Fiche

On doit le terme de « cyberespace » à l'écrivain américain William Gibson, qui l'utilise en 1984 dans son roman *Neuromancien*. *Le Petit Robert* décrit le « cyberespace » comme un « ensemble de données numérisées constituant un univers d'information et un milieu de communication ». Depuis l'avènement officiel d'Internet en 1983, le cyberespace a grandi et la masse de données qu'il transporte sature désormais notre environnement. Les années 1980 à 2000 ont assurément représenté un tournant majeur et complètement redéfini, pour les quatre milliards d'individus disposant d'un accès quotidien à Internet, le rapport à l'information. Elles ont, en conséquence, fait émerger de nouvelles problématiques géopolitiques, liées à l'apparition d'une nouvelle forme de territorialité virtuelle et transnationale et à la montée en puissance de nouveaux acteurs et de nouvelles formes de conflictualité et de coopération. Contrôler les données, protéger les institutions et les entreprises, surveiller les activités sur Internet deviennent autant d'enjeu de pouvoir des États qui rivalisent entre eux ou avec d'autres acteurs pour maîtriser le cyberespace.

I. Le cyberespace, vaste territoire virtuel et transnational

Le cyberespace s'appuie sur un **réseau physique de serveurs et de centres de données** reliés par des câbles terrestres ou sous-marins. Le contrôle de ces infrastructures physiques est de nos jours un **enjeu géopolitique majeur**. À un deuxième niveau, on trouve la couche logicielle qui forme le web. Le world wide web est un logiciel créé par l'ingénieur britannique Tim Berners-Lee au Centre européen de recherche nucléaire (CERN) en 1990 qui permet de consulter, à l'aide d'un navigateur, des pages hébergées sur des sites grâce à un système de liens hypertextes permettant de naviguer de page en page.
Le cyberespace est composé d'une **multitude de sous-réseaux** et de multiples éléments : sites, plates-formes audio ou vidéo, forums, blogs. Les réseaux sociaux sont aujourd'hui un élément primordial du cyberespace : Facebook compte plus de 2 milliards d'utilisateurs actifs et Instagram un milliard. On pourra ajouter à cela le **darkweb**, un ensemble de **réseaux parallèles** utilisant des outils **cryptographiques** pour permettre à leurs utilisateurs de bénéficier d'un anonymat complet. L'essor de **l'intelligence artificielle (IA)** ajoute encore une dimension au cyberespace, faisant cohabiter les internautes avec des robots.

Exercice n°1

II. Le cyberespace : enjeux économiques et géopolitiques

Le cyberespace constitue un espace transnational qui confronte les États à des problématiques juridiques complexes et invite à une forme de **gouvernance mondiale**. En 2019, parmi les **dix premières entreprises numériques au monde**, on ne comptait que des firmes américaines, sud coréenne ou chinoises : Apple, Microsoft et Samsung Electronics pour les trois premières. Cette situation pose la question de la souveraineté numérique des États. Ainsi, le fait que les premières structures physiques d'Internet aient été créées aux États-Unis confère à la première puissance mondiale un énorme avantage dans le domaine numérique. La Chine a, quant à elle, développé depuis 1999 son **grand pare-feu national** qui permet au gouvernement de contrôler l'accès des internautes chinois au réseau mondial. Pour combler son retard, l'Union européenne a lancé en 2014 le **projet Horizon 2020**, avec un budget de 80 milliards d'euros sur 7 ans.
Les États se trouvent désemparés face au développement de deux phénomènes, l'un massif et l'autre plus marginal, que sont les **réseaux sociaux** et le **darkweb**. L'importance des réseaux tels que Facebook dépasse aujourd'hui celle des médias traditionnels et peut représenter un danger pour les institutions démocratiques. Facebook a été ainsi accusé d'avoir influencé les élections présidentielles américaines en 2016 ou le vote du Brexit la même année. Quant au darkweb, composé de réseaux confidentiels et cryptés, il peut donner asile à des trafics illégaux, très difficiles à contrôler pour les États du fait de l'anonymat de ces réseaux et de leur caractère transnational qui pose un problème juridique. Ces réseaux servent aussi de base au développement d'une véritable **économie mondiale du piratage**. En **mai 2017**, une vague sans précédent de près de 80 000 cyberattaques simultanées a touché plus de cent pays et bloqué des institutions, des entreprises, des particuliers et même des hôpitaux. Face à cette recrudescence de la **cybercriminalité**, la **cybersécurité** est aujourd'hui un enjeu majeur et un secteur en plein développement.

Siège de Facebook, Menlo Park, Californie.

© JasonDoiy/iStock

Exercice n°2

Exercice n°3

Exercice n°4

Exercice n°5

III. La position de la France

Dans les années 1980, la France investit dans un réseau dont le terminal est nommé **Minitel** (Médium interactif par numérisation d'information téléphonique). Le Minitel connaît un succès important, mais il est finalement supplanté par Internet et cesse ses activités en 2012. La France continue à assurer largement sa présence sur le cyberespace et dans les domaines technologiques qui lui sont liés. Cela se traduit par des politiques économiques et des décisions politiques en faveur de la préservation de la souveraineté numérique. Selon Médiamétrie, la France comptait **52,6 millions d'internautes en août 2019, soit 83,9 % de la population**. Si la France ne dispose pas encore de géant du numérique capable de tenir tête à Google, elle tente de promouvoir ses propres outils, à l'instar de **Qwant**, le moteur de recherche garantissant à ses utilisateurs la protection de leurs données personnelles. Mais le chemin est encore long. Le moteur de recherche tricolore lancé en 2013 annonçait avoir dépassé les dix milliards de requêtes en 2017 quand Google revendiquait la même année 3,3 milliards de requêtes... par jour.

La France dispose cependant d'un **vivier technologique et industriel** dynamique : les start-up et entreprises innovantes françaises ont ainsi attiré, en 2019, **634 millions d'investissements étrangers**, permettant à la France de dépasser la Grande-Bretagne et Israël, et de se hisser dans le top 5 mondial des industries numériques les plus attractives. Elle fait aussi partie du top 5 des pays investissant le plus dans le domaine de l'IA, avec 665 millions d'euros financés par l'État en 2019. La France s'est dotée aussi d'une politique spécifique en termes de cybersécurité avec la création de l'**Agence nationale de sécurité des systèmes d'information (ANSSI)**, qui compte 600 employés, et le lancement en 2015 d'une Stratégie nationale pour la sécurité du numérique.

Cette stratégie prend place au sein de **l'ensemble européen** et s'accompagne de décisions qui ont des conséquences globales pour l'économie numérique. L'entrée en application du **règlement européen sur la protection des données (RGPD) le 25 juillet 2018**, forçant les GAFA – entre autres – à se conformer à une législation plus contraignante en matière de protection des données et de la vie privée sur Internet, a été largement soutenue par la France. De même que la **taxe GAFA**, voulue par le ministre de l'Économie Bruno Le Maire, adoptée par le Parlement en juillet 2019.

Zoom sur...

Se protéger contre le piratage informatique

En mai 2017, un virus malveillant nommé WannaCry infecte près de 300 000 ordinateurs dont il chiffre les données afin d'exiger une rançon pour les déchiffrer. Le virus se transmet très vite et infecte notamment les hôpitaux britanniques, l'entreprise Renault, la Deutsche Bahn ou le ministère de l'Intérieur russe. Il s'agit d'une attaque d'une très grande ampleur, qui met en lumière la vulnérabilité informatique de nombreuses organisations. Elle révèle aussi que la NSA, l'agence de renseignement et de cyberdéfense des États-Unis, avait repéré et conservé secrète, afin de l'exploiter, la faille de Windows dont profitait WannaCry.

Stuxnet, quand les États-Unis et Israël attaquent l'Iran

À partir de 2006, les États-Unis et Israël développent un ver informatique afin de ralentir le programme nucléaire iranien en infectant les installations du pays. Les deux pays n'ont pas reconnu la paternité de l'attaque, mais le niveau de complexité du ver est très élevé, et un général israélien a reconnu la paternité du ver en 2011. L'opération est une réussite, car elle a mis hors service près de mille centrifugeuses d'enrichissement d'uranium iraniennes. Elle révèle l'importance que l'arme informatique a prise dans les conflits géopolitiques.

Cyberattaques et riposte armée à Gaza

Les armes numériques peuvent être mobilisées par des individus relativement isolés et dépourvus de moyens, comme dans le cas des conflits asymétriques. Le 4 mai 2019, Israël a bombardé un immeuble de Gaza. Il s'agissait, d'après l'armée israélienne, d'une riposte à une attaque informatique menée par le Hamas et déjouée par les services israéliens. L'objectif était de détruire les infrastructures informatiques à l'origine de l'attaque. Il s'agit de la première fois qu'un État riposte par les armes à une cyberattaque, l'assimilant ainsi à une attaque classique.

La cybersurveillance et les révélations d'Édouard Snowden

En 2013, l'informaticien étatsunien Édouard Snowden, qui travaillait au service de la NSA, révèle depuis Hong-Kong que les États-Unis ont mis en place un système de surveillance généralisée à l'échelle mondiale, permettant la captation d'informations de masse, ainsi que la surveillance d'individus ou d'institutions. Aux États-Unis, Snowden encourt une peine de trente ans de prison pour espionnage. Il s'est réfugié en Russie, mais a sollicité l'asile dans différents pays, dont la France, qui ont pour l'instant refusé. La surveillance de masse est rendue possible par la présence des infrastructures physiques d'Internet aux États-Unis et par le travail d'informaticiens spécialisés au sein de la NSA ; elle constitue un outil politique majeur pour les États-Unis.

Le cyberespace et l'influence politique

En 2016, pendant sa campagne contre Hillary Clinton, Donald Trump a fait appel aux services d'une entreprise britannique, Cambridge Analytica, qui vend de l'analyse des données et des outils d'influence. Or, en 2018, Le *New York Times* et le *Guardian* ont révélé que l'entreprise avait collecté les données de 87 millions d'utilisateurs de Facebook sans leur consentement afin de manœuvrer leur opinion dans l'élection présidentielle. Le cyberespace apparaît ainsi comme un lieu de manipulation politique d'envergure, d'autant que l'accès aux données personnelles y est aisé.