



ASSEMBLEE PARLEMENTAIRE DE L'OTAN

## COMMISSION DE L'ECONOMIE ET DE LA SECURITE (ESC)

Sous-commission sur les relations  
économiques transatlantiques  
(ESCTER)

## MARCHÉS NUMÉRIQUES ET CYBERSÉCURITÉ : LES APPROCHES NORD-AMÉRICAINNE ET EUROPÉENNE

Projet de rapport révisé

Jean-Marie BOCKEL (France)  
Rapporteur

141 ESCTER 19 F | Original : français | 5 juillet 2019

*Tant que ce document n'a pas été adopté par la commission de l'économie et de la sécurité, il ne représente que le point de vue du rapporteur.*

**TABLE DES MATIÈRES**

I.	INTRODUCTION : RETOMBÉES DE L'ÉCONOMIE NUMÉRIQUE.....	1
II.	ÉCONOMIE NUMÉRIQUE, ÉVOLUTION DES MARCHÉS ET AGENDA DU COMMERCE INTERNATIONAL .....	3
III.	ÉCONOMIE NUMÉRIQUE ET SÉCURITÉ NATIONALE : LES CAS DE LA RUSSIE ET DE LA CHINE .....	6
IV.	SÉCURITÉ DES DONNÉES, CONFIDENTIALITÉ ET RÉGLEMENTATION D'INTERNET : PERSPECTIVE EUROPÉENNE ET DIVERGENCES TRANSATLANTIQUES .....	15
V.	CONCLUSIONS .....	17
	BIBLIOGRAPHIE.....	21

## I. INTRODUCTION : RETOMBÉES DE L'ÉCONOMIE NUMÉRIQUE

1. Le développement des technologies numériques façonne de manière croissante l'économie mondiale. Loin de se cantonner aux technologies de pointe, le changement réorganise presque tous les secteurs, jusqu'aux plus traditionnels comme l'agriculture, la production de base, la distribution et les transports. L'accès aux technologies critiques s'élargit rapidement. En 2005, 16% à peine de la population mondiale bénéficiait d'un accès à internet. Aujourd'hui, ce chiffre est passé à 48%, et plus de la moitié de ceux qui bénéficient de cet accès utilise cette technologie à des fins domestiques.

2. De l'avis général, ce sont surtout des entreprises américaines, installées dans la Silicon Valley californienne, qui ont joué un rôle majeur dans l'émergence de l'économie numérique, une économie interconnectée par internet et ouverte à tous aux mêmes conditions ou presque. Cette technologie, dont le développement fut stimulé de manière décisive par des universités et entreprises américaines, aussi bien que par le gouvernement et l'armée des États-Unis, est très vite devenue un agent critique du changement économique, social et même politique. Elle a révolutionné les télécommunications. Elle a aidé à établir des liens entre les gens, de manière inédite et convaincante, par-delà les frontières. Elle a créé des modèles économiques et technologiques fondamentalement nouveaux dans toute une série de secteurs. Des entreprises américaines comme Microsoft, Apple, Google et Amazon jouissent aujourd'hui d'un immense pouvoir sur le marché, ont révolutionné un certain nombre d'industries et inspiré leurs concurrents au-delà des frontières américaines. En 2015, les États-Unis affichaient un excédent commercial de 161,5 milliards de dollars dans les services numériques alors que leur balance commerciale totale était nettement déficitaire (Burwell, 2018). Le réseau internet lui-même est désormais un pivot du commerce mondial. La technologie numérique génère des gains d'efficacité et des richesses considérables. En même temps, elle restructure profondément et rapidement les marchés commerciaux. Quant aux États, ils sont mis au défi d'élaborer des structures réglementaires adéquates.

3. L'Europe s'est aussi imposée comme un acteur mondial sur les marchés numériques. Selon l'OCDE, elle joue un rôle prépondérant dans plusieurs secteurs, notamment ceux de l'informatique quantique et des télécommunications. L'Europe est un partenaire majeur des États-Unis dans le commerce numérique et représente le principal marché extérieur de nombreuses entreprises technologiques américaines de pointe. Les entreprises européennes comptent aussi parmi les fournisseurs critiques de services numériques aux clients américains, de sorte que la relation est à double sens et très conséquente. Le marché intérieur européen est si vaste que ses réglementations peuvent établir, ou, pour le moins, contribuer fortement aux normes réglementaires internationales. Cela crée parfois des frictions transatlantiques, mais cela offre également de nombreuses opportunités aux entreprises américaines, souvent soulagées de pouvoir accéder à l'espace européen (et au-delà) sans devoir affronter un patchwork de réglementations nationales contradictoires.

4. L'optimisme qui entourait la révolution numérique à ses débuts est aujourd'hui tempéré par un certain nombre de préoccupations en matière de sécurité, sur les nouvelles menaces qui pèsent sur la confidentialité et l'apparition d'une fracture numérique entre ceux qui maîtrisent la technologie et ceux qui ne sont pas en mesure d'en recueillir les bienfaits, faute d'y avoir accès. Il n'est guère surprenant que ces derniers en pâtissent sur le marché du travail quand on sait combien la révolution numérique gagne du terrain. Il existe également une fracture entre les jeunes souvent considérés comme des « natifs du numérique » et les personnes qui, dans leur jeunesse, n'ont que très peu été exposées à ces technologies. Dans de nombreuses sociétés, cela pose un défi immense à l'ère du numérique, que ce soit en termes d'apprentissage comme d'équité.

5. Malheureusement, la technologie numérique favorise également la manipulation des politiques démocratiques et de l'opinion publique, à un niveau qu'on n'aurait jamais imaginé quand elle a vu le jour. Comme en témoignent le piratage russe du comité national démocrate américain et de la campagne d'Hillary Clinton, faute de protection suffisante, les appareils et l'infrastructure

numériques peuvent rendre les démocraties ouvertes vulnérables aux interventions étrangères et à des campagnes de propagande massives aux conséquences potentiellement dévastatrices. L'internet est désormais devenu le théâtre à la fois d'activités criminelles et d'une intense concurrence entre États, et donc une véritable source de vulnérabilité et de risque. Aussi les gouvernements prennent-ils de plus en plus de mesures réglementaires défensives, revendiquant leurs droits souverains fondamentaux. L'internet, comme les technologies qui le sous-tendent, n'est plus perçu comme une incarnation idéaliste de la communauté au niveau mondial, mais comme une menace potentielle pour celle-ci. En d'autres termes, la situation est devenue beaucoup plus complexe.

6. La technologie numérique n'est plus seulement un facteur de changement économique et de prospérité, mais aussi un outil d'espionnage et d'action militaire. Lorsqu'elle a envahi la Géorgie par exemple, la Russie a mené simultanément des attaques par déni de service. À une autre occasion, elle est parvenue à bloquer à distance le réseau électrique de l'Ukraine dans le cadre de son agression contre ce pays. En 2007, l'économie estonienne a virtuellement été mise à l'arrêt suite à une attaque menée par des pirates informatiques en lien avec la Russie. La Corée du Sud a dû faire face à des attaques similaires, fomentées quant à elles par le gouvernement de Pyongyang. Des entreprises privées peuvent, par inadvertance, basculer au milieu de rivalités étatiques. Un transporteur maritime danois, par exemple, a subi des pertes estimées entre 200 et 300 millions de dollars après qu'une cyberattaque russe visant des firmes ukrainiennes a contaminé l'espace numérique international (Greenberg, 2018). Sony Pictures a dû revenir au crayon et au papier pendant plusieurs jours lorsque des pirates nord-coréens ont bloqué ses systèmes informatiques, sous prétexte qu'un film Sony dépeignait leur dirigeant sous un jour peu flatteur. Ce sont aussi des agents nord-coréens qui ont pillé la banque centrale du Bangladesh pour tenter de se procurer des devises étrangères très convoitées (Flournoy et Sulmeyer, 2018). Ces agissements sapent la confiance dans la sécurité du marché et nuisent gravement au libre jeu des économies.

7. Si quelques clics de souris suffisent pour paralyser l'économie d'un pays, ce type d'arme devient très attrayant pour les planificateurs de la défense qui, par nature, cherchent le meilleur rapport coût/efficacité. Un logiciel malveillant peut désormais infliger le même genre de dégâts qui nécessitaient autrefois des milliers de raids de bombardiers. Ces outils sont décidément très attrayants pour les sociétés qui n'ont pas les moyens de s'offrir ces bombardiers ou qui préfèrent attaquer sans se dévoiler. Les sociétés riches de l'ère postindustrielle, très tributaires de l'économie numérique, sont devenues extrêmement vulnérables à ces attaques asymétriques. Dans le même temps, des régimes plus autoritaires comme la Chine et l'Iran contrôlent strictement leur internet : tout en limitant les libertés de leurs citoyens, ils réduisent ainsi la vulnérabilité de leurs sociétés aux attaques extérieures. Il s'agit là d'une asymétrie que les planificateurs de la défense doivent prendre en considération et ce, de manière globale en incluant les points de vue respectifs du gouvernement et de la société.

8. Les rivalités numériques internationales croissantes sont également étroitement liées à des valeurs sociétales conflictuelles. Il ne fait aucun doute que le tropisme occidental pour l'ouverture est paradoxalement devenu source de vulnérabilité. Il faudra trouver de nouveaux équilibres entre ouverture numérique et sécurité, ce qui nécessitera une coopération étroite et innovante entre les États, les marchés et les citoyens. Qui plus est, ce dialogue ne concernera pas seulement la dimension internationale du défi. Il faudra également tenir compte de facteurs très importants sur le plan national, comme par exemple le pouvoir croissant de certaines entreprises numériques, leur accès à des informations privées et leur capacité à utiliser ces informations pour en tirer du profit et des avantages commerciaux.

9. Cela étant dit, l'équilibre des pouvoirs sur le plan numérique est clairement en train de changer. Malgré les avantages acquis grâce à leur rôle de pionnier, les États-Unis ne disposent plus désormais d'une mainmise incontestée sur l'internet et l'univers numérique. Et les implications de ce changement sur le plan stratégique sont loin d'être négligeables. En effet, parmi les acteurs

technologiques puissants, certains n'adhèrent tout simplement pas aux valeurs de démocratie, de transparence, de libre concurrence sur le marché, de liberté de la presse et de protection de la propriété intellectuelle. L'internet d'aujourd'hui est donc très différent de la vision de ses créateurs. Comme l'ont noté récemment Michelle Flournoy et Michael Sulmeyer, « les États se servent des armes de la cyberguerre pour saper ce qui constituait le socle d'internet : la confiance. Ils dévalisent les banques, ils s'immiscent dans les élections, ils volent la propriété intellectuelle, ils empêchent les entreprises privées de fonctionner. Résultat ? L'arène sur laquelle le monde s'appuie pour échanger des biens et des informations s'est transformée en un champ de bataille actif » (Flournoy et Sulmeyer, 2018).

10. De nombreuses raisons justifient une coopération plus étroite entre l'Europe et les États-Unis pour gérer l'économie numérique et parvenir ensemble à trouver le bon équilibre entre sécurité, innovation, ambitions commerciales et réglementation. Si les États-Unis ont été le premier pourvoyeur de technologies numériques, l'Europe a, elle aussi, joué un rôle important à cet égard et consomme également ces technologies. En outre, l'Union européenne jouit d'un poids considérable sur le plan réglementaire. L'UE est un acteur critique lorsqu'il s'agit de définir les marchés numériques, non seulement sur son territoire, mais aussi à l'échelle mondiale. Elle s'attache résolument à prendre en compte les intérêts du consommateur et ses inquiétudes quant à l'évolution rapide de ces marchés. Cela suscite parfois des frictions avec les États-Unis, plus partisans du laisser-faire sur les questions de confidentialité, de fiscalité, de transfert des données personnelles et professionnelles entre pays, de droits d'auteur et de concurrence (Burwell, 2018). Ces divergences de vues donnent parfois naissance à des tensions transatlantiques, portant par exemple sur la position à adopter envers de nouveaux acteurs du marché potentiellement puissants – comme la Chine et ses grandes entreprises numériques. À bien des égards, le débat sur ces questions ne fait que commencer et par conséquent, le cadre réglementaire reste hautement versatile.

## **II. ÉCONOMIE NUMÉRIQUE, ÉVOLUTION DES MARCHÉS ET AGENDA DU COMMERCE INTERNATIONAL**

11. Le système commercial international est aujourd'hui soumis à de fortes contraintes. Le protectionnisme est en plein essor car les politiciens réalisent que le libre-échange représente le parfait bouc émissaire pour justifier des changements fondamentaux, y compris dans le domaine technologique, qui perturbent les économies nationales. La croissance du commerce mondial a considérablement ralenti depuis la crise financière de 2008. Parallèlement, les flux financiers franchissant les frontières nationales ont sensiblement diminué. L'année dernière, la croissance du commerce mondial a chuté, alors que les États-Unis ont décidé d'imposer des droits de douane aussi bien à ses alliés qu'à ses adversaires. Cela a déclenché une série de hausse des tarifs douaniers en réponse et, au final, une contraction des investissements et une détérioration de la croissance mondiale (OCDE, 2019). Par ailleurs, les gains d'efficacité apportés par la mondialisation des chaînes de valeur sont aujourd'hui largement réalisés, bien qu'encore incomplètement. À l'avenir, c'est dans l'espace numérique que se situeront les nouveaux gains d'efficacité et le processus sera intrinsèquement mondial. Reste à savoir si les dirigeants politiques soutiendront les échanges technologiques ou s'ils les enrayeront. Telle qu'elle se présente aujourd'hui, la politique commerciale n'augure rien de bon.

12. Mais cette nouvelle vague de mondialisation ne sera plus entièrement dirigée par l'Occident, ni ancrée dans le commerce traditionnel. Elle sera de plus en plus numérique, axée sur les données, influencée davantage par des pays non-occidentaux comme la Chine, mais sera par ailleurs très ouverte à de plus petits opérateurs, qui peuvent désormais se ménager une présence sur le marché dans ce que nous pourrions appeler un univers sans frictions. Aujourd'hui, déjà, la moitié des échanges de services dans le monde repose sur la technologie numérique. Les liens directs tissés par la technologie numérique entre le producteur et le consommateur ont bouleversé le marché de

la distribution. Alibaba, la plateforme chinoise de vente en ligne, prévoit que d'ici à 2020, l'e-commerce mondial touchera un milliard de clients et générera un chiffre d'affaires de quelque mille milliards de dollars, qui sera souvent réalisé par de très petits producteurs qui auraient été exclus des marchés de détail traditionnels. Hébergées sur des plateformes géantes comme Amazon ou Alibaba, ces entreprises accèdent à un marché potentiel qui dépasse de très loin ce qu'elles auraient pu imaginer il y a seulement 15 ans, compte tenu de leur taille. Notons ici que la Chine représente actuellement 42% de la valeur des transactions de l'e-commerce mondial, une part de marché qui augmente régulièrement (Lund et Tyson, 2018). De nouveaux pôles d'e-commerce sont en train d'apparaître partout dans les pays en développement, faisant progresser rapidement les revenus de ces régions.

13. Autre effet de cette évolution : le leadership traditionnel de l'Occident dans le commerce mondial et dans l'e-commerce s'estompe. La mondialisation va se poursuivre, malgré le recul de la la prééminence occidentale. D'après Lund et Tyson, le retrait américain de l'accord de partenariat transpacifique, par exemple, n'a pas empêché les autres pays négociateurs de signer l'accord de partenariat transpacifique global et progressiste (PTPGP). Ce n'est peut-être pas un hasard si cet accord n'évoque plus les mesures de protection des droits d'auteur et de la propriété intellectuelle que les États-Unis voulaient voir figurer dans le partenariat. Pour les Américains, ces mesures sont des priorités dans le cadre de l'économie numérique, mais tous les protagonistes ne sont pas de cet avis. Le message est clair : à l'ère numérique, aucun pays n'est en mesure d'arrêter la mondialisation, et en se retirant du processus, un pays peut saper sa capacité d'influencer, à son profit, une évolution inéluctable.

14. Par ailleurs, l'ère numérique accélère fortement le cycle de vie des produits, raccourcissant le temps dont les entreprises disposent pour exploiter leurs propres avancées technologiques et avantages sur le plan des produits. À peine ont-elles mis un produit en ligne qu'un substitut amélioré apparaît sur le marché. Cela bouleverse toutes les attentes en termes de croissance et de développement, de géographie économique, de marketing et d'avantage concurrentiel. Dans de telles conditions, on peut s'attendre à voir les entreprises chercher à s'implanter non plus dans les endroits où la main-d'œuvre est moins coûteuse, mais là où la connaissance et le savoir-faire sont bien ancrés, là où se trouvent les consommateurs, et là où la réglementation est la moins pénalisante. C'est ce genre de calcul qui a conduit Amazon à installer (du moins au départ) un de ses principaux sièges à New York, malgré le coût élevé des salaires et de l'immobilier dans cette ville. De même, l'industrie automobile pourrait se relocaliser, dans une certaine mesure, non pour des raisons de protectionnisme, mais plutôt parce que des changements technologiques comme l'impression 3D, l'intelligence artificielle (IA) ou les voitures autonomes, auront permis d'abaisser les coûts de production dans les régions où ces technologies sont développées.

15. Dans cet univers, le leadership fait de plus en plus l'objet d'une concurrence acharnée. Il se peut que l'Occident soit en train de perdre du terrain, d'autant que certains pays clés semblent se retirer du processus de mondialisation, ou du moins segmenter leurs marchés. Bien que l'économie numérique engendre des bouleversements majeurs et représente, à l'échelle mondiale, un profond changement de paradigme, elle générera néanmoins une prospérité considérable aux acteurs économiques et politiques prêts à la maîtriser. Au XXI<sup>e</sup> siècle, l'économie numérique sera sans nul doute le premier moteur d'efficacité, d'innovation et de production de richesse. Ceci entraînera un bouleversement de la hiérarchie actuelle des acteurs économiques, une sorte de destruction créative qui a déjà caractérisé les précédentes révolutions industrielles. Aujourd'hui, le processus de changement est toutefois nettement plus rapide que par le passé. Les pays qui dirigent ce processus jouiront vraisemblablement d'une influence démesurée lorsqu'il s'agira de fixer les règles du jeu et leur poids sur le marché pourrait s'en trouver renforcé.

16. La communauté internationale est confrontée à un autre défi : la taxation de l'économie numérique. Cela fait partie de la problématique du transfert fiscal, dit « tax shift », et de l'érosion de l'assiette fiscale que de nombreux pays tentent de gérer à l'aide de nouvelles règles coordonnées

au niveau de l'OCDE. Le processus a permis des échanges, entre 128 pays, d'informations vitales et de rapports grâce auxquels les administrations fiscales des États participants pourront cibler plus facilement les entreprises numériques à l'endroit où elles génèrent leur chiffre d'affaires, même sans être physiquement présentes dans un pays donné. Un accord international est indispensable pour éviter les situations de double non-imposition à une époque où la part de l'économie numérique dans l'économie globale s'accroît inéluctablement. La force du système se mesure au maillon le plus faible de la chaîne. C'est la raison pour laquelle il faut déployer tellement d'efforts pour parvenir à un accord international. Les actifs de certaines entreprises numériques étant majoritairement incorporels, les autorités nationales et locales ont bien du mal à décider comment et où taxer ces contribuables d'un genre nouveau. Sans coordination internationale, il sera très difficile de soumettre à l'impôt cet important secteur commercial. C'est d'autant plus vrai qu'il devient de plus en plus difficile de distinguer les entreprises numériques des entreprises traditionnelles, à mesure que ces dernières digitalisent leurs opérations et leurs ventes.

17. La politique de concurrence est un autre sujet de préoccupation croissante. La puissance commerciale de sociétés numériques comme Facebook devient si écrasante que la distorsion croissante des règles du jeu suscite les inquiétudes de plus en plus vives. Facebook, par exemple, domine le marché des réseaux sociaux et a consolidé sa position en rachetant WhatsApp et Instagram. Qui plus est, les algorithmes de recherche de Facebook favoriseraient, dit-on, les sites web contrôlés par la société. En intégrant ces services dans une plateforme unique, de nombreux consommateurs pensent qu'ils n'ont pas d'alternative viable en matière de réseaux sociaux, même s'ils désapprouvent la manière abusive dont l'entreprise se sert de données privées, son immense pouvoir de décision sur ce qui est acceptable ou non et la manipulation de la plateforme par des acteurs politiques agissant dans l'ombre pour tenter de polariser les sociétés occidentales et affaiblir leurs démocraties. Facebook a aujourd'hui accès à une quantité phénoménale de données à caractère personnel, une quantité qui ne cesse de croître et qui augmente l'emprise commerciale de la société ainsi que son pouvoir d'influence aux plans sociétal et politique (Hughes, 2019).

18. À mesure que ces géants accroissent leur emprise sur le marché, les aiguillons de la concurrence commencent à s'éteindre avec, à terme, un risque de monopole des prix ou d'abus incontrôlé des données. En outre, ces entreprises multiplient les tentatives de s'immiscer dans le jeu politique pour inciter les responsables à ne pas légiférer dans leur domaine d'activité et surtout, à ne pas envisager de mesures qui permettraient par exemple de dissoudre une société violant, apparemment, les lois antitrust (Hughes, 2019). Aujourd'hui, la question figure à l'agenda des milieux politiques. Plusieurs candidats à la présidence des États-Unis et plusieurs dirigeants politiques en Europe envisagent ouvertement de dissoudre certaines des plus grandes sociétés technologiques mondiales. La sénatrice américaine Elizabeth Warren en appelle par exemple à annuler les fusions opérées récemment par Facebook et l'idée commence à faire son chemin dans d'autres sphères dirigeantes influentes. De son côté, le gouvernement chinois poursuit une politique de « champions nationaux » qui accorde à certains acteurs comme Huawei une position de force privilégiée, rivalisant avec celle des sociétés occidentales. Sa stratégie consiste à encourager la consolidation afin que les sociétés chinoises soient davantage en mesure de conquérir des marchés internationaux.

19. Face à l'absence de concurrence dans le monde des réseaux sociaux, une nouvelle approche gagne du terrain : elle repose sur la notion de « portabilité du graphe social » (*Social Graph Portability*). Plutôt que d'appliquer des remèdes antitrust traditionnels face à une concentration excessive, le législateur s'attacherait essentiellement à réaffecter les droits de propriété afin que l'utilisateur puisse être le seul détenteur légal de ses propres données et qu'il soit dès lors en mesure de transférer toutes ses données et ses réseaux privés d'une société à l'autre. En théorie, cela devrait favoriser une plus grande concurrence entre les fournisseurs de réseaux sociaux et mener à une guerre des offres pour conquérir des clients - cette guerre des offres incluant aussi, potentiellement, une meilleure protection de la vie privée et de la confidentialité. Dans cet univers

numérique remodelé, les abonnés à différents fournisseurs de réseaux sociaux pourraient accéder et lire les messages des uns et des autres (Gans, 2017).

20. La définition des règles est devenue une pomme de discorde internationale, au point d'introduire des tensions dans les relations entre Alliés. Les plateformes numériques américaines, par exemple, sont de plus en plus contraintes de respecter les règles européennes. C'est le prix à payer pour accéder au marché unique. Le marché européen est tellement vaste et important que les entreprises américaines n'ont d'autre choix que d'obtempérer. Mais cela n'est pas passé inaperçu au niveau politique. Wilbur Ross, le secrétaire d'État américain au commerce, a récemment qualifié le Règlement général sur la protection des données (RGPD) européen de barrière commerciale déguisée, oubliant que le RGPD s'appliquait indifféremment des nationalités des entreprises. Dans un éditorial du *Financial Times* paru en mai, M. Ross estime que « le RGPD impose des obligations légales importantes mais peu claires aux entités des secteurs privé et public, y compris au gouvernement américain. Nous ne savons pas exactement à quelles règles nous devons nous conformer. Cela risque de troubler la coopération transatlantique en matière de réglementation financière, de recherche médicale, de coordination de la gestion de crise, et de commerce. Il y a là de quoi compromettre le modèle social de part et d'autre de l'Atlantique. Les autorités américaines et européennes des services financiers risquent d'être empêchées de mener certaines actions importantes. Ainsi, on ne sait pas clairement, par exemple, si les autorités de surveillance de l'UE peuvent partager l'information avec leurs homologues américaines, dans le cadre des contrôles de conformité et d'autres vérifications » (Ross, 2018). Ce point de vue ne fait pas l'unanimité aux États-Unis, où un nombre croissant de partisans de la protection de la vie privée voient dans la législation européenne un signe avant-coureur et un modèle potentiel de dispositif de protection des données confidentielles dont les sociétés démocratiques de demain auront grand besoin. L'Europe et les États-Unis doivent coopérer plus efficacement en matière de réglementation.

21. Enfin, les gouvernements doivent déterminer quelle est la meilleure manière de préparer leurs sociétés à prospérer à l'ère numérique. Cet aspect est critique. En effet, comme d'autres révolutions industrielles du passé, la transformation actuelle menace des métiers entiers, même si elle en crée de nouveaux. Les sociétés démocratiques libérales qui chargent leurs gouvernements et institutions de garantir bien-être et prospérité générale sont confrontées à d'énormes défis économiques, sociaux et politiques. À coup sûr, le marché du travail va demander de plus en plus de compétences en mathématiques, sciences, ingénierie et programmation informatique (filiales dites STIM). Les inégalités de revenus entre ceux qui détiennent ces compétences et les autres vont vraisemblablement s'accroître avec le temps. Pour toutes les sociétés, le défi consistera à permettre au plus grand nombre d'accéder aux compétences nécessaires et de saisir chaque opportunité de les améliorer au fil de leur vie professionnelle. Cela ne se fera pas sans une réévaluation approfondie des systèmes éducatifs nationaux. Des systèmes qui, actuellement, se concentrent presque exclusivement sur les jeunes, et ne se soucient souvent qu'après coup de ceux qui sont déjà actifs sur le marché du travail, laissant ainsi échapper des occasions de soutenir des programmes d'apprentissage vitaux tout au long d'une vie, pourtant sources de prospérité. Le changement s'impose partout, et d'autres fractures sont à prendre en compte comme celles entre les genres, les âges, l'accès au numérique en zone urbaine et non-urbaine. Si nous ne les comblons pas, elles se creuseront encore, en aggravant les inégalités de revenus, qui, à leur tour, pourraient déclencher des tensions sociales et politiques.

### **III. ÉCONOMIE NUMÉRIQUE ET SÉCURITÉ NATIONALE : LES CAS DE LA RUSSIE ET DE LA CHINE**

22. Dans les premières années d'internet, les cyberoptimistes voyaient dans la technologie les prémices d'une nouvelle ère de démocratie, de transparence et d'engagement citoyen, ainsi qu'une forme radicale d'ouverture des opportunités de marché à ceux qui en étaient jadis exclus. Ce n'est donc pas une surprise si bon nombre de ces optimistes de la première heure éprouvent désormais



un sentiment de trahison quand ils voient comment l'internet et les technologies numériques ont aidé des forces antidémocratiques à éroder les normes et pratiques démocratiques, propagé de fausses informations, facilité le vol de secrets industriels et de titres de propriété intellectuelle, dégradé la confidentialité, et donné aux régimes autoritaires des outils pour manipuler la politique dans leur propre pays comme à l'étranger.

23. Cette question constitue aujourd'hui une préoccupation majeure parmi les Alliés. Selon les États-Unis, l'opinion publique américaine a vivement été éprouvée par les efforts russes visant à influencer les élections américaines et à mener des opérations d'espionnage dans le pays. Devant l'ampleur du danger, le président Obama a déclaré l'urgence nationale pour affronter la menace. Les États-Unis ne sont pas la seule cible des Russes. En 2014, un groupe soutenu par la Russie, CyberBerkut, s'est immiscé dans le scrutin ukrainien. Il a brièvement paralysé le système de dépouillement des urnes et retardé le comptage (Hennessey, 2017). Alors candidat aux élections présidentielles françaises, Emmanuel Macron a lui aussi fait l'objet d'un piratage juste avant la fin de la campagne. Si de nombreux analystes attribuent cette attaque à la Russie, la France n'a jamais officiellement attribué les actes malveillants constatés sur son sol à un pays. La chaîne de télévision française TV5 Monde a dû interrompre ses émissions lorsque des pirates se sont fait passer pour des agents de l'État islamique (Ranger, 2018). Les États-Unis ont également accusé la Chine d'espionnage industriel à grande échelle, ainsi que de vols de propriété intellectuelle aux États-Unis et ailleurs, par l'utilisation de procédés numériques. Des pressions se sont exercées sur la Chine pour qu'elle s'engage auprès des États-Unis, de l'Australie, de l'Allemagne, du Canada et du Royaume-Uni à ne pas s'adonner au vol de secrets industriels, même si la plupart des analystes estiment que cela n'a pas résolu le problème.

24. Alors que les économies nationales se convertissent au numérique, et s'appuient de plus en plus sur des réseaux et des plateformes de vente en ligne basés sur internet, et que les biens de consommation eux-mêmes dépendent toujours plus d'internet tout en intégrant des technologies, comme l'intelligence artificielle, la vulnérabilité de l'économie de consommation entière au piratage malveillant, - voire à une défaillance systémique en cascade -, devient de plus en plus évidente. Les États et les entreprises doivent prendre en compte les risques de ce type, car le monde évolue vers une économie fondée sur un « internet des objets » entièrement interconnecté. Les chefs d'entreprise et les dirigeants politiques vont devoir prendre des mesures pour atténuer ces risques, notamment en installant des systèmes dissuasifs. La dissuasion pour sa part, exigera des systèmes de sécurité plus difficiles à neutraliser et des capacités de représailles permettant d'identifier et de punir les coupables.

25. À cet égard, il est intéressant de noter que le cybercommandement américain a coupé l'accès internet d'une notoire « usine à trolls » russe le jour des élections de mi-mandat, en novembre 2018. Ce fut le premier exemple connu de cybercampagne offensive à l'encontre de la Russie, le but étant cependant de préserver l'intégrité d'un important scrutin américain (Nakashima, 2019). Il est par ailleurs utile de chercher à incriminer les individus commettant des actes de cybercriminalité pour le compte de régimes hostiles, même si ces personnes sont hors de portée des poursuites judiciaires. Les États-Unis ont récemment accusé des Iraniens et des Russes dans ce contexte ; en guise de sanction, ils ont forcé la Russie à fermer deux représentations diplomatiques. L'objectif est de montrer que la Russie paiera le prix de ses immixtions. Il est clair que l'efficacité de ce type de mesures est renforcée lorsque des coalitions de pays sont activement engagées, comme ce fut le cas lorsque les États-Unis, le Royaume-Uni, le Danemark, la Lituanie, l'Estonie, le Canada et l'Australie ont imputé à la Russie les attaques du logiciel rançonneur *NotPety* (Ranger, 2018).

26. La révolution numérique change aussi la façon de faire la guerre. Les armées d'aujourd'hui sont obligées de se préparer aux éventuelles cyberguerres de demain. Elles n'ont pas le choix. Les outils numériques orientent les stratégies de guerre hybride et de guerre de l'information, tout en offrant de nouvelles cibles aux terroristes qui planifient des attaques asymétriques et potentiellement dévastatrices. Simultanément, le déploiement de l'intelligence artificielle va

profondément transformer le futur champ de bataille. À leur tour, ces changements entraînent une réévaluation du rapport entre les considérations de sécurité nationale de niveau étatique et le secteur privé. En effet, des entreprises toujours plus numérisées risquent fort de devenir le théâtre des hostilités. Si les prestataires de services critiques (énergie, eau, alimentation, etc.) et les facteurs du produit national sont exposés dans l'espace numérique, un belligérant pourrait aller très loin pour affaiblir son adversaire de manière décisive, à un stade critique du conflit. Par ailleurs, l'espace numérique se prête particulièrement bien au lancement d'attaques asymétriques. Les acteurs malveillants infra-étatiques chercheront presque inévitablement à maximiser dans cette arène l'impact politique de leurs attaques.

27. La vision de l'économie numérique et les ambitions de la Chine en la matière représentent un défi complexe pour l'Occident. Antagoniste politique de l'Ouest, la Chine est aussi un grand concurrent technologique et commercial - ce que n'est pas la Russie par exemple. Le défi présente donc de multiples facettes. D'abord, la Chine reconnaît que les leaders industriels de l'économie numérique bénéficieront d'avantages importants car ce sont eux qui établiront les normes, et réguleront l'utilisation et l'intégration des technologies dans l'économie mondiale. Les États-Unis ont bénéficié de cet avantage en tant que pionniers, mais à présent, c'est la Chine qui prétend ouvertement au leadership mondial pour les générations à venir. Le gouvernement chinois juge cette volonté essentielle pour la prospérité économique du pays, la sécurité nationale et la capacité du parti communiste chinois à manier les leviers du pouvoir étatique. Il a détaillé de manière explicite ses ambitions dans son agenda *Made in China 2025*. Ainsi, la Chine vise-t-elle notamment à conquérir des positions dominantes dans la fabrication des semi-conducteurs, la technologie 5G, l'intelligence artificielle, l'informatique quantique et les véhicules autonomes. Dans la plupart de ces domaines, la Chine a déjà fait des progrès mais elle reste très dépendante des semi-conducteurs fabriqués par les Occidentaux (Sanger, mai 2019). En 2018 par exemple, les importations chinoises de puces informatiques s'élevaient à quelque 300 milliards de dollars. Les nouvelles restrictions imposées par l'administration Trump aux ventes à la Chine vont à présent empêcher des entreprises comme QUALCOMM de vendre sur le marché chinois. Cela touche une des cordes sensibles de l'industrie numérique chinoise et il est donc fort probable que la Chine redouble d'efforts pour d'autant plus accentuer le développement de ses propres champions en la matière (Zhong). Cela pourrait être l'une des conséquences fortuites des restrictions commerciales.

28. La Chine veut se rendre imperméable aux éventuelles perturbations du marché provenant de l'étranger, telles que l'ordre du président Trump (finalement annulé) de cesser d'exporter des semi-conducteurs vers ZTE, une grande entreprise chinoise. Les autorités chinoises estimant que leur niveau actuel de dépendance était intolérable ont donné la priorité à la recherche sur les semi-conducteurs, investissant près de 150 milliards de dollars sur dix ans pour soutenir la recherche et le développement (R&D) dans ce domaine crucial. La Chine cherche par ailleurs à acquérir systématiquement des fabricants étrangers de circuits intégrés, notamment pour pouvoir accéder à des technologies développées dans d'autres pays. Les États-Unis, naturellement conscients du risque qu'ils courent en autorisant ces ventes, ont bloqué un certain nombre de tentatives dans ce domaine.

29. La Chine s'est très vite imposée comme un acteur majeur de l'économie numérique, non seulement en termes de matériel informatique, mais aussi, de plus en plus, en termes de logiciels. Les entreprises chinoises, par exemple, font partie des fournisseurs critiques de l'infrastructure de base qui sous-tend l'internet et les réseaux téléphoniques ainsi que des systèmes de commutation qui facilitent la communication entre l'humain et la machine. La Chine fabrique également des systèmes périphériques tels que les stations cellulaires qui relient les téléphones à d'autres appareils. Après s'être contentée de participer à la concurrence en tant qu'assembleur peu coûteux mais fiable des technologies développées en Occident, la Chine est elle-même, aujourd'hui, créatrice de technologies. Le marché domestique chinois, le plus vaste au monde, produit des technologies et des systèmes très concurrentiels sur les marchés internationaux. Plusieurs services de renseignement occidentaux s'inquiètent notamment de la mainmise que pourraient avoir des

entreprises chinoises sur le noyau des nouveaux réseaux de communication 5G. Cela a déclenché dans les pays alliés un débat lourd de conséquences sur des questions commerciales et de sécurité.

30. En deux décennies, la Chine a donc parcouru un chemin considérable dépassant de loin le stade de la simple production. Ses dirigeants veulent faire de l'économie numérique un des piliers de l'économie chinoise de demain. Le président Xi Jinping a annoncé l'objectif de son gouvernement : transformer la Chine en une « cybersuperpuissance » avec des industries dominant les marchés mondiaux.

31. Le gouvernement chinois entend aussi exercer une puissante influence sur le paysage réglementaire international (Segal, 2018). Dans ces conditions, la Chine va vraisemblablement exploiter sa puissance croissante sur les marchés pour projeter ses propres valeurs et intérêts sur le marché mondial. Manifestement, certaines de ces ambitions contrecarrent les intérêts et les valeurs de l'Occident. L'avènement de la Chine dans l'espace numérique est ainsi devenu, à l'international, une source croissante de tensions et de préoccupations sur le plan commercial et en matière de sécurité.

32. À plusieurs égards, la stratégie industrielle numérique de la Chine est pilotée par l'État, même si les grandes entreprises sont souvent privées. Comme nous le suggérons plus haut, le modèle Silicon Valley opère de bas en haut. C'est le produit d'excellentes universités, d'une concentration géographique des talents, d'un marché des capitaux privés qui récompense la prise de risque et de règles de marché qui autorisent un accès aisé, sans sanctionner l'échec. Ces conditions ont permis le genre de destruction créative qui caractérise le marché américain des technologies de pointe. Cela ne signifie pas que l'État n'a pas eu de rôle à jouer. Le département de la défense et la NASA, par exemple, ont contribué à stimuler la demande d'innovations, pour laquelle le secteur privé a répondu.

33. Quant au modèle chinois, il est très différent car il fait une large place à une planification étatique lourde, avec un degré beaucoup plus élevé d'affectation de capitaux décidée par l'État. Selon la législation chinoise, les sociétés nationales sont obligées de partager sur demande les données liées au renseignement avec les services de sécurité de l'État. L'administration Trump et plusieurs services de sécurité occidentaux invoquent cette loi dans leur mise en garde contre une confiance excessive dans Huawei, même si son fondateur, Ren Zhengfei, affirme avec insistance que sa société ne permettra pas au gouvernement chinois d'accéder aux données occidentales passant sur son réseau ni de fermer ce réseau en cas de crise internationale.

34. Paradoxalement, la Chine progresse vite dans le développement des équipements et logiciels nécessaires pour construire une économie de l'information. En même temps, elle cherche à contrôler, voire à limiter la circulation de l'information sur ces réseaux. Décidé à contrôler la liberté des échanges d'informations entre ses citoyens, l'État chinois a développé des techniques avancées pour filtrer les informations indésirables. Il a également acquis des technologies occidentales pour pouvoir se livrer à un cyberespionnage domestique massif, dont les techniques sont évidemment exploitées par les acteurs de la sécurité chargés de recueillir des informations bien au-delà des frontières chinoises. Non contente d'usurper des technologies, la Chine recourt aussi à des cybermoyens pour pratiquer l'espionnage traditionnel. Elle a par exemple pénétré par effraction dans les systèmes du Bureau de gestion du personnel américain et dérobé une mine d'informations concernant les fonctionnaires des États-Unis (Hennessey, 2017). Des pirates chinois ont également notoirement volé les plans du chasseur F-35 (Sanger, mai 2019). Les milieux occidentaux du renseignement craignent fort que la Chine n'utilise l'infrastructure même qu'elle vend à l'échelle internationale à des fins d'espionnage international.

35. La Chine s'oriente vers toujours plus de sophistication technique, de présence sur le marché et d'influence diplomatico-financière. Il est peu probable que ses rivaux occidentaux soient en mesure de l'arrêter. Au mieux chercheront-ils à canaliser l'avènement numérique de la Chine afin

qu'il serve les intérêts du marché mondial au sens large plutôt que ceux, beaucoup plus étroits, de l'élite dirigeante et industrielle chinoise. Naturellement, on peut en dire autant de la montée en puissance de la Chine en général. En un certain sens, ses cyberambitions ne sont qu'une déclinaison de ses aspirations à devenir une puissance mondiale. De plus en plus cependant, l'administration Trump fait tout pour isoler la Chine des marchés technologiques mondiaux – une position qui, selon de nombreux analystes, pourrait avoir des conséquences désastreuses sur le plan économique.

36. Le président Xi Jinping a créé une agence du cyberspace chargée non seulement de promouvoir le développement des cyberindustries, mais aussi de réserver à l'État et à lui seul la capacité de mobilisation politique par des voies numériques. En d'autres termes, le modèle fait de l'État un acteur essentiel du développement technologique, et en même temps l'arbitre ultime des contenus et de l'accès des citoyens à ceux-ci. Comme la Russie, le régime chinois veut que l'univers numérique renforce la souveraineté nationale et les groupes qui la gouvernent. Face à cela, les États-Unis et les pays occidentaux se sont, en général, toujours prononcés en faveur d'un internet mondial homogène, qui ne fasse pas l'objet d'entraves de la part des autorités politiques. Cela pourrait changer alors que les États-Unis observent avec appréhension les ambitions de la Chine et cherchent à l'écartier de la construction des réseaux de demain. Aujourd'hui, certains analystes préviennent qu'un « découplage » technologique et un « rideau de fer numérique » risquent de prélever un très lourd tribut sur l'économie mondiale (Ignatius, 2019). Particulièrement conscients des coûts potentiels de ce type de division, les gouvernements européens analysent dès lors avec plus de prudence comment la Chine pourrait s'inscrire dans ce développement ce qui, manifestement, crée des tensions avec Washington.

37. Xi Jinping veut s'assurer que la Chine pèse sur les futures normes internationales, tout en plaçant des équipements architecturaux de sa fabrique au niveau des concentrateurs, des nœuds et des lignes critiques de l'internet mondial. Ajoutons que son initiative des nouvelles routes de la soie, également appelée *Belt and Road Initiative* comprend un effort important de mise en place d'une « cyberroute » composée de câbles en fibre optique, de réseaux téléphoniques et de relais satellite. Des entreprises chinoises comme Alibaba et ZTE jouent un rôle central dans cette initiative. Elles ont signé des accords avec plusieurs gouvernements le long de cette route pour vendre des services et des équipements dans le cadre de ce réseau. Des efforts de même nature sont en cours dans certaines régions de l'Afrique (Segal, 2018). Accessoirement, si la Chine veut réduire sa propre dépendance aux produits, infrastructures et services numériques occidentaux, ce n'est pas seulement pour des raisons économiques, mais aussi pour se prémunir contre l'espionnage venu de l'Ouest et d'éventuelles cyberattaques.

38. En résumé, les Chinois ne se contentent pas de fabriquer des technologies occidentales : ils veulent aussi produire des technologies de pointe et des plateformes à l'échelle de toute l'industrie, conformément au plan *Made in China 2025*. Dans ce but, la Chine s'attache très activement à jouer un rôle dans le processus de standardisation. Elle a tout fait pour être au cœur de la définition des normes des réseaux 5G qui font actuellement leur apparition sur le marché mondial.

39. De son côté, l'administration Trump, très préoccupée par les aspirations et les méthodes chinoises, demande à certains de ses alliés et partenaires de ne pas collaborer avec le principal acteur chinois des télécommunications, Huawei, pour édifier l'infrastructure des réseaux téléphoniques de cinquième génération (5G), réseaux qui promettent une augmentation spectaculaire du débit et de la capacité des lignes au niveau mondial. D'après des représentants de l'administration Trump et de nombreux experts, l'utilisation de ces équipements ouvrirait l'accès à des informations critiques aux services de renseignement chinois. En mai 2019, l'administration a ordonné que les ventes de technologie américaine à Huawei fassent l'objet d'une autorisation gouvernementale. Google a donc été contraint d'arrêter de vendre sa technologie Android à Huawei, qui l'utilisait pour ses propres téléphones mobiles. Les quatre opérateurs de téléphonie américains - AT&T, Verizon, Sprint et T-Mobile - se sont engagés à ne pas utiliser de produits Huawei sur leurs

réseaux 5G (Nakashima, 2019). Les États-Unis ont également préparé un projet de loi interdisant aux entreprises américaines d'utiliser un quelconque équipement construit en Chine dans leurs réseaux de télécommunications.

40. La controverse a atteint l'opinion publique, alors que l'administration américaine s'engageait dans une guerre commerciale de surenchère et de représailles avec la Chine. Si certains considèrent les mesures prises contre Huawei comme un élément de ce conflit commercial, d'autres y voient plutôt une question de sécurité nationale en même temps qu'un signe de concurrence croissante pour la domination du marché au XXI<sup>e</sup> siècle. Le président Trump a toutefois laissé entendre qu'une résolution des tensions commerciales pourrait amener les États-Unis à alléger les restrictions imposées au fournisseur 5G chinois, ce qui signifie que les enjeux de sécurité pourraient ne pas être aussi importants qu'il le prétend. De fait, l'argument de la sécurité est moins défendable si l'on pense que la résolution des frictions commerciales générales ne ferait pas grand-chose pour apaiser les inquiétudes de ceux et celles qui se soucient de la sécurité américaine. Quoi qu'il en soit, Huawei a déposé devant un tribunal fédéral américain une requête pour que l'interdiction frappant ses équipements soit déclarée contraire à la Constitution (Fifield, 2019).

41. L'administration américaine a en effet fermement suggéré que les législateurs européens en fassent de même. Selon elle, les avantages que pourrait apporter la compétitivité économique et technologique des produits Huawei ne feront pas le poids face à ce que coûtera la sécurité si la Chine est en mesure d'accéder à l'information circulant sur les réseaux en cause. Cette opinion ne fait pas l'unanimité en Europe, où d'aucuns se demandent si l'Europe ne pourrait pas être tentée de travailler avec la Chine au cas où Trump leur imposerait comme seul choix « nous ou eux ». L'imposition récente de droits de douane américains sur un certain nombre de produits de base européens ne facilite pas les choses et sape la coopération commerciale transatlantique. Cela étant, les Européens n'ont pas très envie de s'aligner sur les positions des États-Unis à propos de la Chine, même s'ils partagent certains griefs avec eux. L'Europe et d'autres gouvernements amis n'ont pas apprécié non plus d'avoir été mis devant le fait accompli lorsque Washington a décidé seule, sans concertation préalable, des mesures à l'encontre de Huawei. Et l'on s'en étonnera d'autant plus que des sociétés comme Nokia, Samsung et Ericsson sont parmi les mieux placées pour remplacer Huawei, du moins pour certains composants d'un futur réseau 5G (Ignatius, mai 2019).

42. Alors que l'Australie et la Nouvelle-Zélande ont empêché certains opérateurs télécoms d'utiliser Huawei sur les réseaux 5G, et que le Japon a pratiquement exclu les Chinois, l'Europe s'est montrée beaucoup plus résistante aux pressions américaines. Bien que le cas Huawei suscite clairement des préoccupations en Europe, la question de son exclusion totale du marché européen ne recueille pas de consensus. Les services de renseignement britanniques, par exemple, ont récemment jugé que l'utilisation des équipements Huawei présentait des risques gérables moyennant certaines précautions, y compris le fait de demander à ce fabricant de resserrer ses propres normes de cybersécurité. Au Royaume-Uni, le débat est toujours en cours et les autorités n'ont pas encore pris de décision. Mais l'opérateur télécom britannique Vodafone et EE ont suspendu le lancement des smartphones 5G Huawei aussi longtemps que l'interdiction d'exportation américaine n'aura pas été clarifiée. Le chef de l'agence allemande de cybersécurité a récemment déclaré que l'Allemagne autoriserait Huawei à participer à son architecture 5G, si les instances chinoises apportaient des garanties supplémentaires quant à la sécurité des données (Chazan, 2019).

43. Convaincu par la qualité et le prix proposés par Huawei, le numéro un des opérateurs mobiles néerlandais, KPN, a choisi la société chinoise pour l'équipement de pointe de son réseau 5G. Selon certaines sources, le prix Huawei était 60% moins cher que celui d'Ericsson. KPN indique aussi que le « cœur » de son nouveau système sera fourni par une société occidentale (Nakashima, 2019). Certains prétendent que la compétitivité des prix de Huawei peut s'expliquer par les importantes subventions publiques dont la société chinoise bénéficie, sous la forme de prêts à taux réduit octroyés par des banques d'État, à la fois à la société pour couvrir en partie ses coûts de

R&D, mais aussi aux clients. Huawei peut aussi compter sur une part garantie du marché intérieur chinois, dont les revenus lui permettent ainsi d'abaisser les prix offerts aux clients étrangers. Aucune société occidentale ne jouit de tels avantages. Certains pays voudraient apparemment empêcher Huawei de construire les nouveaux systèmes de commutation, ce que l'on appelle aussi le « cœur » des réseaux numériques 5G, mais l'autoriseraient à jouer un rôle à la « périphérie », où l'on trouve notamment des antennes moins sensibles pour la transmission des signaux téléphoniques. Des responsables américains avertissent cependant que ces distinctions sont moins pertinentes dans la 5G et qu'une présence chinoise, même à la périphérie, pourrait poser de sérieux risques (Nakashima, 2019). En général, les pays européens restent très inquiets et se demandent combien « coûtera » la mise à l'écart de Huawei sur le marché. Ils n'envisagent certainement pas de gaieté de cœur de devoir troquer une architecture existante qui a fait ses preuves contre des substituts occidentaux plus coûteux et pas nécessairement fiables. Cette inquiétude est partagée par les fournisseurs ruraux aux États-Unis, qui utilisent des systèmes Huawei meilleur marché pour compenser l'absence d'échelle de marché dans les zones rurales américaines - un point sur lequel la direction de Huawei insiste clairement aujourd'hui (Fifield, 2019). Dans l'ensemble, les fournisseurs américains sont opposés à l'interdiction qui frappe Huawei.

44. La France examine également de près la question alors qu'elle commence à développer son réseau 5G. Le processus législatif est en cours. Le président de l'Arcep, le régulateur télécom, a annoncé récemment qu'il avait l'intention d'entamer la construction du réseau en 2020, bien que des inquiétudes persistent à propos d'Huawei. Certaines sociétés chercheront sans doute des alternatives, surtout depuis que l'administration Trump a décidé de bloquer le transfert de technologie vers le géant télécom chinois. Bruno Le Maire, le ministre de l'économie et des finances, a indiqué que la sélection des fabricants d'équipements télécoms 5G se fera notamment sur la base de critères de sécurité et de performance et qu'a priori, aucun candidat ne sera exclu (Lee).

45. Alors que les appels d'offres commencent pour les réseaux 5G, les États-Unis veulent que les considérations de sécurité restent au cœur des décisions d'achat. Les Américains refusent catégoriquement que la Chine devienne la plaque tournante mondiale de la 5G. Aux yeux de beaucoup, en effet, la 5G va révolutionner les communications numériques : elle ouvrira la voie aux villes intelligentes, aux véhicules autonomes, à une automatisation plus avancée ainsi qu'à des systèmes de gestion de stock encore plus intégrés, parmi bien d'autres applications. Cette seule liste, cependant, suscite l'inquiétude des experts en sécurité. Elle montre à quel point les systèmes seront vulnérables aux cyberattaques et au cyberespionnage en l'absence d'une protection adéquate.

46. Sur le plan économique aussi, on craint que le pays chargé de construire ces nouveaux réseaux en retire une position dominante dans la future concurrence. De l'avis de certains, les États-Unis mêlent délibérément leurs intérêts commerciaux à leurs motivations militaires et sécuritaires, encourageant leurs alliés à faire de même. La question s'est imposée en juillet 2018 comme le thème central des réunions *Five Eyes* sur le renseignement, à Halifax (Canada) : les pays participants ont décidé d'unir leurs forces pour empêcher la Chine d'installer des réseaux en Occident (Sanger et al., 26 janvier 2019).

47. Dans une certaine mesure, les soupçons de volonté d'hégémonie chinoise sur la 5G sont considérés dans le cadre plus large des tensions commerciales entre les États-Unis et la Chine (Sanger et al., 26 janvier 2019). Fin janvier 2019, le département américain de la justice a accusé Huawei et sa directrice financière, Meng Wanzhou, de mener une action sur plusieurs années pour dérober des secrets commerciaux, faire obstruction à une enquête judiciaire et éluder les sanctions à l'encontre de l'Iran. Bien que le système juridique américain soit totalement séparé de son agenda diplomatique, ces accusations ont naturellement été vues à travers le prisme des litiges commerciaux qui opposent l'administration Trump à la Chine et, plus largement, sa volonté d'exclure la Chine du marché de la cyberinfrastructure occidentale.

48. D'après certaines allégations américaines, Huawei aurait tenté de subtiliser des équipements de test aux laboratoires T-Mobile, dans l'État de Washington. T-Mobile est une société allemande dont le siège se trouve à Bonn. Les États-Unis ont demandé au Canada d'extrader Meng Wanzhou pour qu'elle réponde de ces accusations. Madame Meng, fille du fondateur et président de Huawei, Ren Zhengfei, est assignée à résidence à Vancouver en attendant l'audition d'extradition. L'incident a provoqué une crise diplomatique entre le Canada et la Chine. Cette dernière a récemment arrêté deux Canadiens pour des motifs douteux. Le litige s'est produit juste au moment où la Chine et les États-Unis entamaient des discussions officielles pour résoudre une série de frictions commerciales, menaçant la croissance économique des deux pays.

49. Bien entendu, la liste des préoccupations liées à la Chine ne s'arrête pas là. Le régime chinois a farouchement censuré des contenus internet jugés subversifs. Il a mis en garde les entreprises chinoises qui envisageraient d'héberger des sites encourageant un débat ouvert sur les affaires internationales, l'histoire et les questions militaires (Segal, 2018). Il exerce aussi de très fortes pressions sur les entreprises occidentales pour qu'elles appliquent ces restrictions. Apple, par exemple, a dû retirer les réseaux virtuels privés de ses appareils vendus en Chine : les autorités craignaient en effet que ces VPN ne servent à contourner le « grand pare-feu » chinois. Cette « grande muraille » de l'information est un ensemble de dispositifs technologiques et de règlements qui permettent à l'État de bloquer l'accès du public aux sites et contenus internationaux jugés dangereux. Ces mesures consistent notamment à limiter l'accès aux outils internet comme Google, Facebook et Twitter, à contraindre les entreprises étrangères à se conformer aux législations locales et à ralentir le débit dès que des citoyens chinois consultent des sites internationaux.

50. Le Bureau chinois de la sécurité publique gère aussi le projet « Bouclier d'Or », un système complet de surveillance et de censure dans les rues chinoises. Le programme contrôle les sites domestiques, les courriers électroniques et les recherches jugés politiquement subversifs. Les entreprises opérant dans le pays sont tenues de stocker les données en Chine, et non à l'étranger. Les réglementations de ce type sont naturellement conçues pour renforcer la capacité du gouvernement à contrôler l'économie numérique, à rassembler des renseignements, et à empêcher les entreprises d'aller là où les autorités n'apprécient pas qu'elles aillent. Lourde et pesante, cette politique est de nature à dissuader les investisseurs étrangers, qui jugent ces règles intrusives et inconfortables (Lund et Tyson, 2018). Le système pourrait discriminer une série d'entreprises numériques internationales, en violation des lois et des normes du commerce international. À terme, une réglementation aussi pesante pourrait entraver le développement de l'économie numérique chinoise. Les firmes étrangères déplorent que ces règles puissent faciliter le vol de leur propriété intellectuelle par les autorités chinoises. Selon un récent rapport de la commission sur la propriété intellectuelle, les États-Unis perdraient entre 225 milliards et 600 milliards de dollars par an à cause de ces violations, perpétrées majoritairement à l'instigation des opérateurs chinois (Flournoy et Sulmeyer, 2018).

51. Sur le front industriel, la volonté de la Chine est sans ambiguïté : devenir un leader des technologies numériques. À cette fin, elle a non seulement aligné ses services de renseignement sur cet objectif mais la part des dépenses publiques affectée à cette ambition n'a cessé de croître. Les investissements chinois dans la recherche et le développement ont augmenté de 20% par an en moyenne sur les 20 dernières années. Ils se situent actuellement à 233 milliards de dollars, soit 20% de la part des dépenses mondiales en matière de R&D. Ces ambitions ne sont pas complètement irréalistes, même si le pays a encore un long chemin à parcourir avant de pouvoir les réaliser. Au demeurant, la Chine produit plus de diplômés dans les filières STIM que n'importe quel autre pays du monde. Elle est aussi de plus en plus présente dans les publications académiques (Segal, 2018). Sur les trois dernières années, les entreprises chinoises ont également dépassé leurs homologues américaines dans le classement Nikkei des 50 premiers déposants de brevets pour l'intelligence artificielle (Okoshi, 2019).



52. Bien qu'elle ne compte pas parmi les premiers fournisseurs de produits numériques avancés et ne possède pas le même poids commercial que les États-Unis, la Chine ou l'Union européenne, la Russie a la capacité de tirer parti du numérique pour mener des opérations asymétriques exploitant la dépendance occidentale aux technologies et réseaux informatiques. La publication de courriers électroniques privés des collaborateurs d'Hillary Clinton durant la campagne présidentielle aux États-Unis, par exemple, a jeté le trouble sur les élections américaines. La confirmation officielle du rôle de la Russie n'est venue que plus tard, quand le Bureau du directeur des services américains du renseignement et le département de la sécurité intérieure ont publié un communiqué conjoint selon lequel la Russie avait tiré les ficelles dans le but d'influencer le scrutin (Hennessy, 2017). Le rapport Mueller a également confirmé la nature de la menace. En apparaissant au grand jour, la vulnérabilité d'une société démocratique aussi puissante que les États-Unis a provoqué une onde de choc dans la communauté des nations occidentales et contribué à faire prendre conscience que la malveillance du Kremlin à cet égard ne faisait plus de doute. Naturellement, les États-Unis sont loin d'être le seul pays manipulé de la sorte. Mais l'incident a prouvé que la Russie pouvait atteindre des objectifs importants par la voie informatique, y compris lorsqu'il s'agit de semer la discorde et de saper la confiance dans les institutions démocratiques. Le piratage de la campagne d'Hilary Clinton a révélé une incapacité à dissuader la Russie, un problème qui perdure à ce jour.

53. En un certain sens, la Russie a montré que la cyberguerre était de nature à conférer le même potentiel offensif que les autres à un pays qui n'est pourtant pas un premier contributeur à l'économie numérique mondiale. Cela dit, la Russie s'appuie sur des bases technologiques suffisamment avancées pour former des pirates capables de mener de grandes campagnes de désinformation, voire de désorganiser potentiellement des États, des entreprises et des sociétés, qui jouissent pourtant d'un niveau de sophistication technologique plus élevé. Il est intéressant de noter que le mauvais climat économique qui règne en Russie, entaché de corruption et de sanctions, a paradoxalement gonflé les rangs des cyberguerriers au service de l'État russe. Ces individus talentueux, en effet, n'ont guère d'autre choix économique que de pirater les réseaux occidentaux pour le compte du Kremlin.

54. Dans un pays autoritaire comme la Russie, en déclin démographique, l'univers numérique met tous les acteurs sur le même pied. Il crée un champ de bataille parfait pour la guerre asymétrique. Il permet de retourner les fruits du dynamisme de l'Occident et de son esprit d'innovation contre l'Occident lui-même, de l'affaiblir et de détériorer la confiance du public dans les institutions démocratiques.

55. Aujourd'hui, on connaît bien la piraterie russe, avec ses efforts systématiques pour entretenir l'incertitude parmi les électeurs via les réseaux sociaux, miner la confiance dans les institutions occidentales critiques, promouvoir des partis politiques et des candidats plus favorables aux intérêts russes. Une telle vulnérabilité, engendrée par l'économie numérique et l'omniprésence des réseaux sociaux, est, incontestablement, très inquiétante. Jusqu'à présent, le défi semble échapper aux solutions rapides, qui comprennent les appels adressés aux entreprises numériques pour qu'elles multiplient les efforts afin de filtrer ce type d'intervention.

56. Mais la menace va bien au-delà de la diffusion de fausses nouvelles et d'opérations de trolls. Ces dernières années, des pirates russes ont bloqué une aciérie allemande, interrompu les services de téléphonie et internet de près d'un million d'Allemands et attaqué à deux reprises le réseau électrique ukrainien (Knacke, 2018). Lors de ces attaques sur l'Ukraine, les agents russes ont aussi empêché l'accès à distance au système, compliquant sérieusement la réparation et prolongeant la panne. Il s'agissait d'opérations très sophistiquées et parfaitement planifiées. D'aucuns y voient des répétitions générales avant des cyberattaques plus vastes et dévastatrices, qui pourraient être déclenchées à des moments de fortes tensions internationales. D'une certaine façon, les deux attaques visant le réseau électrique ukrainien ont permis à la Russie à la fois de montrer ce dont elle est capable et de tester ses capacités offensives. Le message est lourd de menaces et particulièrement inquiétant pour les économies technologiquement avancées qui dépendent



fortement de systèmes numériques pour des services de base comme l'électricité, l'eau, les transports ou les communications.

57. Un problème plus tangible réside toutefois dans le piratage russe d'infrastructures occidentales vitales. On a par exemple décelé dans les systèmes énergétiques nord-américains et européens des logiciels malveillants latents, qui pourraient potentiellement stopper la production d'électricité en temps de crise. En 2014, le conseiller américain pour les questions de sécurité nationale a annoncé la découverte, dans des endroits critiques de l'infrastructure vitale des services aux collectivités des États-Unis, de maliciels apparemment développés en Russie. La sécurité de ces systèmes varie considérablement. Mais à cause de leurs étroites interconnexions, un seul point faible peut affecter en cascade l'ensemble du dispositif. Pire encore : comme il est souvent impossible de forcer une intervention manuelle sur ces systèmes, une attaque numérique pourrait littéralement les paralyser sur une période prolongée.

#### **IV. SÉCURITÉ DES DONNÉES, CONFIDENTIALITÉ ET RÉGLEMENTATION D'INTERNET : PERSPECTIVE EUROPÉENNE ET DIVERGENCES TRANSATLANTIQUES**

58. L'Europe pratique un modèle d'investissement dans le numérique très différent de ce qui se fait aux États-Unis. Dans une certaine mesure, cela a influencé le développement des industries numériques européennes. En Europe, les marchés de capitaux sont principalement axés sur des entreprises existantes plutôt que sur des entreprises émergentes. Le système est moins souple que son homologue américain lorsqu'il s'agit de financer des startups. Il n'en reste pas moins que l'Europe est l'un des principaux consommateurs de services numériques et virtuels. C'est aussi un grand producteur de technologies numériques, sans égaler pour autant l'échelle et l'étendue du marché américain.

59. L'Europe apporte sur le marché ses spécificités culturelles, notamment, et c'est important, une préférence généralisée pour la protection de la vie privée et des données, ce qui a déjà suscité quelques désaccords avec les États-Unis, qui semblent moins scrupuleux à cet égard. Le Règlement général sur la protection des données de l'UE incarne les priorités de l'Union européenne en matière de réglementation de cette technologie. Il est devenu l'un des principaux points de discorde dans les relations commerciales transatlantiques actuelles. Il peut arriver que certaines prédispositions culturelles marquent de leur empreinte les politiques commerciales nationales ce qui, à son tour, peut se muer en point de désaccord sur le plan international. Les dernières réglementations de l'UE en matière de protection des données tiennent largement compte des exigences des populations, soucieuses de préserver leur vie privée. Les États-Unis commencent à évoluer en ce sens, mais beaucoup plus lentement qu'en Europe. Cela peut s'expliquer, en partie, par le fait qu'on y trouve certaines des sociétés numériques les plus puissantes au monde ; celles-ci pèsent indéniablement dans l'arène politique et entretiennent des relations avec le gouvernement pour s'opposer au changement. Il se peut également que l'opinion publique américaine soit moins préoccupée par les questions de vie privée, une attitude confirmée par des sondages comparatifs. Mais les choses pourraient changer notamment à cause de l'ingérence russe prononcée dans les élections américaines, de l'usurpation de plus en plus fréquente de données personnelles, des révélations récentes concernant l'importance du partage de données personnelles (y compris des messages privés) entre sociétés, et de la prolifération de fausses informations ou d'informations fallacieuses visant à attiser les désaccords sociaux et politiques. Face à tous ces facteurs, l'inquiétude grandit et la question se pose de plus en plus de savoir si laisser ces marchés aux seules mains de ces mécanismes sert réellement l'intérêt public. Cette évolution des mentalités pourrait être le signe précurseur d'une nouvelle ère de réglementations dans un domaine visiblement sous-réglémenté jusqu'à présent : le marché numérique américain (Gibson, 2017).

60. Mais ces réglementations nationales contradictoires peuvent aussi être considérées comme une forme masquée de protectionnisme. Les nouvelles réglementations de l'UE concernant le numérique sont devenues une source de friction dans les échanges commerciaux. Alors que les États-Unis commencent à réfléchir à de nouveaux régimes législatifs, ils seraient bien avisés de se concerter étroitement avec leurs partenaires de l'UE pour garantir, autant que possible, un certain niveau de cohérence, au-delà des frontières, sur le plan des réglementations.

61. Le RGPD s'appuie sur un grand principe : la confidentialité des données du citoyen est un droit fondamental. Le texte en dégage un ensemble de règles régissant l'utilisation des données suivant ce principe, non sans tenir compte des intérêts légitimes des entreprises et des États. En d'autres termes, il cherche à trouver un équilibre entre les différentes parties prenantes. Ces règles ont pour but de protéger les informations privées contre toute utilisation abusive par les États ou les entreprises et à donner aux citoyens un droit de regard important sur la façon dont leurs données personnelles sont utilisées. Ainsi, les données recueillies ne peuvent être utilisées que pour une fin limitée et explicite, contrairement aux pratiques de nombreuses entreprises qui conservent indéfiniment les données et en font ensuite, sans avertir les personnes concernées, un usage qui pourrait être considéré comme fallacieux, voire dangereux pour la démocratie, comme dans le cas du scandale de *Cambridge Analytica*. Ajoutons que la nouvelle réglementation européenne s'applique directement à l'échelon national. Elle peut être invoquée devant les tribunaux nationaux sans référence à la législation locale car tous les États membres sont tenus par le RGPD (Dixon, 2018). Les nouvelles règles sont extraterritoriales, en ce sens qu'elles s'appliquent aux entités non-UE opérant dans le cyberspace européen. Si des données sont transférées de l'UE vers l'étranger, ces entités étrangères doivent se conformer à la réglementation. Toute organisation (médias, entreprises privées, services médicaux, universités...) traitant des données à caractère personnel est soumise à ces mesures de protection de la confidentialité. Les règles régissent strictement l'utilisation des données personnelles. Elles exposent en grandes lignes le droit des individus à contrôler leurs données personnelles. Ceux-ci peuvent désormais exiger l'effacement de leurs données dans les fichiers des entités précitées. Le but est d'imposer des limites à la collecte de données, de renforcer leur sécurité et de rééquilibrer une relation jusqu'à présent très asymétrique entre le consommateur et le producteur. Les entités doivent signaler sans délai toute violation de la confidentialité. Les régulateurs ont reçu un pouvoir d'injonction. Ils peuvent désormais infliger des amendes considérables aux entités qui ne respectent pas ces règles. Celles-ci présentent aussi une marge d'interprétation permettant aux magistrats d'exercer leur discernement en fonction de la nature de l'infraction (Dixon, 2018).

62. La portée extraterritoriale du RGPD a des répercussions internationales, notamment sur le plan de la protection de la vie privée, comme cela a déjà été clairement démontré. Le Japon et l'Argentine, par exemple, ont eu tôt fait d'adopter leurs propres règles de confidentialité, alignées sur celles de l'Europe. D'autres pays ont commencé à adapter leurs propres règles dans le même esprit. Mais il y a eu aussi des obstacles diplomatiques, notamment dans les relations avec l'administration Trump. Le président américain a qualifié les nouvelles règles européennes de barrière commerciale visant expressément le modèle économique des plateformes américaines et une réglementation peu contraignante. Notons que Google et Facebook ont dégagé les ressources nécessaires pour se préparer à la réglementation et s'y conformer, tandis que des acteurs plus petits, surtout en Europe, ont vu dans cette réglementation un défi beaucoup plus ardu et coûteux à relever. Concrètement, de grands noms du marché ont ainsi pu consolider leur position lorsque certains plus petits opérateurs de publicité en ligne, par exemple, se sont retirés, découragés par le coût de la mise en conformité (Cerulus et Scott, 2018).

63. Comme ce projet de rapport l'a déjà suggéré, les conceptions de bonne gouvernance d'internet sont aussi nombreuses que variées. Fidèles à leur vision d'un internet essentiellement autorégulé, les États-Unis estiment qu'il appartient à l'industrie elle-même de tenir les rênes de la gouvernance, avec l'appui d'organes techniques, de la société civile, et dans une moindre mesure, des gouvernements nationaux. Tout le monde, cependant, ne partage pas cette vision. La Chine, par

exemple, veut une gouvernance centralisée, aux mains de l'État (pour toutes les raisons déjà évoquées plus haut). Elle a vivement insisté pour que la gouvernance soit confiée aux Nations unies afin que les États puissent jouer un rôle pivot dans la réglementation. La Chine presse les entreprises numériques occidentales d'appliquer ses propres règles en échange de l'accès au marché chinois, même si la conception chinoise de l'ouverture et de la liberté d'expression s'oppose fondamentalement à l'interprétation occidentale. Certaines sociétés américaines comme Facebook réclament même un certain degré de réglementation afin d'alléger la charge que représente le développement de protocoles internes qui font encore l'objet de critiques et risquent de mettre en péril ces entreprises sur le plan juridique ou d'entacher leur réputation. Une réglementation leur procurerait un degré minimal de certitude, tout en les protégeant lorsque leurs services sont piratés à des fins malveillantes.

## V. CONCLUSIONS

64. L'économie numérique déclenche, dans l'économie mondiale, une révolution fondamentale qu'on n'arrêtera plus, mais la situation doit être mieux gérée. Chercher des modèles dans le passé n'est pas une option. Un changement économique révolutionnaire exige de nouveaux paradigmes dans les réglementations publiques ainsi qu'une collaboration internationale. Ce dernier aspect est particulièrement important. Personne ne peut relever à lui seul le défi réglementaire. Les démocraties doivent donc travailler de concert pour affronter à la fois la concurrence économique et les défis posés sur le plan de la sécurité numérique et de l'économie par des rivaux aux objectifs politiques, sociaux et internationaux très divergents. L'Union européenne et les États-Unis doivent intensifier leur coopération sur tout un éventail de questions réglementaires et autres, soulevées par l'avènement de l'économie numérique. Ces deux partenaires doivent agir en gardant à l'esprit leurs valeurs sociétales communes : défense des normes et institutions démocratiques, protection des droits individuels y compris la confidentialité, défense des intérêts de la sécurité nationale et collective, prévention des monopoles commerciaux, taxation des entités opérant au-delà des frontières de sorte à être en mesure de se soustraire au paiement d'impôt, et dissuasion des cyberattaques (Dixon, 2018).

65. Les sociétés occidentales doivent aussi se préparer soigneusement à fonctionner dans une économie numérique en évolution constante et rapide. Cela demande de la flexibilité, un bagage mathématique et scientifique solide à tous les niveaux de la société, ainsi qu'un esprit d'entreprise, de l'imagination et de la collaboration, sans parler de bien d'autres compétences encore. Les systèmes éducatifs devront améliorer l'enseignement des branches STIM à tous les élèves de tous âges, pour que ce domaine ne soit pas exclusivement réservé à une élite de mandarins. Ce sont en effet ces compétences-là qui garantiront demain la sécurité de l'emploi. Il faudra aussi que les écoles encouragent plus systématiquement la réflexion indépendante, l'entrepreneuriat, l'aptitude à anticiper le changement de manière innovante et la capacité à discerner les données volontairement faussées. Les écoles qui ne parviendront pas à inculquer aux enfants un certain degré de scepticisme sur le monde numérique vouent ces derniers à se faire exploiter tout au long de leur vie. Les sociétés capables de transmettre ces facultés indispensables à leurs citoyens prospéreront dans la nouvelle économie. Celles qui n'y parviendront pas se feront distancer et seront la proie de politiciens démagogues accusant les autres d'être la cause de leurs problèmes nationaux. De la même manière, les sociétés devront s'habituer à faciliter le passage des anciennes industries aux nouvelles. À cette fin, il faudra améliorer l'éducation tout au long de la vie, ainsi que les systèmes de soutien économique et social aux personnes en transition professionnelle.

66. L'Alliance atlantique est avant tout une alliance fondée sur des valeurs : ses membres partagent dans une large mesure une vision commune de l'importance des libres marchés et du besoin constant d'innovation. Les pays de l'Alliance ont donc toutes les raisons de collaborer à la mise sur pied d'une économie numérique ouverte, libre, sûre, flexible, capable d'habiliter les individus et de les aider à améliorer leur vie. Nos pays doivent avoir confiance dans leurs convictions

et se préparer à promouvoir ces valeurs face à la Chine ou à la Russie, qui voient dans l'espace numérique des instruments pour asseoir le pouvoir de leur régime. Aucun de ces pays ne devrait être en mesure d'imposer les normes de l'internet mondial. Les sociétés occidentales ont intérêt à se méfier de la propension de ces États à exploiter ces technologies pour limiter la liberté des individus, recueillir des renseignements, manipuler la politique et plus généralement miner les intérêts de sécurité des Alliés.

67. Vu la rapidité du changement technologique et l'évolution dans la manière d'utiliser internet (et d'en abuser), il est primordial d'actualiser les réglementations. Mais tenter de réglementer ces secteurs d'activité revient à viser une cible mobile. Un dialogue constant entre l'industrie, les groupements de consommateurs, les gouvernements et les experts en sécurité pour trouver le juste équilibre entre innovation, dynamisme et sécurité est nécessaire. Pour régir le commerce international en ligne, nous avons besoin de meilleures règles, autant pour faciliter cette forme d'échanges que pour veiller à la protection du consommateur. Ce point est particulièrement important pour les petites et moyennes entreprises et devrait figurer à l'agenda du commerce transatlantique (Burwell, 2018).

68. Des efforts bien plus concertés sont nécessaires pour protéger une infrastructure vitale toujours plus tributaire de la technologie numérique contre des opérations de reconnaissance et des cyberattaques. Des systèmes de dissuasion doivent être installés afin que les pays soutenant l'implantation de virus dans des infrastructures vitales soient confrontés aux très graves conséquences de leurs actes, y compris par l'imposition de sanctions dures ou une éventuelle contre-attaque. L'OTAN a un rôle à jouer à cet égard. Les enjeux sont d'une importance cruciale : ces systèmes jouent un rôle central dans la cohésion et le fonctionnement de base de nos sociétés. Si un simple clic suffit pour les mettre à l'arrêt, le degré de vulnérabilité est manifestement inacceptable et il faut y remédier. Cela nécessitera des investissements substantiels, non seulement de la part des États, mais aussi du secteur privé. Ce dernier, en effet, semble de plus en plus vulnérable aux cyberattaques qui tentent de paralyser les économies ou de dérober la propriété intellectuelle ou des actifs tangibles. Cette vulnérabilité va devenir d'autant plus importante que les marchés de la consommation seront connectés à ce que l'on appelle l'« internet des objets ». À bien des égards, le secteur privé est nettement plus fragile que les organisations militaires ou les réseaux du secteur public. Tout bien considéré, à quoi sert-il de construire une défense conventionnelle et nucléaire crédible si l'ennemi peut détruire furtivement les infrastructures critiques, indispensables à la cohésion et à la cohérence nationales ?

69. Les réseaux sociaux doivent endosser des responsabilités supplémentaires. Ils sont les gardiens d'une riche mine d'informations privées qui, entre de mauvaises mains, pourrait aisément et rapidement être transformée en arme par ceux qui ne veulent pas du bien à nos sociétés démocratiques. Ces entreprises doivent s'attacher à bien mieux protéger les informations de leurs clients, même si cela occasionne des coûts et empiète sur leurs bénéfices. Il est important d'identifier les risques que l'inaction fait peser sur la sécurité collective. Les responsabilités de ces entreprises, d'ailleurs, dépassent largement la défense de la confidentialité lorsque l'on sait que les réseaux sociaux sont devenus les vecteurs d'une propagande terroriste et antioccidentale malveillante, une source d'informations fabriquées de toutes pièces pour produire un impact politique et social maximal. Cette technologie révolutionnaire a aussi créé de nouvelles vulnérabilités sociétales, ce qui appelle à adopter des approches plus proactives pour tenter de résoudre ce problème. La Russie s'est montrée particulièrement active en tentant d'influencer notre système politique par des moyens numériques. La Chine, l'Iran et d'autres États (ainsi que d'autres acteurs infra-étatiques) suivent avec une grande attention les agissements russes. Cela exige une réaction collective et une capacité démontrée d'identifier et de punir les auteurs de tels actes.

70. Les entreprises privées doivent faire partie de la solution à la menace. La société Microsoft, par exemple, a fait appel au système judiciaire américain pour qu'il bloque les domaines des pirates russes associés au dénigrement dans la campagne Clinton et s'en est prise également aux pirates

nord-coréens, entre autres. Elle a cherché à faire jouer la loi américaine pour limiter l'espace dans lequel ces pirates opèrent et étudie actuellement les moyens de réagir plus rapidement pour enrayer de telles attaques (AP-OTAN, juin 2019).

71. Un effort beaucoup plus concerté s'impose en effet pour dissuader des pays aux intentions hostiles de poursuivre ces pratiques. Tout pays qui ne respecte pas les processus et la culture démocratiques des Alliés s'expose à de lourdes sanctions. Bien que l'on ait assisté à un effort de codification des normes de bonne cyberconduite au sein du G-7 et du G-20, il n'est évidemment pas facile de dissuader les « mauvais » acteurs de mener des actions répréhensibles dans le cyberspace. Il faut que ces normes deviennent des règles *de facto*, dont la violation entraînera de graves conséquences, y compris des mesures de rétorsion. Les États-Unis ont sanctionné la Russie pour ingérence électorale, et fermé une usine à trolls en prévision de leurs importantes élections de mi-mandat. C'est probablement dans ce sens que les efforts à venir devront aller pour encourager les bons comportements.

72. Des mesures bien plus fortes seront par ailleurs nécessaires pour lutter contre l'usurpation de la propriété intellectuelle, tremplin virtuel des stratégies économique et technologique chinoises à long terme. Si les Chinois continuent de violer la lettre et l'esprit de la protection des brevets, la communauté internationale, et en particulier les créateurs de propriété intellectuelle, doivent se préparer à exiger des malfaiteurs une indemnisation bien plus élevée en guise de représailles. La Chine tire d'énormes bénéfices du système commercial international, à la hauteur bien sûr de la contribution qu'elle y apporte. Ce pays est en effet devenu un acteur incontournable sur le marché (Laskai et Sacks, 2018). Mais s'il continue de saper les règles du jeu, en affaiblissant l'avantage comparatif critique des sociétés post-industrielles dynamiques et orientées sur les services, celles-ci doivent s'apprêter à repenser les éléments de leurs relations commerciales avec la Chine. En agissant collectivement plutôt qu'unilatéralement, elles accroissent leur force de frappe. Certains estiment en effet regrettable que les États-Unis, leader de la libéralisation du commerce mondial, se soient lancés tous azimuts à l'assaut de l'ordre commercial mondial, alors qu'ils auraient pu œuvrer de manière efficace avec leurs alliés pour relever le défi chinois.

73. Simultanément, les forces de sécurité de l'OTAN doivent développer des capacités de représailles offensives dans le cyberspace, dans le cadre du dispositif général de dissuasion. Les sanctions ne suffiront pas toujours, à elles seules, à décourager ceux qui sont bien décidés à attaquer l'Occident, particulièrement en temps de crise internationale. L'Occident doit être capable de faire très mal à un régime ou à un acteur infra-étatique qui veut paralyser des infrastructures occidentales vitales, dérober nos propriétés intellectuelles ou semer la discorde dans nos sociétés et nos systèmes politiques (Sulmeyer, 2018). Cette capacité doit permettre notamment de frapper préventivement les pirates avant qu'ils ne s'attaquent à une infrastructure occidentale critique, lancent des campagnes de désinformation ou ne volent des informations vitales. Il est essentiel de pouvoir surprendre et paralyser l'ennemi. La détermination à s'engager dans de telles actions préventives sera aussi clairement annoncée aux adversaires potentiels, et nous devons réfléchir davantage à la meilleure manière de maîtriser tout risque d'escalade, pour ne pas déclencher une cyberguerre totale, voire pire. De toute évidence, la crédibilité reposera sur une capacité défensive bien développée et une résilience qui a fait ses preuves. Il y a par ailleurs aussi des progrès à faire en termes de criminalistique numérique pour identifier plus vite et plus précisément les attaquants, et punir les coupables d'attaques malveillantes. À cet égard, l'OTAN constitue une excellente enceinte de concertation transatlantique sur ces questions essentielles.

74. Le renforcement de la sécurité doit passer par des incitations. L'instauration de normes de sécurité plus strictes et de redondances dans l'espace numérique doit devenir une condition obligatoire pour survivre en cas d'attaque. Des programmes d'inspection doivent voir le jour afin de déterminer constamment si les infrastructures vitales ont été compromises et si les défenses sont de nature à répondre aux menaces actuelles et futures (Knacke, 2018). Il en résultera inévitablement

une augmentation du coût des technologies et des services de base, mais il faut le voir, essentiellement, comme le prix d'une assurance pour augmenter ses chances de survie.

75. Après une cyberattaque, les institutions publiques et les entreprises privées doivent faire preuve d'une plus grande ouverture envers le public. C'est le meilleur moyen pour développer la résilience et une culture de vigilance largement ancrée face à cette nouvelle menace.

76. Il ne sera pas moins essentiel de former une nouvelle génération d'experts en sécurité numérique, prêts à assumer des rôles plus proactifs dans nos systèmes de défense informatique collective. Le besoin en experts concerne à la fois le secteur public et privé. Mais c'est plus facile à dire qu'à faire. Les systèmes éducatifs doivent améliorer la formation à ces compétences complexes, dont beaucoup deviendront indispensables sur le marché du travail au sens large durant les décennies à venir. Cela exigera des investissements ainsi qu'un nouveau regard créatif sur les systèmes d'enseignement nationaux, du primaire à l'université. Nous aurons tout autant besoin de systèmes permettant de former que de reconvertir les adultes.

77. Il faut réfléchir plus sérieusement à la manière de protéger des élections démocratiques contre toute cyberattaque. Dans cette optique, il s'agit notamment de rendre les sociétés démocratiques plus résilientes face à la prolifération de la désinformation. Il est essentiel de pouvoir comprendre et déchiffrer le numérique. Les jeunes devraient être mieux équipés pour faire la distinction entre de vraies nouvelles et de la propagande ou de la désinformation. Les outils techniques aussi peuvent être utiles. « Épingler » les sites douteux où le détournement de l'information est flagrant et appliquer un système de notation global pourraient permettre au consommateur d'évaluer la fiabilité de l'information présentée sur ces sites. Il faut aussi mieux sécuriser la mécanique électorale même et recourir au chiffrement pour éviter les fraudes. Des bulletins de vote en papier redondants peuvent toujours servir de recours en cas de piratage ou de résultats particulièrement douteux.

## BIBLIOGRAPHIE

- ABC News, "Chinese authorities use "gait surveillance to identify people by their body shape and walk, 6 novembre 2018  
<https://www.abc.net.au/news/2018-11-06/chinese-gait-recognition-tech-ids-people-by-how-they-walk/10469974>
- AP-OTAN, rapport de mission, Seattle, juin 2019 (bientôt disponible sur [www.nato-pa.int](http://www.nato-pa.int))
- Associated Press, "The Latest: Huawei: US Actions Should Worry Other Firms Too," published in The New York Times, 21 mai 2019.
- Bockel, Jean-Marie, rapport d'information au nom de la commission des affaires étrangères, de la défense et des forces armées, cybersécurité, Rapport du Sénat N. 681, Session extraordinaire de 2011-2012.
- Burwell, Frances, G., "Making America First in the Digital Economy: The Case for Engaging Europe," The Atlantic Council, 8 mai 2018  
<https://www.atlanticcouncil.org/publications/reports/making-america-first-in-the-digital-economy-the-case-for-engaging-europe>
- Cerulus, Laurens and Mark Scott, "Europe's new privacy rules: 1 month in, 7 takeaways-Here's what's already changed on the world wide web," Politico, 25 juin 2018,  
<https://www.politico.eu/article/gdpr-europe-new-privacy-rules-7-takeaways/>
- Chazan, Guy, "German cyber security chief backs 5G "no spy" deal over Huawei," Financial Times, 28 février 2019, <https://www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663>
- Dixon, Helen, "Regulate to Liberate: Can Europe Save the Internet?," Foreign Affairs, 14 août 2018,  
<https://www.foreignaffairs.com/articles/europe/2018-08-13/regulate-liberate>
- Fifield, Anna, "Huawei files motion to block U.S. ban, calling it an affront to global human rights," The Washington Post, 20 May 2019, [https://www.washingtonpost.com/world/huawei-files-motion-to-block-us-ban-calling-it-an-affront-to-global-human-rights/2019/05/29/fac5ce3e-81bb-11e9-9a67-a687ca99fb3d\\_story.html?utm\\_term=.96455fd9460f](https://www.washingtonpost.com/world/huawei-files-motion-to-block-us-ban-calling-it-an-affront-to-global-human-rights/2019/05/29/fac5ce3e-81bb-11e9-9a67-a687ca99fb3d_story.html?utm_term=.96455fd9460f)
- Flournoy, Michele, and Michael Sulmeyer, "Battlefield Internet: A plan for Securing Cyberspace," Foreign Affairs, septembre/octobre 2018,  
<https://www.foreignaffairs.com/articles/world/2018-08-14/battlefield-internet>
- Fouquet, Helene and Marie Mawad "Huawei Woes Multiply as France Risks Becoming Next Challenge," Bloomberg, 14 décembre 2018, <https://www.bloomberg.com/news/articles/2018-12-14/huawei-woes-multiply-as-france-risks-becoming-its-next-challenge>
- Gans, Joshua, "Is social graph portability workable," Digitopoly, [https://digitopoly.org/2017/07/03/is-social-graph-portability-workable/amp/?fbclid=IwAR1IKnF7oSOqFVn9X7wm-Xw8Cdb9XCyCydibQX\\_xj6WCjRKUY26jJiNbKno](https://digitopoly.org/2017/07/03/is-social-graph-portability-workable/amp/?fbclid=IwAR1IKnF7oSOqFVn9X7wm-Xw8Cdb9XCyCydibQX_xj6WCjRKUY26jJiNbKno)
- Gibson, William E. "Online privacy a major concern, AARP Survey shows," AARP, 17 mai 2017  
<https://www.aarp.org/home-family/personal-technology/info-2017/survey-shows-online-privacy-concerns-fd.html>
- Greenberg, Andy, "The Untold Story of NotPetya, the most Devastating Cyberattack in History," 22 août 2018,  
<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
- Hennessey, Susan, "Deterring Cyberattacks: How to Reduce Vulnerability," Foreign Affairs, Vol. 96, No. 6, novembre/décembre 2017.
- Hughes Chris, "Its Time to break up facebook, the New York Times, 9 May 2019,  
<https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html>
- Ignatius, David, "Trump loves walls. But he should be careful about a digital barrier with China," The Washington Post, 21 mai 2019, [https://www.washingtonpost.com/opinions/global-opinions/trump-loves-walls-but-he-should-be-careful-about-a-digital-barrier-with-china/2019/05/21/7280a146-7c13-11e9-a5b3-34f3edf1351e\\_story.html?utm\\_term=.de83235f0fec](https://www.washingtonpost.com/opinions/global-opinions/trump-loves-walls-but-he-should-be-careful-about-a-digital-barrier-with-china/2019/05/21/7280a146-7c13-11e9-a5b3-34f3edf1351e_story.html?utm_term=.de83235f0fec)
- Knacke, Rob, "Defending the U.S. Electricity Grid from Russian hackers," Foreign Affairs, 19 juillet 2018,  
<https://www.foreignaffairs.com/articles/north-america/2018-07-19/next-cyber-battleground>

- Laskai, Lorand and Samm Sacks, "The Right Way to Protect America's Innovation Advantage," Foreign Affairs, 23 octobre 2018.
- Lee, Jason, "France to push ahead with 5G launch despite Huawei problems, 21 mai 2019, RFI, <http://en.rfi.fr/france/20190521-france-go-ahead-5g-launch-planned-head-telecoms-watchdog>
- Lund, Susan and Laura Tyson, "Globalization Is Not in Retreat: Digital Technology and the Future of Trade," Foreign Affairs, mai/juin 2018, <https://www.foreignaffairs.com/articles/world/2018-04-16/globalization-not-retreat>
- Mayer-Schoenberger and Thomas Range, "A Big Choice for Big Tech," Foreign Affairs, Vol. 97, Number 5, septembre/octobre 2018.
- Nakashima, Ellen, "U.S. Cyber Command operations disrupted Internet access of Russian troll factory on day of 2018 midterms," The Washington Post, 27 février 2019, [https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9\\_story.html?utm\\_term=.dc3b16e9ea56](https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?utm_term=.dc3b16e9ea56)
- Nakashima, Ellen, "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible," The Washington Post, 28 mai 2019 [https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe-and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661\\_story.html?utm\\_term=.37da7bc3a3ba](https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe-and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html?utm_term=.37da7bc3a3ba)
- OCDE, Perspectives économiques, mai 2019, "Les incertitudes liées aux échanges freinent la croissance mondiale," <http://www.oecd.org/fr/eco/perspectives-economiques/>
- Okoshi, Yuki, "China overtakes US in AI patent rankings," Nikkei Asian Review, 10 March 2019, <https://asia.nikkei.com/Business/Business-trends/China-overtakes-US-in-AI-patent-rankings>
- Ortiz-Ospina, Esteban, Diana Beltekian and Max Roser, "Trade and Globalization," Our World in Data, octobre 2018 <https://ourworldindata.org/trade-and-globalization>
- Richmond, Shane, "US CLOUD Act raises new data privacy issues," Verne Global, 12 juillet 2018, <https://verneglobal.com/blog/us-cloud-act-raises-new-data-privacy-issues>
- Ranger, Steve, "Can Russian Hackers be Stopped: Here's why it might take 20 years," Tech Republic. 15 juin 2018, <https://www.techrepublic.com/article/can-russian-hackers-be-stopped-heres-why-it-might-take-20-years/>
- Rosemain, Mathieu, Gwenaëlle Barzic, and Elizabeth Pineau, "French Senate rejects tougher telecoms controls despite U.S. Huawei warning," Reuters, 6 février 2019, <https://www.euronews.com/2019/02/06/french-senate-rejects-tougher-telecoms-controls-despite-us-huawei-warning>
- Ross, Wilbur, "EU data privacy laws are likely to create barriers to trade," Financial Times, 30 mai 2018, <https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c>
- Sanger, David E., "Trump Wants to Wall Off Huawei, but the Digital World Bridles at Barriers," The New York Times, 27 mai 2019, <https://www.nytimes.com/2019/05/27/us/politics/us-huawei-berlin-wall.html>
- Sanger, David, Julian Barnes, Raymond Zhong and Marc Santora, "In 5G Race with China, U.S. Pushes Allies to Fight Huawei," New York Times, 26 janvier 2019, <https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html>
- Sanger, David, Katie Benner and Mathew Goldstein, "U.S. charges Huawei and Top Executive with Breaking American Laws," The New York Times, 28 janvier 2019, <https://www.nytimes.com/2019/01/28/us/politics/meng-wanzhou-huawei-iran.html?action=click&module=Top%20Stories&pgtype=Homepage>
- Segal, Adam, "When China Rules the Web: Technology in service of the state," Foreign Affairs, 13 août 2018 <https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web>



- Sulmeyer, Michael, "How the U.S. Can Play Cyber-Offense: Deterrence Isn't Enough," Foreign Affairs, 22 mars 2018, <https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense>
- World War Web (Foreign Affairs), 14 août 2018, <https://www.foreignaffairs.com/articles/2018-08-14/world-war-web>
- Zhong Raymond, "Huawei's U.S. Restrictions Expose a High-Tech Achilles' Heel for China," The New York Times, 21 mai 2019, <https://www.nytimes.com/2019/05/21/technology/huawei-china-us-trade.html>
-