Cyber et géopolitique

En géopolitique, depuis quelques années, tout a tendance à être cyber. Cyberespace, cyberstratégie, cybermonnaie, cyberpolitique… le concept est décliné à l'infini, marquant à la fois une promesse et une inquiétude. Si chacun mesure les progrès accomplis jusqu'à présent grâce au digital, il est en revanche beaucoup plus difficile de prévoir le futur. Beaucoup se souviennent encore du rapport Théry de 1994, dans lequel l'inventeur du Minitel expliquait au Premier ministre de l'époque qu'internet n'avait aucun avenir commercial. La même année, Jeff Bezos créait Amazon. Dans les collèges, on apprenait aux élèves à se servir d'une disquette et à maîtriser les rudiments de la programmation sur DOS, ce qui me laisse toujours sceptique quand je vois l'argent déployé par l'Éducation nationale pour inculquer le numérique aux collégiens aujourd'hui, dont on sait pertinemment qu'il sera complètement dépassé par le numérique de demain.

Dans le domaine du cyber et du digital, les prévisions sont donc très difficiles et il est presque impossible de dessiner le monde de demain. Ce qui n'est évidemment pas une bonne nouvelle pour les stratégistes qui eux doivent penser le monde de demain et s'y préparer.

Le cyber : réseau ou espace ?

Pour certains stratégistes, le cyber est un réseau, prolongeant les réseaux existants. Il est matérialisé par les câbles, les fils, la fibre. Pour d'autres, c'est un espace propre, comme le sont la terre, la mer, l'air et l'espace. Que l'on opte pour l'une ou l'autre définition et les conséquences sont différentes. Si le cyber est un espace propre, alors peuvent s'y développer les éléments classiques de la stratégie : le choc, le feu et la manœuvre. Si c'est un espace, on peut aussi envisager d'y disposer d'une armée spécifique, au même titre que l'armée de terre, de l'air ou la marine. C'est ce qu'a tenté Tsahal en 2015 en annonçant la création d'une armée du cyber, mais cette expérience a été supprimée dès 2017.

Internet fait partie du cyber, mais pas seulement. Il faut y ajouter les réseaux, les fibres, les ordinateurs, les serveurs… Ce monde n'est donc pas que virtuel. Les serveurs et les supercalculateurs consomment de l'énergie et de l'espace. On ne peut les placer n'importe où au

risque de porter atteinte à leur sécurité. Google protège la sécurité de ses serveurs, au même titre qu'Amazon et les autres grandes entreprises. Le cloud n'est donc pas, loin de là, un nuage évanescent et virtuel où nos dossiers sont conservés. Loin d'être virtuel, le cyber rejoint des réalités bien spécifiques : la question énergétique, celle du refroidissement des fermes des serveurs, celle du droit aussi. Si mes dossiers sont stockés dans les serveurs Microsoft, à quelle juridiction sont-ils soumis ? Celle des États-Unis ? Et la CIA et la NSA ont-elles le droit d'exiger de Microsoft de lui fournir mes dossiers en cas de contrôle ? Le droit et la territorialisation sont très présents dans le cyber.

On est parfois confondu par la légèreté avec laquelle des professionnels ou des entreprises traitent leurs données. Qu'est-ce qui m'assure que les fichiers confidentiels de X, entreprise française concurrente de J, entreprise américaine, dont lesdits fichiers sont stockés sur le cloud Google, Apple ou Microsoft, ne vont pas être opportunément transmis à ladite J, qui pourra ainsi me chiper le contrat ? Dans ce cloud virtuel qui s'apparente parfois au royaume des Bisounours, les règles élémentaires de la prudence et de la confidentialité ainsi que les réalités de la guerre économique et de l'intelligence stratégique semblent allègrement oubliées.

Un cyber à plusieurs couches

Le cyber n'est donc nullement virtuel. L'équipement est la couche matérielle du cyberespace. Deux autres couches s'y ajoutent : une couche logicielle, avec les programmes et les protocoles techniques et une couche sémantique, qui donne du sens à l'information en permettant d'associer des chaînes de caractères. Le cyber est donc un entrecroisement de tuyaux dans lesquels circulent des informations. Dans ce cas, ce n'est pas un milieu, mais un centre d'informations. Il n'y a donc pas de guerre du cyber, mais une guerre de l'information, ce qui amène à traiter ces questions différemment. Le cyber est aussi une structure complètement anthropique, à la différence de la terre, de la mer et de l'air, qui n'a pas de limites précises et qui est en évolution perpétuelle.

Internet est lui-même subdivisé en plusieurs parties : *clear web*, *deep web* et *dark web*. Le *clear web* regroupe les sites usuels, ceux que le commun des mortels utilise tous les jours. Il représente environ 5% de la toile. Le *deep web* est la partie non indexée de la toile. Il en représente environ 95%. On y accède avec des navigateurs comme Tor. Le *dark web* est un sous-ensemble du *deep web*, dans lequel on ne peut entrer qu'avec un logiciel spécifique et une autorisation. Le *deep web* peut avoir des activités illégales et illicites, mais aussi des activités légales, publiques ou

privées, que les utilisateurs veulent protéger. Cela renvoie aux questions de confidentialités et de sauvegarde de la propriété privée via les données. Puisque toutes les navigations web sont fléchées et recensées, la vie privée disparaît à cause de la trace laissée sur le net. Avec l'usage de Tor et de Tor Browser, la confidentialité étant respectée, cela permet une navigation davantage sécurisée. On en comprend l'intérêt pour les personnes vivant dans des pays sans liberté ou bien pour la transmission de données confidentielles. Le fait que des criminels utilisent aussi ces réseaux pour leurs activités immorales (pédophilie, drogue, etc.) ne doit pas faire oublier l'intérêt stratégique de ce *deep web* qui est aussi une solution aux problèmes de nombreuses personnes honnêtes.

La question de la cryptographie des données est donc cruciale. Avec les objets connectés, de plus en plus de données pourront être recueillies. À quoi vont-elles servir ? Grâce à « OK Google » et à Alexa, Amazon et Google vont savoir ce que vous écoutez comme musique, à quelle heure vous vous levez le dimanche, ce que vous mangez habituellement, etc. Si ces données collectées servent uniquement à nous envoyer de la publicité ciblée, le risque est minime. Mais elles peuvent servir à plus. La puissance numérique des GAFAM est supérieure à celle de beaucoup d'États. Ils peuvent donc fortement agir sur le cyber, aussi bien dans le domaine juridique que politique.

La nécessaire protection des données

La protection des données est un critère essentiel, dans lequel beaucoup de gouvernements et d'entreprises ont péché par angélisme. On se souvient de la découverte des mises sur écoute des dirigeants européens par la NSA. La même question se pose aussi pour les cadres dirigeants et les chefs d'entreprise. Il faut également éviter les attaques et les piratages de site, que ce soit pour voler des données ou pour détruire le site. Réseau ou milieu, guerre de l'information ou guerre propre, le cyber reprend des éléments de la stratégie classique. Il est un lieu d'affrontement et de guerre où il est nécessaire, là aussi, de gagner.

Les stratégistes ont constaté que la stratégie navale se retrouvait dans les réseaux : guerre d'escadre, de côte et de course.

La guerre d'escadre vise à prendre le contrôle d'une partie adverse et de la détruire. Cela est possible avec des lignes de codes malveillantes, mais cela reste limité dans le temps et dans

l'espace.

La guerre de côte vise à détruire un point d'appui ou une base. En 2009, le ver informatique *Stuxnet* a détruit des centrifugeuses utilisées dans le cadre du programme nucléaire iranien. Idem pour la Corée du Sud qui a subi des attaques informatiques venant du Nord. Le virus *Industroyer* a infecté le réseau ukrainien de distribution d'énergie, provoquant des pannes géantes. Toutefois, jusqu'à présent, il n'y a pas eu d'attaque cyber géante sur les autres puissances. Les réseaux sont tellement connectés entre eux qu'une attaque massive ne permet pas d'évaluer les conséquences de celle-ci. En revanche, il y a de plus en plus d'attaques ponctuelles, qui peuvent faire craindre une montée aux extrêmes numériques.

La guerre de course semble être la forme de guerre la plus adaptée à la cyberstratégie. Le cyberespace est essentiellement un milieu de transit pour les données numériques. La NSA est capable de poser des écoutes sur les câbles sous-marins ainsi qu'écouter les principaux serveurs informatiques. Dans *La mesure de la force*, Stéphane de Lespinois constate que les principes de stratégie de Foch s'appliquent tout à fait au cyber : la liberté d'action, l'économie des forces, le couple sûreté-surprise.

La liberté d'action : chacun est libre de venir dans le web et d'y agir. Des États comme la Russie et la Chine aimeraient pouvoir contrôler une partie du web et le soumettre à leur juridiction. Les États essayent de réguler le web, mais comme ils ne sont pas d'accord entre eux ils n'arrivent pas à établir de règles juridiques internationales.

Le principe d'économie des forces est fondé sur la manœuvre. Dans le cyber, elle est facile, car le domaine se recompose sans cesse. Les réseaux sont très plastiques. L'élément le plus important en matière d'économie des forces réside dans la capacité de calcul. C'est un enjeu essentiel pour la cryptologie et l'intelligence artificielle. Il faut manœuvre les réseaux, déchiffrer les codes malveillants, calculer des algorithmes, rassembler et synthétiser des informations, et cela le plus vite possible. Il faut avoir des superordinateurs pour le calcul des données, ainsi que l'électricité qui va avec. Avec sa puissance hydroélectrique et ses faibles températures, le Canada dispose de sérieux atouts pour l'avenir. La Chine en revanche manque de ressources électriques et son climat chaud n'est pas toujours compatible avec la présence de grandes fermes de serveur qu'il faut refroidir. La quête des ressources pour le cyber va peut-être téléporter les combats vers les pôles.

Quant à la sûreté, elle est difficile à garantir. Il y a beaucoup de failles que l'on ne connaît que lorsque l'on est attaqué. Cela conduit les stratégistes à faire une analogie entre la guerre pour le

cyber et les défenses de Vauban. Il s’agit en effet de dissuader grâce à des défenses importantes, de faire usage de coercition en cas d’attaque (ce qui suppose un emploi limité de la force) et de faire usage d’action (emploi de la force sans restriction). La nouveauté apportée par le cyber n’est donc pas tant dans la stratégie, car on y retrouve aisément les cadres classiques pensés par Foch ou Corbett, que dans le changement des acteurs. Ce ne sont plus ici uniquement les États, mais aussi les grandes entreprises, qu’elles soient ou non liées aux États. L’irruption de l’entreprise dans la guerre, la diplomatie et les relations internationales est l’un des changements majeurs de ces vingt dernières années.