Thème 6 – L'enjeu de la connaissance

Axe 3 conclusif – Le cyberespace : conflictualité et coopération entre les acteurs

I- Jalon 5 : Le cyberespace : un espace géopolitique entre réseaux et territoires

Comment (et à quelles échelles) les acteurs du cyberespace construisent leur puissance ou défendent leur souveraineté sur et avec Internet ? Dans quelle mesure le cyberespace abolit-il (ou réactualise) la notion de territoire ?

Définitions des termes du sujet :

- Le mot **cyberespace** est géopolitique car il est utilisé pour parler des enjeux de cyberdéfense, sinon, on parle tout simplement d'Internet ou de « numérique » (pour les enjeux sociétaux). Étymologiquement, ce mot exprime une dualité entre le pouvoir étatique territorial et la liberté absolue d'un réseau universel : le mot « cyber » vient du grec *kybernetes* qui veut dire « pilote, chef » et « espace » signifie « universel ». C'est ce qui commande l'universel. Le mot oppose donc deux idées : 1- un pouvoir politique étatique fort contrôlant un **territoire** national (délimité par des frontières). 2-un réseau universel, illimité et ubiquiste abolissant totalement les distances, réseau totalement libre et au-dessus des **territoires** qui sont dépassés.

L'étymologie se retrouve dans l'histoire récente du cyberespace : 1-Le mot est d'abord inventé pour parler de liberté, invention d'un auteur de science-fiction (William Gibson) en 1987 dans *Gravé sur Chrome*. En 1996, le poète John Perry Barlow rédige même la déclaration d'indépendance du cyberespace dans laquelle on a l'idée que cet espace ne doit avoir aucune limite (et surtout pas les lois des États).

2- Le mot tombe un peu en désuétude mais ressurgit au milieu des années 2000 dans le discours des États pour parler de menace et de danger pour les États. Les États reprennent le terme pour mettre en garde les populations contre les menaces informatiques : ils veulent développer la **cyberdéfense** pour reprendre le contrôle de leurs territoires respectifs en créant des **réseaux nationaux** pour retrouver leur **souveraineté numérique**.

- Les géographes définissent le cyberespace en 3 couches :
  - La couche matérielle des infrastructures du cyberespace (**2p382**) câbles océaniques et des serveurs ou datacenters (gérés par des entreprises privées) menant aux ordinateurs du monde entier.
  - La couche logicielle faite de l'adressage (une adresse d'un site est associée au serveur hébergeur) et de protocoles gérant les ordinateurs (adresses IP et algorithmes gérant le routage).
  - La couche des données ou le Data.

A) À l'échelle mondiale : un réseau dominé par les États-Unis : une cyber-puissance hégémonique

1) « Tous les chemins mènent aux États-Unis » : **vidéo 1 (de 3'23 à 5'42) câbles**
https://submarine-cable-map-2018.telegeography.com/

- Un réseau mondial de **câbles sous-marins** posés par des **acteurs privés**. Au total, environ 430 câbles font 32 fois le tour de la terre pour 1,2 million de km. Ils transportent 99 % de nos données et polarisent ou concentrent les flux de données sur un **axe**, sorte d'**autoroute principale circumterrestre** passant par certains **lieux** (détroits concentrant les câbles sous-marins, aiguillages entre réseaux ou routeurs, portes d'entrée et de sortie avec les territoires nationaux puis relais pris par des câbles terrestres nationaux) : ce **réseau favorise les États-Unis** pays le mieux relié aux deux autres pôles riches de la « Triade élargie ».

Certains pays ne sont reliés au réseau que par un seul (ou quelques) câble(s). Ils sont donc menacés de rupture de câble comme en 2015 pour l'Algérie privée d'internet pendant 1 semaine (3 cas possibles : tremblement de terre, passage d'un sous-marin nucléaire ou attaque de requin), cas des Tonga en 2019.

- Le transit généralisé des données par les États-Unis : classer avec **6p383** (1cm = 1 500 km) 3 trajets possibles d'un mail envoyé d'un ordi de Pékin à Paris. Quel trajet aura ce mail ? Pour la Chine, quel serait le meilleur trajet ? Pourquoi ?

La logique de la distance voudrait un passage par la Russie : trajet **le plus court** de Pékin à la Russie puis à Paris (7 cm x 1 500 = 10 500)

- **Vidéo 1 (de 9'48 à 10'11)** 2e trajet est par l'océan Indien (11 cm x 1 500 = 16 500 km). La **souveraineté numérique chinoise** voudrait que le mail passe par l'océan Indien car il passerait par un câble contrôlé par des firmes chinoises, le SeameWe5 qui a l'avantage d'éviter la Russie, tout comme le projet de futur câblage par l'Asie centrale.
- **Vidéo 1 (de 6'43 à 7'43)** Trajet par les États-Unis (8 cm x 3 000 km = 24 000 km) est **le plus long** mais **le plus rapide et le moins cher**. La rapidité technique veut que le trajet du mail passe par les États-Unis car les débits des câbles transitant par les États-Unis sont les plus élevés du monde. 97 % des flux Asie-Europe et **80 % des flux mondiaux transitent par les États-Unis** quoiqu'il arrive. Cela 1-permet ou a permis à la NSA d'espionner les données mondiales plus facilement et cela 2-oblige les pays du monde à stocker leurs données sur le territoire américain.

- Les autres moyens de domination des États-Unis sur le réseau :
  - La **gouvernance technique** contrôlée par les États-Unis : comme le premier réseau Internet (Arpanet) est né entre 1969 et 1972 aux États-Unis, l'adressage est contrôlé par l'**ICANN** (Internet corporation for assigned names and numbers) localisée à Los Angeles.
  - Les **GAFAM** (Google, Amazon, Facebook, Apple et Microsoft) détiennent la majorité des données versées gratuitement par les utilisateurs et stockent ces données dans leurs **datacenters** souvent installés aux États-Unis y stockent 1/3 des données numériques mondiales. Leurs profits sont énormes (les GAFAM détiennent 5 des 10 premières capitalisations boursières) et elles fixent parfois leurs sièges sociaux dans des paradis fiscaux pour échapper aux impôts.
  - Les **serveurs racines** ou **routeurs** (les aiguillages du cyberespace) sont aux États-Unis pour 10 des 13 mondiaux.

2) Une extra-territorialisation du droit américain : **vidéo 1 (7'43 et 9'25)**

a) Le renseignement états-unien sur le cyberespace :

- La NSA a mis sur écoute le monde de trois façons surtout depuis 2001 (avec le ***Patriot Act*** : il autorise la collecte collective de données dans les datacenters, où qu'ils soient localisés, par la NSA, sans demande préalable formulée à un juge). **Edward Snowden** révèle en 2013 l'existence d'un triple système d'espionnage du cyberespace basé sur :
  - **PRISM** permettait à la NSA de collecter dans des datacenters les données de citoyens américains et étrangers sans en avertir les victimes et surtout sans demande préalable faite à un juge.
  - **MUSCULAR** : un sous-marin nucléaire américain capable de se connecter à n'importe quel câble sous-marin dans le monde.
  - **FIVE EYES** : au début de la Guerre Froide, 4 pays alliés des États-Unis (Australie, Nouvelle-Zélande, Royaume-Uni et Canada) chargés de capter les données pour les États-Unis aux portes d'entrée de ces pays.
- Depuis 2013, l'espionnage américain du cyberespace s'est poursuivi :
  - Certes, le ***Freedom Act*** de 2015 oblige la NSA à demander une « lettre de sécurité nationale » pour « écouter » et « l'écoute » doit être individuelle.
  - Mais, en 2018, Trump fait voter le ***Cloud Act*** : on revient à la situation d'après 2001 car la collecte collective des données est à nouveau autorisée, sans aucune demande à faire à un juge et sans en avertir la victime.

b) Mais, tous les pays espionnent le cyberespace. Ex : en 2015, un navire océanographique russe, le Yantar est arrêté par la marine américaine car il stationne dans les eaux intérieures américaines au-dessus d'un câble sous-marin : la marine américaine découvre à bord du navire tout un matériel pour télécharger les données transitant par ce câble.

B) Défendre sa souveraineté numérique : l'apparition de réseaux nationaux

1) La défense de la souveraineté numérique européenne : légiférer pour protéger les données

Après l'**affaire Snowden** (2013), l'Union Européenne a voté en 2016 la **RGPD** (règlement général sur la protection des données) qui rentre en application en 2018. Elle crée un droit européen numérique contrant le droit américain. Toute entreprise qui collecte des données en Europe doit sécuriser ses données car elle en est responsable en cas de vol => elle doit pouvoir être jugée. Tout citoyen européen peut porter plainte pour vol de données (et il doit même pouvoir exiger qu'on lui efface ses données passées, c'est l'anonymat numérique).

2) La défense des souverainetés numériques chinoise et russe : construire un réseau national matériel sécurisé

Pour la Russie, le Brésil ou la Chine, Internet doit être une compétence régalienne des États : pour imposer cette conception, recours des BRICS à/au :

a) La **cybercensure** sur le territoire national :

- Le cas le plus extrême est celui de la Chine. La Chine a installé des points de contrôle à l'entrée des câbles sur son territoire 1-pour empêcher l'espionnage de la NSA et 2-pour filtrer les infos entrant sur son territoire : c'est donc un Intranet propre censuré. Cette « **grande muraille électronique** » repose aussi sur l'activité de **cyber-censeurs** et de « trolls civils » sous la responsabilité de l'**OI** : office de l'Information dépendant directement du PCC (Parti communiste chinois).
- Les dissidents politiques ont recours à des astuces pour contourner cette cybercensure comme un langage codé car le régime repère automatiquement certains mots-clés : 35 mai au lieu du 4 juin (1989, jour du massacre de la place Tian an men).

b) La construction de **câbles alternatifs** évitant le transit des données par les États-Unis :

- Cas du Brésil qui a construit un câble évitant les États-Unis et reliant directement Brésil et Portugal.
- Câble chinois **SeameWe5** construit par des firmes chinoises pour éviter un passage par le Pacifique donc par les États-Unis.
- Câble **Alba 1** entre Cuba et Venezuela, deux pays alliés et ennemis des États-Unis.

c) La **contrefaçon d'applications** américaines :

La Chine (comme la Russie avec le **Runet** : Vkontakte au lieu de Facebook et Yandex au lieu de Google) possède des applis nationales paramétrées par l'État chinois ce qui facilite la cyber-censure et empêche les GAFAM de s'implanter sur le territoire national (Youku à la place de Youtube, Weibo à la place de Google, Weixin à la place de WhatsApp, Baidu à la place de Twitter, Qzone à la place d'Amazon...).

d) Le **cloud souverain** : il s'agit, pour la Russie, de **relocaliser les datacenters** en 1-construisant des « **territoires disques durs** » dans des régions froides : construction de grands datacenters capables de stocker les données nationales (en Sibérie, là où le refroidissement des datacenters coûte moins cher) 2-légiférant (en 2016) pour imposer le stockage des données des citoyens russes dans des datacenters russes obligatoirement localisés en Russie.

C) Une prise de conscience globale des menaces géopolitiques inhérentes au cyberespace en attente d'une gouvernance mondiale multilatérale

1) Les menaces : « pirates et cyber-combattants du cyberespace »

a) **Cybercriminalité** et **hackers** :

- 3 techniques utilisées par les hackers (image fausse du « pirate à capuche » adolescent avec une **démarche frauduleuse** mais ce sont bien des adultes qui développent ces virus ou malwares ; ce sont bien des professionnels du crime au même titre que les vendeurs de drogue…) :
  - Attaque de la couche de données : 1-des logiciels cryptent à distance des fichiers et demandent une rançon pour débloquer ces fichiers. On parle de **rançongiciel** (car demande de rançon : la seule solution est d'avoir une sauvegarde saine parallèle et de réinstaller tout ; le paiement ne sert à rien, on ne retrouve quasiment jamais ses fichiers) ou **rançonware**. Une cyberattaque typique de la Corée du Nord. 2-L'**hameçonnage** ou **fishing** : un courriel envoyé à la victime imite celui d'une entreprise ou d'une administration pour obtenir des infos privées : 1,7 millions de logiciels d'hameçonnage créés tous les mois, à moitié venant des pays du **Golfe de Guinée** dont le **Nigeria** avec un taux de réussite d'1/3.
  - Attaque de la couche logicielle Windows : les **spywares** (ou logiciels espions) aussi appelés **chevaux de Troie**. Ils infectent des ordis en secret et volent des données sensibles (comme un numéro de carte bleue).
  - Cryptage pour éviter un contrôle policier sur la couche matérielle : c'est le **Dark Web** avec le logiciel **Tor** un logiciel de l'armée américaine capable de crypter les communications : par opposition au web clair, c'est une portion du web cachée avec des serveurs non-indexés, reliés ensembles par Tor qui connecte les ordinateurs à ces serveurs pour les rendre invisibles : il entoure le message de couches de cryptage comme un oignon a différentes couches protectrices d'où le terme d'**Onion web** et l'extension du dark web en .onion : cela brouille la territorialisation des ordinateurs et sert des intérêts mafieux (achats de drogue, d'armes...).
- Le coût de la cyber-criminalité : 400-600 milliards de dollars/an soit un montant supérieur aux profits liés au trafic de drogue. Au-delà du chiffre élevé, ce montant pose surtout la question du réinvestissement : comment ces criminels vont réinvestir cette somme pour rendre leurs attaques encore plus efficaces par la suite ?
- Pour l'instant, l'effet systémique sur les États reste faible car seuls des individus sont visés.

b) **Hacktivisme** :

Pour différencier l'hacker frauduleux du « pirate qui lutte pour une noble cause », on a créé le terme **hacktiviste** : c'est un hacker qui lutterait pour la bonne cause, la liberté… Ex : **Julian Assange**, un islandais, crée en 2006 **Wikileaks** et diffuse en 2010 une vidéo montrant une bavure de l'armée américaine en Irak (un hélicoptère de combat américain a mitraillé en Irak un groupe de journalistes ; la vidéo a été confiée au site par un lanceur d'alerte, un sous-officier américain choqué que ses supérieurs aient étouffé l'affaire). Ex : Les **Anonymous** ont publié en 2011 (au début du printemps arabe) le régime journalier du dictateur Ben Ali alors que la population tunisienne était pauvre et ne mangeait pas à sa faim, pour encourager puis entretenir la révolte.

c) **Cyberguerres** :

- Technique et avantages géopolitiques :
  - La technique actuelle de la cyberguerre étatique est celle des **zombies** : des ordinateurs commandés à distance par d'autres ordinateurs situés à l'étranger pour attaquer un pays ! Il s'agit pour un État de nuire à un autre État en prolongeant la guerre classique par une guerre menée sur le cyberespace : les pays qui lancent (et sont victimes) une cyberguerre sont les mêmes qui sont en guerre officielle ! La première attaque de ce genre date de 2007 : la Russie contre l'Estonie.
  - On retrouve les ennemis traditionnels mais le cyberespace a le gros avantage pour l'État attaquant de…
    1-rendre plus délicate l'attribution de l'attaque. On ne sait pas toujours qui attaque car les États se cachent derrière des hackers anonymes ; or, pour légitimer une **riposte**, en droit onusien, il faut d'abord prouver que l'attaquant est un **État** ce qui est impossible dans une majorité des cas. Ex : Incertitude sur l'attaquant en 2017, le virus **Wannacry** (a attaqué le ministère de la défense russe et des banques au Royaume-Uni) n'a pas été officiellement attribué à la Corée du Nord. On a accusé des hackers nord-coréens mais sans certitude => le cyberespace permet donc à un État, en se cachant derrière des hackers, d'attaquer secrètement un autre État en évitant toute riposte de sa part.
    2-diminuer les coûts de la guerre pour l'attaquant sans pour autant diminuer les destructions pour la cible visée : un pays peut attaquer un ennemi sur le cyberespace alors qu'il est déjà en guerre classique ce qui évite de mobiliser son armée classique sur deux fronts : la cyberguerre devient alors une solution alternative moins coûteuse qu'une guerre classique de plus à mener. Ex : en 2010, les États-Unis cyber-attaquent l'Iran ce qui leur évite de bombarder l'Iran quand leur armée est mobilisée à la fois en Afghanistan et en Irak.
- 4 types de victimes :
  - Les particuliers mais, comme dans la majorité des cas, les rançongiciels ne demandent même plus de paiement, on voit qu'on a basculé dans des cas de cyberattaques pour nuire à des Etats : il est étonnant de voir des hackers brillants ne pas demander de l'argent => on est bien dans des attaques à but géopolitique pour porter atteinte à des États.

- Les entreprises privées : les pertes ou les coûts pour les hackers sont maximisés. Ex : piratage de la messagerie du patron par exemple, ou des résultats des appels d'offre avant la décision, ou des plans d'une invention pourtant brevetée… ce qui permet de vendre ce secret au plus offrant : c'est un véritable **espionnage industriel** en réalité.
- Les États lors d'opérations de **cyberguerre** ou, plus simplement, ce qui est très courant, de **cybersabotage** : certaines « infrastructures critiques » peuvent être facilement attaquées mais elles sont très sensibles (l'énergie dont le nucléaire civil, transports, industrie…).
- Nos institutions démocratiques : en 2016 durant les élections (présidentielles américaines) on soupçonne une ingérence russe. Et, en 2018, scandale de la société de conseil britannique ***Cambridge Analytica*** qui a volé 86 millions de comptes Facebook pour favoriser des messages favorables à l'élection de Trump en 2016 et au Brexit en 2018. Dans ce cas précis, les résultats des élections et d'un référendum n'ont-ils pas été modifié par le cyberespace ?

- Les premières cyberguerres connues au début du XXI^{e} :
  - 2007 : la première cyberguerre de l'histoire de l'Humanité : les sites gouvernementaux d'**Estonie** sont attaqués par la Russie qui veut dénoncer le déplacement d'un monument (à Tallinn) construit en 1945 en l'honneur des soldats russes morts en Estonie durant la 2^{e} GM ce qui avait choqué la forte (25 % de la population) minorité russophone d'Estonie alors que cette ancienne République soviétique rentrait dans l'OTAN ! Pdt 3 semaines, médias et services publics estoniens sont indisponibles.
  - 2010 : la première cyberguerre qui entraîne des destructions matérielles : l'**Iran Stuxnet** (quand l'Iran développe un programme nucléaire) le pays est touché par une cyberattaque d'Israël et des États-Unis (car ils sont en guerre en Afghanistan et en Irak). L'option militaire du bombardement est donc écartée : les ordinateurs iraniens contrôlant les centrifugeuses permettant d'enrichir l'uranium sont infectés et les centrifugeuses s'autodétruisent.
  - 2014 : la Corée du Nord attaque les États-Unis après la sortie en ligne d'un film satirique sur Kim Jong Un de ***Sony Pictures***.
  - 2015 : la première fois qu'un groupe terroriste fait une cyberattaque (relayée par la Russie dans un second temps) : après les attentats à Paris, la France bombarde Daesh en Syrie => Daesh, relayé par la Russie en secret, réplique sur le cyberespace avec son « Unité d'or », un groupe de hackers islamistes qui attaque (sous le nom « ***cybercalifat*** ») des sites administratifs français et TV5 monde, qui ne sont plus accessibles durant une demi-journée.
  - 2019 : le Hamas, organisation terroriste palestinienne stationnée à Gaza attaque l'**Eurovision**, manifestation musicale à laquelle l'État d'Israël (en guerre contre le Hamas) participe : en représailles, l'aviation israélienne bombarde le bâtiment civil d'où est parti l'attaque => c'est la première cyberattaque qui entraîne indirectement des morts (à ce jour, aucune cyberattaque n'a entraîné informatiquement et directement des morts).

2) La multiplication des appels à une gouvernance mondiale du cyberespace : pour l'instant, sans suite

Il n'existe pas encore de gouvernance mondiale du cyberespace. Mais, tous les acteurs sont d'accord pour dire que c'est urgent de créer une institution mondiale favorisant la coopération entre États, firmes et société civile pour sécuriser le cyberespace.

a) Les acteurs privés font partie des tentatives de normalisation du cyberespace => en 2017, le patron de Microsoft a appelé à un « **Genève du numérique** ». Microsoft a aussi demandé à participer à l'Assemblée générale de l'ONU ainsi qu'à avoir une ambassade à New York et Bruxelles pour être proche de l'ONU et des institutions européennes.

b) Les États :

- L'**Appel de Paris** (fin 2018) de l'État français a été signé par beaucoup d'entreprises privées comme Microsoft et Facebook et par des dizaines de pays : il appelle à des « comportements responsables dans le cyberespace pour maintenir la confiance » entre acteurs (mais, c'est flou, pour une entreprise privée comme Facebook, c'est l'idée qu'elle ne doit pas se faire voler ses données en les protégeant, mais quel doit être le rôle des États ?).
- Les BRICS demandent une gouvernance géopolitique multilatérale du cyberespace, gouvernance attribuée à l'ONU par l'intermédiaire d'une branche géopolitiquement neutre de l'ONU, l'**UIT** (Union internationale des télécommunications). Derrière ce projet, on voit surtout l'objectif : il s'agit de supprimer la main mise états-unienne sur le cyberespace en confiant la gouvernance à une institution non américaine, ce que refusent évidemment les États-Unis.

c) L'ONU :

Un **GEIC** ou **groupe d'experts intergouvernementaux du cyberespace** a été créé par l'ONU en 2011 : il réfléchit sur une gouvernance politique du cyberespace et rend des rapports annuels (comme le GIEC pour le climat). En 2013, ce groupe reconnaît que le **droit international** s'applique aussi au cyberespace. Un acte de cyberguerre est donc bien un acte de guerre qui rend légitime la riposte si l'attaquant est identifié ! La **légitime défense** est en effet reconnue par la charte des Nations Unies (article 51).

II- Jalon 6 : La cyberdéfense, entre coopération européenne et souveraineté nationale, le cas français

Dans quelle mesure la France, à la pointe de la cyberdéfense en Europe, a initié la naissance d'une cyberdéfense européenne indépendante des États-Unis ?

A) La cyberdéfense française :

1- Institutions :

- L'État français finance :
    - L'**Agence nationale de la sécurité des systèmes d'information (ANSSI)** qui

1- fait de l'expertise : elle rend des rapports annuels préconisant de renforcer la sécurité dans telle ou telle entreprise privée ou dans telle ou telle administration.

2- lutte au quotidien pour protéger les systèmes stratégiques (l'énergie, les transports, les administrations comme le fisc…).

- Le **COMCYBER** ou **Commandement de la cyberdéfense** créé en 2017 protège 24h sur 24 les systèmes informatiques de l'armée et des troupes en opération (géolocalisation, drones, systèmes d'information des chars, des canons, des Rafales…).

- Au total, entre 3 000 et 4 000 cyber-combattants ont été formés dans une école spéciale à Vannes en Bretagne et travaillent aujourd'hui dans une des deux institutions publiques à Paris et en Bretagne.
- Le contexte est celui d'une montée en puissance des attaques : en France, une vingtaine d'attaques majeures par an. Pour répondre à l'essor du nombre d'attaques, le budget de la cyberdéfense a été augmenté. La dernière loi de programmation militaire (2019-2025) prévoit une augmentation très sensible du budget dédié à la cyberdéfense avec **1,6 milliard d'euros** avec un recrutement prévu de 1 000 cyber-combattants en plus sur la période.

2- Missions :

- Missions défensive et offensive :
    - L'ANSSI **protège** des entreprises privées (stratégiques, prioritairement, comme Dassault, Airbus, Safran… mais aussi toute entreprise lui demandant de l'aide) et l'administration. Elle peut conseiller et aider aussi des particuliers.
    - Elle peut aussi et, si besoin, avec le COMCYBER, **attaquer** (en cas de légitime défense seulement) un pays ennemi.

- Dans ses rapports, l'ANSSI insiste sur le fait que la cyberdéfense est humaine car elle repose sur une bonne formation des citoyens. Car, la plupart des cyberattaques proviennent d'une erreur humaine au départ. Donc, il faut être bien formé pour ne pas faire l'erreur qui va déclencher la cyberattaque. Le grand classique est le phishing : il faut voir que le mail est anormal et ne pas l'ouvrir. En cas d'ouverture, l'ANSSI regrette que la règle soit trop souvent le silence : l'employé a peur de dire que son ordinateur est infecté car peur des sanctions. Mais, plus on attend, plus le réseau entier est menacé. La parade est d'avoir une sauvegarde externe et de tout réinstaller !

Mais, il existe aussi des cas de « trahison » avec une clé USB apportée par un employé payé pour cela par une firme étrangère concurrente.
Ou, l'attaquant laisse volontairement traîner une clé USB en espérant qu'un employé la prenne et l'utilise sur le réseau interne.

B) Une coopération européenne embryonnaire :

1- La France, une cyber-puissance par la norme : la France possède une cyberdéfense très puissante à l'échelle européenne. Dans l'Union, aucun pays n'est à ce niveau de sécurité et la cybersécurité est financée par l'OTAN (une alliance militaire américaine) à Tallinn => la question d'une cyberdéfense européenne autonome est posée !

La France sert actuellement de modèle européen pour les autres pays avec la **Convention de Budapest** (2001) rédigée par le Conseil de l'Europe à l'initiative de la France. Ce texte est le premier en Europe à définir précisément ce qu'est la cybercriminalité : en 2019, il est signé par 63 pays dont les États-Unis et la Chine, mais pas la Russie. Ce texte harmonise à l'échelle mondiale les cybercrimes pour favoriser une lutte plus efficace contre ces délits. Il permet aussi de repérer aussi plus facilement les hackers car il crée une coopération entre les différentes cyberdéfenses du monde.

2- La France à l'origine d'une cyberdéfense européenne : à l'initiative de la France, l'Union Européenne a voté des textes créant un embryon de cyberdéfense européenne.

- En 2016, une directive européenne (la ***Network and information system Security***) oblige toutes les entreprises européennes stratégiques à sécuriser leurs systèmes informatiques. Les fournisseurs d'accès deviennent responsables de la sécurisation de leurs données sur le cloud.
- En 2019, sur le modèle de l'ANSSI, la loi (***Cybersecurity Act***) votée par le Parlement européen, crée l'**ENISA** ou *European network and information Security Agency* (Agence de l'Union Européenne chargée de la sécurité des réseaux et de l'information) première Agence de cyberdéfense en Europe.

C) Une souveraineté numérique française à renforcer :

1- Au niveau de la couche matérielle : l'éventualité d'un « noir numérique » donc de rupture du seul câble reliant le pays au reste du cyberespace est irréaliste car la France est reliée au reste du monde par 6 câbles. Par ailleurs, la France possède des géants dans l'installation et la construction des câbles comme **Orange Marine** et **Alcatel Submarine**. Notre pays est un des trois leaders mondiaux dans le secteur avec les Etats-Unis, la Chine et le Royaume-Uni.

2- Au niveau de la couche logicielle : notre pays est totalement dépendant de Microsoft et des autres GAFAM. Aucun traitement de texte national n'existe ce qui oblige les différents ministères à payer chaque année des licences à Microsoft pour utiliser Windows !

3- Au niveau de la couche des données : les tentatives de « **cloud national** » visant à rapatrier les données des Français sur notre territoire ont toutes échouées car les entreprises françaises financées par l'Etat ont toutes fait faillite : elles n'étaient pas compétitives face à Google et autres géants américains.

La solution sera peut-être de se reposer sur l'Allemagne : Deutsche Telekom a réussi à imposer à Google de stocker les données des Allemands en Allemagne.