SÉCURITÉ ET JUSTICE
LE DÉFI DE
L'INTELLIGENCE
ARTIFICIELLE

JEUDI 7 NOVEMBRE 2019

Intervention de Monsieur Pierre Bellanger
à l'**Institut National des Hautes Études de la Sécurité et de la Justice**
Jeudi 7 novembre 2019

Trois empires et un garde-manger

Le 8 octobre 2019, l'entreprise informatique américaine *Adobe* a fermé tous les comptes de ses clients au Venezuela laissant ainsi, soudain, des milliers d'utilisateurs sans accès à *Photoshop*, le principal logiciel de retouche photographique et à *Acrobat Reader* que nous connaissons pour les documents en *PDF*.

Ce faisant, la société californienne *Adobe* se mettait en conformité avec l'ordre exécutif du président Trump qui, publié début août, interdisait aux sociétés américaines quasiment tout commerce avec le Venezuela.

Ha ! ha ! ha ! Le Venezuela… Cela n'arrivera jamais en France… me direz-vous.

Comme disait, en substance, le général chinois Sun Tzu : *il ne faut pas se demander ce que l'adversaire va faire mais ce que l'adversaire peut faire*. Une telle situation est-elle donc possible en France ? La réponse est oui.

Mais les États-Unis sont nos alliés ! entendra-t-on.

Oui, bien sûr et des alliés précieux. Pour autant, les relations internationales ne sont que rapports de forces. Il n'y a là ni ami, ni alliés inconditionnels, il n'y a que des intérêts communs à un moment donné. Et ces conjugaisons opportunes n'empêchent nullement, et simultanément, entre lesdits alliés, les rivalités les plus dures en termes économiques, en compétition commerciale, en stratégie de renseignement et plus généralement en luttes géopolitiques.

Nous sommes donc à la merci d'autrui.

Les conditions d'utilisation de la plupart des services numériques que nous acceptons, sans d'ailleurs les lire, autorisent ces services à être interrompus pour des *périodes indéfinies* sans que cela ne nous donne droit à une quelconque compensation. Nous avons tous signé et donné notre accord, comme les utilisateurs du Venezuela.

Mais quand même la France, ce n'est pas le Venezuela ! dira-t-on fort justement.

C'est pourquoi nous allons prendre un autre exemple. Un pays qui a près de cinq fois notre PIB : la Chine. Une de ses plus belles entreprises de technologie télécom est *Huawei*. *Huawei* est le second fabricant mondial de mobiles et le premier fournisseur mondial d'équipements de réseaux de téléphonie cellulaire. Après s'être, pour le moins, inspirée de sa concurrence, l'entreprise chinoise s'est désormais propulsée en tête en termes de technologie.

Le 15 mai 2019, le département du Commerce des États-Unis plaçait *Huawei* sur la liste des entreprises *susceptibles de mettre en péril la sécurité nationale.* Dans la foulée, *Google*, *Qualcomm*, *Intel* et *Broadcom* interrompaient leur relation avec *Huawei*. *Huawei* est ainsi privé, pour ses futures ventes de terminaux, d'*Android*, le premier système d'exploitation mondial pour mobile et de ses services associés : *YouTube*, *Maps*, *Gmail* ainsi que de la plateforme d'applications : *PlayStore*. Cette interdiction concerne donc également les fournisseurs de composants, elle s'étend notamment aux processeurs et modems vendus par les sociétés américaines précédemment citées.

Ainsi, dans le cadre d'une tension entre puissances, l'une d'entre elles peut frapper l'autre en utilisant l'arme de la dépendance technologique. Du jour au lendemain, les logiciels, les systèmes d'exploitation, les processeurs et autres équipements informatiques d'une nation peuvent être suspendus par une autre.

Et les données ?

Les échanges sur Internet transitent par quelques centaines de câbles sous-marins. Comme le dit Jean-Luc Villemin, directeur des Réseaux internationaux d'Orange : *la sensibilité d'une économie est proportionnelle à la quantité et à l'importance des informations qui transitent sur ces câbles.*

En France, 80 % du trafic national part aux États-Unis. Ce qu'on appelle le *cloud* et qui est, en fait, l'ordinateur de quelqu'un d'autre, se trouve généralement aux États-Unis. Nous y conservons notre mémoire, notre propriété intellectuelle et notre activité économique.

Une coupure de trafic, à ce niveau de dépendance, à ce niveau d'optimisation des processus par les données, est une interruption de nation. C'est le bouton *off* du pays.

Là encore, les conditions générales d'utilisation de ces services de *cloud* — en français : télématique — sont éclairantes : *dans la mesure où la loi le permet, le service n'offre aucune garantie, expresse ou implicite, quant aux services offerts*. Nous voilà pleinement rassurés, puisque nous avons tous signé.

Mieux encore, la majorité du trafic assuré jusqu'à présent par des opérateurs de télécommunications traditionnels l'est désormais par les principaux acteurs numériques eux-mêmes, cette part prise devrait atteindre les 90 % dans les premières années de la prochaine décennie. Mais, ce n'est pas grave puisque la fameuse *neutralité du Net* garantit l'égalité de traitement… Sauf que cette disposition ne s'applique pas au trafic sous-marin…

On ne va pas couper le trafic d'un pays tout de même !

L'Algérie a vu son trafic interrompu pendant cinq jours en 2015, c'est arrivé aussi en Guinée et au Liban. Une coupure offensive est possible. Les moyens existent et les nations tout autant averties qu'en capacité se testent et s'épient sous les océans.

Plus de logiciels, plus d'informatique, plus de données. C'est tout à la fois le moteur et le carburant qui est sous le contrôle d'autrui. Nous étions des citoyens, nous sommes devenus des utilisateurs.

Certains imaginaient jadis l'Internet comme un métamonde, un ailleurs utopique et bienveillant et prédisaient d'ailleurs la fin des nations, résidus guerriers et autoritaires des siècles précédents. Ils avaient raison, les nations sont supplantées par des empires, des *cyber-empires*.

Une nation est délimitée par ses frontières avec d'autres nations et, à moins d'exceptions, s'en contente. Un empire croît sans cesse, dépasse ses limites, conquiert, absorbe, englobe, soumet et ne s'arrête qu'à la rencontre d'un autre empire… Le réseau est le lieu de ces empires en affrontement constant.

Un cyber-empire contrôle ses données, ses logiciels, ses protocoles, ses adresses, ses chiffrements, ses serveurs, ses composants, ses systèmes et ses processeurs. Un cyber-empire est souverain sur le réseau. Cela s'appelle la maîtrise de son destin numérique, cela s'appelle la *souveraineté numérique*.

Actuellement, le cyber-empire américain règne et deux prétendent accéder à ce statut, chacun à sa manière : le chinois et le russe.

Les États-Unis ont pris politiquement conscience de l'économie de la connaissance et des autoroutes de l'information au début des années 90 avec l'administration Clinton-Gore. L'armée, le renseignement et l'Internet ont depuis formé un écosystème étatique et privé que les guerres antiterroristes n'ont cessé d'amplifier jusqu'à atteindre une puissance globale unique et exceptionnelle. C'est la nouvelle dimension de l'empire américain. C'est, pour ce pays, une nécessité absolue pour amortir le choc numérique, la montée en puissance chinoise et s'assurer, dans ce contexte, la continuité de sa primauté mondiale.

La Chine fut probablement la première puissance mondiale jusqu'au XVIIIe siècle. Deux siècles de perdu que le pays s'oblige à rattraper à marche forcée. Et le déséquilibre démographique qui s'annonce du fait du vieillissement de sa population le contraint à encore accélérer la cadence.

Ici, comme partout, le réseau est la chance de surmonter les épreuves et d'aller encore plus vite. La course chinoise a trouvé son envol par la captation tous azimuts de la propriété intellectuelle occidentale, elle cherche aujourd'hui à garantir son autonomie en développant ses propres ressources.

La Russie, plus vaste pays du monde, mais avec le PIB de la Corée du Sud, a les plus grandes difficultés à se constituer en cyber-empire. Elle s'est pourtant engagée dans cette voie en privilégiant deux axes : l'autarcie et l'offensive. L'autarcie, par la capacité à se couper volontairement du reste du réseau mondial, une loi — la loi *Runet* — a été votée en ce sens à la Douma. La Russie, elle-même très active auprès des câbles sous-marins étrangers, veut se prémunir d'une coupure agressive et garantir le fonctionnement de son réseau. Pour ce faire, elle établit un système d'adressage alternatif, se substituant à l'actuel sous contrôle américain, rapatrie toutes les données sur le territoire russe et centralise les interconnexions des fournisseurs d'accès nationaux.

Quant à l'offensive, il n'est pas un jour sans qu'il soit fait état d'une attaque provenant selon toute vraisemblance de Russie. Le 14 octobre 2019, le secrétaire général de l'*OTAN*, Jens Stoltenberg, a pointé la montée des menaces cyber contre son organisation et a cité un seul *acteur étatique* agresseur : la Russie.

Notre Europe est restée, à bien des points de vue, sidérée par le développement du réseau. Elle y a vu des anges — en anglais : *business angels* — des nuages et des licornes. Elle y a vu des *startups*, des *tee-shirts*, des *likes* et des *smileys*. Elle n'y a pas vu des machines de guerre en croissance exponentielle : une dynamique protéiforme associant de façon symbiotique opérateurs privés et fonds publics. Elle a compris trop tard qu'Internet ne vient pas s'ajouter au monde que nous connaissons, il le remplace.

C'est ainsi que nous avons choisi la subordination, la provincialisation et la colonisation. Nous avons lâché en trente ans près de mille ans d'histoire payés au prix du sang. Et cette Europe qui s'est éventrée - 700 000 victimes françaises et allemandes pour quelques centaines de mètres à Verdun en 1916 - a tout lâché en une flopée de clics.

Jadis, les criminels de guerre se disculpaient en expliquant *qu'ils n'avaient fait qu'obéir aux ordres*. Quant à nous, nous voulions juste jouer à *Candy Crush*.

Nous sommes à cet instant le garde-manger, le minerai numérique ou encore l'éventuel champ de bataille de ces trois empires. À l'instar de cette Afrique disputée par les puissances européennes du XIXe siècle, nous perdons dans ce dépeçage notre substance et notre esprit.

Et c'est d'autant plus tragique que le réseau est notre chance. Notre seule chance de surmonter les défis insensés du monde moderne ; notre seule chance de paix, de liberté et de prospérité.

Intervient ici ce qu'on appelle communément *l'intelligence artificielle*. Je retiens pour définition de l'intelligence : *ce qu'une machine ne peut pas faire* ; je suis donc mal à l'aise avec cette expression. Je lui préfère celle d'*intelligence assistée*. C'est toujours de l'*IA,* mais c'est plus réaliste.

La machine, certes corrige ses erreurs et donc s'améliore par la comparaison entre ses résultats et la réalité, ce qui est remarquable, mais le processus n'en demeure pas moins une somme d'opérations stupides réalisées à grande vitesse.

Steve Jobs avait comparé l'ordinateur personnel à un vélo. Un formidable moyen d'aller plus vite, mais ce n'est pas le vélo qui va vite, c'est le cycliste. C'est le cycliste qui a le sens commun et la capacité de réagir à l'imprévu.

L'*IA* est une source immense de progrès : réduire l'incertitude que nous contrebalancions au XXe siècle par le gaspillage ; supprimer la routine qui a réduit à l'état de machines précaires des générations d'êtres humains et fait perdre un temps considérable à tous. Les automates décisionnels vont nous soulager d'un fardeau considérable. Et, c'est un champ d'innovations formidable qui s'ouvre à nous.

Mais, sans souveraineté numérique, c'est le processus le plus radical pour nous asservir et définitivement vider les meilleurs morceaux restants, tout autant que les dernières miettes du garde-manger numérique européen.

Pour nous sortir de cette nasse, deux moyens :

Il faut tout d'abord arrêter de parler de données personnelles. Une donnée personnelle ne renseigne que sur sa source. Or, aujourd'hui, les données se renseignent mutuellement, se déduisent, se corrèlent entre elles… En ce sens, définir des données par leur degré de confidentialité est bien hardi. Et puis, à qui appartient l'information sur un rendez-vous ? Et ce que j'appelle *mon carnet d'adresses* n'est pas autre chose que les adresses des autres, sur lesquelles je n'ai aucun droit, mais que des devoirs. Les données de chacun et des autres sont indissociables et chacun y conserve pourtant ses propres droits. Elles forment donc une totalité en multipropriété, c'est, en droit, une indivision. Et c'est, pour une nation, un *bien commun souverain*.

Un bien commun régit par nos lois, localisé sur notre territoire, chiffré par nos protocoles, transitant par des télécommunications sous nos lois, alimentant des algorithmes assujettis à nos règles et disposant, comme le dollar, de protections internationales, garanties par nos chiffrements souverains.

Cela vaut aussi pour les métadonnées, ces informations qui qualifient les données, comme la date ou le lieu d'une photo.

Les machines, les appareils, les capteurs, bref les intelligences numériques et leurs systèmes d'exploitation utilisés sur notre territoire intégreront un correctif obligatoire garantissant l'intégrité et les conditions d'usage de nos données, notre bien commun souverain.

Il est probable que cette démarche suscitera des oppositions. Mais, ce n'est qu'une étape : les sociétés américaines opérant en Chine se sont conformées à des mesures analogues.

Avec les données de nos citoyennes et de nos citoyens, nous faisons ainsi nation numérique et y appliquons les lois de la République.

Et n'oublions pas que les machines et services de nos amis américains sont soumises au *Patriot Act* qui donne à leurs agences de renseignement un accès sans mandat à toutes les données transitant, traitées ou stockées par des sociétés américaines et leurs filiales, quel que soit leur territoire d'implantation. S'y est ajouté récemment le *Cloud Act* qui étend cette faculté aux institutions judiciaires et policières américaines. Nous voilà, *de facto*, sous droit américain.

Bien des nations européennes s'en inquiètent, notamment en France et en Allemagne et lancent des initiatives de télématique souveraine. En Allemagne, 96 % de la fonction publique dépend des suites *Microsoft Office* et 69 % des services de l'administration stockent leurs données sur les serveurs de cette belle entreprise.

Le secteur privé n'est pas en reste : 80 % des principales entreprises du *CAC 40* en France et du *DAX* allemand utilisent l'excellent *Amazon Web Services*.

Cette subordination, volontaire ou par défaut, est incompatible avec notre souveraineté numérique.

Elle est illégale, dans les conditions actuelles, dès lors que les données deviennent par la loi un bien commun souverain.

Les composants, les logiciels, les serveurs, les routeurs et échangeurs qui traitent nos données et par lesquels transitent notre trafic doivent également échapper à toute tutelle étrangère.

Cela ne signifie aucunement perdre les services et les appareils que nous apprécions tant. Ils sont bienvenus. Ils fonctionneront simplement dans notre cadre juridique.

Certains disent que nous avons perdu les compétences, que l'avance technologique américaine est telle qu'il est désormais impossible de contester cette situation et plus encore, pourquoi pas, de vouloir se lancer dans des initiatives autonomes. En fait, il est aberrant de s'être mis dans cette situation. Et il est irrationnel de ne pas se donner les moyens d'en sortir.

Le premier point était donc le nouveau statut juridique des données dont la prise en compte de l'organisation en réseau est capitale.

Le second point a trait à la compréhension de l'économie numérique : il faut passer d'une vision d'économie traditionnelle, digne du *bac Sciences économiques et sociales*, à une économie de guerre cyber. Dans cette économie, les données sont la monnaie première et la monnaie fiduciaire est secondaire. Ainsi, un réseau social peut brûler un milliard de dollars avant d'avoir un plan d'affaires, car il vaut bien plus par ses enjeux de renseignement.

Lorsqu'en 1935 le radar est développé en Grande-Bretagne par Robert Watson-Watt, il est probable que s'il lui avait été demandé ses perspectives de rentabilité, il serait resté coi. Dès lors, les aviateurs allemands, leurs chasseurs et bombardiers, indétectables faute de radar, auraient gagné, en 40 et 41, la bataille d'Angleterre.

Nous devons quitter l'écume libérale qui nous est présentée comme motrice de cette mutation numérique et comprendre qu'elle est portée par de colossaux investissements d'État, tout à la fois en provenance de l'armée et du renseignement.

L'État français, quant à lui, s'est engagé à mobiliser un milliard et demi d'euros pour l'*IA* de 2018 jusqu'en 2022. C'est une prise de conscience, un premier pas et un encouragement à l'investissement privé. Cela nous place encore dans la course, mais loin derrière, les États-Unis, la Grande-Bretagne, la Chine ou le Canada. C'est probablement un dixième de l'investissement déclaré, américain ou chinois, sur la même période.

C'est sur trois ans, 16 % du budget annuel 2017 de *Facebook* en recherche et développement et 8 % de celui d'*Alphabet*, la maison-mère de *Google*. C'est certainement pourquoi, pour peser plus, la France inscrit l'*IA* dans l'agenda européen.

Espérons cependant que pour entraîner nos algorithmes apprenants, il nous soit permis d'emprunter nos propres données stockées à l'étranger…

Souhaitons aussi que ces belles initiatives sachent retenir nos talents naturellement tentés à mener cette course ailleurs pour la mener en tête.

Autre défi : l'informatique quantique. Cette technologie est l'application numérique du *en même temps* puisque les bits peuvent simultanément prendre les valeurs 0 et 1. Ce qui démultiplie leur puissance. Ces ordinateurs, qui réalisent en quelques minutes des opérations qui auraient pris des milliers d'années à un supercalculateur traditionnel, vont, eux aussi, bouleverser les rapports de force. En effet, par exemple, la résistance de nos chiffrements classiques est proportionnelle au temps nécessaire pour les déchiffrer. C'est donc avec le quantique, le risque d'une vulnérabilité presque absolue.

Pour bien faire, un plan pour l'informatique quantique va être lancé au niveau national, s'ajoutant à l'initiative européenne de soutien engagée en 2018.

Nous voyons, ici encore, cette bonne volonté publique utilisant tous les leviers à sa disposition pour agir. Régulièrement, les observateurs soulignent cependant la difficulté à passer de la recherche au marché. Ce qui a pour conséquence l'échec, trop souvent, de nos efforts. Probablement parce que l'on oublie que, dans le numérique, la passerelle entre le laboratoire et le commerce, ce ne sont pas les fonds d'investissement, qui interviennent plus tard et sur des critères économiques, ce sont les financements et les besoins de l'armée comme du renseignement.

Dès les années 30, le creuset innovant d'ingénieurs en électronique proches de l'université de Stanford, cerveau de la *Silicon Valley*, fut propulsé par les commandes de guerre en radars et en dispositifs pour l'aéronautique. Puis, au début des années 60, la course à l'espace et l'invention du transistor en relancèrent l'expansion : *Silicon Valley* est la réponse à *Sputnik*. L'investissement indistinctement public et militaire est le père nourricier depuis 90 ans de tout l'écosystème électronique puis numérique américain. Il n'y a pas de *Silicon Valley*, hier comme aujourd'hui, sans l'apport considérable de l'armée américaine et de ses dérivés en recherche, ressources et carnets de commande.

Plus récemment, le *CyberSpark*, ouvert à Beersheba en 2014 en Israël est un campus hybride qui rassemble entreprises et centres de recherche dédiés à la cybersécurité : il a pour moteur initial et continu l'investissement et l'expertise militaires.

La dynamique et l'attraction de cette pépinière créative soutenues par plusieurs milliards de dollars d'investissement combinés sont telles qu'Israël reçoit 20 % des financements privés mondiaux consacrés à la cybersécurité et se place ainsi au second rang mondial derrière les États-Unis. L'armée est le catalyseur et le réacteur de ce succès.

Dans le monde numérique, la distinction entre le civil et le militaire n'est pas pertinente. Le réseau est une zone de guerre et chaque terminal est à la fois arme contre nous ou avec nous, selon qui le contrôle. Le réseau est civil et militaire tout à la fois. Il est *civilitaire*. Les trois cyber-empires russes, chinois et américains ne fonctionnent pas autrement. Seuls les écosystèmes civilitaires sont compétitifs.

Il est probable qu'un nouveau champ de compétition confirmera encore cette alliance : le *new space*, le nouvel âge spatial, c'est-à-dire l'ouverture de l'espace aux acteurs du marché, comme *Space X* et *Blue Origin*, mais aussi à de nouveaux états aux ambitions spatiales tels que l'Inde, le Brésil ou la Malaisie… Et les dimensions militaires et civiles seront ici aussi inséparables. La Norvège lance deux satellites pour l'Arctique, ils seront dotés de capacité défensive. Et les grandes nations, y compris la France, se préparent à la militarisation de l'espace.

Je l'ai dit la catégorisation des données est une fiction puisqu'elles se déduisent les unes des autres. Une information collectée par une appli de jogging sur le parcours d'un sportif, lorsque c'est un militaire, est une information militaire.

De la même manière, croire qu'un collecteur de données ne les réserve qu'à son usage est au-delà du naïf. Les données circulent comme l'argent.

Toute donnée collectée par un opérateur privé est à la disposition de son État d'origine, de même toute information recueillie par un agent public, ou sous contrat, est communiquée aux entreprises de sa nation en compétition à l'étranger. Les mêmes circuits qui servent à la capture d'un terroriste sont employés pour récupérer des plans de turbine ou la configuration d'une molécule. S'y intercalent d'ailleurs officines grises et hybridations en tout genre. Le renseignement d'État et l'intelligence économique sont indissociables et consubstantiels l'un de l'autre.

La pire situation dans cette guerre numérique et de se croire en paix et de continuer à raisonner exclusivement en intérêt économique alors que la compétition, aux apparences trompeuses de pures entreprises, s'appuie en fait sur des ressources illimitées. C'est le pays qui est en jeu et pas le rendement des capitaux. Quand on se bat, on ne compte pas.

Il faut fonctionner avec trois monnaies. Une monnaie de long terme : la sécurité nationale commanditée par l'armée ; une monnaie immédiate, la donnée, financée par le renseignement. Et enfin le marché, qui s'intercale utilement entre les deux, avec ses ambitions de retour sur investissement à moyen terme et avec pour monnaie l'euro, mais qui, on le constate, ne peut être seul à porter la nation entière.

Nous n'avons aucune chance si nous continuons à être unidimensionnels dans notre calcul de valeur alors que notre compétition est tridimensionnelle.

C'est la raison de l'absence de géant de l'Internet européen.

Pourquoi cette naïveté de notre part ? Nous sommes les peuples des Machiavel, Talleyrand et Bismarck… Pourquoi sommes-nous à présent les Petit Nicolas de l'Internet ?

J'ironise pour alerter. Je sais les engagements, les talents qui œuvrent au quotidien et certainement j'ignore bien des développements en cours. Je les salue ici avec respect et reconnaissance.

Cependant, c'est pour mieux encore valoriser et faire effet de levier sur ces initiatives qu'il faut placer notre investissement collectif sur l'*IA* dans ce contexte de guerre cyber. Il ne nous sera laissé aucune place, aucune chance, aucun espace qui n'aura été conquis ou défendu. Comme jadis et toujours, seule notre volonté fait face à l'adversité.

Je vous remercie.