LE CYBERESPACE, UN OUTIL GÉOPOLITIQUE

Définition: *cyberespace:* espace d'information généré par l'interconnexion de systèmes d'information et de communication représenté d'une part par *l'internet* et d'autre part *un espace virtuel*

***Internet: une histoire américaine**

1° Aux origines

Années 60, une agence du Pentagone créée pour trouver *un système de communication capable de résister aux effets d'une attaque nucléaire*

1969 mise en place d ***arpanet***, 1980 Arpanet se divise en un réseau *militaire* et un réseau *universitaire*, 1984 4 millions de *noeuds interconnectés* reliés à plus de 1000 ordinateurs dans le monde

2° Mainmise américaine

Les Etats Unis contrôlent majorité des serveurs ,ont droit de regard sur l'attribution des adresses IP.

1998 relais donné à une société privée californienne: ***Internet Corporation for Assigned Names and Numbers*** **ICANN** coordonne le réseau internet mondial

Début 2000 contestation de cette hégémonie venant d'Europe et d'Asie mais refus US car c'est un enjeu géopolitique majeur afin d'exercer le leadership mondial sur le commerce de l'information privée

Apparition de la notion de ***smart power = puissance intelligente*** qui vise à créer des dépendances dans le domaine et la production de connaissances. **Suzanne Nossel** (1969/-) en est la créatrice, sera adoptée par **Hillary Clinton** (1947/-) secrétaire d'état de **B. Obama.** *Le smart power* permet le contrôle de la recherche scientifique,de l'éducation, de l'édition à l'échelle de la planète + toute l'économie numérique

***Cyberespace et souveraineté nationale**

1° Au début , un espace sans entrave

Affirmation que le cyberespace a sa propre souveraineté reposant sur une totale liberté cf **Elon Musk** et *twitter , les hackers* (white hat, black hat, grey hat) les *hacktivistes*

2° Pour les états, une souveraineté à conquérir

Années 2000, les états prennent conscience que le cyberespace est une menace pour leur sécurité nationale ,soumis à de fortes tensions géopolitiques. Les états ne peuvent faire appliquer leurs lois que si les plateformes sont sur leur territoire or *Google* est aux Etats Unis, *Weibo* en Chine et *RuNet* en Russie

Des règles de droit international ont été adoptées par l'ONU, le G20, le G7 mais non contraignantes

Problème majeur: surveillance de l'internet versus protection des libertés cf *le bras de fer Apple/FBI* en 2016 et 2019

3 souverainetés en compétition dans le cyberespace: face à la ***prédominance du cyber-power US***

d'une part le **RuNet** depuis 2000 repose sur une *stratégie informationnelle* et un *volet civilisationnel* associés à une cyberdéfense, une cybersécurité et un savoir faire exceptionnel dans le cyberespionnage

d'autre part **la grande muraille électronique chinoise** au service du nationalisme sous le contrôle du pouvoir, politique, développement de plateformes strictement chinoises(Baidu, Alibaba,Wechat, Weibo), contrôle strict de la cyberdissidence

Face à ces 3 approches, l'Europe peine à trouver sa place, milite pour la protection de la *donnée personnelle* en invalidant le *Privacy Shield* de 2016 entre UE et USA, nouvel accord en mars 2022 en cours de validation.....

***Quelques exemples concrets**

1°Les autoroutes de données stratégiques

450 cables sous marins assurent 98% du trafic web: "*levier stratégique pour asseoir sa puissance technologique"* car résultats d'un travail de haute technicité, d'enjeux financiers considérables. Problème majeur de sécurité (si coupure=casus belli) d'espionnage (cf révélations d' **Edward Snowden** en 2013)
Affrontement Chine/Etats Unis autour de la 5G et l'Intelligence Artificielle

2°Désinformation, rançongiciels

-*le phénomène TIK TOK :* sujet de contentieux géopolitique entre les Etats Unis et la Chine car la plateforme collecte sans aucune réglementation les données personnelles donc problème majeur de sécurité, diffuse des fake news pour manipuler les opinions et déstabiliser les démocraties
-*les rançongiciels:* cyberpiraterie sur 3 niveaux intrusion via les identités-développement de virus-exécution et rançon. Le groupe le plus important est basé en Russie disposerait de 14 milliards de fiches accessibles et donc à vendre à qui veut rançonner.Tout se joue entre la **Russie** et sa *troll factory (Internet Research Agency* IRA) les **Etats Unis** et son *United States Cyber Command* et la **Chine** avec *Wechat* et *Tiktok*

3°Cyberattaques et cyberconflits

-Prise de conscience des états que les outils informatiques font partie intégrante des conflits géopolitiques via les *malware: ex NotPetya* et *Stuxnet*
-Remise en cause par pays émergents, les régimes autoritaires de la position dominante des Etats Unis ,menace de concurrence des pouvoirs régaliens, crainte de ne pouvoir assurer la sécurité des territoires nationaux
-Cyberattaques mal identifiables, mal qualifiables entre simple virus et acte de guerre délibéré d'où la rédaction du ***manuel de Tallinn 2.0*** en 2012, revu en 2017 pour appliquer les régles du droit international aux cyberconflits
-L'exemple ukrainien: **Elon Musk** met à disposition les ***kits Starlink*** pour connecter civils et militaires dés la fin février 2022- **Microsoft** cyberprotecteur de l'Ukraine en signalant toutes les attaques des hackers russes, en transférant toutes les données gouvernementales ukrainiennes dans le cloud protégées par un *hyperscaler*
CSQ: les hyperscalers (microsoft, google, amazon) sont désormais des composantes géopolitiques intégrées comme telles par l'exécutif US et un puissant vecteur du smart power. Nécessité de délimiter qui est du côté défensif et du côté offensif dans ce nouveau type de conflit (*guerre hybride)*

Conclusion

-le cyberespace est un enjeu de rivalités de pouvoir entre états
-La suprématie étatsunienne, un des éléments de son smart power, provoque un rejet de la part d'un grand nombre d'états :occident contre le reste du monde
-2 visions s'affrontent celle des démocraties occidentales face à celle des états autoritaires
-Le cyberespace: nouveau territoire d'affrontement géopolitique avec l'apparition d'un nouveau type de guerre: ***la guerre hybride*** (ex ukrainien)

Bibliographie:

TH. Gomart*: guerres invisibles, nos prochains défis géopolitiques* Tallandier 2021
Collectif d'auteurs: *cyberdéfense: politique de l'espace numérique* Colin 2018
Y. Salamon :*cybersécurité et cyberdéfense, enjeux stratégiques* Ellipses 2020
M. Quemener/J. ferry : *cybercriminalité, le défi mondial* economica 2009
B. Boyer: *cyberstratégie, l'art de la guerre numérique* Nuvis 2012