THEME 6 : L'enjeu de la connaissance

Fiche cours n'° 4

OTC : le cyberespace : conflictualités et coopérations entre acteurs

En 1996, la « Déclaration d'indépendance du cyberespace » rédigée par J.P Barlow pose le principe de la liberté d'expression et de l'open data. **Le cyberespace** est un espace de communication constitué par l'interconnexion mondiale des systèmes d'échange de données numériques (le « big data »). Virtuel, il repose sur des infrastructures utilisées par une grande diversité d'acteurs individuels et collectifs. D'abord conçu comme un espace où chacun peut consulter, produire et diffuser de la connaissance, ses usages sont l'objet d'une surveillance de plus en plus forte de la part des États, qui veulent y affirmer leur souveraineté, tandis que les données personnelles des utilisateurs sont de plus en plus récupérées par les acteurs privés. La maîtrise de ce nouvel espace constitue donc un enjeu politique et géopolitique majeur pour les États qui, victimes de cybermenaces, mettent en place des politiques de cyberdéfense élaborées, sources de conflictualités et de coopération.

⇨ **Problématique : Comment le cyberespace génère-t-il de nouvelles conflictualités ? Peut-on limiter ces tensions par la coopération entre acteurs ?**

I / Le cyberespace.

=>Comment le cyberespace, pensé comme un lieu d'échanges et sans frontières, a-t-il pu devenir un espace de luttes d'influences, de rivalités, et parfois de cloisonnements ?

A / L'organisation des réseaux au sein du cyberespace.

1. Le fonctionnement du cyberespace.

Il se présente comme un ensemble de couches superposées :

- La 1ère couche est l'**infrastructure physique du réseau (hardware)** : elle est composée de **terminaux** (ordinateurs, smartphones...) communiquant entre eux et avec des serveurs (**data center**) par l'intermédiaire de **câbles** ou de **satellites**, permettant la circulation des données sur de grandes distances de façon quasi-instantanée. Près de 99 % du trafic intercontinental est assuré par les lignes sous-marines qui sont de véritables « autoroutes de l'Internet ». 450 câbles, soit plus de 1,2 million de kilomètres, sont au fond des océans.
- La 2ème couche est **l'infrastructure numérique (software)** qui comprend les **systèmes d'exploitation** (Windows…) et les **applications** assurant la transmission des données.
- La 3ème couche est celle du contenu échangé entre utilisateurs (informations, réseaux sociaux…). Ce sont les **données numériques**.

2. La territorialisation.

Internet a été conçu comme un territoire indépendant, « sans frontières », où les États ne possèdent aucune souveraineté. Mais à partir des années 2000, les États le conçoivent comme un territoire à conquérir et à contrôler, ils veulent y faire appliquer les lois afin de garantir leur sécurité. Pour eux, le cyberespace est donc perçu comme un territoire au sens classique. Il y a aujourd'hui une véritable « territorialisation des données ». On le voit avec les data centers. A l'échelle mondiale, l'Amérique du Nord, l'Europe occidentale et Asie de l'Est en ont le plus et à l'échelle locale, les métropoles sont les hubs numériques. Les E-U dominent (38 % des data centers), mais il y a une politique de territorialisation comme en Russie où leur développement s'inscrit dans le cadre légal de voir toutes les données des citoyens stockées sur leur territoire. Des pays comme la Chine ou l'Iran ont mis en place un **routage** (= empêcher que des données issues d'un territoire puissent transiter par un autre), les isolant du reste de la planète.

B / Des acteurs en tensions.

De multiples acteurs coopèrent et s'affrontent dans le cyberespace. Outre les internautes :

THEME 6 : L'enjeu de la connaissance

1. Les entreprises.

Parmi elles, des firmes transnationales comme les **GAFAM américaines** (Google, Amazon, Facebook, Apple et Microsoft) ou les **BATX chinoises** (Baidu, Alibaba, Tencent, Xiaomi) qui sont des entreprises jeunes (Microsoft, la plus ancienne, est née en 1975) et qui ont acquis un nombre d'utilisateurs qu'aucune autre entreprise n'avait jamais connu auparavant. Ainsi, Facebook en compte près de 3 milliards. Les GAFAM fondent leur puissance sur de gigantesques budgets de recherche et développement (>130 milliards $) et sur leur capacité à s'approprier l'innovation en acquérant les startups les plus prometteuses. Elles exercent une influence croissante sur les contenus disponibles en fournissant les infrastructures (possèdent la majorité des data centers, déploient et contrôlent de plus en plus les câbles…). Ainsi les GAFAM assurent 90% des recherches planétaires sur internet. Leur rôle de support des « réseaux sociaux » leur donne une place particulière dans la formation ou dé(sin)formation des opinions publiques.

2. Les Etats.

Ils contrôlent une partie des infrastructures comme les satellites. Parce que le cyberespace est intégré à un nombre croissant d'activités (militaires, politiques, économiques), ils légifèrent pour protéger le transit de données. Les E-U y exercent un contrôle qui cause des tensions avec d'autres États (97% des données numériques échangées entre l'Europe et l'Asie passent par les É-U). D'autres États, comme la Chine, visent le contrôle total des données échangées par leurs citoyens en censurant et en imposant leurs propres outils numériques (moteur de recherche Baidu…). La place des États dans le cyberespace est assez particulière. Leurs pouvoirs semblent remis en question au profit des géants du numérique (perte de contrôle des données, dépendance vis-à-vis de solutions techniques étrangères - ex : Ministère français des Armées équipé par les GAFAM). Mais les États voient aussi leur influence s'affirmer : les GAFAM sont au service de la puissance américaine, comme par la diffusion des systèmes d'exploitation ou les conditions générales d'utilisation (CGU) qui sont de droit étasunien.

3. Les groupes criminels.

Des acteurs malveillants animent les « zones grises » du cyberespace (**dark web et deep web** = portions non indexées par les moteurs de recherche, ce sont les cyberlieux des transactions illicites, payées en cryptomonnaies comme le bitcoin). Ces acteurs sont les **hackeurs** et les organisations **« hacktivistes »** (pirates informatiques). Des groupes structurés s'affirment, désignés sous l'acronyme APT (Advanced Persistent Threat) qui peuvent agir pour leur compte mais aussi en lien étroit avec un État. Le crime n'est pas la seule activité. Certains cherchent aussi à défendre l'idéal de liberté de l'internet, comme Anonymous et Wikileaks qui s'en prennent aux sites gouvernementaux ou d'entreprises privées pour rendre leurs données publiques.

C / Le cyberespace : une gouvernance difficile.

1. Les enjeux.

- Associées à des algorithmes, les données analysent nos déplacements, nos centres d'intérêt... Ces traces permettent des analyses prédictives sur nos comportements à des fins **commerciales ou politiques**. Elles poussent à collecter, stocker, croiser et exploiter les données : c'est devenu le moteur de la croissance économique et de l'exercice du pouvoir, mais avec des enjeux éthiques, démocratiques.
- Les années 2010 ont vu l'émergence du cyberspace comme un **nouveau domaine militaire**. Les cyber opérations font partie de l'arsenal des armées et viennent en appui de tous les moyens utilisés pour faire la guerre. La transformation numérique des sociétés les rend dépendantes au cyberespace, dont la stabilité est désormais essentielle à leur bon fonctionnement (voir II). Les États sécurisent leurs réseaux (les É-U envisagent de sécuriser leurs câbles sous-marins en

déployant des barrières soniques) et les surveillent via leurs services de renseignement pour lutter contre les groupes terroristes.

2. Quelle gouvernance ?

Entre ceux qui conçoivent l'Internet comme un espace de liberté absolue pour échapper à la souveraineté des États et ceux qui veulent le contrôler, la régulation à l'échelle mondiale est difficile. L'opposition se joue entre partisans d'une gouvernance intégrant les géants du numérique et ceux privilégiant une gouvernance multilatérale relevant des seuls États. C'est le cas de **l'ICANN** (Internet Corporation for Assigned Names and Numbers) qui doit 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, la Russie et la Chine s'opposent à cette gouvernance qui laisse la part belle aux E-U.

II / La cyberdéfense.

=>Comment penser la souveraineté d'un État comme la France dans un cyberespace ouvert et avec des outils techniques largement dépendants d'acteurs non nationaux ?

La cyberdéfense renvoie aux moyens permettant à un Etat d'assurer la cybersécurité des systèmes d'information vitaux. Stratégies défensives et offensives se complètent : en amont, les Etats développent des techniques destinées à protéger les données et sécuriser les accès aux comptes sensibles ; en aval, ils développent des stratégies de riposte (en utilisant « l'arme cyber «).

A / Une nécessité face à la multiplication des menaces.

La France est confrontée à des cybermenaces émanant d'ennemis multiformes : puissances étrangères, cybercriminels, groupes d'hacktivistes. En moyenne, il y a 20 attaques graves par an. Elles peuvent être regroupées en trois catégories principales.

- **Le sabotage** : l'objectif est de provoquer des dommages, en touchant la couche logicielle. Des activités peuvent être paralysées (ex : attaque russe contre l'Estonie en 2007). Les « rançongiciels » (bloquent le fonctionnement d'un système informatique jusqu'à ce que la victime s'acquitte d'une rançon) en font partie (ex : virus Wannacry en 2017). Un des risques majeurs concerne aujourd'hui les systèmes électroniques embarqués, dans les domaines automobile, aéronautique ou maritime.
- **L'espionnage** vise à récupérer des données. Le cyber-espionnage industriel est présent dans nombre de secteurs d'activités (aéronautique, automobile, constructions navales de pointe…). Les révélations de Snowden en 2013 ont montré l'ampleur de l'espionnage réalisé par la NSA en explorant les communications électroniques, y compris de dirigeants alliés.
- **La subversion** : vise 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 connu, elle s'est faite par 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 (12 millions de tweets automatisés). Lorsque les menaces deviennent des attaques, elles peuvent déstabiliser en profondeur les États et les sociétés.

B / Un enjeu majeur : la coopération de la France à différentes échelles.

1. A l'échelle mondiale et régionale.

Une cyberdéfense à l'échelle mondiale est complexe à mettre en place car le droit international est limité. Le Conseil de sécurité de l'ONU reconnait aux États le droit de répliquer uniquement si la cyberattaque a eu lieu dans un conflit armé « classique ». De plus, il est difficile d'établir précisément

l'identité d'un cyber-agresseur et ses liens avec un Etat. Par ex, dans l'affaire de la campagne électorale américaine, le procureur n'a pas réussi à prouver la collusion entre Trump et la Russie. Des initiatives existent tout de même. Depuis 2006, un Forum mondial de la gouvernance d'Internet a lieu chaque année, sous la tutelle de l'ONU. Mais c'est finalement à l'échelle régionale que les coopérations sont les plus efficaces : l'OTAN a adopté en 2008 une stratégie ambitieuse de cybersécurité (formation de ses membres, dont la France, avec le « Centre d'excellence de cyberdéfense coopérative» en Estonie).

2. A l'échelle européenne.

La France est intégrée aux politiques de coopération européenne de cyberdéfense. L'UE a pour ambition de coordonner l'action des États et de favoriser les échanges pour lutter contre les cybermenaces (ex: en 2019, l'entreprise européenne Airbus est victime d'une cyberattaque de ses sous-traitants, à des fins d'espionnage industriel). Elle se dote donc d'experts et d'organisations : créée en 2004, l'Agence européenne chargée de la sécurité des réseaux et de l'information **(ENISA)** est chargée de mettre en œuvre cette coopération. Son activité consiste à aider à l'élaboration des stratégies nationales de cybersécurité et à coordonner le travail des équipes d'intervention en cas d'urgence informatique dans un pays membre. L'UE a établi un cadre de certification de cybersécurité qui impose des normes contraignantes aux différents acteurs du numérique, afin de renforcer la sécurité des produits connectés et des infrastructures. Toutefois, l'harmonisation des pratiques européennes est limitée : l'UE ne dispose pas d'outil autonome des GAFAM, et la coordination des pratiques des États membres n'est pas totale.

C / La cyberdéfense française en action : les luttes informatiques.

Compte tenu des limites de la coopération internationale et européenne, la France s'est dotée dès 2015 d'une stratégie nationale pour la sécurité du numérique. En cas de cyberattaque, la France se réserve le droit de riposter et d'employer en opérations extérieures l'arme cyber à des fins offensives.

1. Une prise en compte récente mais croissante.

La prise en compte des risques liés au cyberespace s'est faite de façon progressive en France. **Le Livre blanc sur la défense et la sécurité nationale** de 2008 est le premier à faire état de risques d'attaques. Celui de 2013 a mis les cyberattaques au 3ème rang des menaces susceptibles d'affecter la vie de la nation (après les agressions d'un autre État sur le territoire et les menaces terroristes).
La cyberdéfense française est structurée autour de l'Agence nationale pour la sécurité des systèmes informatiques **(ANSSI)** qui est chargée de la prévention et de la réaction aux incidents informatiques visant les institutions sensibles (aéroports, centrales nucléaires, ministères, etc.) par la veille, la détection, l'alerte et la riposte aux attaques informatiques. L'ANSSI emploie 600 civils et agit aussi en développant des campagnes de sensibilisation des particuliers et des entreprises à la protection de leurs données. Elle peut intervenir afin de stopper une attaque comme en 2015 lorsque TV5 Monde a dû interrompre la diffusion de ses programmes. Il y a également le commandement de la Cyberdéfense **(COMCYBER)** qui vise à détecter les attaques contre le ministère des Armées et qui a une dimension offensive. Il a plus de 4000 cyber combattants 2025.

2. Une stratégie à la fois défensive et offensive.

Le modèle français distingue les acteurs menant la l**utte informatique défensive** (LID) de la **lutte informatique offensive** (LIO). Il diffère des pays anglo-saxons, où la cyberdéfense relève des acteurs du renseignement.
La LID est civile et militaire. Elle est axée sur le développement de comportements vigilants et la protection/restauration des systèmes et ressources numériques. La LIO s'impose à partir de 2019.

THEME 6 : L’enjeu de la connaissance

Elle est du ressort de l’État qui peut mobiliser ses capacités de renseignement avant d’engager une action offensive et en mesurer les risques, qui sont différents de ceux d’opérations conventionnelles. En effet, 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 entraîner une escalade du fait de la multitude de connexions réseaux. Ces éléments expliquent aussi que les opérations de LIO doivent rester secrètes.

Conclusion

Objet de toutes les utopies, le cyberespace est aussi un lieu de tensions et d'affrontements entre acteurs publics et privés aux intérêts divergents. Espace virtuel de la libre circulation de la connaissance, il contribue à la mise en place de sociétés de l’information. Espace d'expression des cybermenaces et des politiques de cyberdéfense des États, il est le moyen et l’objet d’un contrôle de plus en plus étroit des citoyens par les grandes entreprises et les gouvernements, et donne naissance à des sociétés de la surveillance obsédées par la cybersécurité. Seule la coopération internationale peut limiter les conflits du cyberespace. Elle passera par la création d’un droit international dédié pour combler le vide juridique actuel. Ce qui nécessitera que les États abandonnent leur désir d’assurer leur souveraineté sur le cyberespace, et donc qu’ils cessent de l’envisager comme un territoire au sens classique du terme.