Thème n° ② – L'enjeu de la connaissance

Objet de travail conclusif – Le cyberespace : conflictualité et coopération entre les acteurs

🕐 DUREE INDICATIVE

7 heures environ

CE QUE DIT LE PROGRAMME

- Le cyberespace, entre réseaux et territoires (infrastructures, acteurs, liberté ou contrôle des données…)
- Cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français.

📖 OBJECTIFS

A la fin du cours, je dois être capable :

✍ **de définir et de maîtriser le sens** des notions suivantes : cyberespace, *data center*, *dark web*, *deep web*, souveraineté, *open data*, hacktiviste, *hacking*, cybercriminalité, logiciel malveillant, cyberdéfense.

✍ **d'expliquer** le fonctionnement du cyberespace et en quoi son développement participe à modifier les modalités de la diffusion de la connaissance.

✍ **d'expliquer** dans quelle mesure le cyberespace contribue à développer une société de la connaissance, mais aussi de la surveillance.

✍ **d'expliquer** comment la France assure sa cybersécurité et s'organise avec l'UE face à des cybermenaces protéiformes.

✍ **d'expliquer** en quoi le cyberespace constitue un enjeu de souveraineté nationale pour États, dont la France.

1. Le cyberespace, entre réseaux et territoires

1.1. Infrastructures et acteurs du cyberespace : un territoire sans frontières ?

🗎 **DOCUMENT 1 :** VIDEO – « Câbles sous-marins la guerre invisible » – Source : *Le Dessous des cartes*, Arte, le 14 avril 2018

🗎 **DOCUMENT 2 :** Les acteurs de la gouvernance du cyberespace

Avec le cyberespace, les outils de puissance ne sont plus seulement l'apanage des États. Ils le sont aussi d'acteurs non-étatiques. Effectivement, à la fois de très grandes entreprises technologiques comme les GAFAM aux États-Unis et les BATX en Chine, mais aussi des pirates informatiques, des groupes criminels, terroristes, des organisations mafieuses, etc., sont dorénavant inextricablement impliqués dans le cyberespace. De plus, ils entretiennent des relations très équivoques avec les États, entre concurrence et coopération, voire connivence. Beaucoup de pirates deviennent des « proxies », sortes de corsaires informatiques, au service d'États qui s'appuient sur leur expertise, mais qui, surtout, se servent de ces intermédiaires pour lancer des attaques sans que l'on puisse remonter jusqu'à eux. Cette implication des acteurs non-étatiques est l'un des enjeux majeurs du XXIe siècle : elle accentue le passage d'une violence internationale (interétatique) à une violence transnationale, où la conflictualité n'est plus l'affaire des seuls États-gladiateurs.

Charles THIBOUT, « Cyberespace : vers quelle gouvernance ? », www.iris-france.org, 16 novembre 2018.

🗎 **DOCUMENT 3 :** La censure en Chine

Rebel Pepper est un dessinateur de presse chinois installé aux États-Unis.
Radio Free Asia est une radio privée émettant depuis les États-Unis en neuf langues asiatiques.

Dessin de Rebel Pepper, *RFA*, 11 janvier 2018.
« Stage d'entraînement : Comment détruire la liberté d'expression ».

🗎 **DOCUMENT 4 :** Daech, maître du cyberespace

Le grand défi qui met la plupart des armées en déroute est la capacité de Daech à exploiter l'Internet et les réseaux sociaux pour pousser à la radicalisation des milliers de jeunes […] Le cyberespace offre à Daech une diffusion massive et planétaire. La technologie est largement accessible et à bas coût, les réseaux sociaux sont gratuits et immensément populaires parmi les jeunes dans le monde entier. Leurs activités sont transfrontières. Les jeunes Français utilisent massivement les réseaux sociaux et autres services du Web juridiquement basés aux États-Unis. […] Le cyberespace offre ainsi des zones de flou juridique qui permettent à Daech d'échapper aux forces de l'ordre. La France n'a en effet pas autorité sur les entreprises américaines. […] Daech exploite également les ressources technologiques du cyberespace pour échapper aux forces de l'ordre, comme les outils de chiffrement et d'anonymisation qui leur permettent de garder leur identité et le contenu de leurs échanges confidentiels. Ces outils permettent aux djihadistes de masquer leurs traces, il est impossible de savoir où ils sont, d'où ils communiquent et donc où frapper pour la défense.

Frédérick DOUZET, « Le cyberespace, troisième front de la lutte contre Daech », *Hérodote*, 2016.

🗎 **DOCUMENT 5 :** Géopolitique de la cyberguerre

Depuis 2007, les cyberattaques politiques se multiplient : virus Stuxnet en Iran en 2010, ingérence russe dans les élections américaines de 2016… En 2014, la Corée du Nord est accusée du piratage du studio de cinéma américain Sony, contraint d'annuler la sortie d'un film sur un complot fictif de la CIA pour assassiner le leader nord-coréen Kim Jong-Un. En 2015, TV5 Monde subit à son tour une attaque. En mai 2017, Wannacry fait 200 000 victimes dans 150 pays, paralysant le système de santé britannique, le ministère russe de l'Intérieur, des entreprises… En juin, le ver informatique[1] NotPetya exploite des failles de sécurité pour se propager sous la forme d'un ransomware. Cette nouvelle cyberattaque internationale touche des banques, des entreprises pétrolières et de transport. Aussi le cyberespace apparaît-il désormais comme un territoire sur lequel il faut faire respecter ses frontières, sa souveraineté et ses lois. Depuis quelques années, la prise de conscience par les États de l'enjeu géopolitique du cyberespace engendre une course aux cyberarmes. Vingt-six États possèdent une force de frappe cybernétique, les États-Unis, la Chine et la Russie en tête. […] Le cyberespace est indéniablement le siège de conflits. Il accroît, en les renouvelant, les menaces et modes d'actions hostiles. La capacité à participer à cette cyberguerre et à s'en prémunir est aujourd'hui une composante géopolitique majeure d'une stratégie de sécurité et de puissance pour un État.

Soline TOUSSAINT, « Le cyberespace : champ de bataille du XXIe siècle », Diplomates, 19 décembre 2017.

1. Logiciel malveillant qui se propage plus vite qu'un virus.

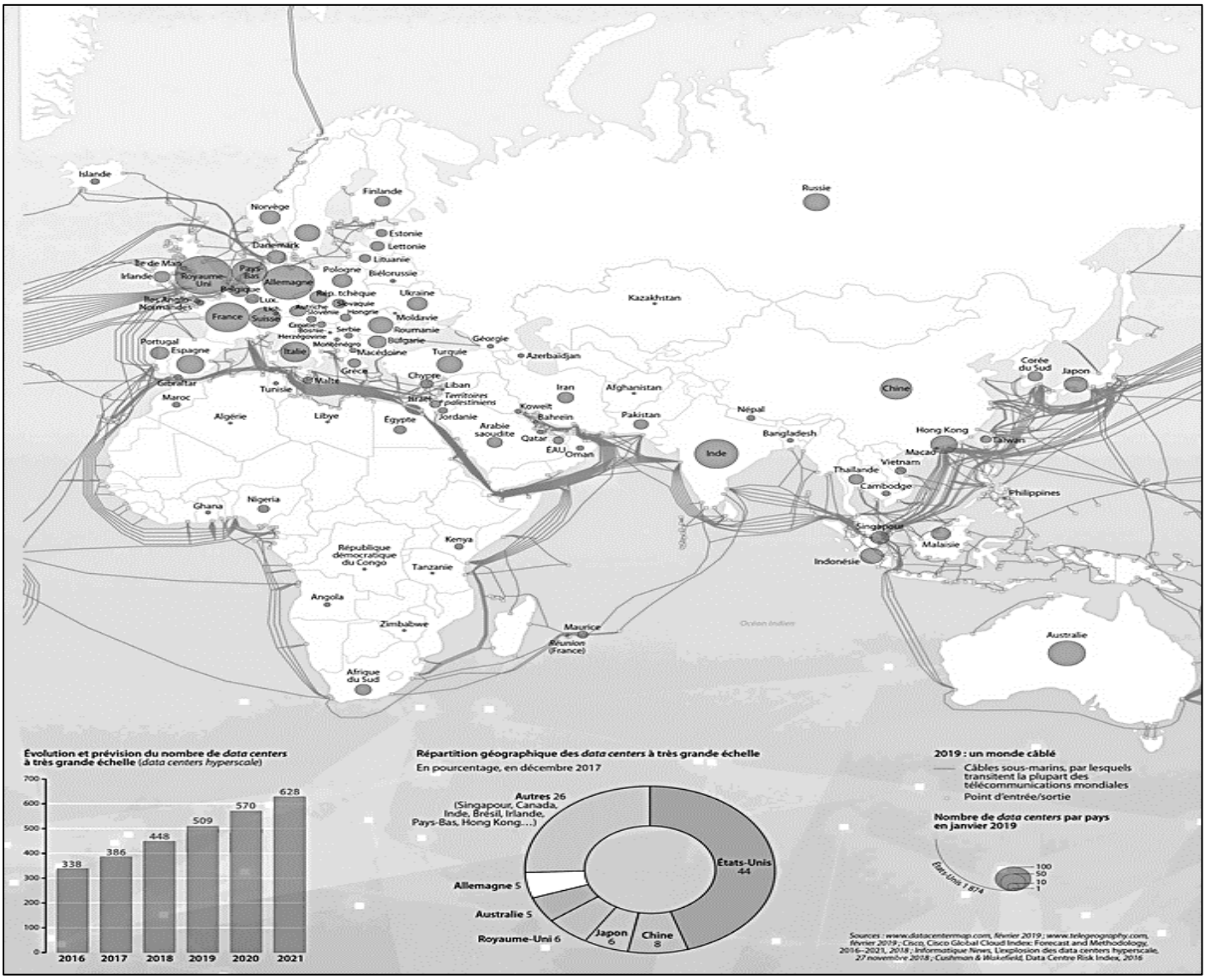
🗎 **DOCUMENT 6 :** Le cyberespace est-il un territoire ?

[...] 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.

🗎 **DOCUMENT 7 :** Réseaux de câbles sous-marins et *data centers*



✐ QUESTIONS

1. Comment circulent les données dans le cyberespace (**Documents 1 et 7**) ?
2. Pourquoi les câbles marins constituent-ils la « colonne vertébrale du web » ? Montrez que les sociétés sont devenues vulnérables face aux coupures du web. (**Documents 1 et 7**) ?
3. Montrez que le cyberespace échappe en partie au contrôle des États **(Documents 2, 4 et 5).**
4. Identifiez les types d'actions menées par les États pour maîtriser le cyberespace **(Documents 3, 5 et 6)**.
5. **POUR CONCLURE ①.** Montrez, **à partir de l'ensemble des documents**, que le cyberespace modifie les modalités de la diffusion de la connaissance (cf. Axe 1).
6. **POUR CONCLURE ②** Montrez, **à partir de l'ensemble des documents et particulièrement du document 6**, que le contrôle du cyberespace constitue un enjeu politique et géopolitique pour les États (Cf. Axe 2).

1.2. Liberté ou contrôle des données ?

🗎 **DOCUMENT 8 :** La déclaration d'indépendance du cyberespace

Militant américain des libertés sur Internet, John P. Barlow écrit lors du forum de Davos en 1996 une réponse à la loi sur les télécommunications adoptée la même année. Elle comprend des dispositions contre les contenus « indécents » et le harcèlement. Cette première tentative de régulation d'Internet est jugée anticonstitutionnelle par la Cour suprême des États-Unis au nom de la liberté d'expression.

Gouvernements du monde industriel, géants fatigués de chair et d'acier, je viens du cyberespace, nouvelle demeure de l'esprit. Au nom de l'avenir, je vous demande, à vous qui êtes du passé, de nous laisser tranquilles. […] Vous n'avez aucun droit de souveraineté sur nos lieux de rencontre. […] Je déclare que l'espace social global que nous construisons est indépendant, par nature, de la tyrannie que vous cherchez à nous imposer. Vous n'avez pas le droit moral de nous donner des ordres et vous ne disposez d'aucun moyen de contrainte que nous ayons de vraies raisons de craindre. […] Le cyberespace n'est pas borné par vos frontières. Ne croyez pas que vous puissiez le construire, comme s'il s'agissait d'un projet de construction publique. […] C'est un acte de la nature et il se développe grâce à nos actions collectives. […] Nous créons un monde où tous peuvent entrer, sans privilège ni préjugé dicté par la race, le pouvoir économique, la puissance militaire ou le lieu de naissance. Nous créons un monde où chacun, où qu'il se trouve, peut exprimer ses idées, aussi singulières qu'elles puissent être, sans craindre d'être réduit au silence ou à une norme. Vos notions juridiques de propriété, d'expression, d'identité, de mouvement et de contexte ne s'appliquent pas à nous. Elles se fondent sur la matière. Ici, il n'y a pas de matière. […] Vous vous efforcez de repousser le virus de la liberté en érigeant des postes de garde aux frontières du cyberespace […] mais ils n'auront aucune efficacité dans un monde qui sera bientôt couvert de médias informatiques.

John P. BARLOW, éditions Hache, 1996.

🗎 **DOCUMENT 9 :** Le mouvement *Anonymous*

Les Anonymous (Anonymes) forment une cybercommunauté d'hacktivistes, apparue dans les années 2000 sur le site 4chan, forum de partage d'images américain, assurant l'anonymat de ses membres. Leurs actions les plus notables sont les cyberattaques, la diffusion illégale de contenus, les manifestations en ligne. Ils accusent les gouvernements de mettre en place des sociétés de la surveillance et de limiter les libertés des individus dans le cyberespace.

Étudiants de l'Université polytechnique de Hong Kong portant le masque du conspirateur anglais du XVIIe siècle, Guy Fawkes, symbole des Anonymous, le 30 octobre 2019.

🗎 **DOCUMENT 10 :** L'enjeu de la protection des données des utilisateurs sur Internet

[…] En septembre 2018, Twitter et Google étaient auditionnés devant le Sénat américain à propos de la protection des données. A cette occasion, Damien Kieran, responsable de la protection des données chez Twitter, plaidait pour "un cadre de protection de la vie privée robuste, qui protège les droits individuels (…) tout en préservant la liberté d'innover". De son côté, le responsable de la confidentialité chez Google, Keith Enright, déclarait : "*nous reconnaissons avoir commis des erreurs par le passé, desquelles nous avons appris et avons amélioré notre solide programme de protection des données*".

Ces prises de position peuvent paraître assez curieuses quand on sait que la flexibilité dans l'utilisation des données personnelles constitue le fondement même de leur business model, mais elles répondent à la déferlante de critiques qu'a provoqué l'affaire Cambridge Analytica. Le 17 mars 2018, The Guardian et The Financial Times publient une enquête sur cette société. Les deux journaux affirment que cette dernière se serait emparée des données personnelles de 50 millions d'utilisateurs de Facebook à des fins politiques. Les informations s'affinent avec les révélations du lanceur d'alerte Christopher Wylie, ancien directeur de recherche à Cambridge Analytica. "Nous nous sommes servis de Facebook pour récupérer les profils de millions de personnes. Nous avons ainsi construit des modèles pour exploiter ces connaissances, et cibler leurs démons intérieurs", déclarait-il. En analysant ces données, Cambridge Analytica a eu la possibilité de prédire et d'influencer le vote des électeurs lors de la précédente élection américaine [de 2016].

Alice VITARD, « Pourquoi les GAFAM prennent-ils une posture pro-régulation ? », www.usine-digitale.fr, 23 septembre 2019

🗎 **DOCUMENT 11 :** Le *Dashboard Act*

En juin 2019, deux sénateurs américains déposent une proposition de loi, le Dashboard Act, qui obligeait les plateformes à déclarer les gains obtenus grâce aux données personnelles de leurs utilisateurs.

Combien rapporte un clic sur une mention « J'aime » à Facebook ? Une recherche sur le moteur de Google ? […] Ce n'est un secret pour personne, ces géants sociaux basent leur modèle économique sur la collecte de données personnelles, monétisées par le biais de publicités ciblées. En contrepartie Facebook, Google et les autres mettent à disposition « gratuitement » leurs services sur le Web. Mais pour le démocrate Mark Warner et le républicain Josh Hawley, ce deal implicite entre utilisateur et plateforme est biaisé. « Les gens ne se rendent pas compte de la quantité de données recueillies, et ils ne se rendent pas compte de la valeur de ces données », explique Mark Warner. […] La loi […] imposerait davantage de transparence aux plateformes dépassant les 100 millions d'utilisateurs mensuels. Tous les 90 jours, ces géants seraient ainsi obligés de fournir à leurs inscrits l'ensemble des données qu'ils ont obtenu auprès d'eux ainsi qu'une évaluation financière de ce qu'elles rapportent.

Lucas MEDIAVILLA, « Facebook et Google bientôt obligés de révéler la valeur des données personnelles ? », *Les Échos*, 25 juin 2019.

🗎 **DOCUMENT 12 :** Internet nationalisé, la tentation de la cybercensure

La principale caractéristique du cyberespace réside dans son extension mondiale, et l'émergence du réseau mondial d'Internet sans frontières remonte à 1989. Pourtant, sa territorialisation est en cours aujourd'hui - autrement dit une affirmation de la souveraineté des États sur une partie du cyberespace - et ce, sous l'influence de facteurs technologiques et politiques qui menacent de le faire éclater le long des frontières géopolitiques. Ainsi, tandis que les USA essaie d'imposer leur leadership, la Chine a érigé un Great Firewall, et certains pays comme le Pakistan ont déjà bloqué des pans entiers du web accusés d'être "blasphématoires et non islamiques". Dans la même veine, un pays comme l'Iran possède son intranet national depuis août 2016, baptisé "Réseau national d'information".

Cette approche continue de gagner du terrain puisqu'en Russie, Vladimir Poutine, sous couvert d'obtenir une souveraineté numérique, a signé le 1er mai 2019 la loi sur l'Internet "durable".

Ce texte, entré en vigueur le 1er novembre 2019, vise - selon la gouvernance - à protéger la Russie de toute menace informatique en cas de menace grave. A terme, il s'agirait de couper le RuNet (l'Internet russe) du réseau mondial. Céline LOOZEN, Podcast, Radio France / France Culture / Nicolas Martin, 20 novembre 2019

🗎 **DOCUMENT 13 :** L'idéal intelligence collective

Marqués par leur culture d'ingénieurs mais pétris aussi par la pensée humaniste, les précurseurs de l'Internet […] proposent de connecter en réseau des machines informationnelles, une prouesse technique susceptible de favoriser l'échange entre utilisateurs et le libre accès à la connaissance. […]
Les premiers usages du réseau seront fortement marqués par cette culture de la liberté, de la gratuité et de l'ouverture aux contributions informelles et décentralisées. […] L'extension d'Arpanet à Internet […] ne menace pas ce sentiment communautaire informel, les « internautes » se rassemblant d'abord aisément en groupes d'intérêt à « dimension humaine ». […] Dès 1987, des firmes développent une première commercialisation de services en ligne. […] Graduellement, ces services payants se transforment en services apparemment « gratuits » parce que subventionnés par la publicité. À partir de 1995 – date marquant l'entrée d'Internet dans l'économie de marché – s'affrontent deux visions du développement des services d'Internet : d'une part, une vision mercantile dans laquelle les usagers sont définis d'abord comme des clients, consommateurs de biens et services ; d'autre part, une vision citoyenne, voire libertaire, dans laquelle les usagers eux-mêmes jouent un rôle clé dans la mise en place des applications, services et infrastructures, et la production des contenus selon une logique contributive.

Serge PROULX, Anne GOLDENBERG, « Internet et la culture de la gratuité », *Revue du MAUSS*, 2010.

✐ QUESTIONS

7. Quelle vision du cyberespace John Perry Barlow et le groupe *Anonymous* défendent-ils ? Par quels moyens **(Documents 8 et 9)** ?

8. Quels enjeux soulève la protection des données personnelles **(Documents 10 et 11)** ?

9. Quelles sont les raisons de la cybercensure **(Document 12)** ? A partir de la carte projetée, listez les États qui y ont recours.

10. **POUR CONCLURE.** Montrez, **à partir de l'ensemble des documents et du document 13 en particulier**, que deux visions du cyberespace s'opposent aujourd'hui.

2. La cyberdéfense française entre coopération et souveraineté

2.1. Coopérer pour défendre le cyberespace ?

🗎 **DOCUMENT 14 :** L'avionneur européen Airbus, cible de cyberattaques

Au cours des douze derniers mois, « quatre attaques majeures » ont visé le géant européen de l'aéronautique via des sous-traitants […]. Passant par des sous-traitants, les attaquants auraient tenté à plusieurs reprises de pénétrer les infrastructures informatiques du constructeur afin de lui dérober des données stratégiques. […] Les attaques […] ciblaient le VPN des sous-traitants qui était commun à celui de l'avionneur. Une fois ce réseau privé pénétré, les pirates se faisaient justement passer pour les sous-traitants, afin d'entrer dans le réseau d'Airbus. […] « Les très grandes entreprises (comme Airbus, ndlr), sont très bien protégées, c'est très dur de les pirater, alors que des plus petites entreprises vont être une meilleure cible », confirme un spécialiste du secteur. […] Les pirates ont ciblé des documents techniques de certification, une procédure officielle permettant d'assurer que les différents éléments d'un avion répondent aux exigences de sécurité. […] Les soupçons pèsent sur des hackers chinois. La Chine cherche à mettre au point depuis plusieurs années son premier moyen-courrier, le C919, mais peine à le faire certifier. […] Mais, en matière de cyberattaques, l'attribution reste toujours un point difficile à établir, et les spécialistes sont généralement réticents à désigner des auteurs, difficiles à démasquer.

« Airbus ciblé par une série de cyberattaques, la Chine soupçonnée », *AFP*, 26 septembre 2019.

🗎 **DOCUMENT 15 :** Les chefs d'État européens espionnés

En 2013, les documents transmis par le lanceur d'alerte américain Edward Snowden à des journalistes révèlent un vaste programme de surveillance de la NSA (Agence nationale de sécurité américaine, en charge du renseignement électronique et de la sécurité des systèmes d'information) qui comprend notamment la mise sur écoute de plusieurs dirigeants européens.

🗎 **DOCUMENT 16 :** Un cadre législatif européen pour protéger les enfants sur Internet

La pédopornographie, qui consiste en des images d'abus sexuels commis sur des enfants, et d'autres formes particulièrement graves d'abus sexuels et d'exploitation sexuelle d'enfants […] se propagent par le biais de l'utilisation des nouvelles technologies et de l'Internet. […]

La sollicitation d'enfants à des fins sexuelles est une menace aux caractéristiques particulières dans le cadre de l'Internet, car ce dernier procure aux utilisateurs un anonymat sans précédent qui leur permet de masquer leur identité réelle […]. Il convient de doter les personnes chargées […] de poursuivre les infractions visées dans la présente directive de moyens d'enquête performants. Ces moyens pourraient comprendre l'interception de communications, la surveillance discrète, notamment électronique, la surveillance de comptes bancaires […]. Ces moyens devraient également […] inclure la possibilité pour les autorités répressives d'utiliser une fausse identité sur l'Internet. […] Toutefois, la suppression de contenus pédopornographiques à leur source est souvent impossible […] lorsque le matériel d'origine ne se trouve pas dans l'Union, soit parce que l'État dans lequel les serveurs sont hébergés n'est pas disposé à coopérer, soit parce que la procédure pour obtenir de l'État concerné la suppression de ce matériel s'avère particulièrement longue.

Extrait de la directive européenne 2011/92/UE.

🗎 **DOCUMENT 17 :** L'Agence de l'Union européenne pour la cybersécurité

Compte tenu de leur rôle essentiel dans nos sociétés et nos économies modernes, les ordinateurs, les téléphones portables, les banques et l'internet doivent fonctionner ensemble correctement.

L'ENISA a pour mission d'assurer un niveau élevé de sécurité des réseaux et de l'information. Elle agit de différentes façons:

- En intervenant en tant qu'expert en matière de sécurité des réseaux et de l'information auprès des autorités nationales et des institutions européennes;
- En favorisant l'échange de meilleures pratiques;
- En facilitant les contacts entre les institutions (nationales et européennes) et les entreprises.

L'ENISA, en collaboration avec les instances nationales et les institutions européennes, s'emploie à développer une culture de la sécurité des réseaux d'information dans toute l'Union

Site internet de l'Agence européenne chargé de la sécurité des réseaux et de l'information (ENISA), consulté en mars 2021.

🗎 **DOCUMENT 18 :** Les difficultés de la coopération européenne en matière de cybersécurité

L'Union européenne n'a […] qu'un rôle limité dans la construction de la cybersécurité, et cantonne ses mesures aux activités liées au secteur économique et commercial, dans le respect des libertés individuelles fondamentales qu'elle entend défendre dans le cyberespace […].

Les enjeux de souveraineté, qui inhibent les actions communes de cyberdéfense au sein de l'Otan, sont autant d'obstacles à l'adoption de mesures de cybersécurité plus développées au sein de l'UE. Il apparaît […] que les États membres de l'Union qui ont massivement investi dans ce domaine ne céderont pas plus de terrain sur cette question au sein de l'UE qu'au sein de l'Otan ; en conséquence, les mesures de cybersécurité actuelles reposent majoritairement sur la coopération volontaire par laquelle les centres de cybersécurité nationaux, mais également ceux du secteur privé échangent et partagent des informations selon leurs besoins et leur bon vouloir. Les agences de l'Union européenne […] n'ont ainsi aucun pouvoir de contrainte, et ne peuvent que proposer des recommandations et des conseils relatifs aux bonnes pratiques dans le domaine. […] En raison du caractère particulièrement sensible de ces questions, les États opposent la notion de souveraineté à toute velléité d'extension ou de mise en commun des capacités.

Vincent JOUBERT, Jean-Loup SAMAAN, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE », *Hérodote*, 2014.

🗎 **DOCUMENT 19 :** L'UE renforce ses cyberdéfenses

Le Conseil de l'Union européenne publie sur son site la chronologie de ses décisions.

Le 17 mai 2019

L'UE et ses États membres se préparent pour mieux résister et réagir aux cyberattaques.

Le Conseil a établi un cadre permettant à l'UE d'imposer des mesures restrictives ciblées visant à décourager et contrer les cyberattaques qui constituent une menace extérieure pour l'UE ou ses États membres. Plus particulièrement, ce cadre permet pour la première fois à l'UE d'imposer des sanctions à des personnes ou entités qui […] sont responsables de cyberattaques ou de tentatives de cyberattaques.

Le 9 avril 2019

Le Conseil a adopté le règlement sur la cybersécurité, qui prévoit :

– un ensemble de systèmes de certification à l'échelle de l'UE ;

– une agence de l'UE pour la cybersécurité, qui succédera à l'actuelle Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA). […] L'agence organisera également des exercices réguliers de cybersécurité à l'échelle de l'UE, y compris un exercice global à grande échelle une fois tous les deux ans.

Conseil de l'Union européenne et du Conseil de l'Europe, communiqués de presse, 2019.

✐ QUESTIONS

11. Identifiez les principales cybermenaces présentées dans les documents en précisant pour chacune d'elles les acteurs exposés au risque. En quoi ces acteurs sont-ils vulnérables **(Documents 14,15 et 16)** ?

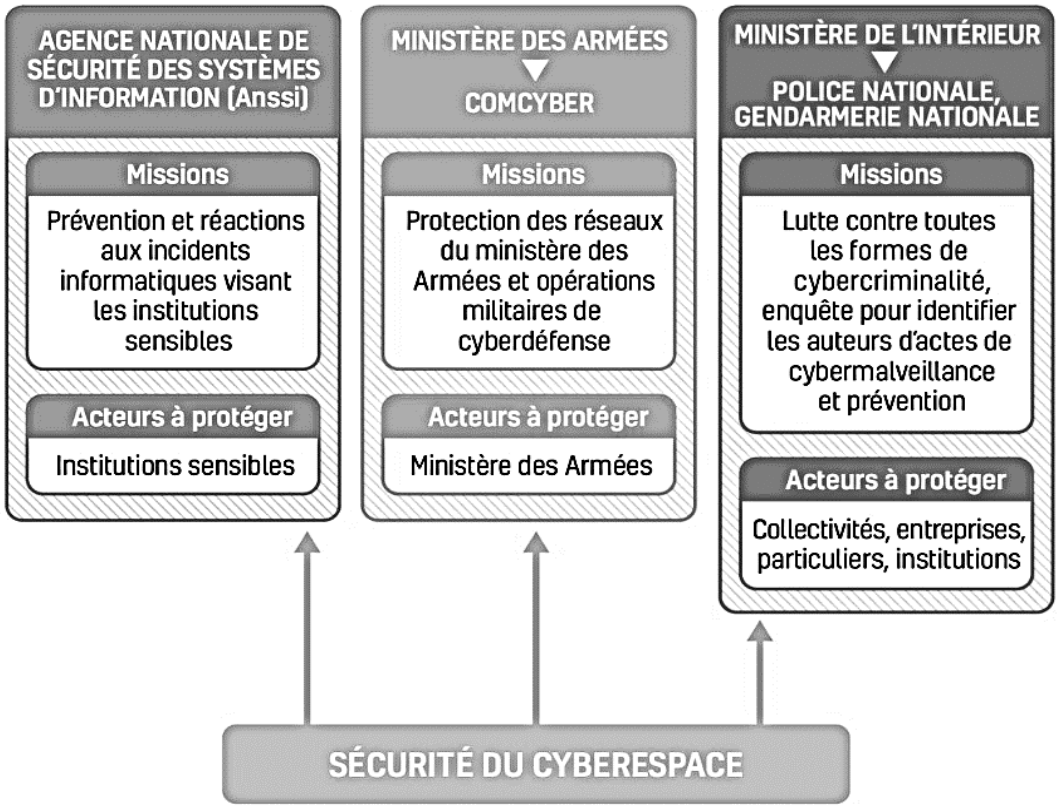
12. Expliquez pourquoi la sécurité est particulièrement difficile à assurer dans le cyberespace **(Document 16)**.

13. Quelles réponses l'UE apporte-t-elle en matière de cybersécurité ? En quoi ces réponses sont-elles limitées **(Documents 16 à 19)** ?

14. **POUR CONCLURE.** Montrez, **à partir de l'ensemble des documents**, dans quelle mesure l'échelle européenne est pertinente pour assurer la sécurité du cyberespace.

2.2. Défendre le cyberespace, quels enjeux pour la France ?

🗎 DOCUMENT 20 : Les acteurs de la stratégie nationale de la sécurité du numérique en France



Manuel HGGSP, Belin 2020

🗎 DOCUMENT 21 : Le Comcyber

Créé en 2017, le Comcyber est l'unité opérationnelle qui commande l'ensemble des forces de cyberdéfense des armées françaises sous l'autorité du chef d'État-major des armées. Il est notamment en charge de la défense des systèmes d'information du ministère des Armées ainsi que de la conduite des opérations militaires de cyberdéfense. Il compte 3 400 cyber-combattants en 2018. Il assure également le développement et l'animation de la réserve citoyenne de cyberdéfense.

🗎 DOCUMENT 22 : La mise en place de moyens dédiés au cyberespace

En 2009, la France fonde l'Agence nationale de la sécurité des systèmes d'information. L'année suivante, les États-Unis créent l'US Army Cyber Command. Le Livre blanc sur la défense et la sécurité nationale de 2013 élève le cyberespace au rang de priorité stratégique en France. En décembre 2016, Jean-Yves Le Drian, alors ministre de la Défense, annonce la création d'un cybercommandement. Entre 2014 et 2019, la France consacrera un milliard d'euros à la cyberdéfense et se dotera d'une cyberarmée de 3 200 hommes. La cyberguerre permet aux États de combattre des ennemis, mais aussi d'espionner des pays alliés en exploitant les failles de sécurité zero-day et les limites des machines. « Nous n'avons pas d'amis », rappelait Churchill.

Après le sommet *Netmundial* de 2014, le Brésil et l'Europe décident d'installer un câble sous-marin pour contourner cette domination. Pour Jean-Yves Le Drian, « si une attaque cyber s'apparente à un acte de guerre, une riposte adéquate s'imposera, dans une logique de conflit ouvert », conformément à l'article 51 de la Charte des Nations unies pour les conflits conventionnels. Toutefois, la difficulté d'établir les responsabilités rend les représailles délicates. Trouver l'origine d'un programme malveillant sophistiqué est plus complexe que suivre la trajectoire d'un missile. Sans oublier que la propagation des virus peut faire des victimes collatérales.

Soline TOUSSAINT, « Le cyberespace : champ de bataille du XXIe siècle », *Diplomates*, 19 décembre 2017.

🗎 **DOCUMENT 23 :** La doctrine cyber offensive

La cybersécurité, c'est un sport collectif.
La faille peut venir de partout. Les hackers sont pleins d'inventivité. […]
En 2017, les réseaux de la défense ont subi 700 événements de sécurité dont 100 cyberattaques. […]
Et non seulement le nombre d'attaques augmente mais les attaquants ont toujours des profils aussi variés. Un adolescent peut pirater les mails de la chancelière allemande pour s'amuser, presque par hasard. Un groupe anonyme peut s'en prendre à nos industries, nos transports, nos hôpitaux sans raison apparente. Un État, enfin, peut chercher à affirmer sa puissance en nous espionnant, nous manipulant ou même en sabotant nos capacités. […] La guerre cyber a bel et bien commencé […] et nous allons nous y préparer.
J'ai annoncé devant le Commandement cyber […] que la France revendiquait d'utiliser l'arme cyber au même titre que toutes les armes conventionnelles. J'ai pu énoncer les grands principes de notre nouvelle doctrine cyber offensive et le renforcement de notre défense cyber.
L'arme cyber n'est pas seulement pour nos ennemis ou nos fictions. Non. Nous aussi, en France, pouvons défendre, répliquer et attaquer.
En opération, nous employons déjà l'arme cyber. Nous avons publié les grandes lignes de cette doctrine pour le faire savoir […].

Discours de Florence PARLY, ministre des Armées, janvier 2019.

🗎 **DOCUMENT 24 :** Le rôle des entreprises du numérique

L'omniprésence du numérique dans tous les aspects de la vie quotidienne fait des entreprises du numérique des acteurs à part entière de la sécurité nationale. Ces entreprises, qui gèrent le réseau au quotidien, sont les premières à observer les attaques. Elles conçoivent également les produits et les services de sécurité informatique utilisés dans la détection et la protection contre les attaques. Elles sont également les opérateurs des plateformes d'intermédiation (réseaux sociaux) utilisées par les djihadistes pour leur propagande. Elles touchent ainsi jusqu'aux fonctions les plus régaliennes de l'État. Dès lors, la coopération entre le secteur public et ces entreprises du numérique est devenue non seulement une nécessité, mais une condition même à la sécurité nationale. La France est fortement dépendante d'entreprises étrangères, tant en matière de plateformes que de produits et services numériques. Face au déficit d'acteurs privés du numérique d'envergure, elle a développé une posture réactive en mettant en œuvre des dispositifs de certification de produits et services de sécurité, mais aussi certains produits « souverains » jugés particulièrement critiques en termes de sécurité nationale. L'objectif est de garantir la pleine maîtrise de la conception de ces produits.

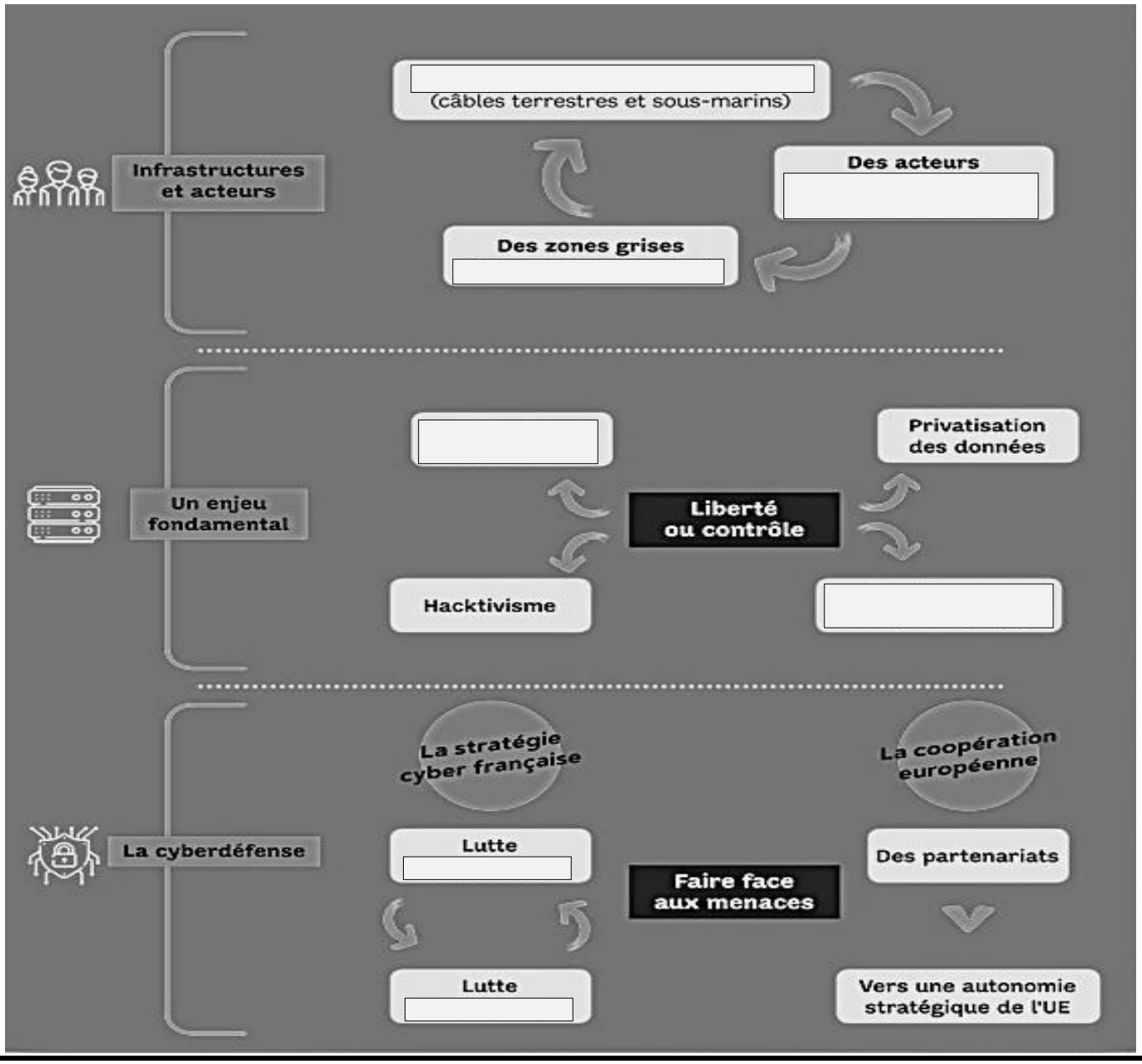
Alix DESFORGES, chercheuse au sein de la chaire Castex de Cyberstratégie, « Défense et sécurité de l'espace numérique : la nécessité d'une stratégie globale et inclusive », *Les Champs de Mars*, 2018.

✐ QUESTIONS

15. Présentez les missions du Comcyber **(Documents 20 et 21)**.
16. Comparez les rôles du ministère des Armées et du ministère de l'Intérieur dans le cadre de la stratégie nationale de la sécurité du numérique **(Documents 20 et 21)**.
17. Montrez que l'année 2019 constitue un tournant en matière de cyberdéfense **(Document 22)**.
18. En quoi le **document 24** peut-il expliquer la citation de la ministre des Armées : « *la cybersécurité, c'est un sport collectif* » ?
19. **POUR CONCLURE ①.** Montrez, **à partir de l'ensemble des documents**, comment la France entend assurer sa souveraineté numérique.
20. **POUR CONCLURE ②** Montrez, **à partir de l'ensemble des documents**, que le renforcement par l'État du contrôle d'internet constitue l'un des enjeux de la nouvelle économie de la connaissance (Cf. Axes 1&2).

🕮 SCHEMA BILAN – Le cyberespace

✍ **Complétez le schéma suivant en retrouvant les expressions ou termes manquants dans les rectangles.**



🕮 DATES CLÉS

🕮 LEXIQUE

➲ Cyberespace : Ensemble des données numérisées (logiciels et documents textuels, sonores, graphiques ou visuels) disponibles sur Internet et des infrastructures matérielles et logicielles qui assurent leur diffusion.

➲ *Data Center* (Centre de données) : Établissement industriel dont le rôle est d'héberger des données informatiques et de permettre leur accès à distance.

➲ *Dark web* (« Internet sombre ») : Sites ayant des visées criminelles ou proposant des informations ou des biens illicites. Ils ne sont accessibles qu'à l'aide d'un logiciel approprié.

➲ *Deep web* (« Internet profond ») : Ensemble des pages web que les moteurs de recherche ne peuvent pas identifier.

➲ Souveraineté : Droit propre à un État d'exercer son autorité (exécutive, législative et/ou judiciaire) sur un territoire et une population déterminée.

➲ *Open data* (« données ouvertes ») : Pratique de publication sous licence ouverte qui garantit un accès libre aux données numériques et autorise leur réutilisation sans conditions techniques, juridiques ou financières.

➲ Hacktiviste : Terme forgé à partir de *hacking* (« piratage ») et de *activist* (« militant ») pour désigner les pirates du web qui agissent au nom de la liberté absolue du réseau internet. On parle de cyberattaques pour désigner leurs actes de piratage.

➲ Cybercensure : Surveillance et limitation des contenus internet entravant la liberté d'expression.

➲ *Hacking* : Ensemble d'actions et de techniques visant à « casser » les systèmes de cybersécurité, en particulier ceux des États ou des entreprises. On parle aussi de piratage informatique.

➲ Cybercriminalité : Infractions et crimes subis dans le cyberespace.

➲ Logiciel malveillant (ou *malware*) : Programme développé dans le but de nuire à un système informatique.

➲ Cyberdéfense : Ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité.