HGGSP THEME 6 - L'ENJEU DE LA CONNAISSANCE

AXE CONCLUSIF - LE CYBERESPACE : CONFLICTUALITÉ ET COOPÉRATION ENTRE ACTEURS *(5 heures)*

PROGRAMME

AXE CONCLUSIF : Le cyberespace, entre réseaux et territoires (infrastructures, acteurs, liberté ou contrôle des données…) / Cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français.

(H1)

ACCROCHE - Le 22 août **2019**, **Emmanuel Macron a reçu le Premier ministre de l'Inde** (Narendra Modi) au château de Chantilly. Cette visite a été l'occasion de renforcer la coopération entre les deux États, notamment par la signature d'une « Feuille de route franco-indienne sur la cybersécurité et le numérique ». Voici quelques extraits de ce document :

> **La France et l'Inde** affirment leur attachement à un cyberespace ouvert, fiable, sûr, stable et pacifique. La France et l'Inde reconnaissent la responsabilité partagée d'une **grande variété d'acteurs**, dans leurs rôles respectifs, pour améliorer la confiance, la sécurité et la stabilité dans le cyberespace. Elles appellent au renforcement de l'approche multi-acteurs et soulignent que cela nécessite un effort conjoint des **gouvernements**, de **l'industrie**, du **monde universitaire** et de la **société civile**. […] Par ailleurs, la France et l'Inde reconnaissent qu'il est nécessaire de traiter les problèmes découlant de la prolifération des pratiques et des **outils malveillants dans le cyberespace**. […] La France et l'Inde reconnaissent que la cybercriminalité est un **crime transnational qui requiert une coopération internationale renforcée**. Elles **prévoient de discuter de la prévention** de **la cybercriminalité** avec les **fournisseurs de services** et les **entreprises de médias sociaux** pour rechercher des accords de partage d'informations. [Enfin] la France et l'Inde souhaitent mettre en place un écosystème numérique innovant, sécurisé et respectueux de **la protection des données des utilisateurs**.
>
> Extraits de la *Feuille de route franco-indienne sur la cybersécurité et le numérique* (aout 2019)

➔ Cette feuille de route témoigne de :

- la complexité du cyberespace, qui **dépasse les frontières nationales** et concerne une **très grande variété d'acteurs**.
- l'existence de **menaces dans le cyberespace** (qui sont parfois le fait d'autres États)
- la mise en place d'une cyberdéfense, qui passe en partie par la **coopération internationale**

[A LIRE : ÉLEVES LA RECUPERENT CHEZ EUX] Le **CYBERESPACE** est un espace virtuel constitué par l'interconnexion mondiale des systèmes informatiques et de télécommunication. **Véritable réseau sans frontières** déployé à la **fin du XXème siècle**, le cyberespace repose sur des infrastructures interconnectées, contrôlées et utilisées par une **grande diversité d'acteurs** individuels et collectifs. D'abord conçu comme un espace de liberté, chacun peut y consulter, produire et diffuser de la connaissance. Pourtant, 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 leurs données personnelles des utilisateurs sont de moins en moins protégées. La maîtrise de ce nouvel espace virtuel constitue donc un enjeu politique et géopolitique majeur pour les États qui, victimes de **cybermenaces**, mettent en place des **politiques de cyberdéfense de plus en plus 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 : ENJEU MAJEUR DU MONDE CONTEMPORAIN

A - Réseaux, infrastructures et territoires d'un espace immatériel complexe

➔ LECTURE DU TEXTE 1 p. 430 du MANUEL NATHAN + DÉFINITION DE TERRITOIRE *(cf. ci-dessous)* : **Le cyberespace est-il un « territoire » au sens classique du terme ?**

> Au sens large, le territoire est une portion d'espace appropriée (et non pas simplement l'espace). On peut distinguer trois éléments de définition : la domination (un pouvoir qui s'exerce sur elle), l'aire (dominée par ce contrôle territorial) et les limites qui la ceignent, qui font d'une portion d'espace un territoire.
>
> D'après l'article « Territoire », geoconfluences.ens-lyon.fr, octobre 2018

La **première représentation historique du cyberespace**, portée par les pionniers de l'Internet, le considère comme un territoire indépendant, c'est-à-dire une entité supranationale, « sans frontières », où les États ne possèdent aucune souveraineté pour y intervenir : à l'opposé du territoire classique.

À partir du milieu des années 2000, une seconde représentation du cyberespace, émanant cette fois-ci des **États,** le conçoit désormais comme un territoire à conquérir et à contrôler. Les États veulent y faire appliquer les lois afin de garantir leur sécurité et d'assurer leur défense. Pour les acteurs qui se battent pour se l'approprier, le contrôler, en défendre l'indépendance ou le « militariser », le cyberespace est donc largement **perçu et imaginé comme un territoire au sens classique du terme**.

➔ PROJECTION DE LA CARTE 2 p. 430 DU NATHAN + DOCS 1 ET 2 p. 382 MAGNARD : **Comment le cyberespace fonctionne et s'organise-t-il ? Quels territoires sont privilégiés par ses réseaux ?**

Le **CYBERESPACE** est un espace immatériel constitué à partir du **début des années 1990**. Il désigne l'ensemble des systèmes d'échange de données numériques, si massives qu'on parle de « big data » : chaque seconde, 29.000 Gigaoctets (Go) d'informations sont publiés dans le monde.

Concrètement, le cyberespace se présente comme un **ensemble de couches superposées** :

- MATERIEL : la première couche, l'infrastructure physique du réseau, est composée de **terminaux** (ordinateurs, smartphones...) **communiquant entre eux** et **avec des serveurs** (**DATA CENTER**) **par l'intermédiaire de câbles** (terrestres et sous-marins) **ou de satellites**, permettant permettent 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 ». Aujourd'hui, quelque 450 câbles, soit plus de 1,2 million de kilomètres, serpentent au fond des océans, jusqu'à 8 000 mètres de profondeur.
- LOGICIELS : La deuxième couche est l'infrastructure numérique qui comprend les **systèmes d'exploitation** *(Windows, Linux, macOS...)* et les **applications** assurant la transmission des données numériques par petits paquets, entre l'émetteur et le destinataire.
- DONNÉES : La dernière couche est celle du contenu échangé entre utilisateurs *(informations, discussions, réseaux sociaux, etc.).*

➔ A l'échelle mondiale, les **territoires accueillant les grands DATA CENTER** de la planète sont les mieux desservis par le réseau matériel du cyberespace (entre Amérique du Nord, Europe occidentale et Asie de l'Est). APPORT - *À l'échelle locale, les métropoles sont les hubs numériques.*

(H2) B - Les acteurs du cyberespace

➔ **Quels sont les acteurs du cyberespace ? Quels types de relations entretiennent-ils ?**

De multiples acteurs, **individuels et collectifs, coopèrent et s'affrontent** dans le cyberespace :

- les particuliers (internautes) qui l'utilisent, y trouvent et y échangent des informations
- des entreprises dont des firmes transnationales (DOC. 5 p. 383 MAGNARD), comme les **GAFAM** *(Google, Amazon, Facebook, Apple et Microsoft)* américaines ou les **BATX** *(Baidu, Alibaba, Tencent, Xiaomi)* chinoises, qui exercent une influence de plus en plus forte sur les contenus disponibles sur Internet : **fournissent les infrastructures logicielles et matérielles** *(possèdent la majorité des DATA CENTERS, déploient et contrôlent désormais de plus en plus les réseaux de câbles sous-marins, etc.).* Ainsi les GAFAM assurent 90% des recherches planétaires sur internet.
- les acteurs publics, donc les États. Ils contrôlent une partie des infrastructures matérielles (les **satellites** sont majoritairement leur propriété : mais ils n'assurent que 1% des flux numériques). Parce que le cyberespace est intégré à un nombre croissant d'activités (militaires, politiques, économiques), les **États légifèrent pour protéger le transit de données** de toute manipulation *(par un autre État, par des activistes, etc.).* Les **États-Unis exercent une mainmise sur ce transit**, qui cause des tensions avec d'autres États (97% des données numériques échangées entre l'Europe et l'Asie passent par les États-Unis). D'autres États, comme la **Chine, visent le contrôle total des données** échangées par leurs citoyens : en censurant les informations, et en imposant leurs propres outils numériques *(moteur de recherche Baidu, etc.)* : cf. CARTE 6 p. 383 MAGNARD. Il s'agit dont pour les États de contrôler le cyberespace pour y assurer leur **SOUVERAINETÉ** et le respect du droit international.
- DOC. 5 p. 431 NATHAN - des acteurs malveillants animant les **« zones grises » du cyberespace** *(DARK WEB et DEEP WEB : portions du cyberespace 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, etc.),* poursuivant des objectifs variés *(rançonnage, révélations d'information privées...).* Mais aussi des **groupes terroristes** comme Daech qui recrutent et communiquent via messageries cryptées. Ou des **opposants politiques** utilisant internet comme lieu de protestation (ex : 2011 lors du Printemps arabe).

TENSIONS - Le cyberespace génère des **conflits à toutes les échelles**. À **l'échelle mondiale**, il reflète les tensions internationales. Ainsi la Russie est accusée par les États-Unis de manipulation de l'information, via des hackeurs (ingérence lors des campagnes présidentielles de 2016 et 2020, etc.). De même en mai 2019, pour la première fois de l'histoire, Israël a riposté à une attaque virtuelle par une frappe militaire contre Gaza. **À l'échelle locale**, **acteurs privés et citoyens s'opposent** : au nord de Paris des associations de riverains se sont structurées, critiquant les nuisances sonores et les risques d'explosion associés à la présence de la première concentration de data centers d'Europe.

PODCAST n° 1 JALON 1 : « La puissance des États-Unis dans le cyberespace : atouts et limites »
(Aidez-vous des documents du manuel qui vous donnent des premières pistes de réflexion : pages 448-449 / évoquez le leadership américain dans le cyberespace : maitrise des réseaux et des flux d'informations, géants du numérique, etc. / à partir de quelques exemples de scandales récents et de l'émergence de concurrents, montrez les limites de cette « domination ») ICANN GAFAM

DIFFUSION DU PODCAST REALISE PAR LES ELEVES (fiche méthode sur le site) + REPRISE PAR L'ENSEIGNANT (cf. document mis en ligne dans le « coffre » à la fin de l'axe).

DOCUMENT A ANALYSER (EN FONCTION DU TEMPS) : Texte 1 p. 448 : pourquoi la domination américaine a longtemps entravé-t-elle la possibilité d'une gouvernance collective d'internet ?

(H3) C - Liberté ou contrôle des données ?

LIBERTÉ… - A ses débuts, internet a été appréhendé par ses premiers utilisateurs privés comme un **espace de liberté absolue pour échapper à la souveraineté** et au contrôle des États : c'est le sens de la « Déclaration d'indépendance du cyberespace » rédigée en **1996** par **John Perry Barlow**, qui consacre la liberté d'expression comme principe fondateur (DOC. 1 p. 384 MAGNARD). Le principe de l'**OPEN DATA** matérialise cette vision du cyberespace (« donnée ouverte » : données numériques dont l'accès, l'usage et le partage sont laissés libres aux usagers, sans conditions). Cette philosophie des données ouvertes, défendue d'abord dans les pays anglo-saxons et en France, préconise une libre disponibilité des données pour tous, sans restriction de copyright, de brevets ou d'autres mécanismes de contrôle, favorisant la libre circulation du savoir pour **mettre en œuvre une société planétaire de la connaissance**. Cet idéal presque utopique est également défendu par diverses **organisations militantes** qui agissent parfois aux frontières de la légalité (*Anonymous*), des **hacktivistes** qui piratent les sites gouvernementaux ou d'entreprises privées pour rendre leurs donnés publiques. *L'association Wikileaks fondée en **2006** par Julian Assange défend ainsi cette vision d'un cyberespace libre. Depuis 2010, elle a publié sur son site internet des millions de documents relatifs à des scandales de corruption, d'espionnage et de violations des droits de l'homme concernant des dizaines de pays.*

… OU CONTRÔLE ? Le cyberespace est l'objet **d'une surveillance de plus en plus étroite** de la part d'acteurs privés comme publics :

- le contrôle des données représente un **enjeu économique** essentiel pour les **géants du web** : ils permettent l'usage quotidien d'Internet et, dans le même temps, stockent, contrôlent et échangent les données de leurs utilisateurs à des fins commerciales. Ces géants *(réseaux sociaux, moteurs de recherche, fournisseurs d'accès, etc.)* savent tout de leurs clients : ceux-ci **perdent le contrôle de leur vie privée** dès lors qu'ils acceptent leurs « conditions générales d'utilisation ». Cela suscite régulièrement des **oppositions de la part d'utilisateurs**, mais aussi **d'acteurs étatiques** *(en 2020, l'UE a mis fin à l'accord « Privaty Shield » : elle veut ainsi interdire à Facebook de transférer les données des utilisateurs européens vers les États-Unis).* Dans le même temps, les **entreprises cherchent à protéger leurs propres données** *(en 2014, Domino's Pizza a refusé de payer une rançon de 30 000€ demandée par des hackers : les données d'environ 650.000 clients français ont alors été rendues publiques).*

- CARTE MAGNARD 4 p. 385 les **États cherchent** également **à exercer leur contrôle sur le cyberespace** qu'ils considèrent comme un territoire sur lequel ils entendent exercer leur souveraineté. Pour garantir cette souveraineté, ils **sécurisent leurs réseaux** *(les États-Unis envisagent de sécuriser leurs câbles sous-marins en déployant des barrières soniques)* et **les surveillent via leurs services de renseignement** *(doc. 3 p. 451 HATIER)* pour lutter contre les groupes terroristes. Certains États comme la Chine, l'Iran ou la Russie **cherchent à contrôler les données de leurs citoyens** : ici la **CYBERCENSURE** (surveillance et limitation des contenus internet entravant la liberté d'expression) contribue à la mise en place de **sociétés de la surveillance**. Ainsi le Soudan a créé en 2011 la "Cyber Jihadists Unit" destinée à infiltrer réseaux sociaux et applications (WhatsApp) pour faire taire l'opposition.

PODCAST n° 2 JALON 1 : « Des données personnelles menacées ? Les exemples de l'affaire Cambridge Analytica et du cyberespace chinois » *(Aidez-vous des documents du manuel qui vous donnent des premières pistes de réflexion : pages 450-451 / votre travail ne doit pas être un simple compte-rendu : il s'agit, dans les deux cas, de réfléchir aux conséquences des menaces qui pèsent sur la liberté des données dans le cyberespace, mais aussi de se demander comment le contrôle des données est justifié, tant par les entreprises que par des États)* **GREAT FIREWALL** **BATX**

DIFFUSION DU PODCAST REALISE PAR LES ELEVES (fiche méthode sur le site) + REPRISE PAR L'ENSEIGNANT (cf. document mis en ligne dans le « coffre » à la fin de l'axe) / DOC. 2 p. 450

(H4) II/ ORGANISER LA CYBERDÉFENSE : LE CAS FRANÇAIS

A - La cyberdéfense, un enjeu de défense nationale

En matière de **CYBERDÉFENSE** (ensemble des moyens permettant à un État d'assurer la cybersécurité des systèmes d'information vitaux), stratégies défensives et offensives se complètent :

- **en amont**, les États développent des techniques destinées à protéger les données et sécuriser les accès aux comptes sensibles, ou dans l'expertise des logiciels malveillants.

- **en aval**, de nombreux pays développent des stratégies de riposte *(en utilisant « l'arme cyber », mais aussi par des moyens armés conventionnels, comme Israël en 2019).*

MENACES - La France est confrontée, comme tous les États, à des **cybermenaces émanant d'ennemis multiforme** : puissances étrangères cherchant à interférer dans la vie politique intérieure, comme la Russie régulièrement accusée de pratiquer le ***HACKING*** (ensemble d'actions et de techniques visant à « casser » les systèmes de cybersécurité) d'État pour déstabiliser les démocraties occidentales), mais aussi cybercriminels, ou encore groupes d'hacktivistes. En **2017**, on a relevé **700 alertes** dont **100 attaques** qui ont ciblé les **réseaux du ministère de la Défense**.

STRATÉGIE - Pour faire face, la France s'est dotée dès **2015** d'une **stratégie nationale pour la sécurité du numérique** (DOC. 2 p. 452), pour garantir la souveraineté nationale française dans le cyberespace. En **2019,** une **doctrine officielle** de « Lutte informatique offensive » (LIO) a été définie (DOC. 2 p. 432 NATHAN) : 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 (MAGNARD 3 p. 386).

ORGANISATION (DOC. 4 p. 387 MAGNARD) - Divers acteurs contribuent au dispositif français :

- **l'Agence nationale de la sécurité des systèmes d'information** (ANSSI), créée en **2009**, est l'autorité nationale en matière de LID (Lutte informatique défensive). Dépendant du 1er ministre, elle 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.

- Le **ministère des Armées** assure la protection de ses réseaux numériques et se charge, avec la **DGSE**, du **combat numérique (LIO)**. Pour renforcer cette composante de l'armée française, un commandement de cyberdéfense (COMCYBER) est créé en **2017**. L'armée française devrait compter plus de 4.000 cyber combattants en 2025 (budget de 1.6 milliard d'euros sur 2019-2025).

- Pour renforcer ses capacités opérationnelles, l'armée française s'est dotée en **2016** d'une **Réserve citoyenne de cyberdéfense (RCC)**. Composée d'un réseau de volontaires organisé en unités militaires réparties sur l'ensemble du territoire, elle a vocation à intervenir pour fournir l'expertise de ses 4.400 membres en cas de cyberattaque.

PODCAST n° 3 JALON 2 : « La cyberdéfense française à travers deux exemples : la réaction à la cyberattaque contre TV5 monde (2015), et l'exercice #DEFNET » *(Ne présentez pas le fonctionnement général de la cyberdéfense française : concentrez-vous sur les 2 exemples cités, en vous interrogeant à chaque fois sur les acteurs et les moyens mis en œuvre. Appuyez-vous, en 2nde partie, sur le contenu concret d'une édition DEFNET de votre choix, et récente. Que nous apprennent ces exemples de la « cyberdéfense à la française » ?)* **ANSSI COMCYBER**

DIFFUSION DU PODCAST REALISE PAR LES ELEVES (fiche méthode sur le site) + REPRISE PAR L'ENSEIGNANT (cf. document mis en ligne dans le « coffre » à la fin de l'axe) / DOC. 2 p. 456 HATIER

ALLER PLUS LOIN - France TV, « La Cyberdéfense française » (6')

(H5)

B - La France dans la coopération internationale de cyberdéfense

DANS LE MONDE - Une **cyberdéfense** efficace à l'échelle mondiale est **complexe** à mettre en place : le droit international est limité. Le Conseil de sécurité de **l'ONU reconnait aux États** victimes de cyberattaques **le droit de répliquer** uniquement si la cyberattaque a eu lieu dans un conflit armé « classique ». De plus, il est très **difficile d'établir précisément l'identité d'un cyberagresseur**, de même que ses liens avec un donneur d'ordres étatique. ***EXEMPLE*** *: En 2016, 12 millions de tweets automatisés provenant de Russie ont été émis durant la campagne électorale américaine, mais le procureur américain n'a pas réussi à prouver la collusion entre le candidat Trump et la Russie.*

De **nombreux freins** se posent **à une gouvernance mondiale** du cyberspace : leadership américain, oppositions de plusieurs États (Russie, Chine, etc.). 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. En **2018**, « **l'Appel de Paris** pour la confiance et la cybersécurité dans le cyberespace » a reçu 73 signatures d'États, 358 signatures de FTN (Microsoft, Facebook, etc.), et a contribué à relancer le cycle de négociations des groupes d'experts de l'ONU à ce sujet, qui demeure freiné. 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 États membres, dont la France, via le « Centre d'excellence de cyberdéfense coopérative de l'OTAN » situé en Estonie).*

FRANCE ET EUROPE - DOC. 1 p. 432 NATHAN La France est intégrée aux politiques de coopération européenne de cyberdéfense. **L'Union européenne (UE)** a pour ambition de **coordonner l'action des États membres** en matière de cyberdéfense et de **favoriser les échanges** pour lutter contre les cybermenaces. L'UE se dote donc d'experts et d'organisations à l'échelle européenne pour répondre aux menaces qui pèsent sur elle *(EX : en 2019, l'entreprise européenne Airbus est victime d'une cyberattaque de ses sous-traitants, à des fins d'espionnage industriel)* :

➔ Créée en **2004**, l'**Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)** est chargée de mettre en œuvre cette politique de coopération. Son activité consiste principalement 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.

➔ Ce dispositif a été complété par l'adoption, en **2019**, du *Cybersecurity Act* destiné à parvenir à l'autonomie stratégique européenne en matière cyber. Il **renforce le mandat de l'ENISA** pour soutenir les États membres dans la lutte contre les cybermenaces, et établit un **cadre européen 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 critiques.

➔ Toutefois, **l'harmonisation des pratiques européennes est limitée** : l'UE ne dispose pas d'outil autonome, et la coordination des pratiques des États membres n'est pas totale (chaque État ayant à cœur de préserver sa souveraineté en matière de cybersécurité).

PODCAST n° 4 JALON 2 : « La cyberdéfense européenne à travers deux exemples : le « Projet SPARTA H2020 », et le Forum International de la Cybersécurité de Lille » *(Ne présentez pas le fonctionnement général de la cyberdéfense européenne : concentrez-vous sur les 2 exemples cités, en vous interrogeant sur les acteurs et les moyens mis en œuvre. Appuyez-vous en particulier sur deux éditions du Forum FIC de votre choix, plutôt récentes, dont l'édition 2020 : une ou plusieurs actions / partenariats mis en avant lors de ce forum, qui nous renseignent sur les réalisations et les limites de la « cyberdéfense européenne »)* **HORIZON 2020**

DIFFUSION DU PODCAST REALISE PAR LES ELEVES (fiche méthode sur le site) + REPRISE PAR L'ENSEIGNANT (cf. doc. mis en ligne dans le « coffre » à la fin de l'axe) / DOC. 3 p. 455 HACHETTE

CONCLUSION

Objet de toutes les utopies libertaires, 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.