Le Monde
DIMANCHE 22 - LUNDI 23 JUILLET 2018

Cyberespace
La guerre mondiale des données

Espionnage, destruction, propagande, attaques... Internet est devenu le miroir des tensions géopolitiques et un facteur de reconfiguration des relations internationales. Dans cette course au pouvoir, la Chine concurrence déjà les Etats-Unis

Les données sont le liquide vital de l'économie numérique. La plupart des géants du Web se sont développés grâce à elles, et elles chamboulent les modèles d'affaires des entreprises dans tous les secteurs de l'activité humaine.

Jusqu'à présent, les Etats-Unis dominaient culturellement et économiquement cet espace, profitant d'être le pays où a été inventé Internet et où sont nés les principaux mastodontes du secteur. Cette suprématie est pourtant de plus en plus contestée, notamment par la Chine, qui a su créer des géants technologiques, protégés par sa grande muraille numérique, qui n'ont presque plus rien à envier à leurs homologues d'outre-Pacifique. L'empire du Milieu toise désormais la Silicon Valley et mise beaucoup sur les technologies d'intelligence artificielle, dont le développement repose justement sur la quantité des données à disposition.

Déstabiliser des sociétés entières

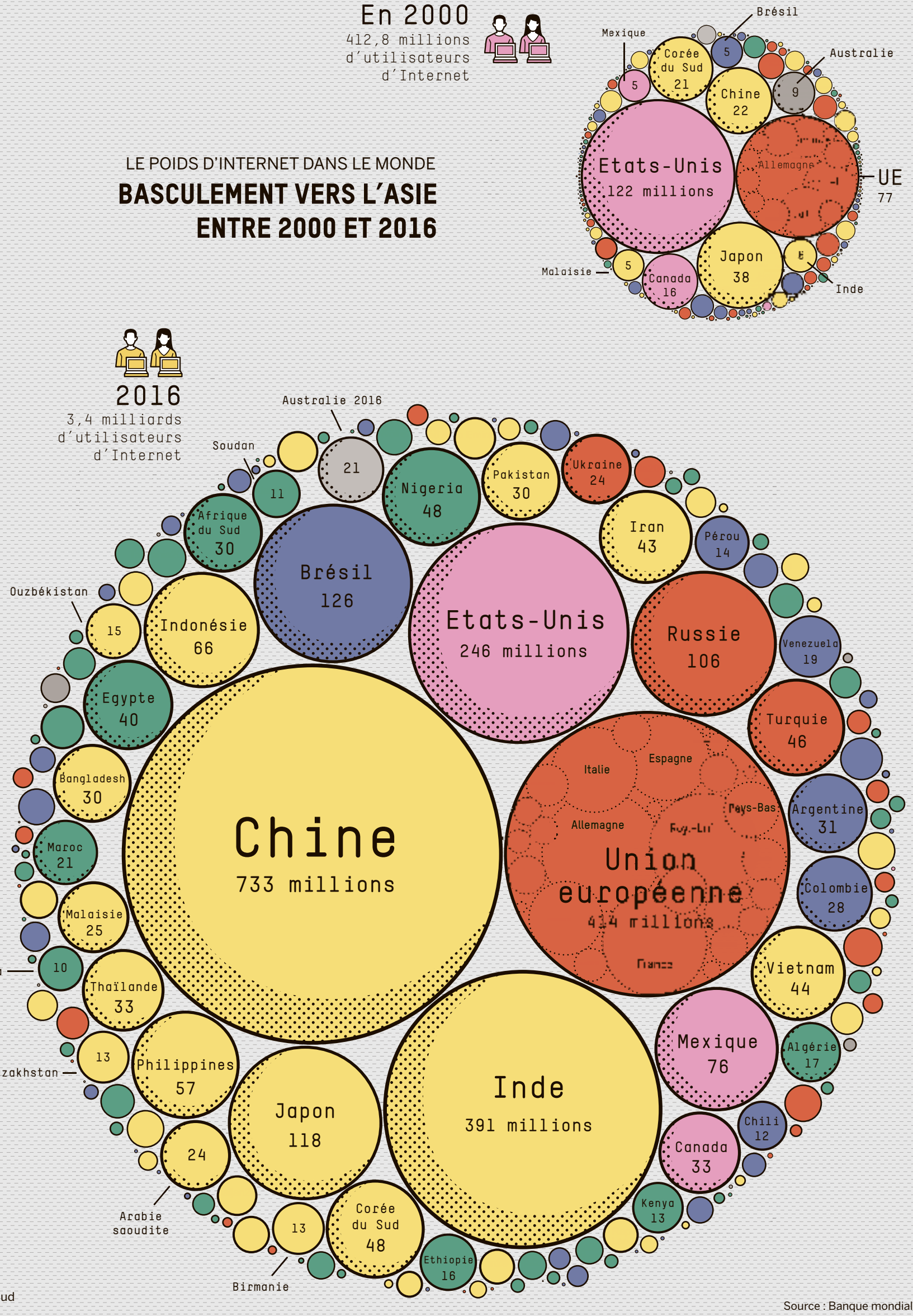
Les conflits dans ce qu'il est désormais admis d'appeler le « cyberespace » ne sont pas seulement économiques et n'opposent pas uniquement – tant s'en faut – Washington à Pékin. En offrant une palette d'offensives variées (espionnage, destruction, propagande...) peu coûteuses, rarement suivies de ripostes, difficiles à attribuer et faciles à nier, Internet est devenu un miroir des tensions mondiales et un facteur de reconfiguration des relations internationales. Des Etats l'utilisent pour éteindre des centrales électriques, ralentir une usine d'enrichissement d'uranium ou se financer à peu de frais. On voit aussi se dessiner, avec la tentative d'ingérence russe dans l'élection américaine de 2016, l'émergence d'attaques hybrides, où l'information et la donnée elle-même sont instrumentalisées pour déstabiliser des sociétés entières.

Les milliards d'internautes et les outils sur lesquels reposent leurs vies numériques sont désormais forcés de côtoyer la puissance de feu des Etats, lorsqu'ils n'en sont pas les victimes, directes ou indirectes. Personne ne sait encore comment pacifier ce cyberespace en conflit larvé permanent, sans doute parce que personne ne veut se passer de ce qui est devenu un nouvel instrument de pouvoir. ■

MARTIN UNTERSINGER

LE POIDS D'INTERNET DANS LE MONDE

BASCULEMENT VERS L'ASIE ENTRE 2000 ET 2016



INFOGRAPHIE : Mathilde Costil, Sylvie Gittus-Pourrias, Audrey Lagadec, Véronique Malécot, Delphine Papin

Dossier réalisé avec l'aide des chercheurs de l'IFG (Paris-VIII) et de la Chaire Castex de cyberstratégie (IHEDN) à l'issu du colloque international "cartographie du cyberespace", organisé en mars 2018

Nombre d'utilisateurs, en millions

- Asie
- Afrique
- Océanie
- Europe
- Amérique du Nord
- Amérique centrale et du Sud

Source : Banque mondiale

Les Etats-Unis, contrôleurs du numérique européen

Les données venant d'Europe sont un vivier d'informations pour le renseignement américain

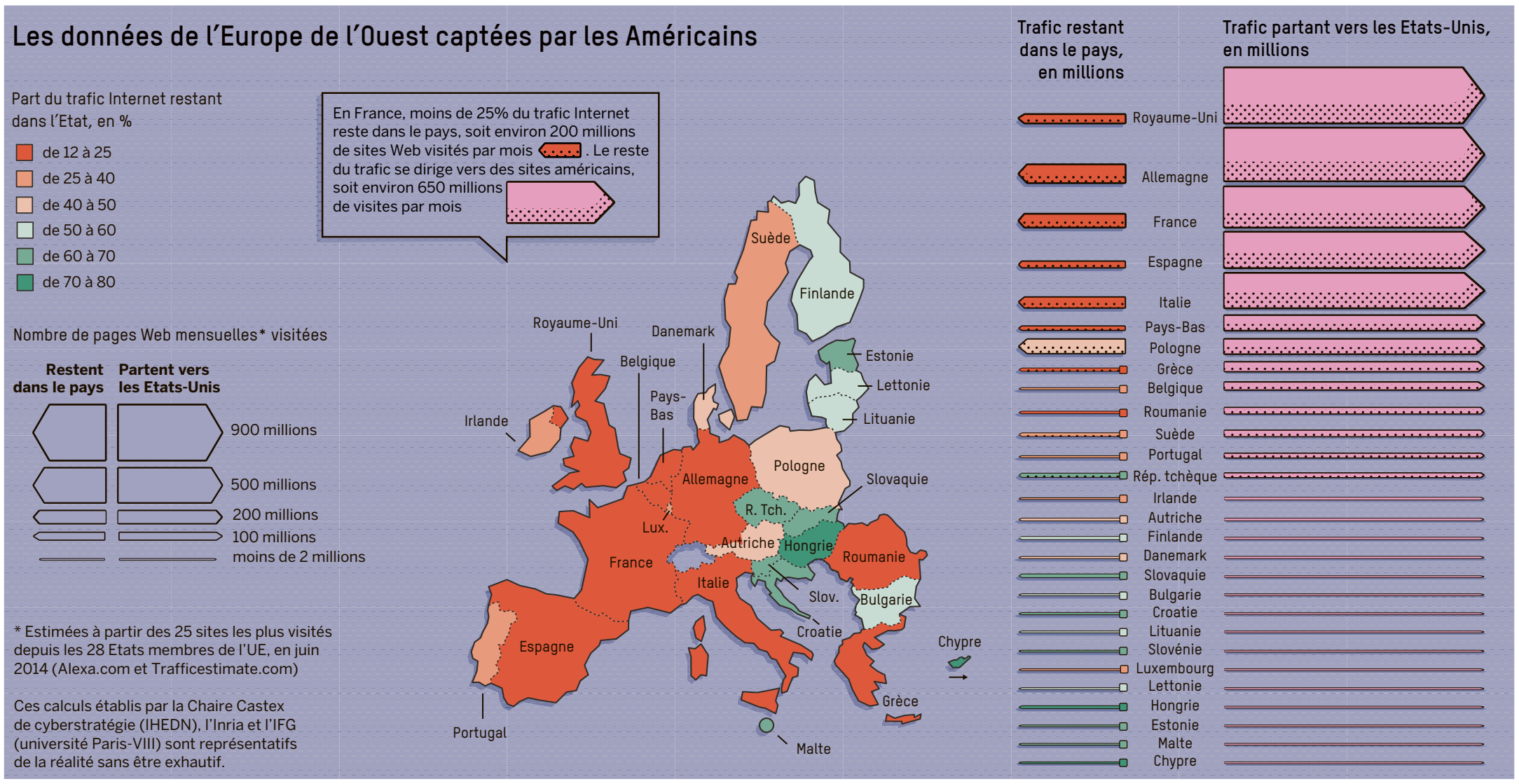
Les Etats-Unis dominent largement l'univers numérique. C'est dans ce pays qu'est né Internet, et c'est là que se trouvent les mastodontes du secteur, très gourmands en données personnelles. Même si celles-ci sont stockées sur des serveurs en Europe, les citoyens européens ont de facto mis leurs vies numériques entre les mains d'entreprises américaines.

C'est vrai pour les réseaux sociaux – le seul concurrent sérieux de Facebook en la matière, VKontakte, n'est populaire qu'en Russie et dans certains pays d'Europe de l'Est –, mais également pour la recherche et la vente en ligne, où Google et Amazon ont mis leurs rivaux à la peine. La prépondérance des géants américains est quasi totale dans le domaine de la publicité en ligne, où la croissance combinée de Google et Facebook dépasse la croissance globale du marché.

Cette influence des Etats-Unis place ce pays dans une position privilégiée pour longtemps. Les masses de données collectées par les sociétés du numérique constituent aussi un atout concurrentiel dans de très nombreux secteurs de pointe. La technologie du deep learning, utilisée pour produire des intelligences artificielles performantes, est particulièrement consommatrice de données.

La domination américaine sur les données ne concerne pas seulement le domaine économique. Les données collectées par les géants du Web sont également exploitées par les forces de l'ordre et les services de renseignement américains, en vertu d'une législation accommodante qui leur permet d'accéder aux données d'utilisateurs. Y compris à celles d'utilisateurs européens, même si un accord international garantit théoriquement des protections aux internautes résidant en Europe. ■

M. U.

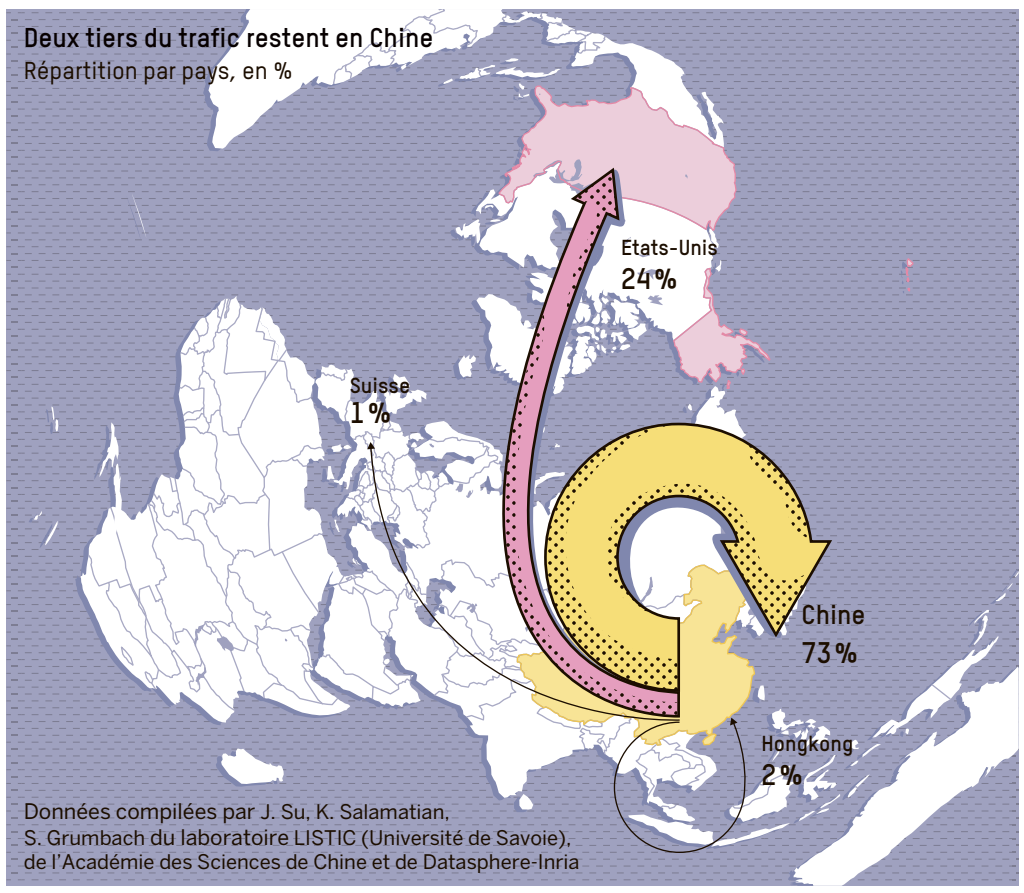


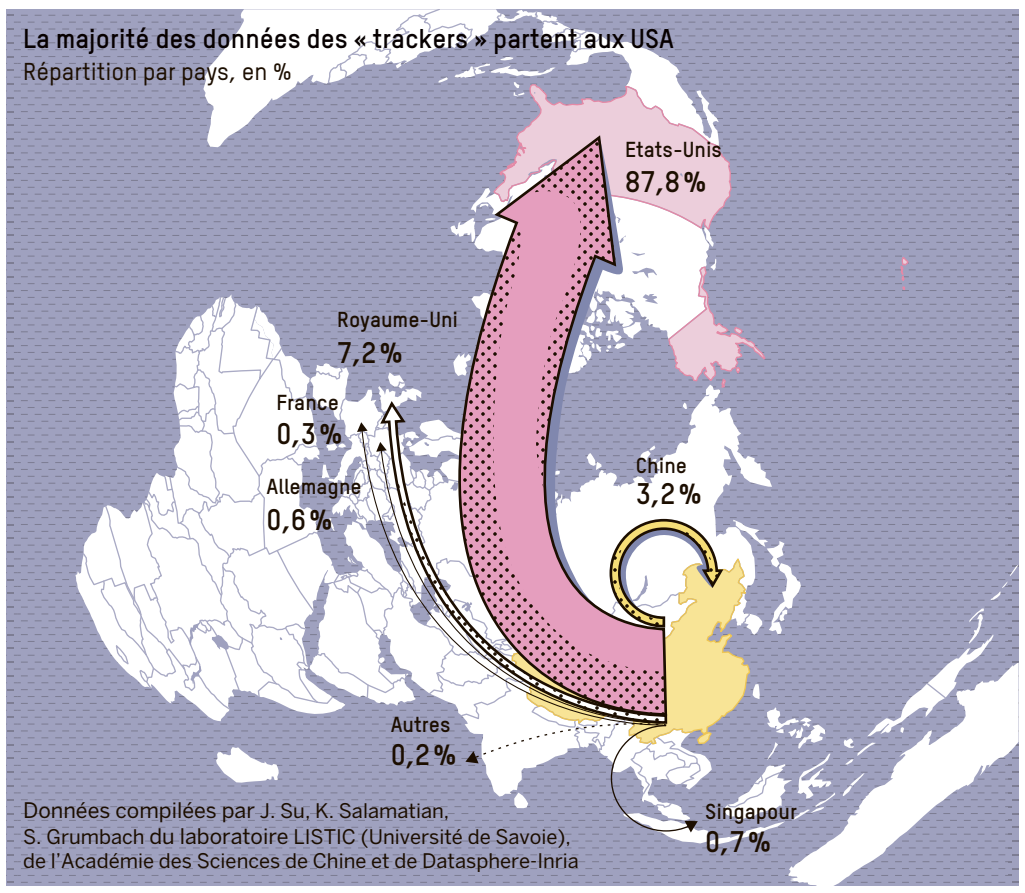
Chine : la grande muraille du Web

Pékin a posé quantité de filtres pour protéger les réseaux du pays

Autour de ses réseaux nationaux, la Chine a élevé une grande muraille numérique, capable de filtrer presque tout ce qui entre et sort. En observant les requêtes DNS d'un grand fournisseur d'accès à l'Internet chinois, sur une période de deux jours, plusieurs scientifiques chinois et français ont découvert que cette isolation était loin d'être parfaite, et qu'une part conséquente de l'activité des Chinois sur le Web sortait du pays, en direction des Etats-Unis.

Le DNS (Domain Name System, « système de noms de domaine ») est le système d'aiguillage du Web. Il permet de traduire une adresse Internet lisible par un humain (www.lemonde.fr, par exemple), en une adresse IP (pour « Internet Protocol ») constituée d'une suite de chiffres ou de lettres destinée aux machines. Cet élément est indispensable au fonctionnement du Web. L'examen des requêtes qui lui sont adressées permet de dessiner une carte de l'activité des internautes. ■





La fuite des « trackers » chinois

Malgré les filtres, la plupart des données partent aux Etats-Unis

La très grande majorité des pages Web embarquent, en plus de leur contenu (texte, photos, vidéos...), des composants publicitaires appelés « trackers ». Ces derniers transmettent des informations concernant les internautes, avec l'objectif de leur adresser des publicités ciblées.

C'est à ce stade que la « grande muraille » numérique chinoise se met à ressembler à une passoire. En effet, 87 % du trafic des trackers publicitaires en provenance de Chine aboutissent aux Etats-Unis contre seulement 3 % qui demeurent à l'intérieur de l'empire du Milieu. Les trackers restants aboutissent au Royaume-Uni et, marginalement, en France et en Allemagne.

Alors que les trois quarts du trafic vers les pages Web restent à l'intérieur de la Chine, une très grande quantité d'informations sort malgré tout du pays, par le biais de ces trackers publicitaires, et ce, en dépit du filtrage mis en place par les autorités de Pékin. ■

Le Monde
DIMANCHE 22 - LUNDI 23 JUILLET 2018

Frédérick Douzet « Les actions offensives dans le cyberespace sont permanentes »

La course au cyberarmement a commencé, prévient cette spécialiste en cyberstratégie. Des lois internationales régulant le monde numérique sont devenues indispensables

ENTRETIEN

CHAIRE CASTEX DE CYBERSTRATÉGIE

Frédérick Douzet est professeure à l'Institut français de géopolitique (université Paris-VIII) et titulaire de la chaire Castex de cyberstratégie. Ses recherches portent sur les enjeux géopolitiques du cyberespace, c'est-à-dire sur les rivalités de pouvoir liées à l'expansion globale d'Internet et de l'espace de communication qu'il génère entre des acteurs de plus en plus nombreux (Etats, entreprises, individus, hackeurs, criminels...).

Peut-on parler de frontières dans le cyberespace ?

La frontière, dans sa définition classique, désigne la limite du territoire sur lequel s'exerce la souveraineté nationale. Or, le cyberespace défie les conceptions classiques du territoire en permettant des échanges transfrontaliers quasi instantanés. On peut aussi comprendre la notion de frontière au sens métaphorique, comme une discontinuité géopolitique qui est le fruit de rivalités de pouvoir, et sa représentation peut être très mobilisatrice. Les Etats cherchent à transposer leurs frontières dans le cyberespace, à réintroduire du contrôle et de la régulation dans ce qu'ils se représentent comme relevant de leur souveraineté, et à exercer leurs pouvoirs régaliens dans l'espace numérique.

La Chine a construit l'Internet autour de points de connexion qui relient l'Internet national au reste du cyberespace. Ces points permettent de filtrer des contenus, de bloquer l'accès à des sites. Ils s'apparentent ainsi à une frontière. Mais, dans la réalité, la rapidité de circulation des données de l'information et leur ubiquité inédite rendent difficile l'exercice de ce contrôle. D'autant que, pour tirer bénéfice de la connexion à l'Internet global, il faut être dans une dynamique d'ouverture et d'échange. Les autorités chinoises, tout en contrôlant l'information et les citoyens, s'inscrivent dans cette dynamique. La Chine développe le commerce et les services en ligne avec le reste du monde et se perçoit comme une grande puissance du cyberespace global.

Parler de souveraineté nationale a-t-il encore du sens, dans le monde numérisé d'aujourd'hui ?

Oui, mais les contours de la souveraineté évoluent, et son exercice est plus complexe dans l'espace numérique. Tout dépend de quelle couche du cyberespace on parle. S'il s'agit des infrastructures physiques, qui sont l'ancrage terrestre du cyberespace, les frontières de la géographie physique et politique s'appliquent. Un câble ou une infrastructure situés sur un territoire relèvent clairement de la souveraineté de l'Etat.

Les données, les informations, les cyberattaques, en revanche, traversent les frontières à toute vitesse et peuvent provenir de sources difficiles à identifier, transiter par différents endroits de la planète, être soumises au contrôle de différents acteurs. Le problème n'est pas tant l'absence de souveraineté que l'enchevêtrement des souverainetés et les conflits de juridictions que cela produit.

Diverses conceptions de la souveraineté s'opposent parfois, car l'ubiquité des données entraîne un enjeu d'extraterritorialité. La question s'est posée dans le conflit entre Microsoft et le département de la justice américain. Elle se pose à nouveau avec l'adoption du Cloud Act *[une loi récemment adoptée aux Etats-Unis qui va permettre au gouvernement de négocier des traités bilatéraux pour que les enquêteurs américains puissent accéder directement aux données stockées à l'étranger]*. C'est aussi valable pour le règlement général sur la protection des données (RGPD), l'Europe considérant que les données de ses citoyens, quelle que soit leur localisation, sont soumises à sa juridiction.

Il est donc objectivement difficile de plaquer des frontières physiques sur l'espace numérique. Par ailleurs, des fonctions régaliennes, comme la sécurité nationale, vont s'exercer différemment dans l'espace numérique. On le voit dans la lutte antiterroriste : les réseaux sociaux utilisés par les djihadistes pour diffuser leur propagande en France, et par les jeunes de notre pays susceptibles d'être embrigadés, ne sont pas de droit français. La lutte nécessite une coopération judiciaire, principalement avec les Etats-Unis, mais aussi une coopération directe avec des entreprises privées étrangères. Il faut donc repenser la façon dont s'exercent les pouvoirs de l'Etat.

Jusqu'à présent, en cas de conflit de juridiction, c'est souvent la souveraineté des Etats-Unis qui a prévalu...

Les Etats-Unis ne se posent pas la question de la souveraineté. Les pays en position de suprématie soulèvent rarement le problème. C'est plutôt une réaction défensive qui va amener un Etat à se pencher sur le sujet, quand ses pouvoirs régaliens sont mis au défi. Le concept de souveraineté numérique a ainsi émergé en France à la suite des révélations d'Edward Snowden *[en 2013, des fuites sur des programmes de surveillance électronique de citoyens, d'entreprises et d'Etats, par plusieurs agences de renseignement]*.

L'enjeu est exprimé par la Chine, dans sa volonté de protéger son droit à contrôler les contenus au sein ce qu'elle se représente comme son cyberespace national, en vue de préserver la stabilité et la prospérité de son régime. Dans cette stratégie, la Chine a développé ses propres plates-formes, grâce à la taille critique de son marché intérieur, et elle mise aujourd'hui sur le big data et l'intelligence artificielle.

La notion de souveraineté de « l'espace informationnel » est apparue plus tard en Russie, comme une opportunité politique, après les révélations de Snowden. Les régimes les plus autoritaires ont une approche plus stratégique de l'information, et depuis plus longtemps.

Le cœur du sujet est la représentation que chacun se fait de la menace. La représentation américaine, ou française jusqu'à récemment, était très technocentrée, et portée sur les aspects militaires. Nos pays craignaient d'abord pour leurs infrastructures, leurs systèmes de communication, avec les risques d'intrusion, de sabotage, de vol ou de manipulation des données. Les autorités étudient dans ce cadre des scénarios catastrophe d'attaques sur les infrastructures d'importance vitale, pouvant causer des morts. Alors que la Chine, qui a suivi de très près l'effondrement de l'URSS, les « printemps arabes », les révolutions de couleur, regarde prioritairement, tout comme la Russie, la menace informationnelle qui peut engendrer une déstabilisation interne.

Cette différence explique l'impréparation occidentale face à la propagande djihadiste en ligne. Il y a eu beaucoup de tâtonnements. On a vu la stupeur de l'administration américaine face aux opérations russes, lors de la présidentielle de 2016. Elles ont provoqué un choc, car cette menace n'était pas anticipée. Le piratage des emails du Parti démocrate résultait d'attaques techniquement de bas niveau, mais l'angoisse s'est vite portée sur les machines à voter et sur la possible corruption technique du processus électoral. Finalement, les opérations russes, avec une manipulation multicanaux de l'information, ont créé suffisamment le doute pour obtenir un effet déstabilisateur, avec un investissement très minime.

La stratégie française, très technocentrée au départ, a une approche désormais globale des enjeux et des menaces liés au cyberespace.

Les rapports de force sont-ils recomposés dans cet espace ?

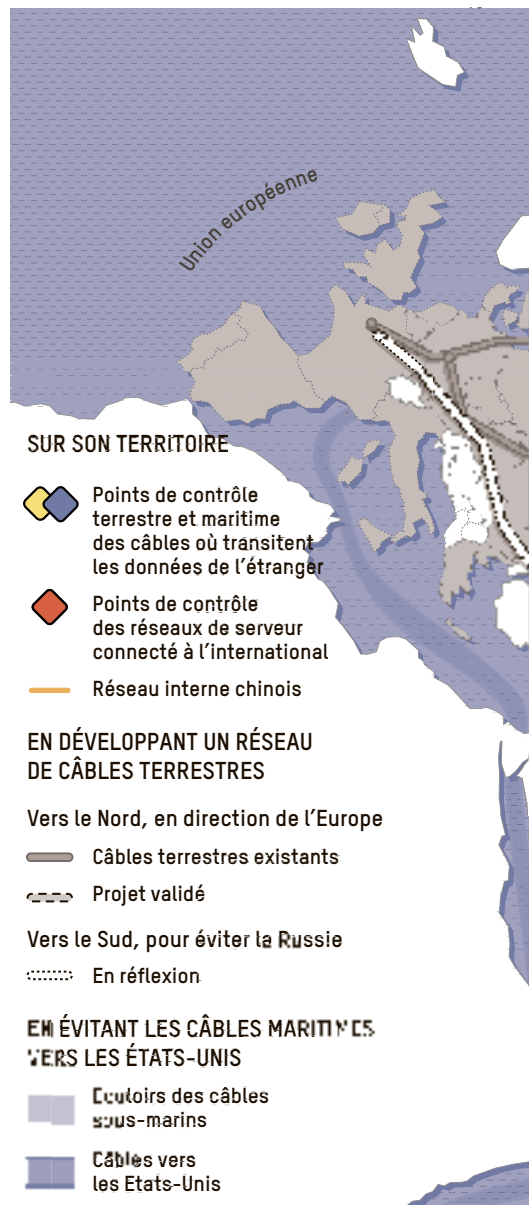
Tout ce qui se passe dans l'espace numérique est le fruit des rivalités de pouvoirs qui existent par ailleurs. C'est un prolongement des conflits géopolitiques, avec des moyens d'action différents. Actuellement, les conflits franchement ouverts entre les nations sont moins nombreux, et les frontières entre l'état de paix et l'état de guerre se brouillent. Dans l'espace numérique, ce brouillage est d'autant plus important que l'on peut y mener des actions très offensives, difficiles à détecter ou à attribuer, et qui ne causent pas nécessairement de dégâts majeurs ou visibles. D'un autre côté, on assiste aussi à une certaine retenue de la part des Etats. Les actions qu'ils mènent dans le cyberespace restent pour l'instant sous le seuil de l'agression armée.

Il est d'ailleurs intéressant de voir que la première édition du Manuel de Tallinn, en 2013 *[rédigé par des experts mandatés par l'OTAN, il propose une transposition du droit international aux cyberconflits]*, se focalisait sur l'application du droit international au cyberespace dans le cadre de la guerre, alors que la deuxième édition, en 2017, s'intéresse aussi à ce qui se passe en temps de paix.

Cela dit, les Etats mènent en permanence des actions offensives dans le cyberespace. Certains poussent leur avantage. Or, il reste difficile de déterminer qui est derrière une cyberattaque et quel est son but. Le risque d'escalade en raison d'une erreur de calcul ou d'interprétation est réel. Il est indispensable d'établir des règles qui définissent ce qui est acceptable ou non.

Les acteurs les plus offensifs dans ce domaine sont-ils prêts à accepter une régulation internationale, voire des traités ?

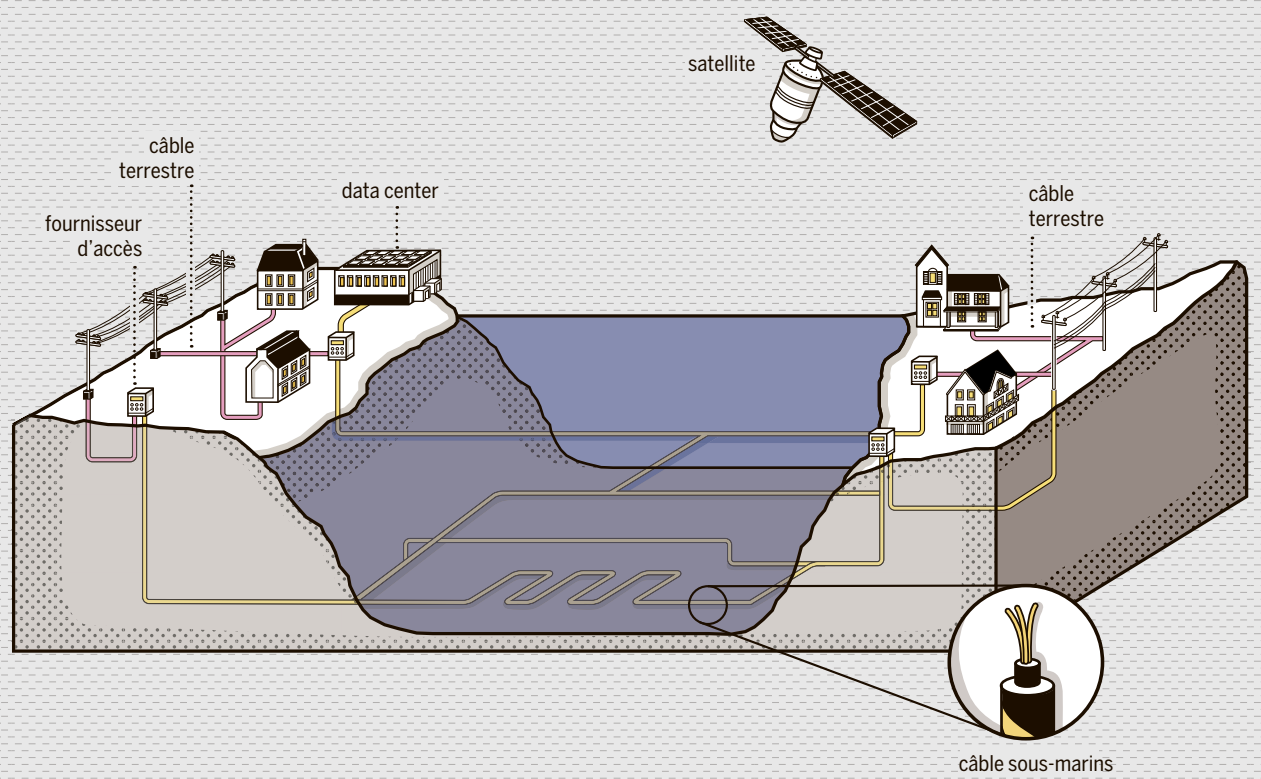
La dynamique des discussions est globalement positive, il y a eu des avancées majeures, même si les progrès ne sont pas linéaires. Le



Comment circulent les données à travers les trois couches du cyberespace

1 LE RÉSEAU PHYSIQUE

La première couche, base de l'Internet, est celle des infrastructures du réseau composé de câbles, de serveurs, d'ordinateurs, principalement gérés par des entreprises privées. Ces biens matériels sont soumis aux contraintes de la géographie physique et politique. Ces infrastructures étant dépourvues de sécurité intégrée, les données non chiffrées qui circulent via les câbles sont faciles à aspirer.



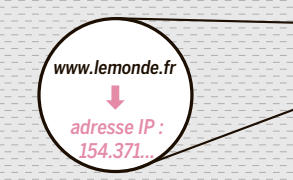
2 LA CIRCULATION DE LA DONNÉE

Ex. Faire une requête en ligne

La deuxième couche, qualifiée de « logique », est formée de tous les « protocoles » et applications qui permettent à l'information de circuler en petits paquets de l'expéditeur au destinataire. L'architecture globale repose sur le protocole TCP/IP, qui sert de language commun à tous les ordinateurs et serveurs. D'autres protocoles permettent par exemple un échange entre les différents réseaux de serveurs (*autonomous system*) pour déterminer la route la plus courte pour faire circuler les paquets d'informations.

flux qui va chercher la donnée

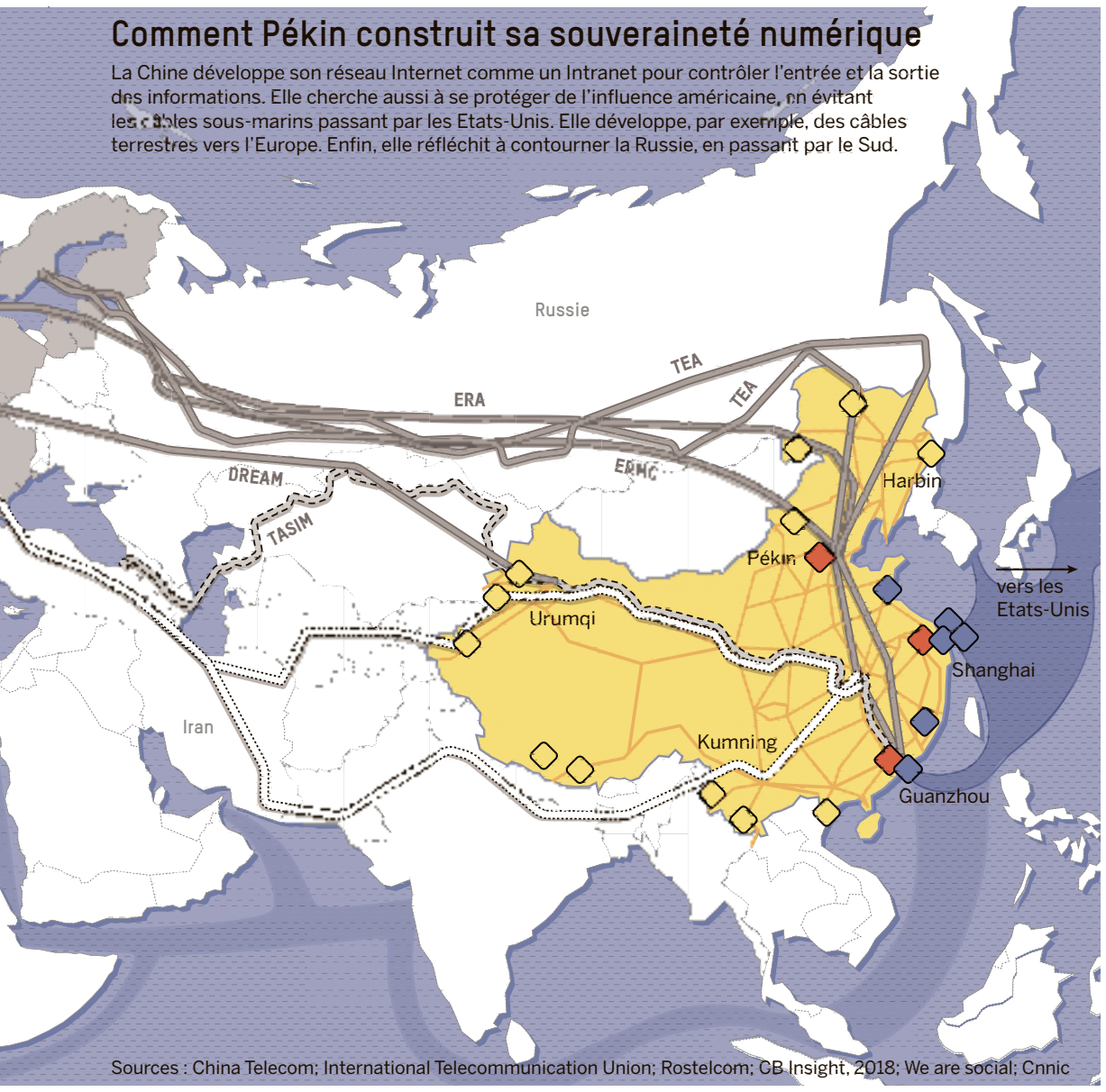
flux qui rapporte la donnée



1 Consultation d'un site Internet
Le protocole (DNS) transforme l'adresse Internet en adresse IP.

Comment Pékin construit sa souveraineté numérique

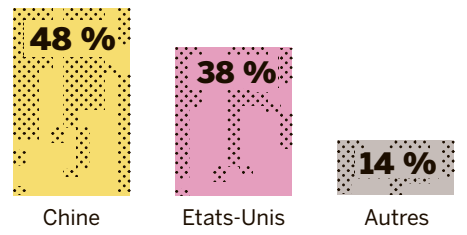
La Chine développe son réseau Internet comme un Intranet pour contrôler l'entrée et la sortie des informations. Elle cherche aussi à se protéger de l'influence américaine, en évitant les câbles sous-marins passant par les Etats-Unis. Elle développe, par exemple, des câbles terrestres vers l'Europe. Enfin, elle réfléchit à contourner la Russie, en passant par le Sud.



Sources : China Telecom; International Telecommunication Union; Rostelcom; CB Insight, 2018; We are social; Cnnic

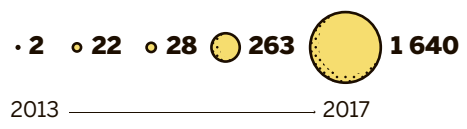
Le pari de l'intelligence artificielle...

La Chine, première destination de l'investissement mondial dans les start-up IA, en 2017



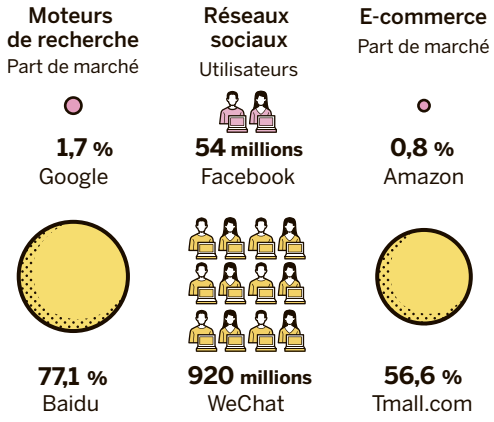
La Chine, à la pointe des techniques de reconnaissance faciale

Investissements en dollars (contrats et subventions)



... qui s'appuie sur l'écosystème des services Internet chinois

Utilisation de services Internet américains et chinois en Chine, en %



groupe des experts gouvernementaux de l'ONU a reconnu, en 2013, l'applicabilité du droit international, en particulier la Charte des Nations unies, au cyberespace. En 2015, les Etats ont convenu entre eux de normes et de mesures de confiance, notamment de ne pas attaquer leurs infrastructures critiques ni leurs centres de réponse d'urgence. Ils se sont entendus pour se porter assistance mutuelle en cas d'incident cyber majeur. Malgré l'échec de nouvelles discussions en 2017, ni la Russie ni la Chine ne remettent en cause ces normes.

Actuellement, les instances multilatérales sont affaiblies, les grandes puissances s'affirment, et il est plus difficile d'avancer. Mais des initiatives continuent d'être prises par d'autres acteurs, car les enjeux sont majeurs pour la société civile et la vie économique.

Les Etats sont pris dans un dilemme sécuritaire. D'un côté, ils reconnaissent que la menace cyber crée un risque systémique. A l'image des pandémies, ces menaces sont très complexes, traversent les frontières et se répandent rapidement. Elles peuvent avoir un impact massif et sont difficiles à stopper. Cette vision tire dans le sens d'une réduction des armes, d'une forte collaboration internationale et d'une régulation du cyberespace, car il est dans l'intérêt de tous de stopper la contagion qui pourrait avoir des effets dévastateurs.

Mais, dans le même temps, les capacités cyber sont aussi utilisées par les Etats pour accroître leur puissance dans le cadre des rapports de force géopolitiques. Elles servent pour le renseignement, l'espionnage, l'influence, la guerre... La menace cyber est alors perçue comme une menace géopolitique traditionnelle qui incite les Etats à développer des capacités pour assurer leur sécurité et affirmer leur puissance. Cette vision prédomine clairement aujourd'hui. Plus de trente Etats revendiquent le développement de capacités offensives. On assiste à une véritable course aux cyberarmes.

Quels sont les risques de cette course aux cyberarmes ?

Les Etats sont les acteurs les plus puissants et les plus dangereux dans le cyberespace, par la sophistication des outils qu'ils développent et les ressources dont ils disposent. On trouve aussi des individus dangereux, des terroristes, des mercenaires motivés par le profit ou encore des hackeurs patriotes qui peuvent créer de graves perturbations. Mais, pour mener une attaque de grande ampleur, il faut du renseignement humain et technique, et des ressources.

« EN FRANCE, LE CONCEPT DE SOUVERAINETÉ NUMÉRIQUE A ÉMERGÉ À LA SUITE DES RÉVÉLATIONS D'EDWARD SNOWDEN, EN 2013 »

FRÉDÉRICK DOUZET

De plus, les outils développés par les Etats peuvent être volés ou récupérés et retravaillés, puis réutilisés. Les concepts d'attaque peuvent être copiés. Ces actions contribuent à faire augmenter le niveau global de sophistication des attaques et le risque systémique.

Les attaques destructives WannaCry et NotPetya *[en 2017, ces logiciels malveillants réclamant des rançons ont infecté des centaines de milliers d'ordinateurs de par le monde]*, qui se sont propagées de manière incontrôlée, ont utilisé EternalBlue, un outil développé par la NSA qui exploitait une vulnérabilité de Microsoft. EternalBlue a été volé et diffusé publiquement, ce qui soulève de sérieuses questions. Qui est responsable ? Ceux qui ont volé l'outil au gouvernement et l'ont utilisé, bien sûr. Mais quelle est la part de responsabilité de l'Etat qui a développé l'outil et se l'est fait voler ? Et quid des entreprises qui mettent sur le marché des produits encore truffés de vulnérabilités ? Il est important d'établir les responsabilités éthique et juridique des Etats et des entreprises pour réduire le risque systémique. D'où l'importance d'avoir des processus de coopération, des mesures de confiance et des normes.

Comment trouver un intérêt commun pour réduire le risque systémique ?

La question est de savoir s'il faudra arriver à une catastrophe majeure pour que la prise de conscience du risque systémique soit entière. Nous avons déjà connu de sérieuses alertes. Pour l'instant, il y a une volonté des Etats de poursuivre les discussions, mais pas au point que ceux-ci soient prêts à renoncer à certaines pratiques et capacités offensives. Or, les Etats aux capacités les plus avancées sont aussi les plus connectés, et ainsi les plus exposés aux risques. Si la seule préoccupation était la sécurité et la stabilité du cyberespace, les Etats révéleraient systématiquement aux entreprises les vulnérabilités détectées et coopéreraient plus activement entre eux. Mais les rapports de force géopolitiques restent prédominants, au risque de nous conduire vers une situation dont nous ne voulons pas.

Au sein de la Global Commission on the Stability of Cyberspace, nous travaillons à promouvoir la sécurité et la stabilité du cyberespace. En novembre 2017, nous avons proposé une norme pour sanctuariser le cœur public de l'Internet (le système d'adressage, les routeurs, les câbles...), de manière à ce qu'aucune opération ne vienne perturber le fonctionnement de l'Internet global et porter atteinte à la stabilité du cyberespace. Il en va de la sécurité et de la stabilité de nos sociétés.

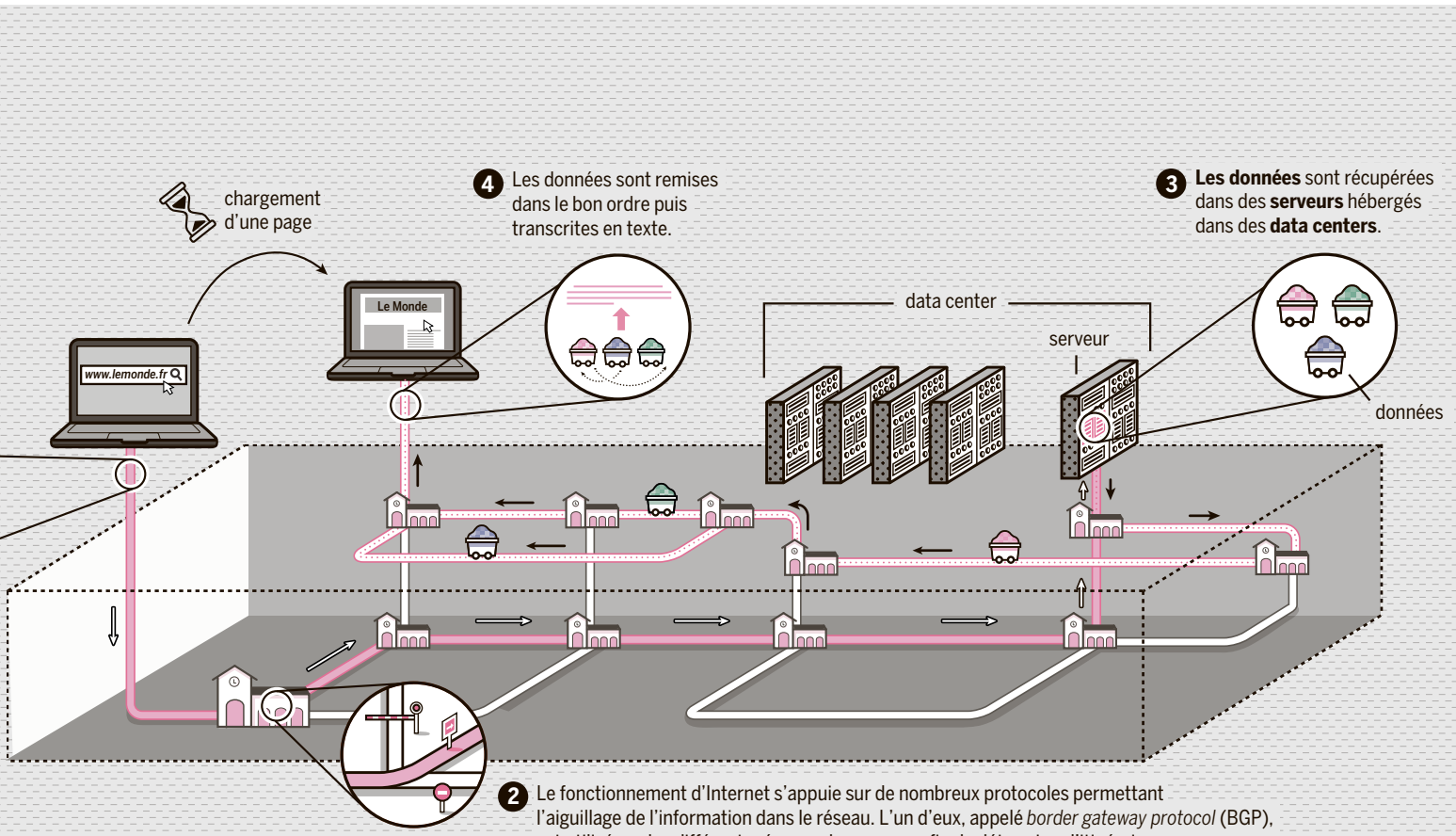
Quel serait le rôle des entreprises privées ?

La proposition de Microsoft, en février 2017, d'une convention de Genève dans le cyberespace aura eu le mérite de mettre le débat sur la table. On ne peut pas faire l'économie du secteur privé ni du monde académique pour arriver à une régulation efficace. Les acteurs privés des marchés de masse, parce qu'ils ont des clients au niveau mondial, ont un intérêt à la stabilité du cyberespace. Ces entreprises voient passer les attaques. Elles sont souvent les premières à les détecter et à y répondre. Elles ont une visibilité que les Etats n'ont pas et sont parties prenantes de l'application des normes. Ce sont des partenaires incontournables des Etats.

De la même façon, le secteur académique, qui a inventé l'Internet et possède la légitimité et la compétence, doit rester impliqué pour définir des règles qui ont du sens d'un point de vue technique et tiennent compte des interactions entre les domaines civils, économiques, militaires inhérents au cyberespace, comme de l'imbrication des enjeux.

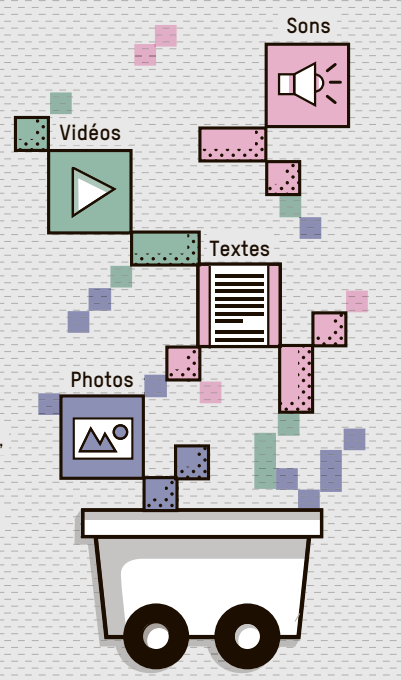
Dans le contexte actuel de la course aux cyberarmes, ces acteurs peuvent intervenir pour dépasser les blocages entre Etats. Les forums de discussion permettent de faire avancer le travail de fond sur les points litigieux d'interprétation du droit international, comme la légitime défense ou les contre-mesures, et de proposer de nouvelles normes. Cela permet d'anticiper pour être en mesure de produire de meilleures politiques lorsque la volonté politique sera là. In fine, la régulation internationale relève de la compétence des Etats. Mais nous avons tous un rôle à jouer. ■

PROPOS RECUEILLIS PAR NATHALIE GUIBERT ET MARTIN UNTERSINGER



3 LE CONTENU

La troisième couche est celle du contenu présent sur le Web, c'est-à-dire les informations, les réseaux sociaux, les discussions, et échanges. C'est la couche des utilisateurs, sur laquelle on peut analyser la diffusion d'une information, les groupes qui interagissent entre eux, l'influence et la propagande d'individus, de groupes et de pays...



Sources : « Le Cyberespace, un enjeu de géopolitique majeur », F. Douzet, Inaglobal.fr, 2016; « Le Routage, enjeu de cyberstratégie », entretien avec Kavé Salamatian par Dominique Lacroix, Lemonde.fr, 2012