LA SOUVERAINETÉ NUMÉRIQUE,

CONDITION DE LA SECURITÉ NATIONALE ET DE LA DÉFENSE

Intervention de M. Pierre Bellanger

Le 28 septembre 2015

Assurer l'intégrité du territoire et la protection des populations contre les agressions armées ; garantir la souveraineté, l'intégrité territoriale et l'indépendance politique, si elles sont mises en cause ; enfin, contribuer à lutter contre les menaces à l'encontre de la sécurité nationale - c'est-à-dire la vie de la nation - : telles sont, en quelques mots, les missions de la Défense.

Dans ce contexte, le développement du cyberespace, de ses machines et de ses réseaux, a mis en évidence un nouveau champ de dangers qui font l'objet aujourd'hui d'une prise en compte sérieuse par la Défense, et par les pouvoirs publics en général, avec tout autant de réflexions prospectives et stratégiques que d'actions opérationnelles concrètes.

Ainsi, ce nouveau risque est venu s'ajouter aux domaines d'intervention existants pour que s'y déploient les réponses appropriées.

Tel ne sera pas l'objet de mon propos.

En effet, chaque secteur de la société confronté au réseau numérique s'adapte pour y apporter une réponse catégorielle souvent pertinente. Mais l'efficacité et la permanence de ces efforts sont fragiles, car ils n'ont pas de fondations solides : leur point d'appui est le réseau. Or, nous ne sommes pas souverains sur le réseau.

L'internet est un changement global qui oblige à une réponse globale. Sans cette prise de conscience, qui est le cœur de la souveraineté numérique, toutes les initiatives partielles sont vouées, à terme, à l'échec, y compris en matière de sécurité nationale et de Défense.

L'Internet et son environnement informatique ne vient pas seulement donner une nouvelle dimension au monde que nous connaissons. Il le remplace.

Et, en le remplaçant, il remet en cause les bases de la société : son ordre public, sa sécurité nationale et sa défense.

Qu'advient-il, en effet, du territoire, de la loi, de l'indépendance, de la souveraineté, lorsqu'une part croissante de la vie de la nation se transfère sur le réseau ?

Tel est le défi de la souveraineté numérique.

*

L'idée centrale est la suivante : sans souveraineté numérique, la mission de défense n'est plus exécutable.

La souveraineté numérique est la condition de la Sécurité nationale et de la défense.

Il en résulte pour l'institution militaire l'obligation urgente d'alerter la Présidence et le Gouvernement sur cette nécessité.

*

Mon propos s'articulera ainsi :

- La dynamique du réseau
- L'effet du réseau sur la société
- Les mythes et réalités d'Internet
- La souveraineté numérique et les conséquences de son absence : sur la société, sur la sécurité nationale
- Le modèle américain
- Le réseau et les États
- La souveraineté numérique : une décision politique
- Trois actions pour établir la souveraineté numérique
- Comment agir maintenant ?

*

La dynamique du réseau :

L'efficacité des systèmes informatiques qui composent le réseau double tous les ans. Entre 1995 et 2015, leur puissance, à prix égal, a été multipliée par un million.

La vitesse d'exécution des logiciels a, quant à elle, progressée 43 fois plus rapidement.

Ainsi ces vingt dernières années, la performance conjuguée des programmes et des machines a été multipliée par 43 mille milliards de fois et doublera, pour les seuls systèmes, dans les douze prochains mois.

Cette double exponentielle technique et logique est multipliée à son tour par l'effet réseau.

L'effet réseau statue que la valeur d'une machine est proportionnelle au nombre de machines auxquelles elle se connecte.

On le comprend intuitivement : la valeur d'un téléphone est proportionnelle au nombre de personnes avec lesquelles il vous permet de communiquer.

Une machine, connectée à neuf autres, vaut, puisqu'il y a 10 machines au total, 10 au carré, soit 100. Une onzième machine se connecte. La valeur de chacune passe à 11 au carré, soit 121. 21 % de croissance de valeur avec une seule machine.

Des centaines de milliers de machines rejoignent le réseau chaque jour.

Le nombre de machines et d'appareils reliés au réseau est passé de 200 millions en 2000, à 15 milliards en 2015 et sera de 40 milliards en 2020.

C'est donc une triple exponentielle technique, logique et économique. C'est un vertige au-delà de notre compréhension.

Nous ne savons pas nous représenter les exponentielles. Un exemple : plions une feuille de papier en deux, puis en quatre, cinquante fois de suite. Quelle est l'épaisseur finale du pliage ?

La réponse étonne : 114 millions de kilomètres, soit les ¾ de la distance de la Terre au Soleil.

L’effet réseau s’applique aussi à l’humanité.

Trois milliards de connectés, déjà 40 pour cent de la planète, et 5 milliards prévus en 2020. Jamais autant d’individus dans le monde n’ont eu autant de possibilités, de choix, d’informations et d’échanges. Jamais, il n’y eut une telle puissance informatique disponible pour chacun et en réseau.

Notre émancipation est égale au carré de toutes les émancipations auxquelles elle se connecte.

L’humain est un devenir constant. Ainsi, l’amélioration de chaque connecté accroît notre propre valeur et celles de tous les autres.

Ainsi, l’humanité peut faire un saut évolutif sans précédent avec le réseau. Ce qui nous changera tous intimement et collectivement.

Le réseau est notre chance.

L’effet du réseau sur la société :

Les efforts, les projets, les investissements recherchent le meilleur rendement, c’est-à-dire la croissance de valeur la plus rapide. C’est ce que leur donne l’effet réseau.

L’effet réseau reconfigure la société : les machines informatiques se lient en réseau : ce sont les grappes de serveurs ; les réseaux de machines se lient en réseau : c’est Internet ; les documents se lient en réseau : c’est le Web ; les personnes se lient en réseau : ce sont les réseaux sociaux. Et maintenant les objets, les capteurs et nos corps qui les portent se connectent à leur tour.

Le réseau des réseaux informatiques, Internet, chaque jour plus productif, efficace et rapide, devient le grand concentrateur de valeur.

Il capte ainsi la valeur de la société, de toutes les industries, de tous les services, car il les remplace par une meilleure productivité, un meilleur rendement et surtout un meilleur service.

Les mythes et réalités d'Internet :

Il nous a fallu collectivement du temps pour comprendre l'Internet.

Voilà tout d'abord, ce qu'il n'est pas :

L'Internet n'est pas une utopie libertaire et mondialisée, hors-sol. Si en surface, prévalut une dynamique généreuse à la *Flower Power* des années 60 ; en profondeur, son origine date des années 50 et de la *Guerre Froide*. L'Internet est une extension de la nation américaine.

L'Internet n'est pas seulement le terrain de jeu d'entrepreneurs talentueux et de jeunes sociétés de technologie. Il répond depuis des décennies d'une volonté sans précédent des États-Unis, tout à la fois politique, scientifique et militaire.

L'Internet n'est pas gracieusement mis à notre service. Sa matrice et son moteur est l'industrie du renseignement. Sa fonction première est la collecte d'informations. En tant qu'utilisateurs, nous sommes comme les dindes qui, certainement, pensent, jusqu'à Noël, que tout le monde s'affaire pour leur bien-être.

L'Internet n'est pas un phénomène singulier, hors du droit par nature. Au contraire : vous n'avez jamais signé, d'un clic, autant de contrats pour en utiliser les services.

L'Internet n'est pas virtuel. Il est constitutif du réel. Le réel, c'est ce qui fait mal. L'Internet fait mal.

L'Internet n'est pas un nouveau secteur de l'économie ou de la société. Il devient l'économie toute entière. L'Internet ne s'ajoute pas au monde que nous connaissons, il le remplace.

L'Internet n'est pas un futur réservé à des passionnés de technologie, il est notre présent et notre quotidien. De l'inscription à la cantine scolaire jusqu'à l'existence même de millions d'entreprises, petites ou grandes, Internet est indispensable à tous aujourd'hui.

L'Internet n'est pas une bataille perdue dont on se contentera des miettes. En fait, il n'y aura même pas de miettes. En fait, rien n'est encore définitivement joué.

Enfin, l'Internet n'est pas une menace, mais notre chance. Il sera notre premier problème seulement si nous ne savons pas en faire notre principale solution.

La souveraineté numérique et les conséquences de son absence :

Sur la société :

Nos machines, les réseaux, les programmes et les services que nous utilisons ne répondent pas de nos lois.

Un exemple l'illustre tragiquement.

En juin dernier, un attentat terroriste en Isère se conclut par la décapitation du directeur commercial d'une usine de gaz industriels et le criminel, qui en est l'auteur, poste sur le réseau la photo de la victime décapitée.

La publication de la photo de cette personne ainsi mutilée, dans une macabre mise en scène, est constitutive d'atteintes graves à la dignité humaine, ainsi qu'à la vie privée et familiale, toutes interdites par la loi.

En France, ce droit à la dignité de la personne humaine est un principe à valeur constitutionnelle.

La *Grande Chambre de la Cour européenne des droits de l'homme*, la *CEDH*, a confirmé cette doctrine après la publication des photos du Préfet Érignac, assassiné en 1998.

Mais notre constitution et nos lois ne s'appliquent pas aux réseaux sociaux étrangers.

Ils répondent de leurs conditions générales d'utilisation et en dernier ressort de la loi de leur pays d'origine.

Ces conditions générales sont extraordinairement rigoureuses pour interdire l'exposition du corps humain dans sa beauté : les photos laissant apparaître des tétons féminins y sont, par exemple, proscrites et immédiatement supprimées.

D'ailleurs, face à cette censure sans appel, des associations de victimes de cancer du sein ont dû batailler pour obtenir une précaire dérogation.

En revanche, la violence bénéficie d'une large tolérance. Ces services laissent en ligne des images particulièrement choquantes, dès lors qu'elles ne bénéficient pas d'un cautionnement explicite, ou encore ne s'accompagnent pas de menace directe contre des personnes ou des groupes de personnes identifiées.

La photo sanglante n'entrant pas dans ces catégories est ainsi laissée en ligne et se distribue sur plusieurs réseaux sociaux.

Le gouvernement français n'a aucun pouvoir coercitif direct pour appliquer la loi. Les lois de police sont inapplicables. Il ne peut ni agir, ni ordonner dans l'urgence.

Une procédure judiciaire, quant à elle, se heurterait à une demande des avocats de ces services pour que le Tribunal de Grande Instance se déclare incompétent au profit des juridictions, pour les plus habituelles, du district nord de Californie et du Tribunal de San Mateo County.

Là-dessus, la Justice hésiterait entre plusieurs jurisprudences contradictoires. Pendant ce temps, le mal serait fait et amplifié avec la puissance du réseau.

Nos autorités en furent donc réduites à demander à ces services de bien vouloir avoir la bienveillance de retirer la photo.

Bien qu'une procédure amiable et spécifique de saisine exceptionnelle par les pouvoirs publics eut été mise en place peu de temps auparavant, un des services ne s'exécuta qu'après douze heures, le second, trois jours plus tard.

Douze heures, trois jours. Ce sont des éternités sur le réseau.

C'est le temps d'atteindre ses objectifs pour un adversaire qui veut frapper les opinions.

Le terrorisme est une forme de guerre. Une guerre qui efface la distinction entre intérieur et extérieur, réel et réseau. Une guerre informationnelle. Une guerre sur notre territoire.

Comment gagne-t-on une guerre lorsqu'on est désarmé ?

La photo est publiée, transmise sur des réseaux courants dans notre sol, ou diffusée sur notre spectre hertzien par les antennes de télécommunications. Elle est vue sur le territoire national par nos citoyens et pourtant nous n'y pouvons rien.

Elle restera accessible le temps que l'éventuelle plateforme client en Irlande d'un de ces services en décide, ou choisisse d'en référer au siège, non loin de San Francisco ; ou bien encore, depuis peu, que leur cellule dédiée veuille bien accéder aux sollicitations polies de l'État français.

En Grande-Bretagne, la vidéo de décapitation d'un otage britannique, David Haines, publiée sur les réseaux sociaux, suscita un sentiment d'effroi et une demande de retrait de la part du gouvernement.

Après l'avoir enlevée, un des réseaux sociaux prit finalement la décision de maintenir les vidéos de décapitation, pour autant qu'elles soient assorties d'un commentaire négatif.

Le premier Ministre britannique qualifia ce revirement comme "irresponsable", sans pour autant pouvoir agir.

Ce seul commentaire d'accompagnement de ces images : "Défi : est-ce que quelqu'un arrivera à regarder cette vidéo ?" fut suffisant pour qu'une vidéo de décapitation soit maintenue en ligne sur ce réseau social et, éventuellement, assortie d'un message d'avertissement.

Notons que, soucieux d'entrer sur le marché chinois, dont il est exclu, le principal réseau social américain détruit sans délai les vidéos d'auto-immolation de résistants tibétains ou les publications d'activistes chinois, militants des droits civiques dont il ferme d'ailleurs les comptes.

Mais ici, en Europe, la seule règle est l'impuissance publique.

L'absence de loi viole la loi. L'absence de loi est contraire à l'ordre public. L'absence de loi sur le réseau est contraire au maintien des libertés.

Sans loi, sans ordre public, sans autorité - ni de droit, ni de fait - sur le réseau. Que reste-t-il de la République ?

La souveraineté numérique est l'inverse de cette impuissance.

La souveraineté numérique est la maîtrise de notre destin sur les réseaux informatiques. C'est l'extension de la République dans cette immatérialité informationnelle qu'est le cyberespace.

Sans souveraineté, pas d'ordre public donc pas de droit ; sans droit, pas de liberté. Et sans liberté, que reste-t-il ?

C'est en même temps, tout notre édifice économique et social qui s'effondre.

Nous sommes, sur le réseau, sous tutelle étrangère.

La formidable chance du réseau est partie pour être compromise et aboutir à l'effet exactement inverse : appauvrissement, asservissement et destruction.

De tant de promesses, il ne restera que les périls.

En effet, toute la valeur qui se transfère vers le réseau, et que celui-ci multiplie, nous quitte pour ailleurs.

Toutes les données qui fondent cette nouvelle économie sont siphonnées.

Une étude du *Boston Consulting Group* estime que d'ici 2020, les données personnelles de 500 millions d'Européens, actuellement pillées, représenteront une valeur de 1000 milliards d'euros.

Le travail, les idées, les emplois, les richesses sont aspirés et tout l'écosystème national, tout l'équilibre social mis en péril.

Les réseaux sociaux sont en Californie et les plans sociaux en Picardie.

Ce que la mondialisation a fait aux classes populaires, Internet commence à le faire subir aux classes moyennes.

Selon l'université d'*Oxford*, la moitié des emplois seront automatisés, c'est-à-dire remplacés par des machines, d'ici deux décennies. La moitié !

Certes, de nouveaux postes et compétences apparaîtront, mais comment financer la transition si les ressources créées par le réseau sont ailleurs et souvent aux îles Caïmans ?

Selon John Chambers, dirigeant de *Cisco*, - une des principales sociétés informatiques spécialisée dans les serveurs et les réseaux - un tiers des entreprises devrait disparaître ces dix prochaines années, compte-tenu de la numérisation. Les deux-tiers restantes tenteront de devenir des versions numérisées de leur activité, mais près de la moitié échoueront. Ne resterait finalement qu'un tiers d'entreprises survivantes parce qu'ayant réussi leur mutation numérique, mais désormais subordonnées aux puissances du réseau.

Que laissera ce bouleversement ? Probablement, une société déchirée entre une hyperclasse propulsée par le réseau et une masse en rupture, précarisée, disputant aux machines le travail restant.

Il subsistera une société aux mains des grands acteurs d'Internet qui contrôleront le réseau en en concentrant la productivité et la fortune. Ils seront devenus les nouveaux maîtres, les nouveaux états.

Ce régime numérique est en train de réussir, avec notre consentement, un coup d'État invisible et non violent, nous faisant croire que sa domination est la condition du progrès.

Nos libertés n'auront comme espace que ce que leur permettront les conditions générales d'utilisation qui alors auront remplacé le droit.

L'ordre public répond de notre droit de vote. Ce nouvel ordre privé ne répondra qu'à ses intérêts.

Le citoyen vivra dans un monde informationnel qui orientera ses achats et ses choix à son insu.

Une étude récente montre que la manipulation du rang des premiers résultats sur un moteur de recherche fait varier, en une seule cession de consultation, de vingt pour cent le choix d'électeurs indécis à la primaire américaine.

La collecte de données de santé et de comportements permettra d'agréger des communautés par risque et ainsi de faire exploser ce qui reste des logiques collectives de mutualisation, que cela soit pour les assurances, les prêts bancaires et bien entendu pour la sécurité sociale.

À chacun selon ses données. À chacun, piégé par ses données, de devenir une équation à traire ou à éjecter du système.

Le réseau fonde de nouvelles solidarités qui fragmentent les entraides et coopérations traditionnelles. Pourquoi pas, si c'est pour mieux servir chacun et l'intérêt général. Mais si ces nouvelles solidarités sont hors du droit et ne répondent que d'objectifs privés, au lieu de maintenir le tissu social par un effort de répartition, elles le démembreront jusqu'à faire de chacun l'ennemi de l'autre.

Tel est l'horizon.

L'absence de souveraineté numérique saigne notre pays comme un animal.

Sur la sécurité nationale :

Pour défendre une indépendance, une souveraineté, une population, encore faut-il qu'elles existent.

Que reste-il à défendre ?

La défense du territoire est conçue pour repousser un ennemi. Mais là, nous ne sommes pas envahis par une armée, nous sommes envahis par un territoire : le réseau lui-même.

Et nos citoyens migrent en masse sur ce réseau : une nation entière de doubles numériques s'y est agrégée, comme l'océan de débris de plastique au milieu du Pacifique, foule apatride de sans-papiers numériques, dont l'existence dépourvue de droit dépend de nations étrangères.

Et cette multitude de cyber-migrants ne cesse de croître, rejointe par des entreprises, en nombre, assujetties à des contrats léonins et dont le chiffre d'affaires est soumis, sans recours, à l'arbitraire de plateformes numériques lointaines aux conditions irrationnelles.

Comment défendre un morceau de sucre plongé dans un verre d'eau ?

Enfin, nous sommes entrés dans l'âge des réseaux.

Les nations historiques affrontent des réseaux de services numériques dont la puissance en fait des états. La capitalisation des cinq premières entreprises mondiales d'Internet est de 1 600 milliards de dollars avec des trésoreries de centaines de milliards de dollars. D'ailleurs, avec 65 milliards de dollars de chiffre d'affaires, une entreprise comme *Amazon* a un revenu supérieur au PNB de la moitié des pays du monde.

En 2011, le chiffre d'affaires d'*Apple*, 73.7 milliards de dollars, a dépassé pour la première fois le solde de trésorerie du gouvernement américain. Le chiffre d'affaires d'*Apple* en 2014 était de 183 milliards de dollars, sa capitalisation boursière était de 700 milliards de dollars, soit 100 milliards de plus que le budget militaire américain la même année.

Les nations historiques affrontent, par ailleurs, des puissances économiques immatérielles que sont les masses financières qui s'échangent annuellement sur les réseaux électroniques : deux millions de milliards de dollars, soit 25 fois la production de richesses annuelles de la Terre.

Les nations historiques affrontent enfin des organisations criminelles organisées en réseau : des mafias mondialisées jusqu'aux mouvements radicaux terroristes. Leur organisation en réseau polymorphe, insaisissable et évolutif en est la principale force.

Enfin, nous sommes sur le réseau dans une situation nouvelle.

L'atome a conduit au concept de guerre impossible par la probable destruction mutuelle des belligérants.

Le réseau engendre celui de paix impossible.

L'augmentation constante du nombre de connectés et la croissance exponentielle du pouvoir de nuire de chacun rend la paix statistiquement impossible. Nous sommes en état de paix impossible.

Chaque grain de sable peut faire sauter la plage.

Comment maintenir la sécurité nationale lorsque, désormais, elle sera perpétuellement atteinte et menacée en son sein par des acteurs, intérieurs ou extérieurs, indécelables et non identifiés ?

Ici, comme désormais à chaque fois, le réseau est central.

Mais les machines, leurs processeurs, les systèmes d'exploitation qui pilotent ces machines, les programmes, les services que nous utilisons et finalement le chiffrement qui protègent le secret des informations, tout cet écosystème numérique répond d'une souveraineté étrangère.

En conséquence :

Il n'y a plus de secret. Toutes nos actions, nos pensées, nos paroles sont transparentes à autrui et donc accessibles, pour nous affaiblir et nous nuire.

Et il n'y a pas de système informatique durci, conçu comme étanche au réseau global, qui puisse empêcher cette disparition du secret. Car le choix est alors entre efficacité et secret. Fermé au réseau, le système perd son effet multiplicateur ; ouvert à un réseau - aujourd'hui non maîtrisé et donc possiblement hostile - le système clos devient vulnérable à toutes les intrusions. Que cela soit par erreur ou négligence humaine ou bien par faille logicielle, ces systèmes, de fait pseudo-fermés, finissent toujours perméables au réseau.

Nous sommes en état de transparence forcée.

L’échange d’informations avec les alliés est de plus en plus asymétrique. Même s’il nous reste le travail de terrain et quelques grands réseaux physiques, nos secrets sont éventés et se dévaluent.

Nous devenons dépendants d’une information collectée par d’autres, sans moyen autonome d’en vérifier la véracité ou l’intégrité.

La collecte de données sur nos citoyens, faite à partir de toutes les machines et services informatiques en réseau sur le territoire national, nous échappe de plus en plus - les informations partent pour la plupart sur des serveurs outre-Atlantique - en conséquence, les fonctions de recherche et de détection relèvent trop souvent de l’accès conditionnel à des bases de données étrangères.

C’est une vassalisation par l’information.

Sans contrôle sur le chiffrement, les conversations électroniques sur notre territoire deviennent peu à peu impénétrables aux services en charge de la sécurité nationale.

Deux terroristes utilisent une application populaire de messagerie sur mobile protégée par une cryptographie forte que nous n’avons pas les moyens ou le temps de décrypter. Que se disent-ils ? On ne sait pas.

Et si la nouvelle loi contraint les prestataires de cryptologie à transmettre les clefs de leurs codes, la question demeure posée de l’application réelle de la loi à des prestataires étrangers de services étrangers sur des plateformes étrangères. Et dans quels délais …

Nous devenons opaques à nous-mêmes.

Les machines étant contrôlables à distance à notre insu. Toutes les manipulations sont possibles, multipliant les erreurs, les fausses pistes et les incriminations erronées. Il n’y a plus de preuves, d’information, ni de fait certain.

Nous ne pouvons plus faire confiance au réseau.

Les machines, les détecteurs, les armes intelligentes peuvent être limités pour que, sciemment, des personnes ou des informations échappent au contrôle. Déjà, certains drones verrouillent dans leur processeur de géolocalisation des zones aériennes devenues interdites ; parfois même des emplacements survolés n’apparaissent plus sur les photos, à la surprise de leurs opérateurs.

L'actualité vient de montrer que *Volkswagen* avait pu équiper 11 millions de véhicules, à l'insu des États et pendant des années, avec un logiciel de trucage faussant les mesures de pollution.

Quels sont les logiciels cachés qui s'abritent actuellement dans nos machines et nos réseaux ?

Demain, des individus ou des dispositifs pourraient ainsi échapper à tout repérage électronique, par le fait même des machines sensées les surveiller.

Nous ne pouvons plus faire confiance à nos machines.

Les chaînes de commandement pyramidales sont particulièrement sensibles à des tromperies issues de réseaux et de machines susceptibles de répondre d'instructions occultées ou provenant de portes dérobées. Les ordres sont-ils véritablement les ordres ? Les informations montantes ne sont-elles pas faussées ? Ne sont-ce pas des intrusions indétectées parce qu'indétectables ?

Nous ne pouvons plus faire confiance à nous-mêmes.

D'un point de vue militaire, il faut voir le terrain européen de demain comme un maillage de millions de micro-intelligences en réseau. Les capteurs, les processeurs seront partout et en résonnance. Il sera impossible d'agir sans dialoguer constamment en profondeur et en confiance avec ce réseau. Si ce réseau joue contre l'informatique militaire, c'est le risque de paralysie, sans ressources, sans visibilité, perdus dans un état hallucinatoire. Que faire quand son propre système nerveux devient ennemi ?

Enfin, la vitesse est ici capitale. L'accès à toutes les machines et à toutes les puissances de calcul est déterminant. Plus on a de données et de capacité à les analyser, plus on va vite et plus on ralentit le temps.

L'œil d'une mouche gère deux cents images par seconde, huit fois plus vite qu'un humain. Lorsqu'il pleut les gouttes descendent huit fois moins vite relativement pour une mouche que pour humain. La mouche se faufile entre les gouttes. L'acquisition et la vitesse de traitement des données ralentissent le monde.

Seule cette capacité de ralentir le monde par le traitement sera en mesure de compenser l'afflux d'informations au cours d'une action d'envergure et donc de donner les moyens de l'anticipation et de la décision.

Sans maîtrise du réseau, l'initiative sera adverse et le brouillard de la bataille ne sera que de notre côté.

La population, quant à elle, doit être comprise, grâce aux téléphones mobiles, comme un réseau dynamique de dizaines de millions de super-ordinateurs de poche. Ils sont sous le contrôle d'une puissance étrangère et nous ne pourrons échanger avec nos propres citoyens, pour les alerter ou les mobiliser, qu'avec son aval. À contrario, nous ne pourrons arrêter les messages de manipulation, de propagande ou de désinformation sur 70 millions de terminaux.

Jadis, une balle perdue tuait une estafette à cheval porteuse d'un message capital et le sort de la bataille chavirait en faveur de l'ennemi. Aujourd'hui, le message finirait dans le dossier "courrier indésirable".

Toute la société peut être désorganisée à partir d'un clavier et d'un écran. Les couloirs aériens, les distributeurs de billets, le réseau électrique, les feux de circulation, l'accès à Internet, les télécommunications, les sites et applis d'information sont des cibles.

Des drones peuvent semer la panique et mille autres disruptions que nous n'imaginons même pas peuvent être déclenchées de partout par des acteurs mal identifiés et ce d'autant plus facilement que nous n'avons plus prise sur nos réseaux.

Enfin les soldats : chaque soldat a sur le réseau une bonne part de son existence et une quantité considérable d'informations collectées sur lui.

Ce soi immatériel et intime est soudain otage d'une autre puissance. Cette vulnérabilité exploitée par des programmes experts en déstabilisation et massivement utilisés peut désorganiser des unités entières.

Les armes sont désormais des systèmes d'informations complexes. L'avion de combat *Rafale* équivaut, par exemple, à une centaine d'ordinateurs combinés et est équipé d'une somme de capteurs de haute technicité échangeant des données. Voilà autant de risques de connexions malveillantes à un réseau dont la logique serait devenue adverse.

Dans ce contexte, la confrontation militaire conventionnelle ne sera pas le premier coup mais le coup de grâce.

Pour ces raisons, le combat est perdu d'avance. Quels que soient la volonté et le courage de ceux qui y seront engagés.

Ne pas être souverain sur le réseau, c'est renoncer à la mission de défense.

C'est croire à l'illusion d'un pays physique dont il ne restera que le décor, un monde vidé et déjà conquis. L'activité, la valeur, l'information, le pouvoir seront dématérialisés en systèmes et terres étrangères. Et ce pays logique, n'est pas le nôtre. En une guérilla désespérée, nous tenterons de protéger une fiction avec une autre : nos armes faussées contre des adversaires déjà vainqueurs et depuis longtemps chez eux.

Il est à craindre, enfin, qu'une population somnolente que les pouvoirs publics auront laissé collectivement et intimement devenir otage du réseau, redoute tout conflit aux enjeux incertains et choisisse d'emblée le parti des nouveaux maîtres.

Voilà la réalité de notre situation.

Le modèle américain :

On ne peut pas comprendre l'Internet sans entrer en profondeur dans ses racines américaines et par conséquent rappeler l'histoire de cette grande et belle nation.

Les États-Unis d'Amérique sont nés d'une guerre civile et coloniale brutale qui était perdue d'avance. Les colons rebelles entre l'incroyable puissance britannique, le lointain Royaume de France et l'immense empire espagnol au Sud n'avaient que l'espoir du désespoir.

C'est contre toute attente que cette nation ruinée, riche seulement de terres futures, sortit victorieuse du conflit. Lui restera une angoisse existentielle qu'elle transmutera en légitimité d'une volonté impériale globale.

Née de la bourgeoisie et non de la noblesse, ce qui la rendit par nature mercantile et entreprenante, la nation américaine associa dès le départ, pour redresser ses finances, son destin politique et ses forces économiques.

Deux thèses s'affrontaient cependant. Celles de Thomas Jefferson, prônant le moins d'État possible et celle d'Alexander Hamilton, partisan déterminé de l'action publique. L'essor phénoménal de l'économie américaine au XIXème siècle grâce à l'investissement anglais, accru ensuite par l'or de Californie, consacra la suprématie de Jefferson.

La crise de 29 força le retour d'Hamilton. Mais les États-Unis, tels que nous les connaissons aujourd'hui, sont nés avec la Seconde Guerre mondiale.

L'effort de guerre américain dégage définitivement le pays du marasme. Au sortir du conflit, les États-Unis représentent la moitié du PNB mondial. Leur domination est totale.

Dès l'économie de guerre, le *Pentagone* travaille étroitement avec les autres agences de sécurité nationale mais aussi ensuite les agences gouvernementales aéronautiques et atomiques et participe à la coordination de plusieurs milliers de chercheurs.

Politiquement, cette organisation est théorisée et pilotée par Vannevar Bush, conseiller scientifique du Président Roosevelt. Il ressortira de cette coopération des technologies comme les ordinateurs, les avions à réaction, le nucléaire civil, le laser et le début des biotechnologies.

Un nouveau modèle économique et politique s'affirme.

C'est la naissance du complexe militaro-industriel. L'armée est le principal commanditaire et le premier client. Les logiques commerciales et militaires sont combinées. Les investissements sont massifs, la coopération exemplaire et les intérêts financiers majeurs.

C'est aussi avec le projet *Manhattan* de fabrication de la bombe atomique, la naissance d'un état profond au cœur de l'État, une infrastructure qui ne rend pas de compte, fondée sur le secret et sur la toute-puissance extraconstitutionnelle de l'exécutif et donc du Président, maître ultime et solitaire de l'arme absolue.

Cette double logique de puissance industrielle et de secret va considérablement se développer grâce à la menace soviétique. La dissuasion nucléaire va structurer le déploiement militaire des bases étrangères, un millier, et l'organisation de l'armée de l'air. Les agences de renseignement civiles et militaires vont prendre une dimension inconnue jusqu'alors.

En 1957, *Spoutnik*, premier satellite artificiel à tourner autour de la Terre n'est pas américain mais russe. C'est un coup de tonnerre et une onde de choc. L'Amérique décide alors d'associer, dans un nouveau dispositif, la puissance militaire et l'effort de recherche scientifique, afin de garantir sa suprématie par l'innovation tous azimuts.

Une agence est créée en 1958, *l'Advanced Research Project Agency*, l'*ARPA*, qui deviendra la *DARPA*, avec un *D* supplémentaire pour *Defense*. Son budget actuel est de trois milliards de dollars annuels. Une seconde agence gouvernementale, la *National Science Foundation*, la *NSF*, démultiplie le dispositif avec un budget annuel de 7 milliards de dollars.

Nous devons, directement ou indirectement, au couple *DARPA*/*NSF*, nombre des innovations majeures de l'informatique de la seconde partie du vingtième siècle et du début du vingt et unième et au premier rang d'entre elles le micro-processeur et l'Internet.

Au cours des années 80, l'industrie informatique japonaise des circuits intégrés est en passe de devenir hégémonique, marginalisant la société américaine *Intel*, alors dixième société mondiale du secteur. Le gouvernement américain considère que la perte de contrôle sur les processeurs est hors de question tant en termes économique que stratégique. Il en ressort un soutien considérable apporté à *Intel* qui en fera la locomotive de l'avènement de la micro-informatique populaire.

Mais c'est avec l'administration Clinton-Gore, entre 1993 et 2001, que va se fonder le nouvel état numérique américain. L'exécutif est alors convaincu que le réseau, et donc les industries du savoir et de la connaissance, sont le cœur de la nouvelle dynamique américaine. L'activisme technologique au sommet de l'État, engage ainsi le renouveau des États-Unis par l'innovation scientifique et informatique. C'est, par le cyberespace, la renaissance de l'empire américain total.

Et cette vision extraordinaire va s'allier au complexe militaro-numérique, déjà opérationnel depuis des décennies, pour considérablement le renforcer.

La fameuse *Silicon Valley* est la partie émergée d'une dynamique publique dans laquelle l'administration, l'armée et le renseignement ont investi plusieurs centaines de milliards de dollars.

Avec les attentats du 11 septembre 2001, toutes les dernières barrières et verrous constitutionnels sautent. La nation fait corps et coalise en une alliance patriote l'industrie de l'Internet et le renseignement pour donner naissance à une industrie du renseignement.

Le budget fédéral consacré au renseignement atteindrait, une centaine de milliards de dollars annuels dont plus de dix pour cent consacré à l'informatique.

Des fonds de recherche, des fonds d'investissements bienveillants qui garantissent les autres investisseurs, appuient généreusement les entreprises qui auraient un quelconque intérêt stratégique. Le fonds de la *CIA*, *In-Q-Tel*, a déjà apporté son concours à plus d'une centaine de nouvelles entreprises de technologies.

Un réseau social nominatif mondial, arme de numérisation massive, va ainsi pouvoir brûler un milliard de dollars avant même d'avoir un plan d'affaires solide.

La *DARPA* évolue parallèlement. Sa mission initiale de créer un écosystème d'innovations destiné à donner à l'armée une avance technologique incontestable s'élargit désormais à l'utilisation de ces technologies pour la compétitivité économique d'entreprises utiles au renseignement.

Le *Pentagone* dépense environ 60 milliards d'euros annuels en recherche et développement, irriguant un écosystème de milliers de sociétés informatiques de toutes tailles.

Identification biométrique, robotique, drones, réalité virtuelle, simulation de combat, intelligence artificielle, géolocalisation, cartographie satellitaire, reconnaissance vocale, informatique distribuée, modélisation du cerveau, capteurs, données massives, cybersécurité, détection des fraudes, chiffrement, tous ces secteurs et bien d'autres font l'objet de financement et de recherche croisés entre l'armée et les entreprises. Sur le réseau, il n'y a plus de différence entre les technologies militaires et civiles.

L'industrie du renseignement fusionne les dimensions civiles et militaires de façon indissociable : personnes, budgets, projets, financement, les frontières disparaissent. L'industrie du renseignement est civilitaire.

Prenons en mains, un *iPhone*. L'Internet, auquel le terminal se connecte, a pour origine la *DARPA* ; la technologie de téléphonie cellulaire provient de l'armée américaine ; le micro-processeur et la mémoire cache de la *DARPA* ; le micro disque dur du *département de l'Énergie* et de la *DARPA* ; les algorithmes de compression - automates logiciels pour réduire la taille des fichiers - de *l'Army Research Office* ; l'écran tactile des *Département de l'Énergie* et *de la Défense*, de la *NSF* et de la *CIA* ; le *NAVSTAR-GPS* des *Départements de la Défense* et *de la Marine* et enfin la batterie Lithium-Ion du *Département de l'Énergie*.

Ajoutons, pour conclure, qu'*iOS*, le système d'exploitation du mobile d'*Apple* est dérivé d'*OS X*, le système d'exploitation du *Mac*, dont il partage les fondations. *OS X* a pour origine le système d'exploitation *MACH - M.A.C.H* - conçu en 1985 par l'université *Carnegie-Mellon* et financé par la *DARPA*.

En ce qui concerne *Google*, le développement du moteur de recherche, de 1995 à 1998, a non seulement été une initiative de la *NSF* financée par la *NASA* et la *DARPA* mais ressortait de la *Digital Library Initiative*, *DLI*, un programme stratégique du *Pentagone* et du renseignement américain qui y joua un rôle particulièrement actif.

S'y ajoutait le parrainage de la *Massive Digital Data Systems* (*MDDS*) *Initiative* issue des services de renseignements et supervisée notamment par la *CIA*.

Google est le modèle de l'entreprise civilitaire.

Google intervient dans plusieurs structures de l'État fédéral américain qui se préoccupent des technologies de sécurité nationale comme la *Task Forces du National Research Council*, l'*Institute for Defense Analysis* ou le *Defense Science Board*.

Google cofinance des programmes de recherche au côté de la *DARPA*, de l'*Office of the Director of National Intelligence*, *ODNI* - coalition de 17 agences et organisations de renseignement - et de la *NSA* : 170 de ces programmes ont été identifiés par un chercheur allemand et 75 d'entre eux impliquaient directement des employés de *Google*.

Google n'est pas seule. *Microsoft*, *Adobe*, *Facebook*, *Amazon*, *Intel*, *nVidia* sont directement engagés dans des projets de la sécurité nationale américaine.

Enfin, *Google* est intimement liée à l'influence et à la diplomatie américaine par l'intermédiaire d'un ensemble impressionnant d'organisations et d'associations gouvernementales ou privées. Son rôle va jusqu'à l'accompagnement informatique et politique de la déstabilisation de régimes en place. Ce fut le cas lors du "Printemps arabe".

L'administration Obama a assumé et amplifié cette hybridation et a fait des principales entreprises du réseau les équivalents étato-mercantiles des *Compagnies des Indes* du XVIIIème siècle qui furent lancées par les nations européennes à la conquête du monde et de ses richesses. Ces entreprises numériques du réseau sont des extensions directes du pouvoir d'État américain.

La menace terroriste, bien réelle, sert aussi de prétexte à la mise en place d'une plateforme d'intelligence économique à l'échelle mondiale recueillant de l'information sur l'humanité connectée entière, individu par individu, entreprise par entreprise, aux fins premières de renforcer l'économie et la puissance américaine qui ne font qu'un.

C'est un état de fait qui est aujourd'hui un fait d'État.

À tel point, d'ailleurs, que l'affaire Snowden qui levait le voile sur cette industrie du renseignement et provoqua un scandale mondial ne suscita de la part des Américains ni déni, ni excuses, ni changement profond et durable de politique.

Tout juste, un effort cosmétique pour faire croire à une fâcherie entre l'administration et les géants numériques au sujet du chiffrement.

Le modèle américain est un cyber-État en cours de constitution, un État qui se refonde par le réseau, impérial et mondial, civil et militaire.

Pour ce premier cyber-État, à la manière des empires coloniaux de jadis, le monde se divise entre dominions, terres à conquérir et empires rivaux.

Le réseau et les États :

On l'a compris, l'alliance organique entre l'Amérique et le réseau donne à cette conjugaison un avantage majeur. Mais pas la suprématie. L'absolue domination requiert la faiblesse des autres nations.

Ce qui n'est pas le cas. L'État et le réseau ont réalisé leur alliance dans plusieurs pays et cela sous deux formes.

Soit ouverte sur le réseau global et l'utilisant à leur avantage, comme la Corée du Sud, Israël ou l'Estonie.

Soit fermée, en filtrant le réseau pour constituer un écosystème protégé économiquement et politiquement, au détriment des libertés publiques. C'est le cas de la Russie, mais surtout de la Chine dont les géants numériques qui en sont issus ont des ambitions mondiales.

Le reste du monde, le Tiers-Internet, n'a pas réalisé l'alliance entre le réseau et l'État. Le Sud-Est asiatique, le Japon, l'Australie, le Canada, l'Inde, l'Orient, l'Afrique, l'Amérique latine et l'Europe sont à la traîne. Des entreprises d'exception y réussissent pourtant, malgré les handicaps. Mais leur vulnérabilité est grande, tant elles dépendent des services américains.

La souveraineté numérique : une décision politique

Un État se définit par un territoire délimité par des frontières sur lequel s'exerce une loi commune déterminée par la volonté populaire.

Cette volonté suprême, cette maîtrise indépendante de son destin, c'est la souveraineté.

La souveraineté numérique consiste à continuer la République et ses droits dans la dimension des réseaux numériques, ce cyberespace, selon le terme devenu officiel lors de sa reprise par l'*ONU*.

Pour ceux qui craignent que cette démarche soit attentatoire aux libertés qu'ils sachent, par exemple, que la dernière loi sur le renseignement est moins intrusive que les fonctionnalités connues des services de messagerie gratuite sur le Web ou sur mobile.

Il m'est arrivé de recevoir des messages d'amis m'alertant sur ce texte législatif avec une adresse de courriel provenant d'un service que son utilisateur autorisait à scruter et enregistrer toutes les conversations.

Pour ceux qui craignent que cette démarche freine le progrès et l'innovation, qu'ils sachent que notre statut actuel de colonie numérique n'est pas le meilleur terrain pour inventer et changer la donne.

En effet, une belle idée européenne, et il y en a de nombreuses, grandira au risque constant d'être expulsée ou concurrencée par les plateformes qui l'hébergent pour ensuite, si, contre toute attente, elle parvient à s'affirmer, n'aura pour meilleure issue que de rejoindre la dynamique d'acteurs étrangers aux ressources incomparables. Et cela est valable tant pour les entreprises que pour nos talents les plus prometteurs.

Pour ceux qui y voient un nationalisme de repli ou un antiaméricanisme, qu'ils sachent que la liberté est universelle et que la défendre ici, comme une nation civique, c'est la défendre partout. C'est donc d'ailleurs aider les associations de défense des libertés civiles américaines. Maintes fois, déjà, la France a servi de modèle de progrès. Et si l'Amérique s'irrite parfois d'un allié qui ne lui soit pas subordonné, elle sait cependant que cette autonomie est notre meilleure qualité quand l'adversité commune nous rapproche. Et, qu'enfin, nos alliés américains sont nos amis. Mais même mon meilleur ami ne prend pas mes décisions à ma place.

Pour ceux qui concluent, d'emblée, à l'impossibilité d'agir au seul niveau national, qu'ils n'oublient pas que si les quatre premières entreprises de services sur Internet réalisaient plus de 300 milliards de dollars de chiffre d'affaires en 2013, soit le PIB du Danemark, 55ième économie mondiale, le PIB français est dix fois supérieur.

Pour ceux qui considèrent que l'échelle européenne est la seule pertinente. Ils ont raison mais dans un second temps. La souveraineté numérique ne doit pas se dissoudre d'emblée dans le marais d'une administration communautaire parfois trop attentive aux allégeances et aux influences. En revanche, les initiatives nationales, y compris juridiques comme sur le droit des données, peuvent prendre une ampleur considérable lorsqu'elles sont relayées au niveau européen. L'Europe est la seconde étape pas la première. Nous trouverons alors des alliés pour reprendre et renforcer notre démarche. Le premier d'entre eux sera certainement l'Allemagne. Enfin, il nous faut bâtir ensemble une souveraineté européenne, une eurosouveraineté.

Qu'ils sachent, enfin, que de nombreux pays prennent conscience de leur absence de souveraineté sur le réseau. L'affaire Snowden a joué pour cela un rôle de révélateur explosif.

Il faut avoir le courage de s'affirmer de manière positive face aux États-Unis. Ce n'est plus à la portée de la France ? Serait-ce un pays trop petit ? Pauvre ? Isolé ? Trop usé ?

Regardons l'exemple de l'Équateur et de quinze autres pays d'Amérique latine. Ils affirment leur *soberanía tecnológica*, pour établir leur indépendance numérique et, dans une première étape, s'émancipent des licences des logiciels commerciaux, la plupart américains, pour utiliser des logiciels en source libre, dont les utilisateurs peuvent légalement contrôler et modifier le programme.

La Suisse, aussi, a pris conscience du danger et investit dans une nouvelle architecture de communication protégée, civile et militaire, pour sécuriser au niveau national ses communications et ses données. Le Conseil fédéral a donné son feu vert au *réseau de données sécurisées* (*RDS*) qui s'adossera au *réseau de conduite suisse* développé par la Défense.

Un pays comme la France, sixième budget militaire mondial, est incapable de garantir à ses citoyens le secret de la correspondance et de la vie privée ; incapable de garantir à ses entreprises le secret de leurs propriétés intellectuelles. Et c'est ce peuple-là, abandonné, qu'on livre aux prédateurs de données ? Et c'est cette économie rongée et trahie, que l'on envoie au front de la mondialisation ?

Aucune force économique ou sociale ne peut résoudre seule cette problématique. L'État est le seul à pouvoir sortir notre société qui s'abîme dans ces sables mouvants logiques.

Après les réseaux de résistance, vient maintenant la résistance des réseaux.

Le temps n'est plus aux adaptations dispersées et bricolées dans la confusion générale par chaque entreprise. Les pouvoirs publics, quant à eux, ne doivent plus seulement raisonner, comme le veut la tradition administrative, en filières, subventions et infrastructures. Enfin, il faut cesser de tout attendre des « start-up », petites entreprises qui répondent d'une mythologie californienne que nous avons trop aimé croire.

Tout cela est dépassé. Le temps est désormais celui de l'urgence.

L'Internet est un projet politique qui nécessite une réponse politique.

Seul un réseau peut rivaliser avec un réseau.

Et notre pays ne s'est pas encore repensé autour et avec le réseau.

Et notre pays n'est pas souverain sur le réseau.

La souveraineté numérique est une décision d'État. Une décision politique majeure qui décidera de notre avenir.

Trois actions pour établir la souveraineté numérique :

Les conditions de la souveraineté sont le territoire et la loi.

Première action : établir un territoire

Peut-on avoir un territoire sur Internet ?

Si un pays fait le choix de se fermer partiellement ou de filtrer les accès au réseau, la problématique est simplifiée. Mais le prix en est la restriction des choix et des libertés.

Dans une société ouverte, la question est plus complexe.

Un territoire physique se définit par sa frontière : on passe ou on ne passe pas.

Un territoire immatériel se définit par son chiffrement : on a la clef pour déchiffrer ou on ne l'a pas.

La frontière sur le réseau, c'est le chiffre.

La souveraineté sur le réseau, c'est le code informatique.

Les protocoles de chiffrement doivent être sous contrôle public et définis par l'autorité publique. C'est une question de libertés individuelles et de sécurité nationale.

Cette vérité a été affirmée récemment par le Premier Ministre britannique, David Cameron, qui a menacé les sociétés de services de conversation sur Internet qui n'accepteraient pas de fournir au gouvernement leurs clefs de déchiffrement.

Toute donnée chiffrée demeurera enfin sous notre droit, où qu'elle se trouve, à la manière des billets de banque américains dont la souveraineté est extraterritoriale.

Nous avons donc une frontière, c'est le chiffre.

Quel est le territoire, son sol, sa substance ? Ce sont les données.

Les données sont toutes les informations générées par les utilisateurs du réseau.

Seconde action : le statut des données

Le statut des données est un enjeu capital de souveraineté.

C'est pourquoi, il faut comprendre que les données ne sont plus personnelles depuis longtemps.

Nous voyons les données personnelles comme un sac de billes. Je prends une bille dans le sac sans que cela n'affecte les autres et je la remets ensuite.

Dans les faits, les données personnelles ne sont plus des billes. Le sac de billes est devenu une pelote de laine : je tire une donnée et cela entraîne toutes les autres.

Pourquoi ? Parce que les données sont liées entre elles et forment un réseau. Avec une application mobile, vous donnez accès à votre agenda, votre carnet d'adresses, vos conversations… Il ne s'agit pas de données isolées mais de données associées en réseau : un rendez-vous, par exemple, implique une multitude d'informations liées entre elles ; et ces données ne concernent pas que vous mais aussi toutes les autres personnes qui s'y rapportent.

De même, il est possible de déduire par corrélation et probabilité des informations à partir des uns sur les autres. Les informations recueillies sur des personnes atteintes d'une pathologie spécifique renseignent sur toutes celles qui souffrent du même trouble.

Avec les informations sur une moitié du public d'une conférence, imaginez tout ce que l'on peut apprendre, prédire et supposer sur l'autre moitié. À qui appartient ce qu'ils ont en commun, ce réseau d'informations qu'ils partagent ?

En fait, les données appartiennent à tous ceux sur qui elles renseignent directement ou indirectement.

Si une donnée dite personnelle n'informe pas exclusivement sur sa source mais également sur autrui, elle n'est plus seulement personnelle : elle est toujours à la personne qui en est à l'origine mais elle appartient aussi aux autres personnes concernées, et cela de façon indissociable.

Les données ne sont plus solitaires, elles sont solidaires et forment en droit une indivision, un bien commun essentiel. Un bien commun souverain.

Tel est notre territoire dans le cyberespace.

En conséquence :

Tout échange, collecte, traitement, conservation de données sur le territoire national doivent, pour être agréés, répondre notamment des conditions suivantes :

- utiliser les protocoles de chiffrement autorisés. Ces protocoles garantissent, tout à la fois, la protection de la vie privée et l'ordre public ;

- localiser physiquement ou juridiquement les serveurs sur le territoire national ou européen. Nous quittons Sacramento pour Nanterre ou Montpellier ;

- faire concorder la domiciliation fiscale et la source des données. L'impôt est payé où la donnée est collectée. C'est un processus entamé par un accord international en cours. C'est la clef du financement du coût social de la transition numérique.

Il nous faut maintenant une loi.

Troisième action : faire que la loi soit le code

Qu'est-ce qu'une loi dans le monde matériel ? L'interdiction pour une personne de traverser au feu piéton rouge est soumise à son libre arbitre. Dans le cyberespace, et c'est pour cela qu'il porte le nom d'espace gouverné, il n'est pas possible de traverser à ce feu rouge. Ce n'est plus une décision du piéton, c'est une ligne de code informatique.

Dans le cyberespace, la loi c'est le code.

Dans le monde matériel, les lois répondent toutes d'un texte fondateur qui détermine, l'organisation et le fonctionnement de l'État, ce texte c'est la Constitution.

Dans le cyberespace, cette organisation centrale dont tout dépend, c'est le système d'exploitation, c'est-à-dire le programme informatique qui pilote chaque machine.

Dans le cyberespace, la Constitution, c'est le système d'exploitation.

Et pas n'importe quel système d'exploitation : le système d'exploitation à l'âge du réseau.

Jadis, un système d'exploitation s'assurait du bon fonctionnement de l'ordinateur de bureau ou du terminal mobile.

Aujourd'hui, le même noyau logiciel va se retrouver dans tous les ordinateurs et les terminaux mobiles - bien sûr - mais aussi dans la voiture, la maison, dans tous les objets connectés, les puces de cartes de paiement ou d'assurance santé, les robots, les capteurs, la signalisation et finalement les infrastructures logiques de villes entières.

Ces systèmes d'exploitation se mettent en réseau, échangent constamment. Ils deviennent notre interface avec Internet, notre intermédiation avec les autres et le monde. Ils sont l'intelligence d'accès au réseau et le contrôlent.

À la manière des lois qui s'appuient sur la Constitution, toutes les applications et services dépendent de ce réseau de systèmes.

Il nous faut un système d'exploitation souverain. Ce sera notre Constitution dans l'immatériel. Il garantira la sécurité des données, les libertés individuelles, le droit et l'économie des entreprises, il mutualisera les ressources et engagera la nation entière dans le renouveau et la croissance.

La Chine et la Russie ont déjà annoncé leur système d'exploitation souverain. J'entends la critique légitime. Mais ce ne sont pas que les états autoritaires qui s'y engagent. Les États-Unis ont trois systèmes souverains principaux, que vous utilisez certainement.

Certains considéreront qu'un système d'exploitation est une tâche impossible. Faut-il rappeler qu'*Android*, le système d'exploitation promu par *Google* et qui équipe aujourd'hui plus de 80 % des mobiles intelligents, a été lancé par une équipe d'une demi-douzaine de développeurs avec un budget initial à seulement six chiffres et à partir d'un noyau *Linux* en source libre, d'ailleurs d'initiative européenne ?

Un tel système d'exploitation souverain, ou *SESO*, ne réussira jamais par la contrainte mais parce qu'il sera meilleur, plus agile, plus sûr, plus efficace, plus ouvert, plus libre, plus coopératif et foisonnant d'initiatives dont il ne sera pas concurrent mais garant.

Nous le retrouverons dans la carte *Vitale* pour protéger nos données de santé, dans nos automobiles, qui ne seront plus otages de logiciels provenant d'entreprises qui lancent leurs propres véhicules concurrents. Il en va de même de nos systèmes de paiement, ce qui donnera aux pouvoirs publics une visibilité nouvelle sur l'économie nationale et permettra peut-être, en contrepartie, de réduire les taxes spécifiquement pour les utilisateurs du *SESO,* selon le même principe des avantages accordés pour la déclaration en ligne des revenus.

Avec la logique de chiffrement, de solidarisation des données et de système souverain, nous retrouvons dans le cyberspace les fondamentaux qui garantissent notre République.

C'est le retour du droit et de l'ordre public sur le réseau.

Et, point essentiel : nous ne devrons plus opposer sûreté et liberté.

Comment, en effet, protéger le secret des individus, fondement de la démocratie, alors que ce même secret peut devenir une arme contre la collectivité. Comment se prémunir des bombes fabriquées dans l'isoloir ?

La souveraineté numérique permet, parce que l'on maîtrise les protocoles de chiffrement, de chiffrer différemment les identités et les informations collectées sur cette identité.

Une clef pour les identités, une clef différente pour les informations.

Il sera possible ainsi de balayer un grand nombre d'informations sans déchiffrer les identités.

Ce déchiffrement spécifique sera réservé à la Justice ou à des cas précis de sécurité nationale.

En garantie supplémentaire, le système des bases de données décentralisées en chaînes de blocs, utilisé pour les monnaies virtuelles comme Bitcoin, pourra s'appliquer à nos données.

Ainsi, parce que la donnée chiffrée sera accompagnée de métadonnées recueillant son historique d'usage, il sera malaisé de la détourner de ses emplois autorisés sans laisser de traces.

La ré-identification non autorisée devient alors un délit.

La faculté de brasser, trier et agréger un nombre considérable d'informations ouvre la possibilité d'élaborer et de perfectionner sans cesse des algorithmes de détection et alors, sur décision judiciaire ou urgence légitime, de suivre des individus précis ; sans perturber à grande échelle le secret d'autrui.

Repérer ainsi les comportements à risque pour prévenir et anticiper, pour reconstituer les réseaux, sans pour autant s'engager sur la surveillance de masse des personnes identifiées, telle est la feuille de route.

Ce monitorage contrôlé sera demain la clef de notre ordre public sur le réseau.

La souveraineté numérique nous libère du choix tragique entre la liberté et la sûreté, dilemme qui nous oblige à des compromis douloureux et insatisfaisants. La souveraineté numérique en combine les exigences pour une meilleure efficacité, respectueuse du droit.

Oui, bien sûr, rien n'est simple et de tels dispositifs supposent un contrôle juridique, technique et démocratique ainsi que des contre-pouvoirs vigilants. Comme toujours, une administration transparente et contestable, une administration qui rend compte de ses actes sont à la base du fonctionnement de la République.

Bien sûr, nous n'échapperons pas au danger et à l'inquiétude. Nous serons toujours vulnérables. Mais notre courage de chaque jour s'appuiera sur une nouvelle confiance. Nous ne serons plus comme des enfants soumis au bon vouloir des grands. Nous serons des adultes, maîtres de notre destin sur le réseau.

La Défense, la Sécurité nationale, s'appuieront alors sur des fondations solides : un réseau ouvert mais doté de sécurités et de garanties, un réseau d'intelligences connectées souverain et maîtrisé. Nous aurons toujours des ennemis mais nous serons désormais capables de véritablement nous défendre.

Comment agir maintenant :

Le 11 Juillet 1944, le chimiste français Bertrand Goldschmidt, qui participe au développement de la bombe au côté des Alliés, prévient le Général de Gaulle lors de sa brève visite au Canada, de l'imminence de sa mise au point et de ce qu'elle va changer.

Par l'ordonnance du 18 octobre 1945, le gouvernement provisoire présidé par le Général de Gaulle fonde le *Commissariat à l'énergie atomique*.

Sa mission : fabriquer la bombe. Et cette mission répond d'un choix politique préalable décisif : l'indépendance nationale. La souveraineté passe désormais par la souveraineté nucléaire.

Le numérique est l'équivalent aujourd'hui du nucléaire. Il est planétaire, remet en cause les souverainetés et met en jeu le destin même des populations et des nations.

La réponse est la même : choisir l'indépendance nationale. La souveraineté passe désormais par la souveraineté numérique.

Il faut donc un *Commissariat à la souveraineté numérique*.

Le gouvernement a déjà pris en compte le numérique par un secrétariat d'État, des politiques d'investissement, des postes cyber dans plusieurs ministères régaliens, ainsi que par le renforcement de la sécurité des systèmes d'information des opérateurs les plus critiques.

Mais ces efforts sont entravés par une absence de coordination et, par ailleurs, aucune administration n'est en charge spécifiquement de promouvoir la souveraineté numérique.

La mission du Commissariat est de préparer les politiques garantes de notre souveraineté numérique et de suivre leur mise en œuvre.

Sous l'autorité du Premier ministre, il est, pour le numérique, le pendant civil et le partenaire du *Secrétariat Général de la Défense et de la sécurité nationale*.

Il propose en interministériel d'instruire les projets susceptibles de favoriser notre souveraineté numérique.

Il est en lien avec la *délégation interministérielle à l'intelligence économique* et le *secrétariat général aux Affaires européennes* afin d'étudier les textes internationaux susceptibles d'avoir un impact sur notre compétitivité ou notre sécurité numérique.

Il pilote enfin - et surtout - la création du système d'exploitation souverain et l'élaboration des protocoles souverains de chiffrement des données.

Tel est le chemin.

Maintenant il faut emporter la décision politique qui en décide. Le projet est sur la table du gouvernement.

La question de la souveraineté numérique est aujourd'hui publiquement posée.

Si rien ne bouge… Quel degré de dislocation de notre pays faudra-t-il atteindre pour provoquer une prise de conscience et l'action ? Faudra-t-il le sang de victimes d'un terrorisme aggravé par notre impuissance numérique pour que surgisse la volonté d'agir ?

Espérons tout le contraire.

Quant aux Gardiens de la Nation, puisque leur mission est en cause, il est de leur devoir de le faire savoir.