconde démarche qui est envisagée ici.

On peut ici présenter sous forme de tableau d'une part les grands thèmes abordés par la ministre dans ce discours et les éléments qu'elle amène pour les présenter, d'autre part les éléments qu'un enseignant peut apporter afin de contextualiser ou mettre en perspective son propos et les modalités possibles de travail des élèves.

Thème présenté dans le discours	Éléments mis en évidence dans ce discours	Éléments à apporter pour contextualiser le document ou interroger le propos	Modalités possibles de travail
Le cyberespace, un espace de menaces	Présentation de différentes attaques d'ampleur mondiale et/ou ayant touché des cibles françaises. Évocation de différentes modalités de déploiement de cyberattaques.	Proposer différents documents permettant d'envisager la diversité concrète des formes de cyberattaques afin de relier ces dernières aux propos de la ministre.	Travail en groupe des élèves pour analyser les documents proposés. Faire réaliser un classement des différentes formes de cyberattaques, en fonction des couches du cyberespace visé, des finalités des attaques, etc.
La structuration de la cyberdéfense	Une menace identifiée et prise en compte à travers des augmentations budgétaires, la structuration d'un commandement militaire spécifique. Un souci de sécurisation des outils et pratiques mené avec l'ANSSI.	Évocation par l'enseignant de différents documents visant à définir les grands principes de la stratégie de cyberdéfense française (Livre blanc de 2013, Revue stratégique de cyberdéfense de 2018) Document complémentaire : schéma d'organisation de la cyberdéfense.	Éléments à présenter par l'enseignant.
« organiser une chaîne cyberdéfensive "de bout en bout" »	En arrière-plan, la question de l'autonomie stratégique dans le monde du numérique. L'importance des partenariats, notamment au niveau européen. La nécessité de se doter de moyens technologiques en favorisant le déploiement d'entreprises innovantes.	Donner aux élèves un document permettant de comprendre le sens de l'autonomie stratégique à la française. Proposer un ou plusieurs documents permettant d'évoquer les tentatives de développer un *cloud computing* à la française (et son échec), ou certains projets européens (Quaero). Ces documents viennent en contrepoint de la présentation de la ministre et permettent de mettre en évidence la volonté d'ouvrir différentes pistes pour se doter d'outils nationaux ou européens en matière de cyberdéfense.	Travail en groupe permettant de mettre en perspective la volonté de développement d'entreprises innovantes en matière de cyberdéfense au regard de projets et d'initiatives passées. Cette mise en perspective permet aussi de montrer la complexité voire la difficulté à conserver la maîtrise technique de sa cyberdéfense.

Thème présenté dans le discours	Éléments mis en évidence dans ce discours	Éléments à apporter pour contextualiser le document ou interroger le propos	Modalités possibles de travail
Au-delà de la cyberdéfense défensive, assumer une cyberdéfense offensive	Possibilité pour la France de déployer une stratégie de cyberdéfense offensive mais uniquement en riposte à des attaques. Importance d'agir dans le cadre de règles internationales, notamment celles envisagées dans le cadre de « l'Appel de Paris ».	Proposer un ensemble de documents sur la stratégie française de cyberdéfense du ministère des Armées aujourd'hui, permettant de mettre en évidence l'articulation entre lutte informatique défensive, lutte informatique offensive et lutte informatique d'influence. Proposer aussi un document sur l'Appel de Paris.	Travail en groupe amenant à envisager la palette des outils de la cyberdéfense militaire. Il peut être intéressant d'insister sur le caractère circonscrit de la cyberdéfense offensive (enjeu ici des risques d'effets retours, mais aussi d'une volonté de faire vivre quelques principes clés en matière de droit international dans le cyberespace).

Le travail proposé à partir de ce document permet d'engager une réflexion sur la souveraineté numérique et le rôle du ministère des Armées dans son exercice pour ce qui concerne son déploiement opérationnel, son inscription dans un cadre juridique international lui-même en construction et le développement d'outils et de technologies susceptibles d'en permettre la maîtrise technique. De ce fait, et comme y invitent les diverses références faites par la ministre des Armées dans son discours, la cyberdéfense française s'inscrit dans un cadre européen, qu'il s'agisse de coopération technique ou opérationnelle, ou encore d'actions sur le terrain diplomatique. La coopération européenne participe à la construction de l'autonomie stratégique de la France en matière de cyberdéfense. Cette logique peut être précisée ici à travers l'analyse qu'en a faite le vice-amiral d'escadre Arnaud Coustillière[59] et qui peut venir en complément du discours de Florence Parly ou être intégrée à l'un des axes de travail proposés (le troisième).

L'autonomie stratégique de la France en matière de cyberdéfense

« La souveraineté numérique, c'est-à-dire l'autonomie stratégique dans le domaine numérique, doit pouvoir être garantie par une capacité d'action. L'autonomie nécessaire à la souveraineté ne doit pas être confondue avec une indépendance ou une autonomie totale des moyens. Les armées n'ont pas la possibilité de contrôler de bout en bout l'autonomie de leur production en électronique et en informatique. Le recours à des éléments produits par des entreprises privées et/ou étrangères est inévitable et comporte un risque intrinsèque. Partageant, sur ce point-là, la position d'autres partenaires, la France a fait le choix de prioriser la sécurisation des moyens vitaux. Les armées n'ont ainsi besoin de maîtriser que certains composants bien précis pour pouvoir sécuriser un ensemble composé de briques. Cette démarche repose tout d'abord sur le développement et la mise en œuvre d'outils de cryptographie souverains pour assurer l'intégrité et la confidentialité des données. Ensuite, la maîtrise des réseaux passe par la possession de sondes de détection entièrement fiables et maîtrisées, afin de garantir la disponibilité des données. Enfin, il faut des algorithmes nationaux pour assurer le traitement de ces données. »

Arnaud Coustillière, « La transformation numérique du ministère des Armées », *Hérodote*, 2020-2/3 (n° 177-178), p.165-177.

59. Arnaud Coustillière a été directeur général du numérique et des systèmes d'information et de communication (DGNUM) au sein du ministère des Armées.

Cette logique, visant à s'assurer la maîtrise des opérations et données les plus sensibles dans le cyberespace, dans un environnement technique et de communication ouvert, est également à l'œuvre au-delà du ministère des Armées.

Bibliographie et ressources

Sur l'introduction

- Michel Durampart (dir.), *Société de la connaissance. Fractures et évolutions*, Paris (CNRS éditions), 2009.
- Torben Iversen, « Réinventer le capitalisme. La transition vers l'économie du savoir », communication pour le 10e anniversaire du CEE (Centre d'Études européennes, Sciences Po), en juin 2019 (accessible en ligne). Il y présente les grandes lignes de son l'ouvrage corédigé avec David Soskice, *Democraty and Prosperity. Reinventing Capitalism through our Turbulent Century*, Princeton University Press, 2019. Le site *La Vie des idées* présente également les réponses de l'historienne Jenny Andersson et de l'économiste Cyril Benoît, « Les démocraties sont-elles vraiment résilientes ? », 17 juin 2020.
- Christian Jacob (dir.), *Lieux de savoir*, Vol. 1. *Espaces et communautés*, Paris (Albin Michel), 2007 ; Vol. 2. *Les mains de l'intellect*, Paris (Albin Michel), 2011.
- Alain Mounier, « Critique de la société de la connaissance : les paradoxes de la réforme éducative en Thaïlande », *in* M. Carton, J.-B. Meyer (dir.), *La société des savoirs : trompe-l'œil ou perspectives ?*, Paris (L'Harmattan), 2006, p. 233-261. Disponible en ligne.
- Dominique Pestre (dir.), *Histoire des sciences et des savoirs* (3 volumes), Paris (Seuil), 2015.
- René Sigrist, « Les communautés savantes européennes à la fin du siècle des Lumières », *M@ppemonde*, vol. 2, n° 110, 2013, accessible en ligne.
- Laurent-Henri Vignaud, « Sciences et techniques : histoire d'un champ disciplinaire », *Histoire des sciences et des techniques*, Paris (Armand Colin), 2020, p. 11-52.

Sur l'axe 1

Grandes étapes de l'alphabétisation des femmes du XVIe siècle à nos jours dans le monde

- Pascale Barthélémy, « Instruction ou éducation ? », *Cahiers d'études africaines*, n° 169-170 (2003), p. 371-388.
- Catherine Coquery-Vidrovitch, « Les femmes et l'école », *Les Africaines. Histoire des femmes d'Afrique subsaharienne du XIXe au XXe siècle*, Paris (La Découverte), 2013, p. 225-252.
- Maud Delebarre, Florence Wenzek, « Donner accès à la connaissance : grandes étapes de l'alphabétisation des femmes du XIXe siècle à nos jours, en Europe, Afrique et Asie », Encyclopédie d'histoire numérique de l'Europe [en ligne].
- Pavla Miller, Jennifer M. Jones, « Literacy and Numeracy », *The Oxford Encyclopedia Women in World History*, Oxford (Oxford University Press), 2008.
- Marina Roggero, « L'alphabétisation en Italie : une conquête féminine ? », *Annales. Histoire, Sciences Sociales*, 2001/4-5 (56e année), p. 903-925.

Recherche et échanges des hommes et des femmes de science sur la question de la radioactivité de 1896 aux années 1950

- Pierre Barthélémy, « Il y a 75 ans, le Nobel de physique récompensait… une incroyable erreur », billet de blog publié sur lemonde.fr le 6 octobre 2013.
- Margaret W. Rossiter, « L'effet ~~Matthieu~~ Mathilda en sciences », *Les cahiers du CEDREF*, 11 | 2003, p. 21-39 (accessible en ligne).
- Roger H. Stuewer, *The Age of Innocence : Nuclear Physics between the First and the Second World War*, Oxford (Oxford University Press), 2018.
- Pierre Verschueren, « Produire de la connaissance scientifique : recherche et échanges des hommes et des femmes de science sur la question de la radioactivité de 1896 aux années 1950 », Encyclopédie d'histoire numérique de l'Europe [en ligne].
- Pierre Verschueren, *Des savants aux chercheurs. Les sciences physiques comme métier (1945-1968)*, Paris (ENS Éditions), 2024 [en ligne].

Sur l'axe 2

Sur le renseignement au service des États

- Alexis Débat, « La CIA et l'exploitation du renseignement aux États-Unis », *in* Georges-Henri Soutou, Jacques Frémeaux, Olivier Forcade (dir.), *L'exploitation du renseignement*, Paris (Economica et Institut de Stratégie Comparée), 2001.
- Michelle Fimes, *Farewell, l'espion qui aimait la France* (film documentaire), Kalisté productions, 2019.
- Olivier Forcade et Sébastien Laurent, *Secrets d'État. Pouvoir et renseignement dans le monde contemporain*, Paris (Armand Colin), 2005.
- Rémi Kauffer, *Les maîtres de l'espionnage,* Paris (Perrin), 2017.
- Rémi Kauffer, *Les espions de Cambridge. Cinq taupes soviétiques au cœur des services secrets de Sa Majesté*, Paris (Perrin), 2022.
- Gildas Le Voguer, *Le renseignement américain entre secrets et transparence (1947-2013)*, Rennes (PUR), 2017.
- Yann Lledo-Ferrer, « Les mutations du renseignement à la lumière de la guerre en Ukraine », *Brève stratégique de l'IRSEM*, n° 57, 21 mars 2023.
- Hugues Moutouh, Jérôme Poirot (dir.), *Dictionnaire du renseignement*, Paris (Perrin), 2018.

Sur les enjeux politiques et géopolitiques de la connaissance en Inde

Bases de données statistiques

- Statistiques sur le site de l'Unesco : http://data.uis.unesco.org/Index.aspx#
- Statistiques de l'*Institute of International Education* (pour des statistiques sur la fréquentation des établissements d'enseignement supérieur étasuniens) : https://www.iie.org/en/Research-and-Insights/Open-Doors

Articles et ouvrages scientifiques

- Pawan Agarwal, « India's Growing Influence in International Student Mobility », Bhandari, Rajika, Blumenthal, Peggy (dir.), *International Students and Global Mobility in Higher Education. National Trends and New Directions*, New York (Palgrave MacMillan), 2011.
- Ross Bassett, « Aligning India in the Cold War Era: Indian Technical Elites, the Indian Institute of Technology at Kanpur, and Computing in India and the United States », *Technology and Culture*, vol. 50, n° 4 (octobre 2009), p. 783-810.
- Ross Bassett, *The Technological Indian*, Cambridge-Londres (Harvard University Press), 2016.
- Jean-Joseph Boillot, *L'économie de l'Inde*, Paris (La Découverte), 2016.
- Christophe Jaffrelot, *L'Inde contemporaine de 1990 à nos jours*, Paris (Fayard), 2006.
- Pooja Jain-Grégoire, « La singularité de la géopolitique indienne en Afrique », *Hérodote*, vol. 173, n° 2, 2019, pp. 49-65.
- *L'Inde, une puissance singulière : Questions internationales* n° 106, mars-avril 2021.
- Frédéric Landy, Aurélie Varrel, *L'Inde. Du développement à l'émergence*, Paris (Armand Colin), 2015.
- Sara Legrandjacques, « Circulation et formation des étudiants, transfert de technologie et puissance économique. », Encyclopédie d'histoire numérique de l'Europe [en ligne], mis en ligne le 19/11/22.
- Guillem Monsonis, « Puissance et dépendance : l'Inde et les importations d'armement », *Hérodote*, vol. 173, no. 2, 2019, p. 173-193.
- Aparajith Ramnath, *The Birth of an Indian Profession: Engineers, Industry, and the State, 1900-47*, Delhi (Oxford University Press) , 2017.
- Pierre-Yves Trouillet, « Les populations d'origine indienne hors de l'Inde : fabrique et enjeux d'une "diaspora" », Géoconfluences, septembre 2015, disponible en ligne.
- Schiv Visnavathan, « Sciences et savoirs dans l'État développementiste », *in* Dominique Pestre (dir.), *Histoire des sciences et des savoirs, t. 3 Le siècle des technosciences*, Paris (Seuil), 2015.

Sur l'objet de travail conclusif

- Olivier Blondeau (éd.), *Libres enfants du savoir numérique*, Paris (éditions de l'Éclat), 2000, p.47-54 [en ligne].
- Philippe Boulanger, *Géopolitique des médias*, Paris (Armand Colin), 2014.
- Amaël Cattararuzza, *Géopolitique des données numériques. Pouvoirs et conflits à l'heure du Big Data*, Paris (Le cavalier bleu), 2019.
- Arnaud Coustillière, « la transformation numérique du ministère des armées », *Hérodote,* 2020-2/3 (n° 177-178), p. 165-177.
- Rogier Creemers, « Comment la Chine projette de devenir une cyber-puissance », *Hérodote* 2020/2-3 (n° 177-178), p. 297-311.
- Didier Danet, Alix Desforges, « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques », *Hérodote*, vol. 177-178, n° 2-3, 2020, p. 179-195.
- Serge Sur, « De quoi les GAFAM sont-ils le nom ? », *Questions internationales* n° 109, septembre-octobre 2021 (dossier : Les GAFAM, une histoire américaine), p. 4-12.
- Daniel Ventre, « Le cyberespace : définitions, représentations », *Revue de Défense Nationale*, n°751, 2012, p. 33-38.