Groupe académique de formateurs
HISTOIRE GÉOGRAPHIE GÉOPOLITIQUE SCIENCES POLITIQUES

Présentation des thématiques

académie Clermont-Ferrand
RÉGION ACADÉMIQUE AUVERGNE-RHÔNE-ALPES
MINISTÈRE DE L'ÉDUCATION NATIONALE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATION

Thème 6 : L'enjeu de la connaissance
Objet de travail conclusif : Le cyberespace, conflictualité et coopération entre les acteurs

Le concept de **cyberespace** apparaît dans la littérature de science-fiction (William Gibson, *Neuromancer*, 1984). En 1996, John Perry Barlow (1947-2018) publie la « déclaration d'indépendance du cyberespace » qui rappelle l'esprit d'émancipation des premiers acteurs du Web face aux Etats. Il est défini dans les années 2000 par les acteurs étatiques et privés comme un espace d'information généré par l'interconnexion globale des systèmes d'information et de communication dans lequel les données sont créées, stockées, partagées. Il est caractérisé par trois **couches stratégiques** : **matérielle** ou physique (ensemble des infrastructures comme les câbles, serveurs, satellites, appareils connectés…), **logicielle** ou applicative (espace d'échange entre les machines géré par le code et les protocoles qui comprend les systèmes d'exploitation et le cloud), **sémantique** ou cognitive (ensemble des données qui permettent de produire un savoir). Un ensemble de stratégies, de coopérations et de concurrences, de rivalités sont visibles dans les trois couches du cyberespace. On voit alors se dessiner une **géopolitique du cyberespace** entre les Etats, entre Etats et acteurs privés (GAFAM), entre Etats – acteurs privés – société civile (individus, ONG…). Ce concept de cyberespace soulève plusieurs problématiques entre **réseaux et territoires** : autour des relations entre les Etats entre **conflictualités et coopération** (souveraineté, territoires numériques et territorialisation des données, frontière), la dimension stratégique politique, économique et culturelle de l'économie numérique qui illustre des **représentations idéologiques** du cyberespace, de la **gouvernance de l'Internet** et ses enjeux pour les **citoyens**.

L'année 2013 et l'affaire d'Edouard Snowden marque une rupture. Cette affaire de surveillance de masse pratiquée par une démocratie entraîne une prise de conscience mondiale à toutes les échelles (locale par les individus, régionale par les réseaux d'acteurs, nationale par les Etats, internationale par les institutions mondiales). Elle interroge sur la **question des données**. C'est une question de sécurité et de vulnérabilité des Etats (données stratégiques) et des individus (protection des données personnelles), un enjeu de puissance (contrôle des infrastructures), un enjeu économique (secteur industriel numérique). Le cyberespace compte 40 000 milliards de données en 2019 et ce chiffre est doublé tous les 18 mois, 80% sont stockées dans les datacenters, 20% sur les appareils mobiles.

La notion de **données** fait référence à toute information transcrite numériquement par le processus de « datafication » c'est-à-dire la mise en nombre binaire d'une réalité. Mais il ne s'agit pas de simples chiffres et algorithmes neutres ou encore « vrais / faux ». L'esprit critique doit rester de mise face à ces calculs mathématiques. La donnée est en fait un **produit socio-spatial** créée par une machine, un individu ou groupe d'individus qui répond à des finalités révélatrices des représentations et des stratégies des acteurs.

OBJET DE TRAVAIL CONCLUSIF

Internet est perçu comme un espace virtuel sans frontière qui donne accès à des connaissances. Vecteur de changement comme le fut l'écriture et le livre, il représente un espace de liberté et de pouvoir inédit. Cette représentation qui associe communication et liberté existe depuis la Renaissance. En 2019, 57% de la population mondiale a accès à Internet (dont 70% en dehors du monde occidental). Internet et cyberespace sont liés mais répondent à des définitions différentes.

Le cyberespace, entre réseaux et territoires.

- **Le cyberespace, un espace géopolitique**

a) Les Etats-Unis, une cyberpuissance…

Internet est né aux Etats-Unis et ils ont gardé cette avance technologique dans les **infrastructures** (câbles terrestres et sous-marins, datacenters). Ils possèdent les dix serveurs racines mondiaux (sur treize), un réseau centralisé des câbles sous-marins sur leur territoire, nœud incontournable pour 95% des données et communications mondiales. Ils contrôlent les grands **systèmes d'information** (règles et normes internationales, protocole TPC/IP, logiciels). Ils s'appuient sur les postures oligopolistiques des **industries du Web**, GAFAM, et une stratégie de stockage des données (*cloud computing*). Enfin, ces industries numériques profitent d'une porosité entre intérêts économiques et politiques pour trouver des appuis au sein de l'administration. L'affirmation de la puissance américaine passe par la capacité à créer une dépendance dans le domaine de la production des connaissances et ils usent d'un arsenal législatif, normatif et technologique. Cette position hégémonique entraîne des réactions défensives des autres puissances.

b) …mais confrontée à l'affirmation de la souveraineté des Etats

Les puissances émergentes, Russie et Chine, ainsi que des pays occidentaux contestent cette suprématie. En Russie depuis 2012, l'Internet est de plus en plus sous le contrôle de l'Etat qui le considère comme un média et veut le soumettre aux mêmes lois (loi 2.0 contre Facebook, Twitter, YouTube pour restreindre l'accès au contenu). Depuis 2016, les données personnelles des citoyens russes en Russie et en dehors de la Russie doivent être hébergées sur le territoire. Les méga datacenters en Sibérie sont construits depuis 2015 le long du transsibérien (dorsale internet de St Pétersbourg à Vladivostok). C'est le passage d'un contrôle des contenus à un contrôle des infrastructures, d'autant plus qu'en 2019 l'Internet russe « souverain » fait scission avec le monde. C'est à la fois l'affirmation autoritaire et nationaliste de la **souveraineté** et une **surveillance de la société**, la volonté d'une indépendance face aux firmes américaines, une main mise sur un **revenu commercial** (profilage des internautes). On parle alors d'une relocalisation des données numériques et de nouvelles frontières. De plus, la Russie tente de projeter sa **puissance numérique** avec l'Internet russophone RuNet et le réseau social VKontakte en Europe centrale, en proposant les espaces de stockage de ses datacenters aux Républiques d'Asie centrale et à la Chine. Cette tendance s'observe depuis longtemps en Chine, mais également au Brésil, en Inde…

c) …et des acteurs plus nombreux

Le cyberespace n'est pas un domaine technique, mais politique et stratégique sous l'effet d'une multitude d'acteurs qui sont en interactions et connaissent des rapports de force. L'exemple des câbles est révélateur : en effet, les acteurs étatiques et non-étatiques tentent de contourner la dépendance aux Etats-Unis avec des alternatives comme la construction de câbles par les **pays émergents** (Brésil en 2013 vers Venezuela, 2018 vers Angola) ou les **entreprises du Web** (câble entre Etats-Unis et Espagne financé par Facebook et Microsoft en 2017, entre Los Angeles et Hong Kong par Google et Facebook en 2019, Huawei et le projet PEACE). On peut y voir un moyen de s'affranchir du contrôle étatique et/ou un moyen de pression sur les Etats et populations dépendantes de ce réseau. L'actuel bras de fer entre les Etats-Unis et

la Chine, au sujet des équipements de la 5G par l'entreprise Huawei (1er fournisseur télécoms et 2ème vendeur de smartphones au monde), illustre une guerre commerciale et technologique entre les industries numériques (GAFAM et BATX).

La question du routage des données, avec une volonté des Etats de développer des routages nationaux pour éviter le passage des données via les Etats-Unis, souligne une **territorialisation des données** dans laquelle les **fournisseurs d'accès** deviennent des acteurs majeurs. L'affaire Snowden a marqué une rupture dans les choix stratégiques des Etats et instauré une défiance à l'égard des Etats-Unis.

- **Le cyberespace, un espace idéologique**

a) Des représentations dichotomiques du cyberespace réticulaire et territorialisé

Il y a deux représentations du cyberespace qui s'opposent et déterminent les choix des acteurs. D'une part, l'Internet touche toutes les composantes de la société et les Etats ne peuvent pas intervenir. C'est une vision **libertaire, utopique et dérégulée** d'un Internet libre, ouvert, global, pacifique et animé de multiples acteurs à égalité (société civile, industriels et Etats). L'Internet semble « neutre » et apolitique. Cette représentation est défendue aujourd'hui par peu d'acteurs car même les géants du numérique s'accordent pour faire du cyberespace un espace du droit pour en garantir la stabilité. De plus, l'Internet n'est pas seulement un produit technologique, c'est un produit politique et social organisé par le **code** qui participe à l'organisation de la société (Lawrence Lessing, « *Code is law* », 1999). Les citoyens doivent donc être informés des choix technologiques. D'autre part, l'Internet peut être considéré comme un champ supplémentaire des relations internationales, un avatar de la souveraineté où s'exerce le droit. C'est une vision **légaliste et contrôlée** qui légitime les interventions des Etats mais il n'existe pas de consensus entre eux : les Etats-Unis, la Russie et Chine, la France (forum de l'UNESCO à Paris sur la gouvernance de l'Internet en 2018).

b) …et une position américaine dominante

Depuis 2001, les Etats-Unis se caractérisent par une « extraterritorialisation du droit américain ». Le *Patriot Act* donne jusqu'en 2015 le droit à l'administration de consulter toutes les données stockées sur le territoire américain et par les entreprises américaines à l'étranger. En 2015, le *Freedom Act* limite en partie cette surveillance par l'Agence de Sécurité Nationale (NSA), mais en 2018 le *Cloud Act* facilite l'accès aux données par simple mandat. Le droit devient un rapport de force entre les Etats-Unis et l'Union européenne (RGPD en 2016), entre l'Etat américain et les GAFAM. Malgré l'affaire Snowden en 2013, la surveillance de masse reste possible voir légitime selon les Etats-Unis qui gardent un discours sécuritaire.

Plusieurs acteurs de la société civile réclament une constitution ou traité de l'Internet qui prendrait en compte les multi-parties (industries du Web, communauté d'experts techniques, Etats, société civile segmentée…). Cette construction profiterait aussi sans doute aux Etats-Unis puisqu'acteur omniprésent.

- **Le cyberespace, les enjeux d'une gouvernance**

a) Les coopérations entre Etats face aux nouvelles menaces

La gouvernance de l'Internet est un objet de conflictualité internationale, à la croisée entre mutations technologiques et une évolution vers plus de transparence et de pluralisme. Les tensions autour de la **gouvernance de l'Internet** reflètent la revendication de souveraineté des Etats, la volonté des Etats de s'imposer sur les autres acteurs, la coopération inter-gouvernementale. En l'absence de gouvernance mondiale de l'Internet, ce sont les divisions du monde qui risquent de transformer cet espace inédit de liberté et de puissance.

Le rapport de l'ONU de 2015 montre une hausse des actes malveillants qui menacent la paix internationale et la stabilité des Etats d'où une coopération nécessaire entre Etats, entre Etats et entreprises contre les écosystèmes criminels. La **cybersécurité** est à la fois une question de sécurité nationale pour les

Etats, un marché pour les industries du numérique, une défense des droits de l'homme. Elle se décline dans les trois couches du cyberespace (sécurisation des infrastructures, sécurisation des lieux stratégiques comme les datacenters, sécurisation des contenus). Il existe une Convention internationale de la cybercriminalité dite Convention de Budapest qui réunit 63 Etats en 2019.

A partir des années 1980, les conflits armés se prolongent dans « l'informatisation des forces » ou encore « la guerre en réseau ». Les années 1990 voient l'arrivée de nouvelles formes d'affrontement et de déstabilisation des puissances traditionnelles par des acteurs non étatiques et asymétriques, puis les années 2000 sont marquées par des **cyberattaques** (2007 en Estonie, 2008 Géorgie, 2012 Iran, 2014 Ukraine, 2016 France, 2017 virus planétaire WannaCry…). Les conflits intègrent donc une dimension cybernétique (propagande sur les réseaux sociaux, attaques de *malware*..) dont les acteurs et objectifs sont difficiles à identifier (hackers, groupes politiques, Etats…) dans un **marché d'armes cybernétiques** qui est à la frontière entre l'Internet et le *dark web* (appelé aussi *deep web*). Les Etats développent alors des capacités offensives dans le cadre de la cybersécurité ou cyberdéfense.

b) Les choix complexes dans un contexte géopolitique et technologique mouvant

Il est difficile de cartographier le cyberespace car il est en expansion et reconfiguration permanente, animé de conflictualités qui prolongent les tensions géopolitiques existantes, et connaît des flux exponentiels de données.

Les Etats sont confrontés à des choix difficiles entre le **risque systémique** causée par une cyberattaque potentielle et déstabilisatrice sur le plan politique (interventions dans la vie politique, infrastructures vitales paralysées…), sur le plan économique (espionnage industriel…), sur le plan social (protection des données personnelles…) qui nécessite une **coopération internationale** et la volonté de garantir sa **souveraineté** et sa capacité offensive à des fins géopolitiques. Un équilibre à construire entre liberté, sécurité et raison d'Etat. Dans les faits, il semble difficile pour les Etats et les populations de se passer des deux géants américain et chinois : l'Allemagne a choisi l'entreprise américaine Cisco pour son *Cloud* « national », l'entreprise Huawei cherche à conquérir le marché européen avec le projet d'une usine d'antennes mobiles en France qui viendrait s'ajouter aux centres de R & D et aux centres de cybersécurité existants. Les choix technologiques ne sont pas neutres et posent la question de la **dépendance** des Etats et des populations.

Plusieurs tendances, qui seront peut-être des **ruptures**, sont pointées : les enjeux de l'impression 3D avec son réseau de partage de données et la potentielle ubiquité de la production, l'intelligence artificielle adaptée à tous les domaines sociétaux, la montée en puissance de la *blockchain* support des cryptomonnaies. Le cyberespace interroge, parce qu'il modifie les sociétés et les notions clés de la géopolitique : le pouvoir et le territoire. Le cyberespace modifie notre rapport à ces deux concepts.

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

En 2019, la France finit 1ère aux *Locked Shields*, le plus grand et complexe exercice international de cyberdéfense organisé par l'OTAN depuis 2010 où une vingtaine d'Etats étaient représentés. Signe d'une maîtrise du cyberespace ? Cette performance tranche avec une réalité plus prosaïque tout en révélant un potentiel.

- **La cyberdéfense en France : une histoire récente et des enjeux pluriels**

La cyberdéfense est définie par le Ministère des armées comme « ensemble des activités conduites afin d'intervenir militairement ou non dans le cyberespace pour garantir l'effectivité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère. La cyberdéfense est à différencier de la cybercriminalité qui correspond à l'ensemble des crimes et délits traditionnels ou nouveaux réalisés, via les réseaux numériques » (site du Ministère de la Défense consulté en mars 2020).

C'est une prise de conscience, depuis le milieu des années 2000, qui se retrouve dans les Livres Blancs sur la Défense (2008 et 2013) en soulignant les enjeux de **sécurité nationale** et de **développement économique**. A partir de 2009, on voit se multiplier plusieurs agences ou organisations au sein de la Défense tandis que la France connaît des cyberattaques.

La cyberdéfense est **globale** et a un **caractère défensif et offensif** en France. L'Etat, « responsable de la cyberdéfense de la nation » s'appuie sur plusieurs organisations militaires de la Défense (Commandement de la Cyberdéfense, Agence Nationale de Sécurité des Systèmes Informatiques, Direction Générale de l'Armement, Agence de l'Innovation de Défense, Direction du Renseignement de la Sécurité de la Défense, Direction du Renseignement Militaire). Le Commandement de la Cyberdéfense (COMCYBER) créé en 2017 et implanté à Paris et Rennes a pour mission la protection des systèmes d'information de l'état-major des armées, la défense des systèmes d'information du ministère des Armées (hors DGSE et DRSD), la conception et conduite des opérations militaires dans le cyberespace, l'anticipation en matière de cyberdéfense. Ce sont des unités spécialisées en cyberdéfense interarmées qui regroupent 3400 cybercombattants et la Réserve de cyberdéfense. La Loi de Programmation Militaire (2019-2025) prévoit un budget de 1,6 milliard et un recrutement de 1000 cybercombattants supplémentaires. L'Etat reconnaît donc l'importance stratégique du cyberespace et des enjeux de cybersécurité. L'organisation de la cyberdéfense distingue les missions défensives et offensives pour garantir les libertés individuelles et la protection de la vie privée, mais peut souffrir d'une dispersion des forces. Ce modèle d'organisation est différent du modèle anglo-saxon.

Il s'agit d'une part de **sécuriser les opérations militaires** sur le terrain qui dépendent des systèmes d'information : c'est une « numérisation du champ de bataille » (géolocalisation, véhicules autonomes…) et **sécuriser les infrastructures matérielles** (protection effectuée par la Marine Nationale des câbliers…). Cette sécurisation peut passer par une opération militaire réelle ou dans le cyberespace. D'autre part, la sécurisation des données stratégiques nationales militaires et civiles (secteurs de l'approvisionnement en énergie, financier, transports, santé, eau). Enfin, la **sécurisation des données** des citoyens, entreprises et collectivités territoriales. La loi de Programmation Militaire replace l'humain au cœur de la cybersécurité. Il n'est plus perçu seulement comme une menace, mais une réponse aux cyberattaques ce qui modifie les représentations homme-machine et rappelle les enjeux de la formation des citoyens et des experts (multiplication des formations dans les écoles informatiques, dans les écoles spécialisées du BTS à St Cyr).

La cyberdéfense ne concerne pas qu'un domaine militaire : en effet, les principales entreprises qui équipent les armées françaises ont signé en 2019 une convention cyber : Airbus, Ariane Group, Dassault, MBDA, Naval Group, Nexter, Safran et Thalès. Cette convention repose sur le partage de l'information au sein d'un cercle de confiance, l'évolution de l'organisation dans une gouvernance partagée, l'acculturation et sensibilisation au cyber, la volonté commune de maîtriser les risques cyber. Ces entreprises stratégiques font appel à un tissu industriel dense de sous-traitance et de recherche (PME, laboratoires de recherche et universités…). C'est donc une **multitude d'acteurs** économiques qui sont impliqués à des degrés divers dans un contexte de cyberattaques permanentes, l'Europe étant l'espace le plus attaqué dans le monde (fraude : vol de données personnelles ; sécurité industrielle : vol de brevets, arrêt d'une production par un piratage des fichiers ; intérêts vitaux : infrastructures, information…).

La France a deux objectifs dans la politique de cyberdéfense : **assurer sa souveraineté** et **coopérer** avec les autres Etats à l'échelle européenne et plus. Elle tente alors de s'affirmer dans les couches matérielle et logicielle du cyberespace, d'affirmer son influence dans le domaine normatif et judiciaire à l'échelle internationale.

- **La France : une cyberdéfense en construction et fragile**

S'interroger sur la cyberdéfense de la France à partir des trois couches du cyberespace peut être opérante.

D'une part, la place de la France dans la couche matérielle du cyberespace montre **force et vulnérabilité**. La France semble échapper à l'éventualité d'un « noir numérique » en cas de rupture de câbles sous-marins puisqu'il en existe quatre qui assurent sa connectivité. Les entreprises françaises de construction et installation de câbles, comme Orange Marine et Alcatel Submarine, font partie des leaders

mondiaux aux côtés des Etats-Unis et Grande Bretagne. Mais les câbles sont centralisés sur les Etats-Unis et pose la question de la confidentialité et sécurité des données. De plus, l'Union européenne constitue un marché disputé entre les puissances américaine et chinoise dans le développement de la 5G.

D'autre part, la France est **dépendante** des solutions numériques étrangères comme Microsoft. Cette couche logicielle est donc vulnérable car il n'existe pas de cloud « national » car les opérateurs nationaux financés par l'Etat ne sont pas suffisamment compétitifs. Il existe pourtant des solutions comme en Allemagne où la Deutsche Telekom a négocié un accord avec Microsoft qui l'oblige à héberger les solutions logicielles du cloud dans les datacenters allemands. Mais les systèmes matériels semblent sécuriser par des conventions (initiatives OTAN et UE). L'Etat souhaite maîtriser trois technologies clés de la cyberdéfense : le chiffrement des communications (adresses IP dans un marché très morcelé), la détection d'attaques informatiques qui sous-entend un contrôle des composants des systèmes informatiques alors que la France est dépendante des géants pour les composants et logiciels et ne dispose pas d'éditeur national des technologies capable de répondre au marché, idem pour les logiciels d'analyse de codes malveillants (l'ANSSI ne peut effectuer une protection seule de l'ensemble des acteurs économiques sur les postes, serveurs et cloud, absence d'acteur européen à ce jour qui pourrait utiliser l'IA…), les radios mobiles professionnelles (réseau saturé qui devrait évoluer avec le passage à la 5G). La France dispose d'une **base industrielle nationale** qui lui assure une cybersécurité mais sans parvenir à exporter ses compétences dans les domaines de la cryptographie et chiffrement, puis de la carte à puce (Gemplus, Oberthur). Seules les entreprises dans le secteur de la sécurité des réseaux se sont hissées au rang mondial (Bull, Atos, Thalès, Gemalto).

Enfin, la couche sémantique est très vulnérable par le **manque d'acculturation au risque** cyber des différents acteurs. Les entreprises ne s'équipent que peu à peu face aux cyberattaques (rançongiciel, espionnage industriel…), les médias et citoyens manquent encore de **formation** pour identifier, se protéger et réagir aux cybermenaces (propagande, désinformation…).

- **Une coopération européenne frileuse ?**

L'action internationale de la France est une stratégie d'influence : elle intervient dans la définition des normes cyber au niveau européen et international (UE et OTAN, ONU) afin de délimiter les champs de la cybercriminalité. La **Convention de Budapest** en 2001, rédigé par le Conseil de l'Europe et la participation d'autres Etats comme la Chine, est signée en 2019 par 63 pays en 2019 dont les Etats-Unis mais pas la Russie. Cette convention, texte qui fait référence à l'échelle internationale, tend à harmoniser les législations nationales sur les infractions pénales commises via Internet, faciliter la coopération internationale dans les poursuites judiciaires. La **cybercriminalité est mondialisée et multiforme** : elle pose alors la question de la définition des cybercrimes (qui peut différer selon les législations nationales, voir même au sein d'un Etat fédéral), l'identification des auteurs et leur statut (individus, organisations criminelles, Etats), de la territorialité (lieux de départ et/ou de réception de la cyberattaque). On constate une avancée dans les normes qui permettraient une réponse répressive, mais la coopération est encore insuffisante pour rendre son application efficiente.

Cette situation s'explique par l'absence de définition commune du cyberespace et d'un marché commun aux Etats européens de la cyberdéfense qui poserait la **question de la souveraineté des Etats**. Les logiques d'enjeux sécuritaires nationaux semblent l'emporter sur les coopérations. Alors l'Union européenne et la France favorisent depuis 2015 une **cyberdéfense préventive**. Depuis 2016, une directive européenne oblige les entreprises des secteurs stratégiques à sécuriser leurs systèmes informatiques, les fournisseurs d'accès sont responsables de la sécurisation des données stockées dans le *cloud*. Les différents acteurs sont sensibilisés aux enjeux de la cyberdéfense.

Mais cette volonté de défendre des valeurs dans le cyberespace se heurte à la question de la **gouvernance de l'Internet**. L'exemple du RGPD en 2016 est révélateur : comment protéger les données des usagers dans la mesure où ils doivent accepter les conditions générales d'utilisation pour accéder aux services des GAFAM ? Enfin, la question fiscale des GAFAM et BATX est un débat récurrent en Europe. L'UE est-elle en mesure d'imposer le droit à de telles puissances non étatiques présentes sur son territoire ?

Pistes possibles

-Un document de synthèse collaboratif sous forme de **diagramme en étoile** (dit diagramme de Kiviat) mettrait en évidence les couches du cyberespace à partir de l'étude par groupe de plusieurs **puissances** (Etats-Unis, Chine, Russie, France, Allemagne, Grande Bretagne ou Inde). Il serait l'occasion d'exercer l'esprit critique sur les traitements statistiques sous forme de graphiques.

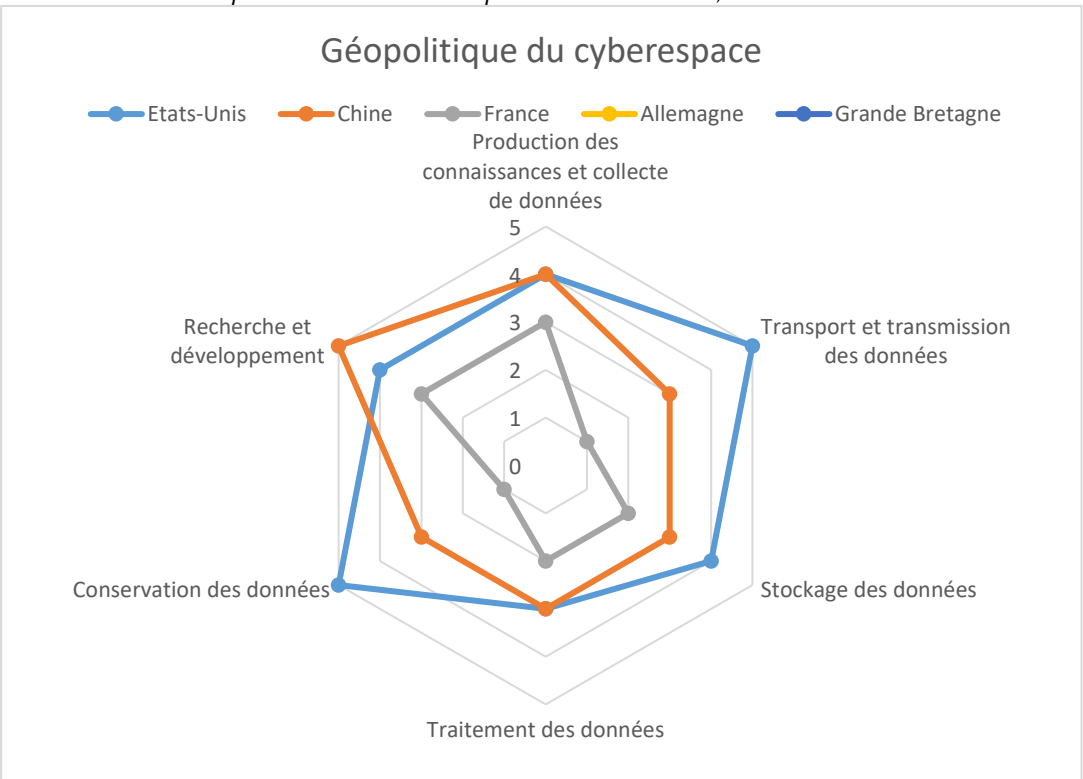
1ère étape : chaque groupe de six élèves travaille sur un Etat au choix (Etats-Unis, Chine, Russie, France, Allemagne…). Chaque élève dans le groupe travaille sur un thème (production et collecte de données, transport et transmission des données, stockage des données, traitement des données, conservation des données, recherche et développement consacrés au cyberespace). L'élève effectue une recherche en autonomie (à partir si nécessaire d'une bibliographie et sitographie) pour sélectionner les arguments et identifier les sources fiables qui permettent de positionner l'Etat sur une échelle de 1 (le risque zéro n'existe pas) à 5.

2ème étape : chaque groupe se retrouve pour mettre en commun à l'aide d'un tableur la position des Etats dans les différents thèmes ou domaines étudiés. Un représentant de chaque groupe expose à l'oral les arguments qui expliquent la valeur attribuée par thème à chaque Etat. Cette étape permet de visualiser à l'aide du diagramme en étoile les inégalités, les atouts, les vulnérabilités des Etats.

3ème étape : chaque groupe procède à un choix de graphique à l'aide du tableur, en disposant toujours du même tableau de données, qui met le mieux en avant ses arguments pour situer un Etat par rapport à un autre. L'échelle des valeurs et les formes de graphiques peuvent être modifiées, mais les choix effectués explicités et justifiés. L'enseignant peut confronter et évaluer la pertinence des choix.

Ce travail mobilise plusieurs **capacités** des élèves : analyser, interroger, adopter une démarche réflexive puisqu'il y a confrontation des points de vue au sein et entre les groupes sur les représentations des élèves et le traitement des données statistiques / se documenter de manière autonome / s'exprimer à l'oral / justifier une production. *Durée estimée en classe : 4h + travail hors la classe de lecture et recherche.*

Exemple réalisé avec Excel pour les Etats-Unis, Chine et France



-L'Intelligence Artificielle, révélatrice d'une géopolitique de la connaissance : plusieurs domaines peuvent être étudiés (la cyberdéfense, la médecine, la modélisation en sciences…) et croisés afin d'établir une carte des puissances mondiales de l'IA.

RESSOURCES

Bibliographie

- Amaël CARTARUZZA, *Géopolitique des données numériques. Pouvoir et conflits à l'heure du Big Data*, Le cavalier bleu, 2019.
- Revue *Hérodote*, « Cyberespace : enjeux géopolitiques », n°152-153, 2014. Consulté en ligne [le 4 mars 2020].
- Dominique BOULLIER, « Le « hard » du « soft » : la matérialité du réseau des réseaux », *Cériscope Puissance*, 2013. Consulté en ligne [le 5 mars 2020].
- INA : *La Revue des médias*, « Internet, ça sert d'abord à faire la guerre », une série de onze épisodes rédigés par des experts, 2016-2019.

Sitographie de ressources (scientifiques et/ou didactiques)

- Revue *Hérodote*, lexique du cyberespace, 2014
- Vidéo de l'éditeur Delagrave, manuel SNT (utile pour tous les niveaux) Mise au point sur le vocabulaire

- Arte, émission *le dessous des cartes*, « le cyber, un nouvel espace géopolitique », octobre 2018. (12min)
- Arte, émission les experts du dessous des cartes « Prêts pour la cyberguerre ? », 2019 (8min)
- France Culture, émission *Place de la Toile*, « Cyberespace et géopolitique », 2014. (50min)
- Quartz : Carte animée de l'historique des câbles sous-marins de 1990 à 2016
- *Le Monde*, mars 2019, vidéo « comment la 5G est devenue un enjeu géopolitique »
- Ministère de la Défense, Général Didier Tisseyre, commandant de la cyberdéfense, vidéo « le cyberespace, un nouveau champ de bataille », Forum International de la Cybersécurité en 2020.
- France 24, *Sept jours en France*, « La France face aux menaces informatiques », 2017. (vidéo 12min qui expliquent les missions de la cyberdéfense française)

Liens avec les autres programmes

1ère HGGSP

- Le thème 4 « S'informer : un regard critique sur les sources et modes de communication »

Terminale HGGSP

- Le thème 1 : De nouveaux espaces de conquête / Axe 1 : conquêtes, affirmations de puissance et rivalités / Objet conclusif : la Chine, à la conquête de l'espace, des mers et des océans
- Le thème 2 : Faire la guerre, faire la paix : formes de conflits et modes de résolution / Introduction

⇨ Ces thèmes mobilisent les notions de puissance, de frontière, de territoires déjà travaillées en 1ère.

Seconde SNT

- Les données structurées, Internet, le Web, localisation cartographie et mobilité, les réseaux sociaux, l'informatique embarquée.