Cours terminale HGGSP. Thématique 6. L'enjeu de la connaissance Objet de travail conclusif. Le cyberespace : conflictualité et coopération entre les acteurs.

Frédéric Richard

Les références aux documents renvoient au manuel Histoire – géographie Géopolitique & Sciences Politiques, Hachette Éducation, 2020.

Nous allons voir en quoi le cyberespace illustre-t-il l'ambiguïté des relations entre les différents acteurs pour le contrôle de la diffusion de la connaissance. Ces derniers peuvent coopérer mais aussi s'affronter.

I**) Le cyberespace : à la fois des acteurs, des territoires et des réseaux.**

A) Définir le cyberespace.

Si on retient la définition technique le cyberespace est *un réseau télématique international qui résulte de l'interconnexion des ordinateurs du monde entier utilisant un protocole commun d'échange des données afin de dialoguer entre eux via les lignes de télécommunication (lignes numériques, lignes téléphoniques, câbles). Définition du dictionnaire Larousse.*

Le mot est apparu pour la première fois dans le cadre de la littérature de science fiction dans le roman de William Gibson *Neuromancien* en 1984.

Le cyberespace désigne plus largement l'ensemble de l'espace virtuel accessible par des ordinateurs. L'internet est le moyen d'accès. L'internet a un ancrage physique avec les ordinateurs, les câbles, les satellites, les *data centers*, …. (Voir document 2 page 445 et 3 page 446). Il renferme aussi un ensemble de données numérisées essentielles pour les différents acteurs

Le mot cyberespace a été au départ lié à des valeurs positives. Au cours des années 1990, on l'associait aux valeurs de liberté, de dialogue, comme une nouvelle forme de communication permettant d'accomplir des progrès dans la société.

Le cyberespace est aujourd'hui davantage vu comme en enjeu géopolitique et stratégique où règne aussi la conflictualité. Il appelle aussi une coopération afin de la sécuriser

B**) Le cyberespace, un nouvel espace, une nouvelle frontière et de multiples acteurs**.

1) Des infrastructures importantes et stratégiques

Le nombre d'internautes n'a cessé d'augmenter depuis les années 1990. Ils étaient 500 millions en 2001 et 4,5 milliards aujourd'hui. Soit 40% de l'humanité. On peut rapprocher cette

croissance exponentielle de celle des ordinateurs vendus dans le monde et du nombre des serveurs web (200000 aujourd'hui)

Afin d'assurer les services liés à internet, le monde est parcouru par plus de 450 câbles sous-marins équipés en fibre optique. On peut parler d'autoroutes du web. Ils représentent 99% des flux numériques et 1,3 millions de km (32 fois le tour de la terre).Ils sont fragiles car les risques potentiels de coupure sont importants : sabotages et catastrophes naturelles (tremblements de terre, tsunamis). Ils peuvent être victimes d'espionnage. Ainsi, le Danemark aurait laissé les EU espionné ses câbles sous-marins entre 2012 et 2014. Des responsables allemands (dont Angela Merkel), suédois, norvégiens et français auraient été espionnés.

Ces câbles sont installés par des navires câbliers (Document 2 page 445) et sont la propriété d'entreprises privées comme l'entreprise française Alcatel et Orange Marine, des EU TE SubCom, TYCO…et de plus en plus de géants du numérique : les GAFAM et Netflix aux EU, le chinois Huawei, l'indien Tata….L'entretien de ces câbles est coûteux et complexe.

Il y a aussi les satellites. Ils ne représentent que 1% des flux du numérique. Il y en a plus de 2000 en activité. Seulement 37% se consacrent à la communication. Ils sont propriétés des États. Les EU, la Chine et la Russie en ont le plus.

Des entreprises privées sont également sur le marché du lancement de satellites. Ainsi, l'entreprise Space X fondée en 2002 par Ellon Musk aux EU.

Dans le domaine des infrastructures, on peut aussi citer les *data centers*. Ces derniers sont les lieux de stockage des données numériques. Ils sont dotés d'ordinateurs superpuissants. On en compte plus de 4500 dans 122 pays dont pratiquement la moitié aux EU.

Ils consomment énormément d'énergie et s'installent de préférence dans des lieux froids du fait de la surchauffe.

Notons qu'internet consomme 10% de l'électricité mondiale et rejette 4% du CO2. Si c'était un pays, internet serait le 3ème consommateur d'électricité au monde.

2) De multiples acteurs différenciés.

Les acteurs du cyberespace sont très diversifiés et leur hiérarchie reflète bien les enjeux de puissance.

Il y a tout d'abord les États. Ils cherchent à affirmer leur souveraineté sur cet espace et à protéger leurs données numériques et celles de leurs citoyens.

Les entreprises qui se sont développées grâce au numérique sont des acteurs incontournables du cyberespace.

On peut citer les GAFAM, les NATU et les BATX.

Les GAFAM désignent les entreprises des EU qui sont apparus en premier et sont les leaders historiques du numérique.

Elles sont concurrencées par de nouvelles entreprises qui sont apparues plus récemment comme les NATU : NETFLIX, AIRBNB, TESLA et UBER. Leur principe de fonctionnement est différent : souscriptions, location de services fournis par des prestataires (logements, taxis), la plateforme mettant en contact les prestataires et les clients.

Les BATX sont en revanche les concurrents directs des GAFAM en Chine. Il s'agit de BAIDU, le moteur de recherche chinois, ALIBABA l'équivalent d'AMAZON, et de deux entreprises qui fabriquent des téléphones mobiles : TENCENT et XIAOMI.

Ces géants du numérique se retrouvent en situation oligopolistique et ils dominent le marché mondial avec très peu de concurrence.

D'autres acteurs interagissent dans le cyberespace. Les autres entreprises quelque soit leur domaine d'activité sont obligées d'être présentes dans le numérique.

C'est le cas des administrations de l'État, des hôpitaux, des écoles, des universités, des exploitations agricoles, des ONG, des partis politiques, des syndicats, des associations, des groupes criminels, des individus à travers le travail, les loisirs et les réseaux sociaux….Il est devenu difficile de ne pas être connecté au numérique pour des sociétés intégrées à la modernité. Ce n'est cependant pas le cas de tous les habitants de la planète, notamment les populations en marge de la société dans les pays développés et les pays en voie de développement. .

Les *hackers* sont des acteurs à part. Disposant de connaissances très grandes en informatique, ils cherchent à tirer profit du cyberespace ou à défendre une cause.

Le groupe *Anonymous,* créé vers 2003-2004 mène de véritables combats. Ainsi, en 2011 en Tunisie lors du déclenchement des *Printemps arabes* ils attaquent plusieurs sites gouvernementaux car le Président Ben Ali censurent internet pour éviter le succès des révoltes.

En 2015, après les attentats de *Charlie Hebdo*, le collectif *Anonymous* combat le terrorisme islamiste en attaquant plusieurs sites et comptes de mouvements extrémistes islamistes.

3) Le rôle prépondérant des EU dans le cyberespace.

Les EU ont un rôle prépondérant dans le cyberespace. Cela s'explique par leur rôle essentiel dans l'informatique, le numérique et les réseaux sociaux : vente du 1er ordinateur IBM en 1959, création par Apple du premier ordinateur Macintosh en 1984, création d'internet en 1990, de Google en 1998, création de Facebook en 2004, de Twitter en 2006, du smartphone en 2007…

Cependant ce poids prépondérant a tendance à se réduire du fait de l'apparition de régulations, de scandales et de concurrents.

Ainsi en 1998, les EU créent l'ICANN.

L'ICANN est *l'International Corporation for Assigned Names and Numbers.* Il s'agit d'un organisme californien sans but lucratif qui attribue les noms des sites internet et des adresses

IP de ces sites. Elle fut créée sous la présidence de Bill Clinton qui voulait un internet unique dans le monde. Il y avait une volonté de domination des EU.

Depuis 2009, de nombreux États et la Commission Européenne, ont demandé à ce que cet organisme devienne indépendant et ne soit plus sous la tutelle du Gouvernement des EU. La demande est devenue plus forte à partir de 2013 à la suite des révélations d'espionnage d'Edward Snowden l'ex agent de la NSA et de la CIA.

Depuis 2016, l'ICANN est un organisme indépendant géré par une multitude d'acteurs : des États, les institutions de l'UE, des organismes de défense des droits de l'homme, des organismes commerciaux, des organismes des droits de propriété intellectuelle, des organismes qui représentent les internautes… (Voir document 2 page 448)

Les EU doivent prendre en compte de nouveau concurrents. Le plus redoutable est la Chine tant pour le commerce en ligne avec Ali Baba, les réseaux sociaux avec Tencent et Tik Tok, les smartphones avec Huawey … (Voir document 3 page 449). La Chine a mis sur pied un internet contrôlé (Voir document 2 page 451). Baidu assure 77% des recherches chinoises sur internet contre 1,7% pour Google. Avec les EU et la Russie, la Chine a une grande capacité d'action militaire dans le cyberespace, à travers ses hackers notamment.

D'autres États cherchent à échapper à cette centralité des EU. Ainsi, Cuba et le Venezuela ont créé le câble Alba 1. Il y a aussi le projet du *South Atlantic interlink* entre l'Amérique Latine et l'Afrique (plus précisément entre le Cameroun et le Brésil) et qui doit être installé per des compagnies chinoises (Unicom China, Camtel y Huawei Marine Networks)

Les scandales provoqués à partir de 2010 par Julian Assange dans le cadre de l'organisation WikiLeaks et les révélations d'Edward Snowden, un ex agent de la NSA et de la CIA , en 2013 concernant l'espionnage de cette agence, ont montré les limites des EU dans la protection de leurs données numériques même très confidentielles.

II) Un enjeu géopolitique et des conflictualités de plus en plus importantes.

Le cyber est devenu un espace de puissance et de projection de la puissance, notamment pour les États, au même titre que les mers et les océans, et l'espace.

A) Liberté ou contrôle de l'information : un enjeu pour les États et pour les citoyens.

1) Un espace de liberté.

La question de la liberté et de ses limites dans le cyberespace est devenue un enjeu crucial.

Les années 1990 qui furent celles des débuts de l'internet furent marquées par des discours de liberté.

Ainsi, en 1996, en réaction à des lois aux EU qui prétendaient contrôler internet, le poète et militant libertarien (courant politique des EU qui insiste sur la fait que la société doit avoir comme priorité la liberté de chaque individu) John Perry Barlow (1943-2018) publie une *Déclaration d'Indépendance du Cyberespace* affirmant que les États ne pourraient contrôler cet espace.

L'affaire de l'ICANN a montré que l'Internet pouvait encore conserver cet idéal de liberté.

Les scandales liés aux révélations de WikiLeaks par Julian Assange à partir de 2010 (actions par exemple de l'armée des EU en Irak et en Afghanistan contraire au droit international) et celles d'Edward Snowden ex agent de la NSA et de la CIA, en 2013 (Snowden dénonce un système d' espionnage et d'écoute planétaires , par exemple de dirigeants européens pourtant alliés des EU comme la chancelière Merkel, les présidents français Chirac, Sarkozy et Hollande…) montrent que l'Internet est un espace de liberté. Assange et Snowden ont pu diffuser l'information et les documents secrets sur l'internet. (Voir biographie page 456)

Il faut noter cependant que Julian Assange de nationalité australienne est en prison au RU après avoir été réfugié plusieurs années dans l'Ambassade d'Équateur à Londres et les EU ont demandé son extradition pour espionnage. Il risque une peine de prison de plus de 130 ans. Edward Snowden est réfugié en Russie et a obtenu la nationalité russe .

2) La nécessité d'un encadrement.

Il a fallu cependant encadrer certaines pratiques comme le piratage des contenus culturels : musique, films…Il y a les problèmes des *darknets* de plus en plus faciles d'accès. Ils sont utilisés pour des activités illégales et les trafics : drogue, personnes, armes, pédopornographie….

Même les géants du net légaux ont utilisé pendant très longtemps, sans l'accord des internautes, les données produites (les *Big Data),* et en ont fait un profit considérable.

Les États ont cherché à encadrer ces pratiques. En 2009, la loi Hadopi en France crée la Haute autorité pour la diffusion et la protection des droits sur internet. La police tente également de plus en plus de pénétrer les *darknets* afin de pourchasser les activités illégales.

3) Sécurité et contrôle de la population.

Les États utilisent également internet pour renforcer leur sécurité et contrôler la population.

La vidéosurveillance et la reconnaissance faciale se multiplient.

La Chine pratique un contrôle social de sa population de plus en plus important.

De plus en plus de villes chinoises sont équipées de caméras de vidéosurveillances avec reconnaissance faciale. Chaque citoyen possède des points attribués puis enlevés selon son comportement. Chaque citoyen commence avec un capital de 100 points Traverser la rue quand le feu est rouge, jeter un papier ou cracher par terre ….entraine une baisse de points. Dénoncer un acte illégal fait augmenter les points.

Le gouvernement chinois limite également l'utilisation des jeux vidéo par les enfants et les adolescents à 3 heures en fin de semaine.

Le cyberespace est aussi un lieu de propagande. Cela concerne des États comme la Chine et la Russie, des groupes terroristes jihadistes comme DAESH ou AL QAEDA ….

B) La multiplication des conflictualités.

Les cyberattaques ne cessent de se multiplier. Elles se diversifient depuis la délinquance, l'espionnage, la lutte contre la censure et la manipulation politique.

Elles peuvent relever de la délinquance avec les rançongiciels (Voir document 3 page 457) qui exigent des rançons souvent en bitcoin et cryptomonnaie pour débloquer des systèmes et des données. Cela concerne des entreprises, des hôpitaux, des personnes….La protection des données est devenue un problème essentiel (Document 2 page 450)

Cela peut s'inscrire également dans des dénonciations morales. Ainsi en 2015, la mise en ligne des données de sites de rencontre extra conjugales.

La cyberattaque nous l'avons vu avec le groupe *Anonymous* peut servir à dénoncer les pays qui exercent la censure ou attaquer les groupes terroristes.

Il y a aussi les logiciels espions ou de *phishing* pour voler des données.

La dimension peut aller au-delà de las délinquance et prendre une dimension politique.

On peut de nouveau citer les écoutes mondiales par la NSA dénoncées par Snowden.

En 2015, la chaîne de télévision TV5 a été attaquée par des pirates russes qui se faisaient passer pour des jihadistes. La chaîne n'a pas pu émettre pendant deux jours et ses réseaux sociaux diffusaient des messages en faveur de l'État islamique (DAESH)

Il faut situer ce piratage dans le contexte géopolitique de l'époque et qui concernait l'Ukraine. La Russie avait annexé la Crimée et suscité la sécession du Donbass à l'Est du pays. Les relations étaient devenues très tendues et la France avait stoppé la vente de porte-hélicoptères Mistral commandés par la Russie en 2010.

Des interventions peuvent menacer la vie démocratique de certains États. Ce fut par exemple l'Affaire Cambridge Analytica.

Cambridge Analytica est une société britannique spécialisée dans l'analyse de données et l'influence de l'opinion publique à travers les sondages et les réseaux sociaux. Elle aurait joué un rôle d'influence et de manipulation de l'opinion publique dans le cadre du Brexit en 2018 en faveur du vote pour ce dernier, et l'élection présidentielle des EU en 2016. On l'accuse de désinformation, d'utilisation de rumeurs…à travers Facebook en faveur de Trump. Par exemple, l'envoi de messages personnalisés, notamment de *fake news,* aux électeurs via Facebook pour influencer leur vote. Cela aurait concerné 50 millions de personnes et probablement favorisé l'élection de Trump. (Document 1 page 450)

Le piratage peut concerner des personnalités politiques comme nous l'avons vu avec la NSA. Cela peut aussi concerner des personnalités des EU.

Ainsi, la boîte mail de la Secrétaire d'État (Ministre des Affaires Étrangères) Hilary Clinton entre 2009 et 2013 aurait été piratée. Le scandale a été important car elle utilisa une boîte mail personnelle alors qu'elle aurait du utiliser une boîte officielle sécurisée. La polémique fut très vive lors de l'assassinat de Christopher Stevens l'ambassadeur des EU en Libye en 2012.

On accuse la Russie d'être intervenue dans la campagne présidentielle des EU en 2016 en faveur de Trump et contre Hilary Clinton en manipulant notamment les réseaux sociaux (Voir document 4 page 449) grâce à des Hackers nommés des trolls et basés à Saint-Pétersbourg dans des « usines ou des fermes à trolls » et en liens avec les services de renseignement russes. Twitter a reconnu plus de 12 millions de tweets automatisés provenant de Russie durant la campagne électorale. Cependant, le procureur en charge de l'affaire n'a pas pu prouver un lien direct entre le candidat Trump et la Russie.

Face à ces menaces la cyberdéfense est devenue une priorité des puissances.

III) Les progrès de la cyberdéfense entre la coopération et la souveraineté.

A) Une coopération mondiale limité.

L'ONU essaye de mettre en place une coopération mondiale en matière de cybersécurité. En 2015, un rapport a été adopté appelant à la coopération entre les États, la lutte contre les pratiques et les outils malveillants, le respect des infrastructures des Etats**….L'Appel de Paris en 2018** pour la cybersécurité a reçu le soutien de 67 États et 358 entreprises (IBM, FACEBOOK, MICROSOFT…) et 139 organisations internationale. C'est un appel à la coopération internationale dans la lutte contre les cyberattaques. Malgré les bonnes intentions les progrès sont lents. Une gouvernance mondiale (Voir définition vocabulaire page 458) comme dans d'autres domaines (santé, lutte contre le réchauffement climatique, protection de la biodiversité, respect des droits de l'homme…) est difficile à mettre en place.

B) Des progrès plus rapides : l'OTAN, l'UE et les États.

1) L'OTAN.

La coopération à l'intérieur de l'OTAN en matière de cyberdéfense a connu de grands progrès. Chaque **année le Centre d'excellence de cyberdéfense coopérative de l'OTAN**, organise le *Locked Shields.* Ce dernier est un exercice international unique de cyberdéfense réunissant plus de 1200 experts en cyberdéfense des 23 États membres pour tester les capacités à lutter contre des attaques informatiques

2) L'UE

L'UE est consciente de son retard et a mis sur pied une stratégie de cybersécurité. De plus, si des pays comme la France, l'Allemagne et le RU ont des agences de cybersécurité très efficaces capables de sécuriser les infrastructures informatiques, notamment militaires, et de mener des opérations cyber offensives, elles n'ont pas la puissance des structures des EU, de la Chine et de la Russie.

Elle adopte une normative, des agences et des programmes de cybersécurité

En 2016, l'UE adopte la directive SRI (Sécurité des réseaux et des systèmes d'information). Cette directive impose aux prestataires et fournisseurs de services numériques de prendre des mesures de sécurité appropriées pour pouvoir résister à des attaques.

En 2018, elle adopte le Règlement général sur la protection des données. Cela concerne les données des utilisateurs face notamment aux grandes plateformes du numérique et aux révélations de Snowden.

Elle insiste également sur la nécessaire coopération entre les autorités compétentes dans l'ensemble de l'UE. La coopération est difficile car les 27 pays n'en sont pas au même niveau en matière de cyberprotection.

L'agence nommée ENISA (Agence Européenne chargée de la sécurité des réseaux et de l'information) créée en 2004, et nommée aujourd'hui Agence Européenne pour la cybersécurité, est chargée de la cybersécurité.

L'UE à travers cette agence pilote **4 programmes de cybersécurité.**

Ils s'inscrivent tous dans le cadre du programme global européen de financement de la recherche et de l'innovation Horizon 2020. (2014-2020)

CONCORDIA (CyberSecurity Competence for Research and Innovation), ECHO (European network of Cybersecurity centres and competence Hub for innovation and Operations), CyberSec4Europe et SPARTA.

Le projet CONCORDIA est une collaboration à l'échelle européenne de la cybersécurité. Il regroupe 18 États, certains comme la Norvège et la Suisse ne sont pas membres de l'UE, des agences européennes comme *Europo*l (police) et *l'European Defense Agency*, des universités et des centres de recherche comme les universités de Zurich, de Milan, de Lorraine, d'Oslo….et des entreprises : Airbus, BMW, Siemens….(Document 2 page 454)

Pour que des progrès réels voient le jour, il faut que l'UE intègre une logique géopolitique de puissance non seulement dans le domaine de la cyberdéfense , mais aussi dans le domaine militaire, de la diplomatie….au delà des logiques nationales encore dominantes. (Document 3 page 455)

Dans le domaine de la cybersécurité, l'UE est davantage préoccupée par la protection des données de ses citoyens que de définir une stratégie de puissance et géopolitique. Le premier point est important mais pas suffisant.

3) La France et le cyberespace : une puissance en devenir.

C'est à partir des années 1990 et encore davantage 2000 avec l'intensification des attaques cybernétiques contre les États, les organisations internationales, les entreprises….que la protection du cyberespace devient une question de sécurité nationale.

Les pays les plus développés sont souvent les plus vulnérables car leur numérisation est importante.

La France a à la fois une stratégie de coopération et de renforcement de ses capacités nationales.

La stratégie nationale a été officiellement adoptée en 2008 avec la publication du « Livre Blanc sur la défense et la sécurité nationale ». Elle est actualisée avec la publication du nouveau libre blanc en 2013.

La sécurité des systèmes d'information numérique est placée au même niveau stratégique que la dissuasion nucléaire. On voit que la cyberdéfense est prise très au sérieux.

Le livre blanc de 2013 identifie trois types de cybermenace : la cybercriminalité, les tentatives de pénétration dans les réseaux numériques à des fins d'espionnage et les attaques visant à saboter des systèmes d'importance vitale tant militaires que civils.

Le Livre blanc fixe la stratégie française de défense et de sécurité nationale, et précise notamment son articulation avec la politique de sécurité et de défense commune de l'Union européenne et avec l'Alliance Atlantique, et les capacités requises pour la mettre en œuvre.

La France s'est ainsi dotée progressivement d'une doctrine militaire de lutte informatique offensive

Le ministère des armées joue un rôle essentiel. (Voir document 1 page 452**). La perspective de guerre 2.0 et de guerres hybrides qui incluent des cyberattaques, et qui pourraient démarrer par des cyberattaques, est de plus en plus envisagée.**

Divers outils civils et militaires ont marqué cette ambition :

a) **Création en 2009 de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'information).** Elle est directement rattachée au gouvernement et a un budget annuel de 100 millions d'euros.

b) Mise en place d'un « plan défense cyber » d'un montant d'un milliard d'euros en 2014.

c) Renforcement de la défense cyber dans les lois de programmation militaire de 2014-2019 et 2019-2025.

Dans les finances publiques françaises, une loi de programmation militaire (LPM), est une loi visant à établir une programmation pluriannuelle des dépenses que l'État français consacre à ses forces armées. Les lois de programmation militaire ont des durées d'application de quatre, cinq ou six ans.

d) Création du commandement de cyberdéfense (COMCYBER) en 2017. Il rassemble l'ensemble des forces de cyberdéfense de l'armée française. Il dispose de 3400 soldats. Le nombre va augmenter dans le cadre de la loi de programmation militaire 2019-2025.

Les 6 missions de ce commandement sont

- anticiper : éviter les cyberattaques

-protéger : diminuer la vulnérabilité des systèmes informatiques face aux cyberattaques

- détecter : rechercher les indices d'une éventuelle cyberattaque.

-attribuer : identifier l'auteur d'une attaque

-réagir : lancer une opération de lutte informatique défensive(LID) afin de neutraliser l'attaque. Le protocole a été défini en 2011.

- riposter : lancer une LIO, une lutte informatique offensive. Le protocole a été défini en 2014. (Voir document 2 page 452)

La France envisage notamment d'utiliser éventuellement les moyens du cyber avec les moyens militaires conventionnels. (Notion de guerre hybride)

e) Un projet de cybercampus en Île -de-France regroupant des structures étatiques, des entreprises spécialisées dans la cybersécurité, des structures de recherche et de formation (laboratoires, universités…) est en train d'être élaboré (Document 5 page 453)

La France mène des coopérations internationales dans le cadre des politiques de l'UE et de l'OTAN. (Voir III) B) 1 et 2 de cette leçon)

Chaque année elle organise le Forum international de la Cybersécurité de Lille. 400 acteurs publics et privés, notamment des entreprises, des universités…essentiellement européens se réunissent afin de favoriser la réflexion concernant la cybersécurité.

Elle conclut également des accords bilatéraux. Par exemple, depuis 2010 avec l'Estonie. Un pays très numérisé et donc très vulnérable. L'Estonie est d'ailleurs le premier pays qui a du affronter une attaque massive en 2007. (Document 1 page 454)

L'ambition de la France depuis le plan cyberdéfense de 2014 est de devenir une puissance de la cyberdéfense en s'appuyant sur un modèle d'internet qui ne soit ni celui des EU qui donne trop de poids à des acteurs privés, les GAFAM, ni chinois trop contrôlé par l'Etat.

La France préfère dans le cadre de l'Appel de Paris de 2018 un modèle multilatéral qui s'appuie sur une entente entre les États et un droit international qui reste à construite (Document 3 page 453)

Conclusion. Le cyberespace est en train de devenir un espace de puissance et de projection de la puissance où les États et les autres acteurs s'affrontent.

Cet espace de liberté rêvé au cours des années 1990 est entré dans une logique d'affrontements et de contrôle.

La conflictualité entraîne la nécessité de politique de coopération comme pour les mers et les océans, et l'espace.

Bibliographie :

Histoire –géographie Géopolitique & Sciences Politiques, Hachette Éducation, 2020.

Spécialité histoire-géographie géopolitique et sciences politiques, ellipses, 2020.

Spécialité histoire-géographie géopolitique et sciences politiques, Compétences attendues, ellipses, 2020.

Spécialité histoire-géographie géopolitique et sciences politiques, Parcours et méthodes, ellipses, 2020.