

Thème 6 – Conclusion

LE CYBERESPACE ENTRE TENSIONS ET COOPERATIONS

Introduction.

Présentation du sujet.

Définition page 428 : c'est un espace immatériel, reposant sur des infrastructures matérielles, et dont l'influence géopolitique ne cesse de se renforcer.

Problématique.

Quels enjeux sont liés à son développement ?

Annonce du plan.

On peut les distinguer à des échelles différentes, mondiale dans la 1^{ère} partie, nationale et régionale dans la 2^e.

I. Son organisation. [Manuel pages 428 à 431, 434-435]

A) Ses fondements matériels.

1. Des infrastructures.

- Des réseaux.

Ils sont constitués par des éléments physiques interconnectés, permettant la circulation des données sur grandes distances.

Carte 2 page 430 *Question.* *Quels sont ces éléments ?*

Définition page 430 : data center.

- Leur rôle.

Ils sont les vecteurs des infrastructures immatérielles, fondements de l'économie mondialisée.

Leur indisponibilité ou leur destruction aurait des conséquences majeures.

https://www.francetvinfo.fr/sante/maladie/coronavirus/confinement-le-reseau-internet-en-surchauffe_3875165.html

2. Des acteurs variés.

- **Les Etats.**

Ils cherchent à garder le contrôle des informations.

Ils cherchent aussi à développer la **cybersécurité** : voir II.

Document page 428 : les EUA dominant.

- **Les FTN.**

Les grands acteurs économiques des réseaux sont très peu nombreux : **GAFAM** et **BATX**.

Voir **thème 4 du programme de 1^{ère}**.

- **Les acteurs illégaux.**

Il s'agit principalement :

- De groupes criminels.
- D'organisations terroristes.
- D'**hacktivites** : définition page 429.

Ils utilisent souvent l'univers parallèle du **Dark Web** ou **Deep Web** :

https://www.francetvinfo.fr/choix/video-dis-franceinfo-c-est-quoi-le-dark-web_2767665.html

Question : qu'est-ce qui les différencie ?

- **Les usagers.**

Ils aspirent à un accès libre aux réseaux, aux informations.

Mais n'est-ce pas une utopie ?

B) Ses enjeux.

1. Le contrôle des données.

- **Un enjeu politique.**

Texte 1 page 430 *Questions* *Quels acteurs s'opposent ?*
Quels sont les fondements de cette opposition ?

- **Un enjeu économique.**

Il est le résultat des actions des acteurs privés, dont l'intérêt est de contrôler les données à des fins commerciales.

- **Des tensions.**

Texte 4 page 431 *Question* *Quel risque est mis en évidence ?*
Quels acteurs s'opposent ?

Ces attaques peuvent être l'œuvre de criminels (**document 3 page 431**), mais aussi de groupes défendant les principes fondateurs d'Internet.

2. Vers des règles universelles ?

- **Leur utilité.**

Il n'existe pas de vraie législation, ce qui entretient les tensions.

Une coopération internationale permettrait de fixer une réglementation et de se donner les moyens de la faire appliquer.

- **Des résultats limités.**

Pour l'instant les intérêts nationaux l'emportent, sous la pression des EUA.

Il n'existe donc pas de gouvernance mondiale, malgré des appels en ce sens ces dernières années ; par exemple **l'appel de Paris** (2018) :

<https://www.youtube.com/watch?v=Z6003ff7Kn4>

Vidéo *Question.* *Quel est son objectif ?*

Conclusion.

L'absence de règles mondiales pousse donc à prendre des mesures à d'autres échelles.

II. La cyberdéfense française. [Manuel pages 426 à 429, 432 à 435]

A) Ses défis.

1. Répondre aux menaces.

- **Des formes variées.**

Les attaques sont de différentes natures : sabotages, espionnage, vols, subversion.

Exemple TV5 Monde en 2015 :

https://www.francetvinfo.fr/faits-divers/terrorisme/piratage-de-tv5-monde/piratage-de-tv5-monde-retour-sur-une-attaque-sans-precedent_872681.html

- **De multiples acteurs.**

Document 5 page 431 *Questions.* *Quels sont ces acteurs ?
Pourquoi leur identification est-elle difficile ?*

- **Des objectifs difficiles à cerner.**

Document 3 page 431 *Question.* *Que peut-on supposer des objectifs des différentes attaques ?*

Au total, des objectifs politiques, économiques, moraux ...

Il faut y ajouter les attaques matérielles (destruction de câbles...), dont le but est le sabotage.

2. Elaborer une stratégie.

- **Ses principes.**

Texte 2 page 432 *Question.* *Quel est l'acteur principal ?*
Quelle est la stratégie ?

- **Son organisation.**

En 2009, est fondée l'ANSSI : **définition page 428.**

Elle est chargée de la détection des menaces et de l'organisation d'une riposte proportionnée à l'attaque.

Le Ministère des Armées crée un Commandement de Cyberdéfense (**COMCYBER**) en 2017.

Le Ministère de L'Intérieur a créé un service spécialisé contre la cybercriminalité.

B) Ses actions.

1. Des échelles variées.

- **Du cadre national...**

Document 1 page 432 : les acteurs civils et militaires déjà définis entrent en action.

- **... Au cadre européen.**

Document 1 page 432 : ENISA (Agence Européenne de la Sécurité des Réseaux et de l'Information) créée en 2004.

Elle doit permettre une coordination entre états dans toutes les dimensions du problème.

La France milite aussi pour la création d'un droit international :

https://www.francetvinfo.fr/internet/reseaux-sociaux/facebook/internet-macron-ne-veut-pas-laisser-la-maitrise-totale-aux-gafam_3031917.html

2. Des résultats encore limités.

- **A l'échelle nationale.**

Les différents services agissent contre les menaces. Exemple de l'attaque contre TV5 Monde :

Document 5 page 433 *Question* *Comment ont-ils agi ?*
Quels en sont les résultats ?
Quelles sont les limites de ce document ?

La Loi de programmation militaire 2019-25 comprend des mesures spécifiques.

Définition page 428 *Question.* *Quelles sont les deux dimensions de la cyberdéfense ?*
Cyberdéfense. *Est-il facile de les distinguer ?*

- **A l'échelle européenne.**

Le **Cybersecurity Act (2019)** établit un cadre européen de certification de cybersécurité pour les produits et les infrastructures.

La coopération se développe : **photo 2 page 432.**

Conclusion.

Le développement de ces affrontements pose la question de l'équilibre entre liberté et protection, entre une société de la connaissance et une société de la surveillance.

Conclusion.

Reprise.

Les deux réalités abordées révèlent les contradictions et les tensions existant dans le cyberspace.

Réponse à la problématique.

Il est autant un espace de coopération que d'affrontements.

Ouverture.

Au total, il semble que la tendance est au renforcement du contrôle des citoyens par les états, les entreprises...

Complément. Les effets contradictoires du développement du **BIG DATA** :

https://www.podcastjournal.net/Les-enjeux-de-la-data-informatique_a25369.html