CHAPITRE 18 - Le cyberespace : conflictualité et coopération entre les acteurs

Quel enjeu géopolitique le cyberespace constitue-t-il à l'échelle mondiale?

Cours : Le cyberespace : conflictualité et coopération entre les acteurs (p. 428-429)

Pourquoi le cyberespace est-il un enjeu de conflictualité et de coopération ??

I - Qu'est-ce que le cyberespace ?

A. Un espace immatériel complexe

Le cyberespace est un espace immatériel qui émerge au début des années 1990. Il désigne l'ensemble des systèmes d'échange de données numériques, devenues aujourd'hui si massives qu'on parle de « big data » ou « mégadonnées ». Il représente un espace sans frontière, anonyme, de liberté et de partage, ce qui le rend également difficilement contrôlable.

Le cyberespace se présente comme un ensemble de couches superposées. La première, l'infrastructure physique du réseau, est composée de terminaux (ordinateurs, smartphones…), serveurs, câbles ou satellites. La deuxième est l'infrastructure numérique qui comprend les systèmes d'exploitation (Windows, Linux, macOS…) et les applications assurant la transmission des données. La dernière est celle du contenu informationnel échangé entre utilisateurs.

B. Un espace animé par divers acteurs

De multiples acteurs coopèrent et s'affrontent dans le cyberespace. Aux côtés des particuliers, des entreprises (GAFAM) et des acteurs publics (États, collectivités), de nouveaux acteurs nés du numérique l'investissent. C'est le cas des hackeurs et des organisations « hacktivistes » (Anonymous, WikiLeaks) poursuivant des objectifs variés (profit, révélations d'information…).

Le cyberespace est au cœur d'enjeux marchands. Les entreprises externalisent chez des sous-traitants l'hébergement de leurs données. Les données personnelles privées peuvent être exploitées commercialement par les géants du numérique afin de mieux connaître l'identité et les habitudes de consommation des internautes.

II - Une source de conflits

A. Des menaces numériques variées

On distingue plusieurs types d'attaques numériques. L'hameçonnage vise à extorquer les coordonnées bancaires des personnes. L'espionnage consiste à s'introduire dans un système pour y dérober des données. Le sabotage a pour but d'empêcher un système de fonctionner. Au printemps 2007, la première cyberattaque de l'histoire paralyse l'ensemble du réseau informatique de l'Estonie. En 2017, le logiciel malveillant WannaCry prend en otage les données de centaines de milliers d'ordinateurs (ransomware). Enfin, les attaques peuvent être subversives comme lors de la tentative d'ingérence russe dans l'élection présidentielle américaine de 2016.

Le cyberespace génère des conflits à toutes les échelles. À l'échelle mondiale, il reflète les tensions internationales. La Russie est accusée par les États-Unis de manipulation de l'information, via des hackeurs. En mai 2019, pour la première fois de l'histoire, Israël riposte à une attaque virtuelle par une frappe militaire contre Gaza. À l'échelle locale, au nord de Paris, des associations de riverains se sont structurées, critiquant les nuisances sonores et les risques d'explosion associés à la première concentration de data centers d'Europe.

B. Le contrôle du cyberespace, nouvel enjeu géopolitique

Le contrôle du cyberespace devient une priorité stratégique pour les États. Les États autoritaires comme la Chine n'hésitent pas à filtrer les contenus et à bloquer l'accès aux sites. La coupure d'un câble sous-marin peut plonger un pays dans le noir numérique (Algérie en 2015). Le risque de paralysie (systèmes de transport, financiers…) incite les États à se mobiliser. Depuis 2009, la France dispose ainsi de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)et d'une force armée de cyberdéfense de 3 400 cyber-combattants.

Avec la multiplication des objets connectés, les systèmes de surveillance soulèvent des préoccupations en termes de liberté. Le lanceur d'alerte Edward Snowden a ainsi révélé en 2013 un vaste programme d'écoute des internautes par l'agence de sécurité étatsunienne (NSA) portant atteinte à la vie privée des citoyens.

III - Un enjeu de coopérations

A. Nul traité contraignant n’encadre le cyberespace

Deux tendances s’affrontent quant à la gouvernance du cyberespace. Les États-Unis sont partisans d’un Internet libre où acteurs privés (GAFAM) et société civile ont un rôle à jouer aux côtés des États. C’est ainsi une société à but non lucratif, l’Icann, qui est chargée du nommage et de l’adressage (.com, .fr, etc.) d’Internet. Au contraire, Chine et Russie défendent la souveraineté des États sur leurs réseaux.

Des actions sont mises en place au niveau international. Dès 1998, l’ONU adopte une résolution sur la cybersécurité et en 2001, la Convention de Budapest, signée par 63 pays, établit des règles communes permettant d’engager une action internationale contre la cybercriminalité. Depuis, des groupes d’experts gouvernementaux se réunissent sur le sujet, sans parvenir à s’accorder.

B. De la nécessité d’un dialogue mobilisant tous les acteurs

En réponse à ces échecs, des acteurs non étatiques s’impliquent. En 2017 est créée la Global Commission on the Stability of Cyberspace, un groupe international d’experts dont la mission est de renforcer la sécurité du cyberespace. En 2018, 30 acteurs du numérique, dont Microsoft, ont signé le Cybersecurity Tech Accord afin d’inciter les gouvernements à adopter les normes internationales nécessaires à la protection des citoyens dans le cyberespace.

Le cyberespace permet également de nouvelles formes de coopération. Ces initiatives s’inscrivent dans la mobilisation de la société civile associée au cyberespace. Réseaux sociaux (Facebook, Twitter), hashtag (#OccupyWallStreet, #MeToo) et plateformes de pétition contribuent à l’émergence d’une démocratie participative susceptible de peser sur les décisions de politique mondiale.

Jalon : Le cyberespace, entre réseaux et territoires (p. 430 - 431)

Doc 1 p. 430 : Le cyberespace est-il un territoire ?

[…] Historiquement, [la] représentation territoriale du cyberespace est développée par les pionniers de l'Internet dans les années 1990. Elle apparaît au moment de la naissance du web […] pour défendre l'idée d'un territoire indépendant ; un territoire que les États ne devraient pas réguler. […] Il faudra attendre le milieu des années 2000 pour assister à la remobilisation de cette représentation, cette fois dans une acception contradictoire. Elle est en effet fortement présente dans les discours des États qui doivent faire face à des attaques informatiques de plus en plus nombreuses et de plus en plus complexes et qui s'inquiètent de la possible remise en cause de leurs pouvoirs régaliens[1]. Ils mobilisent alors cette représentation pour légitimer des velléités d'action et pour mieux affirmer leur souveraineté dans le cyberespace, en cherchant à y remettre des frontières. […] La représentation d'un cyberespace comme territoire est ainsi mobilisée dans deux conceptions diamétralement opposées. D'une part, celle d'un territoire indépendant, sans frontières, qu'il faut préserver de tout contrôle et, d'autre part, pour les États, celle d'un territoire à conquérir et à contrôler, sur lequel il faut affirmer sa souveraineté, ses frontières et sa puissance.

Frédérick Douzet, Alix Desforges, Kevin Limonier, « Géopolitique du cyberespace : "territoire", frontières et conflits », CIST2014. Fronts et frontières des sciences du territoire, Collège international des sciences du territoire, 2014.

1. Pouvoirs attachés à la souveraineté étatique : défense, sécurité intérieure, justice, etc.

Doc 4 p. 431 : Une restriction des libertés à l'ère de la data surveillance ?

Ces dernières années, les évolutions techniques par le biais d'outils comme […] le GPS ou les smartphones ont ouvert un gigantesque champ pour les activités de surveillance. Mais elles ont également soulevé de nouvelles préoccupations en termes de vie privée. Avec la multiplication des objets référencés et des appareils mobiles géolocalisés, nos positions dans l'espace sont très fréquemment dévoilées, pointées et tracées.

[…]. Ces systèmes de surveillance suscitent de nombreuses inquiétudes pour divers observateurs, comme la Ligue des droits de l'Homme ou la CNIL (Commission nationale de l'informatique et des libertés), qui est chargée de réguler l'usage des nouvelles technologies. De fait, ces outils renforcent considérablement les capacités de contrôle social de l'administration sur ses administrés, en réduisant potentiellement le champ des libertés civiles.

Amaël Cattaruzza, Géopolitique des données numériques. Pouvoirs et conflits à l'heure du Big Data, Le Cavalier Bleu, 2019.

Jalon : La cyberdéfense française, entre coopération européenne et souveraineté nationale (p. 432-433)

Doc 2 p. 432 : La stratégie française de cyberdéfense militaire

En 2017, 700 incidents de sécurité, dont 100 attaques, ont ciblé les réseaux du ministère. En 2018, ce même nombre a été atteint dès septembre. En moyenne, ce sont donc plus de deux incidents par jour qui ont touché notre ministère, nos opérations, nos expertises techniques et même un hôpital des Armées. [...] Certaines sont le fruit de groupes malveillants, d'autres de hackers isolés, mais certaines viennent d'États pour le moins indiscrets, pour le moins... décomplexés. [...] La guerre cyber a commencé et la France doit être prête à y combattre. [...] En cas d'attaque cyber contre nos forces, nous nous réserverons le droit de riposter, dans le respect du droit, par les moyens et au moment de notre choix. Nous nous réserverons aussi, quel que soit l'assaillant, le droit de neutraliser les effets et les moyens numériques employés.

Extraits de la déclaration de Florence Parly, ministre des Armées, sur la stratégie cyber des armées, Paris, 18 janvier 2019.

Points de vue : Le cyberespace : une menace pour les libertés individuelles ? (p. 434 – 435)

Doc 1 p. 434 : Le cyberespace, un espace de liberté

Face à la guerre que se livrent les grands groupes de communication pour dominer la télévision, le cyberespace apparaît comme une échappatoire. La manne qui nous attend concerne, entre autres, les productions d'individus, d'organisations à but non lucratif et de petites entreprises ; la vaste couverture de l'information et des affaires publiques ; les œuvres passionnantes destinées aux enfants ; l'accès aux médias à un coût abordable pour les candidats aux élections et les artistes, qui peuvent s'y exprimer librement ; l'intérêt porté aux différentes communautés ; enfin, l'occasion sans précédent pour l'homme de la rue d'avoir son mot à dire. Cela semble trop beau pour être vrai. Pourtant, grâce à Internet et à ses développements futurs, tout reste dans le domaine du possible. […] Les individus peuvent contrôler ce qu'ils lisent, écoutent et regardent, et libérer une vague sans précédent de créativité et de discours vibrants. Sans plus se soucier de la pénurie des ondes ou du coût des publications imprimées à grande échelle, n'importe qui sera en mesure de diffuser la bonne parole en ligne, par le texte, le son ou l'image.

« Internet. Un espace de liberté à préserver », The Nation, 21 janvier 2005, reproduit dans Courrier International[en ligne].

Doc 4 p. 435 : Big data et libertés individuelles

Les tensions récurrentes qui opposent, ici, le FBI à Apple sur le libre accès aux communications[1], et là, la Commission européenne de Bruxelles à Google sur le stockage des données[2] et, de manière plus générale, les géants de l'Internet aux États sur la gestion du big data, conduisent à une fausse idée. Chaque camp argue qu'il agit ainsi afin de défendre les libertés individuelles. Un argument de pure façade tant il apparaît que jamais la protection du secret des consciences n'a été aussi menacée.

[…] La révolution induite par la circulation des données de communication et la numérisation des vies ont porté un coup sévère à cet espace qui restait jusqu'alors protégé. Un phénomène qui s'est aggravé avec l'irruption des nouveaux moyens de communication. Internet, avec les traces laissées par chaque connexion électronique, et les réseaux sociaux sont autant de béances dans l'univers personnel. […]

Cette évolution n'est pas seulement le fait d'autorités qui voudraient annihiler toute liberté individuelle. Elle résulte aussi des actions volontaires d'individus qui ne voient aucun obstacle à mettre sur la place publique leurs données personnelles. L'idée du « je n'ai rien à cacher », souvent avancée, étend plus encore la capacité des géants de l'Internet, pour des raisons commerciales, et des États, pour des raisons de sécurité, à accéder ainsi à nos pensées. Cette permissivité s'explique souvent parce que ces mêmes personnes associent Internet à la liberté, car c'est gratuit et pratique.

Jacques Follorou, « Lebig data, ce Big Brother qui ébranle les libertés individuelles », Le Monde.fr, 1er avril 2016 [en ligne].

1. Le FBI souhaite pouvoir déverrouiller les iPhones des individus impliqués dans des affaires judiciaires.

2. La Commission européenne reproche à Google une position commerciale dominante qui enfreint les règles de concurrence

Révisions : Le cyberespace : conflictualité et coopération entre les acteurs (p. 436)

SYNTHÈSE

I - Un espace immatériel

Le cyberespace est un espace immatériel complexe qui émerge au début des années 1990. Il désigne l'ensemble des systèmes numériques d'échange de données. Il se décompose en trois couches superposées : physique (câbles, serveurs…), numérique (systèmes d'exploitation et applications) et informationnelle. Perçu comme un espace de liberté, il est également difficilement contrôlable.

De multiples acteurs coopèrent et s'affrontent dans le cyberespace. Des acteurs traditionnels (individus, entreprises, acteurs publics) et de nouveaux acteurs nés du numérique (hackeurs, associations « hacktivistes ») l'investissent. Il est au cœur d'enjeux économiques et notamment de l'exploitation commerciale de nos données privées, notamment de la part des géants du numérique (GAFAM).

II - Une source de conflits

Le cyberespace fait l'objet de menaces numériques variées. Hameçonnage, espionnage, sabotage (ransomware comme WannaCry en 2017) et subversion (tentative d'ingérence russe dans l'élection présidentielle américaine de 2016) constituent les cyberattaques les plus courantes. Des conflits liés au cyberespace éclatent à petite et à grande échelles. Le cyberespace reflète les tensions internationales entre grandes puissances, notamment entre les États-Unis et la Russie, et génère des conflits d'aménagement à l'échelle locale (implantation de data centers à Plaine Commune au nord de Paris).

Le contrôle du cyberespace devient une priorité stratégique pour les États. Le risque de paralysie lié aux cyberattaques incite les États à se mobiliser. En France, la cyberdéfense est un enjeu partagé entre coopération européenne et souveraineté nationale (ANSSI). Certains lanceurs d'alerte comme Edward Snowden en 2013 dénoncent les dérives sécuritaires liées à la surveillance généralisée du cyberespace, susceptibles de restreindre les libertés individuelles.

III - Un enjeu de coopérations

Aucun traité contraignant n'encadre le cyberespace. États-Unis, Chine et Russie sont en désaccord sur la place que doit prendre l'État dans sa gouvernance. Des mesures sont adoptées au niveau international, via l'ONU et ses groupes d'experts ou le Conseil de l'Europe (Convention de Budapest contre la cybercriminalité), mais la coopération internationale pour réguler l'espace numérique est difficile à mettre en œuvre.

Les acteurs non étatiques s'invitent à la table des négociations. Entreprises privées (Microsoft), experts et société civile se mobilisent pour inciter les Etats à élaborer des lois permettant de garantir les libertés individuelles et la sécurité des utilisateurs d'Internet.