**Corrigé DS n° 7 : Le cyberespace, conflictualité et coopération entre les acteurs**

Sujet de dissertation :

Le cyberespace, quelles réalités et quels défis ?

**Introduction :** Cyberespace ⇔ interconnexion des systèmes de données numériques (flux et stockage). Numérisation croissante de toutes sphères d'activités humaines (de la vie ordinaire aux transactions financières en passant par la dématérialisation des administrations et des consultations médicales) ⇔ centralité du cyberespace qui offre de nouvelles opportunités pour les individus, les firmes et les États mais aussi de nouvelles vulnérabilités. Cf scandale de Cambridge Analytica, une firme qui a exploité les données de Facebook pour influencer les comportements électoraux lors des élections présidentielles étatsuniennes et du référendum sur le Brexit en 2016.

***Pbmatique :*** Comment la numérisation croissante des sociétés et des économies engendre de nouveaux défis ?

## I) <u>Les réalités du cyberespace : un réseau global au cœur de la vie des individus, des firmes et des États</u>

a) **D'un projet militaire et scientifique à un réseau global et multiforme :** de 500 millions à 4,7 milliards d'internautes entre 2001 et 2015 / des activités de plus en diversifiées : e-commerce, transactions financières, objets connectés… ⇔ quintuplement du trafic des données entre 2017 et 2022 / rôle central des NTIC (Nouvelles Technologies de l'information et de la communication) dans les organisation productives ⇔ gestion des flux tendus de la DIPP

b) ***La prépondérance des EU dans les trois couches du cyberespace :*** couche matérielle ⇔ 10 des 13 serveurs racines, 43% des data centers, 45% de la pose de câbles sous-marins entre 2012 et 2017 par Te Subcom, firme américaine / couche logiciel et sémantique ⇔ domination des GAFAM (Google = 90% des recherches en ligne / 857 milliards de revenus annuels par les GAFAM)

c) ***Une nouvelle frontière du capitalisme :*** recul de la vision citoyenne, coopérative et gratuite du cyberespace, incarnée dans des projets comme les logiciels libres ou wikipedia au profit d'une vision mercantile / capitalisme de la surveillance ⇔ collecte et exploitation des données par les grandes firmes du numérique en proposant des services gratuit/ criminalisation des pratiques du hacking (piratage pour rendre accessible et disponible les informations) ⇔ protection des droits de propriété intellectuelle

## II) Les défis du cyberespace : des enjeux multiformes et contradictoires à l'origine de tensions et de rivalités

a) ***L'enjeu de la souveraineté numérique :*** Volonté de la part des États de contrôler les flux et les stockages de données pour plusieurs raisons : a) enjeu de puissance et de croissance économique (domination des firmes étatsuniennes) b) enjeu de sécurité (espionnage par les EU du réseau : affaire Snowden en 2013) / Russie : hébergement sur des data centers en Russie des données de ses citoyen·nes et création de Yandex pour concurrencer Google / Chine : soutien des BATX face aux GAFAM, pose de câbles sous-marins chinois, Greatfirewall pour censurer les données venant de l'extérieur / Vers une territorialisation du cyberespace

b) ***L'enjeu de la cybersécurité :*** Dépendance croissante aux réseaux numériques ⇔cible pour des acteurs étatiques ou non étatiques. Cyberattaque ⇔ moyen de déstabilisation comme la Russie avec l'Estonie en 2007 ou les EU avec l'Iran (vers stuxnet) ou moyen d'extorsion comme avec les rançongiciels type wannacry (groupes criminels ou Corée du Nord) / création d'une cybersécurité à l'échelle européenne avec le cybersecurity Act de 2019 (sanctions communes à tous les États membres contre auteur des cybermenaces + certification commune pour les normes de sécurité) et à l'échelle française comcyber (4000 cybercombattants) pour riposter à toute cyberattaque et utiliser arme numérique dans les conflits

c) ***L'enjeu d'une régulation internationale :*** Demande d'une protection de la vie privée ⇔ mise en place du RGPD par l'UE / besoin de restaurer la confiance après des scandales (facebook, cambridge analytica) ⇔ appel de Paris en 2018 par 230 acteurs du cyberespace (États, firmes, ONG) pour une régulation internationale / Mais refus de le signer de la part des EU pour qui le cyberespace relève d'un fonctionnement décentralisé et d'un réseau ouvert (refus des contraintes internationales comme dans le changement climatique ⇔ unilatéralisme) et de la Russie et de la Chine pour qui le cyberespace relève d'une gouvernance étatique.

**Conclusion :** Contrôle des flux et du stockage des données ⇔ facteur de puissance et de richesse pour les États et les firmes ⇔ multiplication des rivalités et des tensions ⇔ territorialisation et appropriation mercantile du cyberespace sous forme de compétition ⇔ question d'une gouvernance mondiale et d'une régulation par un droit international pour maintenir l'ouverture du réseau à l'échelle globale, sinon morcellement du cyberespace

.

# Thème 6 : L'enjeu de la connaissance

**Sujet d'étude critique de documents :**

En analysant le document suivant et en vous appuyant sur vos connaissances, vous montrerez pourquoi et comment la sécurité du cyberespace est devenue un enjeu majeur des relations internationales.

**Introduction :** Le cyberespace désigne l'interconnexion des systèmes de données numériques ainsi que le stockage et les flux de données qui en découlent. Il est devenu central dans le fonctionnement des économies, des entreprises, des Etats… et dans les vies ordinaires. L'article du *Monde* conçu en collaboration avec l'AFP (Agence France Presse) montre que cette numérisation croissante de l'ensemble des activités va de pair avec une vulnérabilité accrue car, en devenant un facteur de puissance et une source de richesse, le cyberespace suscite des actions de la part d'acteurs étatiques ou non étatiques pour s'approprier les données qui y circulent ou déstabiliser des adversaires. Aussi convient-il de comprendre la nature de ces cyberattaques et de ces cybermenaces

## I) <u>Le cyberespace : un espace créateur de nouvelles vulnérabilités</u>

a) ***La dépendance de toutes les sphères d'activité au réseau numérique global et aux GAFAM :*** place centrale du cyberespace et des GAFAM reflétée par l'impact de la cyberattaque à partir de l'exploitation de la faille chez Microsoft évoquée par l'article du Monde : « 30 000 organisations américaine » + grande diversité des activités : « des entreprises aux Etats-Unis par le passé, notamment dans le domaine de la recherche sur les maladies infectieuses, mais aussi des cabinets d'avocats, des universités, des entreprises de défense, des groupes de réflexion et des ONG. » ⇔ Quintuplement du trafic de données entre 2017 et 2022, de 500 000 internautes à 4,3 milliards aujourd'hui, GAFAM = 819 milliards de revenus par an

b) ***Des cyberattaques permanentes qui exploitent des failles nombreuses :*** Article du **Monde** fait le lien entre deux attaques majeures en quelques moins : Solarwinds et Microsoft ⇔ en France, 1 attaque majeure tous les trois jours / exploitation des failles dans des applications ordinaires pour contourner et infiltrer les systèmes de sécurité des entreprises et des administrations : ici Exchange de Microsoft, une messagerie utilisée aussi bien sur des ordinateurs privés que sur des ordinateurs professionnels.

## II) <u>Le cyberespace : acteurs et objectifs des cyberattaques</u>

***a) Des cybermenaces multiformes :*** Vol de données ⇔ nouvelle forme d'espionnage pour acquérir des connaissances et des technologies : « des pirates informatiques chinois tentaient de voler des recherches sur le Covid-19 » dans un objectif de compétition économique ou connaître

des secrets d'États comme dans le cas de l'affaire Solarwinds dans un objectif de rivalités entre puissances / vol de données ⇔ cybercriminalité : « groupes criminels » qui utilisent des rançongiciels comme Wannacry en 2017 (300 000 ordinateurs, 150 pays touchés) / Hacking aussi visant à rendre disponible des informations accessibles et disponibles aussi à toutes et à tous au nom d'une conception démocratique : wikileaks par exemple

b) ***Des acteurs variés :*** Article du **Monde** montre que cyberespace est devenu un théâtre des rivalités géopolitiques : EU accusent Chine et Russie, puissances émergentes concurrentes / Corée du Nord = cyberpuissance (soupçon d'avoir diffusé wannacry dans le but de se procurer des ressources pour financer son programme d'armement nucléaire) / EU également auteur de cyberattaques (stuxnet en 2013 pour détruire programme nucléaire iranien) et espionnage généralisé (affaire Snowden en 2013).

## III) <u>Le cyberespace : les difficultés de la cybersécurité et de la cyberdéfense</u>

a) ***Les défaillances et les insuffisances de la cybersécurité :*** « le directeur de Microsoft, Tom Burt, avait (…) averti. *« Appliquer rapidement les correctifs est la meilleure protection contre cette attaque. »* ⇔ actualisation permanente de la cybersécurité par tous les usagèr.es nécessaires car les groupes de cyberattaquants sont des « acteurs hautement qualifiés et sophistiqués », à la recherche systématique des failles dans les logiciels qui font l'objet de modification régulière. Dans l'UE, mise en œuvre d'une certification par l'ENISA (Agence de cybersécurité européenne) pour qu'il y ait adoption de normes communes de sécurité de l'ensemble des acteurs.

b) ***La cyberguerre, une guerre des ombres :*** Difficulté à identifier les auteurs des cybermenaces et des cyberattaques ⇔ cf Solarwinds imputé à la Russie ou à la Chine par les EU ! / Groupe de hackers comme Hafnium ⇔ corsaires opérant pour des entreprises ou un gouvernement mais lien difficile à établir / opérations menées de l'extérieur des frontières ⇔ en dehors des juridictions d'où difficulté pour les appréhender car implique coopérations entre les États / Développement de doctrines de cyberdéfense ⇔ droit revendiqué par les États de répliquer par des cyberattaques ⇔ cyberguerre

**Conclusion :** Cette article du **Monde** montre que la cybersécurité et la cyberdéfense sont devenus des enjeux majeurs pour les individus, les firmes et les États mais aussi des difficultés à les organiser en raison des spécificités du cyberespace, réseau global qui permet une activité déterritorialisée. Vecteur de puissance pour les EU, il les expose aussi à des nouvelles formes de vulnérabilités.