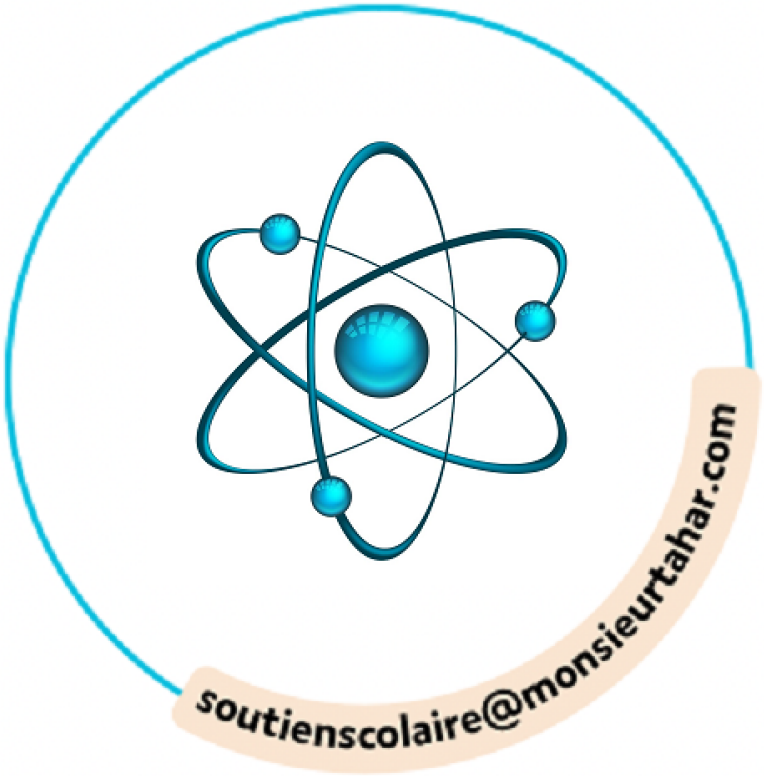
THEME 6



AXE 3

Le cyberespace: conflictualités et coopération

Cours

Le cyberespace : conflictualité et coopération entre les acteurs

Dans quelle mesure le cyberespace est-il un nouvel enjeu de puissance pour différents acteurs publics et privés ?

VOCABULAIRE

ANSSI (Agence nationale de la sécurité des systèmes d'information) : agence créée en 2009, dans le but de mettre en place la politique de cyberdéfense de la France.

BATX : géants du Net chinois.

Darknet : voir p. 450.

GAFAM-NATU : géants américians du Net et de la nouvelle économie. Google, Apple, Facebook, Amazon, Microsoft et Netflix, Airbnb, Telsa, Uber.

***Phishing* ou hameçonnage :** technique utilisée par des fraudeurs pour obtenir des renseignements personnels via Internet dans le but de perpétrer une usurpation d'identité.

Souveraineté numérique : le fait pour un État de pouvoir contrôler la sécurité de ses réseaux numériques et de pouvoir les utiliser à des fins de puissance.

A Le cyberespace : des infrastructures et des acteurs diversifiés

1. Une emprise croissante sur le monde

- Le cyberespace s'est progressivement mis en place à partir des années 1990, au moment où Internet a été ouvert au grand public. La **multiplication du nombre d'internautes** et le développement des nouvelles technologies de l'information et de la communication (NTIC) ont ainsi démultiplié ses possibilités et son importance dans le monde.
- Les 450 **câbles sous-marins**, équipés en fibre optique, représentent aujourd'hui de véritables autoroutes de l'Internet mondial. Ce sont les **vecteurs physiques des flux d'information** mais ils présentent parfois des risques de coupures en cas de sabotage ou de catastrophe naturelle (tremblement de terre ou tsunami). Ils sont installés dans le sous-sol marin par des navires câbliers et ils nécessitent une maintenance régulière. Les grandes entreprises sont d'ailleurs à l'affût de ces marchés stratégiques.

2. Des acteurs qui se diversifient

- Les acteurs du cyberespace sont très diversifiés et leur hiérarchie est révélatrice des **enjeux de puissance**. On trouve ainsi les États qui cherchent à **défendre leur souveraineté**, à être présents dans ce nouvel espace géopolitique et qui s'opposent parfois.
- Les géants du net (**GAFAM**, **NATU**, **BATX**) sont également très présents et se livrent une **concurrence très rude** pour acquérir des parts de marché. Les autres entreprises, les organisations diverses et les citoyens font aussi figure d'acteurs du cyberespace puisqu'ils y interagissent et nécessitent une protection, notamment de leurs données.
- Parmi les citoyens, on peut citer aussi les hackers, ces activistes de l'Internet qui cherchent à tirer profit du cyberespace ou à défendre une cause. C'est le cas des Anonymous, groupe fondé vers 2003-2004, qui s'en prend notamment aux groupes terroristes (Daech) mais aussi à des sectes (Église de scientologie aux États-Unis) ou parfois même à des États.

« Une cyberattaque pourrait faire autant de dégâts qu'une attaque nucléaire. »

Jérémy Straub, chercheur américain en informatique

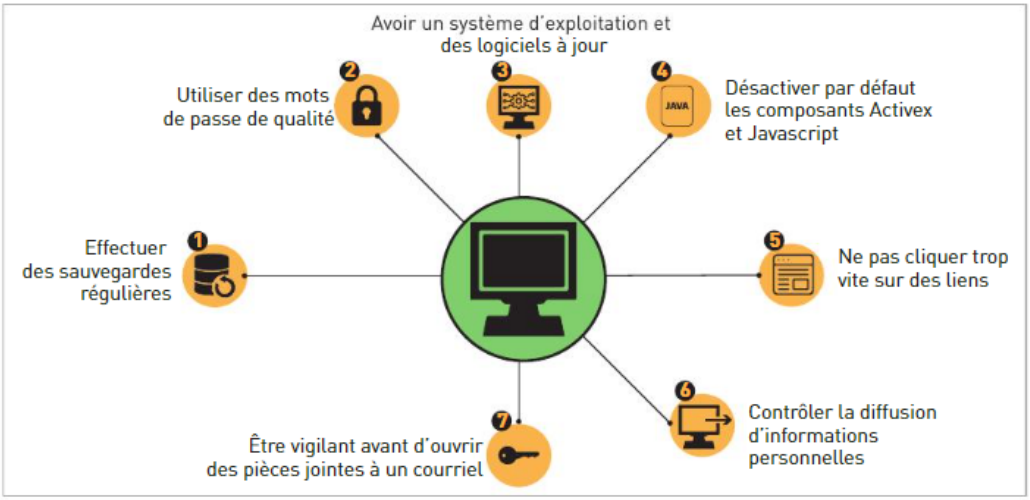
B Le cyberespace : des menaces croissantes

1. Liberté ou contrôle du cyberespace ? ▸ Jalon 1, p. 448

- La question de la liberté se pose sur le cyberespace. En 1996, suite à des lois américaines qui visaient à restreindre la liberté des citoyens sur un Internet encore naissant, John P. Barlow publie une **déclaration d'indépendance du cyberespace**, affirmant ainsi que les États ne pourraient jamais contrôler cet espace. Pourtant, face à l'absence de règles, il a fallu encadrer certaines pratiques. Les **darknets** posent ainsi problème puisque, dépourvus de tout contrôle, ils constituent de véritables opportunités pour des actions illégales et dangereuses dans le monde réel : achat de drogue, d'armes, vidéos pédopornographiques...

2. La multiplication des cyberattaques et leurs enjeux

- Les **cyberattaques ne cessent de se multiplier** contre divers acteurs du cyberespace. Il peut s'agir de l'envoi de rançongiciels qui exigent de l'argent pour débloquer des données, de logiciels espions ou de ***phishing*** (envoi de faux mails) pour voler des données, d'actes de sabotage contre des installations stratégiques (aéroports et gares, centrales nucléaires, sites militaires,...). En 2015, la chaîne TV5Monde a été attaquée par des pirates russes, se faisant passer pour des djihadistes, en réaction au refroidissement des relations entre la France et la Russie (annexion russe de la Crimée).
- Les **actes de malveillance** dans le cyberespace peuvent aussi contribuer à déstabiliser les démocraties. Lors des élections américaines de 2016, la boîte mail de la candidate démocrate Hillary Clinton a été piratée et une entreprise comme Facebook a largement participé, en vendant des données, à la victoire de Donald Trump.



Les bonnes pratiques en matière de cybersécurité

C La cybersécurité et la cyberdéfense : entre coopération et souveraineté nationale

1. À l'échelle internationale et régionale ▸ Jalon 2, p. 454

- Une **gouvernance mondiale** du cyberespace peine réellement à se mettre en place. Les institutions de l'ONU discutent régulièrement des enjeux liés au cyberespace et au renforcement de sa sécurité. Mais les États ne parviennent pas à se mettre d'accord. **L'Appel de Paris** pour la confiance et la sécurité dans le cyberespace, prononcé par le président français Emmanuel Macron en 2018 à l'UNESCO, témoigne d'une certaine volonté de collaboration à l'échelle mondiale.
- L'Union européenne tente, quant à elle, de coopérer afin d'apparaître comme un acteur important du cyberespace. En 2016, la **directive SRI** (Sécurité des réseaux et des systèmes d'information) est un tournant. Cette décision impose notamment aux acteurs fournissant des services essentiels et aux prestataires de services numériques de prendre des mesures de sécurité appropriées pour pouvoir résister à des attaques ou faire face à des problèmes divers. Elle insiste également sur la coopération nécessaire entre les autorités compétentes. Pourtant, cela reste difficile car les 27 pays de l'UE ne sont pas au même niveau de cyberprotection. En 2019, le **Conseil européen adopte un règlement sur la cybersécurité**.

CHIFFRES CLÉS

- **2018 :** 4,4 milliards d'internautes dans le monde.
- **400 à 600 milliards de dollars :** coût annuel des actes de malveillance dans le cyberespace.
- **2019 :** 67 % des entreprises françaises victimes de cyberattaques.
- **1,6 milliard d'euros :** montant débloqué dans la loi de programmation militaire 2019-2025 en France pour les cybersoldats.

2. À l'échelle nationale : l'exemple français

- La France cherche également à préserver sa **souveraineté numérique** et ses frontières dans le cyberespace. Alors que la cyberdéfense a été clairement mentionnée dans le Livre blanc pour la défense et la sécurité nationale de 2013, l'espace numérique constitue un domaine à part entière en matière de défense.
- La France s'appuie sur plusieurs organes : l'**ANSSI**, le commandement de la cyberdéfense, ainsi que 3000 **cybersoldats** (dont le nombre va augmenter à 4000 en vertu de la loi de programmation militaire 2019-2025).