Comment gagner une guerre perdue ?

Pierre BELLANGER

Pierre BELLANGER

Pionnier des radios libres, entrepreneur et expert d'Internet, Pierre Bellanger est le fondateur et PDG de la radio *Skyrock*. Il publie depuis plus de vingt ans sur les médias et le réseau, en 2014, il publie *La souveraineté numérique* aux Éditions Stock. Il a lancé en 2017, SKRED, la messagerie sécurisée, avec aujourd'hui plus d'un million d'utilisateurs dans le monde. Pierre Bellanger est à l'origine de l'adoption en France d'Alerte-Enlèvement, le système national d'alerte en cas d'enlèvement d'enfants.

« *Nous ne reconnaissons pas les choses d'après ce qu'elles peuvent être en soi, mais seulement telles qu'elles apparaissent.* » Voilà ce qu'enseignait le philosophe grec Démocrite, il y a 2 500 ans.

Nous connaissons le monde objectif par la médiation de nos sens dont la compréhension par notre mental établit une représentation. Schopenhauer, poursuivant cette thèse, réduisit notre connaissance du monde à la seule façon qu'a notre esprit d'en élaborer une reproduction : « *le monde est ma représentation* ». Nous appelons réalité la conjugaison collective de ces représentations individuelles mais, entre le réel et notre médiation biologique, formatrice de notre représentation, vient désormais s'intercaler une médiation technologique nouvelle : le réseau numérique.

Notre présent passe par l'écran. Notre quotidien n'est plus envisageable sans un terminal mobile à portée de main. La part d'information provenant de cette intermédiation électronique est croissante. Les machines nous donnent les réponses. Cette interface informatique constitue une nouvelle peau entre le monde et nous, un « technoderme » par lequel l'essentiel transite. Parallèlement, le réseau est le nouveau système nerveux : il innerve la ville, le pays et la planète. De notre battement cardiaque au trafic aérien, il capte, collecte, traite et intègre les données. Cette interface informatique se substitue progressivement à la réalité. Nous allons vivre dans une représentation de second degré : la représentation biologique générée par nos sens à partir d'une représentation numérique produite par autrui. Ce n'est pas un nouvel

aspect du monde, c'est le monde. Ce n'est pas une partie, c'est le nouveau tout et ce simulacre de réalité est hors de notre contrôle.

Peut-être cela s'appelle-t-il fort justement le « théâtre des opérations », car c'est désormais un théâtre dont nous ne maîtrisons ni les rouages, ni les coulisses, ni l'histoire.

Un mot ici sur nos amis nord-américains dont le rôle est, dans cette mutation, majeur. Leur effort entier depuis des décennies est en faveur d'un empire numérique d'emprise mondiale. Ce sont nos alliés historiques et nous sommes ensemble sur plusieurs fronts ainsi que dans la lutte antiterroriste. Mais, même mon meilleur ami, ne prend pas mes décisions à ma place. La souveraineté ne se partage pas car s'il advenait qu'un des détenteurs de cette simulation devienne demain un adversaire, nous nous préparons à combattre en aval, alors que nous avons déjà perdu en amont.

Sun Tzu, le général stratège de l'antiquité chinoise, écrivait : « *Une armée est victorieuse si elle cherche à vaincre avant de combattre, elle est vaincue si elle cherche à combattre avant de vaincre* ». Il ajoutait que, pour ce faire, il fallait « *vaincre l'ennemi dans ses plans* » et par conséquent mettre en place un « *filet invisible* », selon ses propres termes, de collecte de renseignements. Mais ce qu'il n'avait pas envisagé, c'est qu'aujourd'hui à la connaissance de l'adversaire s'ajoutent le contrôle et la manipulation de sa réalité !

Figurons-nous une arène romaine : deux gladiateurs s'affrontent, le rétiaire et le mirmillon. Mais ce que le mirmillon voit dans son casque est une projection décidée par son adversaire. La victoire du rétiaire est inévitable.

Nous avons perdu la bataille de la représentation de la réalité. Le monde objectif nous échappe. Il nous en reste une mystification, pilotée par des intérêts qui ne sont pas les nôtres. Pour la première fois, l'ennemi est la réalité elle-même. Notre réel est leur ruse. Sur le réseau, les composants, les processeurs, les capteurs, les appareils, le code, les programmes, les services en ligne, les applications mobiles, les systèmes d'exploitation, les réseaux, les câbles, les protocoles, les méthodes de chiffrement, les serveurs, les algorithmes, les interfaces, les plateformes transactionnelles répondent d'une souveraineté qui n'est pas la nôtre. Nous nous croyons chez nous, mais, en fait, nous sommes en terre étrangère.

Le siècle s'ouvre sur un grand mouvement, plus important en amplitude et en conséquence que la mondialisation des décennies passées : la réticulation informationnelle, c'est-à-dire la mise en réseau numérique du monde. Les nouveaux réseaux de services numériques deviennent des États et les États traditionnels tardent à devenir des réseaux. Ce mouvement nous échappe. La cérébralisation numérique de notre pays s'effectue hors de notre contrôle. Au lieu d'être l'équivalent d'un processus de développement nerveux endogène et autonome, c'est une forme parasite qui s'installe en absorbant nos ressources. Ce système nerveux numérique exogène croît à nos dépens. Et les bénéfices immédiats qu'il nous apporte sont sans comparaison avec l'affaiblissement général nécessaire à sa croissance. En cet âge, où le fondement de la société devient numérique, notre cerveau cyber collectif et national ne nous appartient pas. Il dépend d'organismes tiers dont il est une extension. Notre perception, notre mémoire, notre coordination, notre réflexion, la continuité de notre identité, notre faculté de communiquer, de commander, bref notre pensée numérique a lieu dans la tête d'un autre. Nous sommes devenus « exocéphales ». Et nous y migrons la totalité de notre immatérialité : nos données régaliennes, militaires, publiques, professionnelles, privées. Nous livrons notre savoir, nos secrets, notre valeur, notre travail, nos richesses, nos armes, nos idées, nos faiblesses et nos forces à une puissance extérieure.

Nous sommes collectivement les premiers collaborateurs – involontaires ou non – de cet abandon en masse. L'adversaire potentiel se sert même de nos jeux pour alimenter ses bases de données : vous voulez constituer la meilleure source de localisation et de photos, y compris à l'intérieur des bâtiments ? Un jeu de chasse aux créatures virtuelles va vous aider : *Pokemon Go*. Figurez-vous la quantité d'images localisées collectées grâce à cinq cents millions de téléchargements dans le monde et, en fin 2016, vingt millions de joueurs quotidiens…

Déjà victimes, déjà vaincus… Le pays se vide et n'est plus qu'un gisement de données, une mine numérique à ventre ouvert, à exploiter tant qu'il y reste quelque chose à prendre. Que reste-t-il à défendre qui n'a pas encore été pris ? Et s'il fallait encore sauvegarder une carcasse vidée, comment faire ? Il faut aussi imaginer notre opinion publique, sans discernement, éclatée par les réseaux sociaux en hallucinations fermées, donc rivales, sans cesse renforcées par les algorithmes et nourries d'injections d'informations manipulatrices. Les Russes appellent cela « la guerre contre la réalité ». Et si ce n'est pas suffisant, des attaques ciblées mettent à mal les processus démocratiques, révélant de façon ciblée ou inventant de nauséabondes coulisses. Tel est notre nouvel espace public. Avec pour risque majeur, pour une démocratie, d'avoir comme chef de l'État, celui-là même que ces manœuvres auront favorisé.

Saper la confiance dans les institutions et le système politique, accroître le cynisme, la confusion et les divisions : cette « contre-information » est une arme de guerre. Elle a été utilisée par les Russes aux États-Unis, mais aussi en Italie, en Suède, en Finlande, en Grande-Bretagne, en Moldavie, en Autriche, en Bulgarie, dans les Pays baltes et a été à l'œuvre pour notre élection présidentielle et ses primaires. Une de nos premières infrastructures vitales est la démocratie elle-même. Ce n'est pas un hasard si elle est devenue une cible prioritaire. Comment ne pas succomber à des intoxications et des piratages venus de Russie, tolérés par des logiciels américains, eux-mêmes installés sur des machines chinoises ?

C'est déjà notre présent. Lorsqu'en 2016 sur l'application mobile de messagerie *Telegram*, d'influence russe, furent mis à mort nommément par Daech une quarantaine de nos citoyens, les propriétaires de l'application refusèrent la demande de l'État français d'en retirer le message, comme les plateformes américaines d'en interrompre la mise à disposition.

Quelle défaite ! Dans le même temps, la Russie obtenait le blocage du site de contacts professionnels Linkedin et la Chine, l'expulsion de l'application du *New York Times* de l'App Store d'Apple, probablement pour un article déplaisant pour les élites économiques et politiques. En France, la somme résignée de nos concessions, de nos capitulations, de ces reculades petites et grandes, prépare et annonce une débâcle d'une ampleur inconnue.

Il faut imaginer un conflit où des ordres ne parviennent pas, où des consignes jamais données circulent. Des machines qui exécutent des instructions transmises à distance par des opérateurs inconnus… Des implants cardiaques aux centrales nucléaires, tout se dérègle. Les réseaux de transports, les marchés financiers, les banques, les fermes de serveurs et réseaux d'ordinateurs, la distribution d'énergie, les télécommunications et le reste sont soudain ravagés. Et il est à douter que les chaînes de commandement et les systèmes d'armes demeurent intacts. Un vaste et immense chaos s'empare du système jusqu'à la catastrophe.

Ce que l'on demande à l'armée aujourd'hui, c'est de défendre un rêve, c'est de protéger une illusion, d'assurer la sécurité d'un fantôme. C'est la métaphore du morceau de sucre. Jadis, défendre un pays, c'était protéger la nation qui, tel un morceau de sucre parallélépipédique, se définissait par sa forme précise et la cohésion de sa masse de grains agglomérés. Il ne reste aujourd'hui que de l'eau sucrée : une dilution de la nation en millions de particules dans un substrat numérique étranger. Et pourtant, rien d'abstrait dans ce cataclysme : les larmes, la douleur, la souffrance, le sang, la misère, la peine, le chagrin, la panique, la peur, la soumission seront là, sans cesse, pour nous rappeler que c'est le vrai monde qui se meurt sous les coups. Dans le même temps, la capacité de nuisance numérique de chacun, amplifiée à la puissance du réseau, ne cesse de croître, multipliant par le nombre d'individus le risque d'attaque. De ce fait, la paix devient statistiquement impossible. La seule situation possible sur le réseau, c'est la guerre. Nous entrons dans l'âge de la « paix impossible ».

Voici donc la situation : une armée conçue pour défendre l'intégrité d'un pays, la souveraineté d'une nation et la fière liberté d'un peuple se retrouve sans territoire, sans frontières et déjà envahie ; avec pour ennemi : personne et la multitude ; en guerre continue, sans maîtrise d'un pays opaque à lui-même et transparent aux autres ; une nation exsangue, subordonnée dans tous ses leviers et systèmes d'information et déjà consentante à la servilité, celle de ses élites, comme celle de sa population.

Comment sortir de la fatalité de décennies de renoncement qui ont conduit à ce naufrage ? Comment accepter, grande nation, une et indivisible, millénaire et libre, de nous retrouver ainsi : province attardée, démembrée et violée, de l'empire technologique d'autrui ? Comment gagner une guerre perdue ? Telle est maintenant la seule question qui reste.

Qu'est-ce qu'Internet ? Un protocole de dialogue entre réseaux de machines. Mais si on enlève cette toile électronique, que reste-t-il ? Les gens. Internet, c'est les gens et ces gens c'est nous. Nous sommes l'alpha et l'oméga d'Internet. La première étape, c'est donc nous. Notre mental individuel et collectif.

Il faut se souvenir de ces batailles héroïques, où, contre toute attente, contre la peur, contre le nombre, contre la raison, vint finalement la victoire. Nous y sommes à ces instants de doute et de solitude, à ces moments où la résistance semble futile et sans espoir. Pourquoi résiste-t-on ? On résiste parce qu'on ne peut pas faire autrement. Telle est notre force. La plus petite probabilité de liberté qui reste pèse soudain plus que l'écrasante fatalité des forces opposées. Notre premier point d'appui est ce refus de la servitude. Ce refus n'est pas négociable, il est impératif et notre combat résulte et s'organise par et pour cette détermination.

Pour ceux qui ont déjà fait cette prise de conscience, la profondeur de la défaite est effrayante. Quelle épreuve que de sortir du déni, de l'apathie, de la zone de confort, de cette illusion utile qu'est la croyance en la persistance du monde d'avant et dont la fonction est tant de nous

éviter la panique que de nous maintenir ensommeillés… Pour l'armée, le constat est sans appel : c'est l'incapacité à assurer la mission de défense. Sans maîtrise du réseau, sans « souveraineté numérique », il n'y a pas de défense possible. Et c'est alors le devoir du pouvoir politique d'engager un combat inattendu pour une nation historique comme la nôtre : une lutte pour l'indépendance.
De colonie numérique subordonnée et pillée, il faut retrouver notre droit, notre intégrité, notre souveraineté, il faut établir la République dans le cyberespace. Qu'est-ce qu'une nation comme la nôtre ? C'est tout d'abord, une population ayant choisi librement, sans tutelle ni contraintes, une règle commune qui s'applique sur un territoire délimité par une frontière. C'est ensuite, plus largement, un vaste système d'interdépendances, d'alliances, d'échanges, d'intérêts et d'influences qui ne saurait être mis en cause. Toute attaque contre cet ensemble dynamique et vivant appelle une réponse militaire.

Force est de constater que la guerre a été perdue sans attaque. Il n'y a plus de territoire, ce sont les machines étrangères où se trouvent nos données ; plus de frontières puisque la plupart des systèmes informatiques et leurs chiffrements répondent d'autres souverainetés ; plus de population, puisque nos doubles numériques, apatrides, ont tous migré dans des serveurs lointains hors d'atteinte et plus de règle commune puisque la loi qui s'applique est majoritairement celle des conditions générales d'utilisation garanties par le droit californien. C'est alors le meilleur moment. C'est parce que d'autres ont accepté la reddition, c'est parce qu'il n'y a plus rien à défendre que nous pouvons tout reconstruire et repenser notre État, notre armée et notre nation. Une nation n'est rien sans ennemis, mais ses adversaires potentiels sont maintenant au cœur de nos systèmes ! Plus qu'une ingérence, c'est une gérance à distance. C'est une situation inouïe. Ce moment d'exception nous oblige, à moins de renier le meilleur de ce que nous sommes, à la fondation de notre nation numérique, de notre République numérique.

EN CES INSTANTS EXCEPTIONNELS, LA DISTINCTION ENTRE LA DÉFENSE ET LE CIVIL S'EFFACE, LA CAUSE EST COMMUNE, L'URGENCE FAIT LE LIEN. IMAGINEZ QU'IL VOUS REVIENNE DE FONDER LA FRANCE. IMAGINEZ LE PAYS OCCUPÉ OÙ LE CONSEIL NATIONAL DE LA RÉSISTANCE (CNR) ÉLABORE LE PROGRAMME DE LA FRANCE DE DEMAIN, PROGRAMME ADOPTÉ EN MARS 1944. AUJOURD'HUI, CE PROGRAMME SERAIT UN PROGRAMME INFORMATIQUE. IL NOUS FAUT ÉTABLIR DANS LA DIMENSION NUMÉRIQUE NOTRE TERRITOIRE ET SA FRONTIÈRE PUIS Y INSTAURER ET GARANTIR NOTRE RÈGLE COMMUNE.

En ces instants exceptionnels, la distinction entre la défense et le civil s'efface, la cause est commune, l'urgence fait le lien. Imaginez qu'il vous revienne de fonder la France. Imaginez le pays occupé où le Conseil national de la résistance (CNR) élabore le programme de la France de demain, programme adopté en mars 1944. Aujourd'hui, ce programme serait un programme informatique. Il nous faut établir dans la dimension numérique notre territoire et sa frontière puis y instaurer et garantir notre règle commune.

Dans l'immatériel, tout est information. Un peuple n'existe que sous forme d'informations. Ici, pas de « données personnelles », sorte de sac de billes où chaque bille est une information qui ne renseigne que sur sa source, place à la pelote de laine : une information renseigne sur plusieurs sources, comme un rendez-vous qui se partage entre tous ceux qui y participent, et ainsi, de loin en loin, implique la population entière. Il n'y a plus de données personnelles, mais un « réseau de données », une indivision nationale qui forme un bien commun. Un bien commun riche en données de sécurité et donc un « bien commun souverain ». Dans l'espace cyber, le réseau indivis de données est à la fois le peuple et le territoire réunis en une même entité.

Nous voici donc avec un peuple et un territoire ; il nous faut maintenant une frontière qui en assure la délimitation et l'intégrité. La frontière est ici le chiffrement. Une frontière physique est le contrôle du passage ; une frontière immatérielle est le contrôle de l'accès et de la compréhension, c'est ce que permet le chiffrement. Ce ou ces chiffrements, sous contrôle souverain, rétablissent le secret privé, clé de voûte de notre démocratie, le secret des affaires, base de l'économie du savoir et le secret étatique et militaire, depuis toujours, essence même de la puissance.

Reste la règle commune, c'est ici le code. Le code informatique fondamental sur lequel vont tourner les machines et finalement la société tout entière. C'est un « système d'exploitation en réseau » qui pilote les

capteurs, les machines, les infrastructures, les serveurs, les terminaux. Et ce réseau de systèmes d'exploitation forme une intelligence globale reliant le tout. Android de Google en est, par exemple, une première étape. La clé de notre souveraineté en la matière est paradoxalement le logiciel libre, c'est-à-dire ces cathédrales numériques sans attaches, bâties par des millions d'intelligences bénévoles. C'est sur cette base et notamment le noyau Linux que nous allons fonder nos développements.

Nous sommes dans une guerre de réseaux. Par l'effet réseau qui établit que la taille démultiplie de façon exponentielle la puissance, l'ouvert gagne toujours sur le fermé. Il n'y a pas de réduit ou de repli – serait-ce militaire –, il n'y a qu'un réseau, le plus grand. Il faut donc concevoir une souveraineté ouverte, seule résistante sur le long terme. Forteresse est synonyme de défaite en informatique. Le logiciel libre est plus fort que les grandes entreprises tentaculaires aux systèmes propriétaires que nous affrontons. Le code de ce système d'exploitation libre et souverain, nous pourrons d'ailleurs le partager avec nos amis européens et africains, seuls changeront les clés de chiffrement, toujours souveraines.

Ce système logiciel de pilotage des machines et des réseaux est l'équivalent dans l'immatériel de notre Constitution : tout s'y rapporte, tout en dépend. Et, par ce code qui sera loi, la défense, les droits civiques, les garanties démocratiques et les libertés individuelles et collectives seront désormais le moteur de la République numérique. Nous voici donc avec un projet d'État-nation numérique avec son peuple, son territoire, son intégrité et son droit. Mais pour aboutir à ce projet fondateur, il faut commencer par quelques mesures d'urgence. Le CNR avait d'ailleurs lui aussi un plan d'action immédiat, le nôtre se décline en sept mesures :

- localisation juridique et physique des serveurs, des algorithmes et des données sur le territoire national ou européen ;

- placement sous droit national des plateformes de services numériques ;

- reconnaissance des données des citoyens comme formant un tout indivis et donc un bien commun souverain ;

- généralisation de l'usage du logiciel libre par les pouvoirs publics, les administrations et les collectivités ;

- instauration de protocoles de chiffrement souverains pour toutes les données de citoyens, d'administration de collectivités et d'entreprises ;

- mise en place d'un annuaire d'adresses Internet (*registrar*) contrôlé et sécurisé ;

- mise en œuvre d'un système d'exploitation en réseau libre et souverain sur la base du logiciel libre.

Il faut bien comprendre que ce qui émerge de ce processus est un État numérique. Un État de droit maîtrisant ses données, ses programmes et ses réseaux placés désormais sous sa souveraineté. Le cœur de cet État moderne est sa dimension numérique. Les logiciels et systèmes publics de l'État sont la matrice, le support et la garantie de toutes les activités économiques et sociales, la garantie de l'ordre public et des libertés. Et c'est ce cœur cyber qu'il faudra savoir défendre avec une armée qui, elle aussi, aura placé le centre de sa stratégie et de son action sur le réseau. L'armée de demain est d'abord une machine apprenante, c'est-à-dire, qui fait évoluer son propre logiciel en comparant ses résultats et la réalité et en se réajustant sans cesse. Cette machine est, en fait, un réseau intelligent qui fusionne en un même espace numérique le pays et sa défense. Partout où l'ennemi peut faire du mal, l'action militaire est légitime. Il peut frapper aujourd'hui en tous lieux, aucun de nos processus numériques ne lui échappe. La mission de défense est intégrée à tous les processus et distribuée dans toutes les machines.

Napoléon disait : « *un espion bien placé vaut 20 000 combattants* ». Votre téléphone mobile est le premier de ces espions et le mieux placé. Et chacune de nos machines et tous nos réseaux, à la main d'intérêts étrangers, constitue la plus immense des armées adverses. Le champ de bataille a tout pénétré : chaque programme, chaque capteur, chaque serveur, chaque processeur.

C'est la conscience de l'intrusion et du danger qui fait de chaque machine une cible ou une arme, de chaque action une menace et de chaque individu un attaquant potentiel. La guerre numérique n'est pas un moment, elle est permanente. Elle n'est pas en un lieu, elle est immanente. Elle ne concerne pas que le personnel militaire, elle nous implique tous. La guerre numérique efface les distinctions sectorielles entre mondes civil et militaire, car ils partagent un même sang : les données. Ils devront les échanger en continu. Cette paix impossible, cette asymétrie folle, qui permettent à une bande criminelle dotée de machines de mettre à genoux un pays, ont une seule riposte possible : le renseignement. En ces temps nouveaux de paix impossible, l'arme cyber est la première arme et sa première force est le renseignement. Le renseignement est désormais le premier déterminant de la bataille et la clé de l'avantage stratégique et tactique.

Louis XIV se félicitait de son réseau d'espions en Europe qui lui permettait « *d'avoir des yeux ouverts sur toute*

la Terre… » Près de quatre siècles plus tard, chaque jour, selon IBM, l'humanité génère 20 milliards de milliards de bits. Nous passons donc à la dimension supérieure : de l'artisanat de jadis, toujours indispensable, à une industrie du renseignement faite d'usines à données au service de la défense. Il s'agit d'un renseignement nouveau qui totalise tous les flux d'informations et les *compute* en continu pour rendre une image non seulement du présent mais, surtout, de la réalité future, parfois avec quelques secondes d'avance, parfois plus, et c'est cette prédictivité qui décide du sort de la bataille. La guerre de demain est une « guerre prédictive ». C'est celui qui prédit le mieux et le plus en avant dans le temps qui gagne. La victoire, c'est l'avance.

Ce « renseignement total » est à la machine ce que le plutonium est à la bombe. Après la course aux armements, la course aux renseignements. Et la machine apprenante au centre du dispositif compare sans cesse sa prédiction et la réalité advenue. Ainsi, elle apprend par itération et se perfectionne. La guerre n'est plus envisageable sans ce moteur algorithmique intelligent au centre des flux de données.

Le renseignement total implique une souveraineté numérique. Il n'est pas possible autrement. Nos adversaires potentiels le savent, c'est une des raisons de notre dépouillement actuel, tant par la doctrine que par les outils et les moyens. Il faut bien comprendre le sens profond de cette guerre prédictive. Pour l'instant la dimension cyber est une couche symbolique qui s'applique sur le monde réel et qui en fait un nouveau lieu immatériel d'affrontement de puissances. Mais l'évolution n'en reste pas là. C'est presque déjà une bataille du passé. La dimension qui s'annonce n'est pas une couche informatique sur le monde, mais la faculté des machines de mettre le réel lui-même en équation. Après le monde du code, le code du monde. Et c'est cette traduction informatique du monde qui constitue le vrai champ de bataille, car elle permet d'être en avance dans le temps. Les prévisions météorologiques permettent de prévoir les conditions atmosphériques avec quelques jours d'avance. La manière pour y parvenir consiste à accélérer un modèle mathématique du climat. Demain, c'est une modélisation du réel, en accéléré, qui sera le prochain champ de bataille.

C'est là, où nous devons concentrer nos efforts : sur cette guerre prédictive. Il nous faut désormais nous armer pour ce combat-là. Il implique de capitaliser le maximum d'informations en temps réel sur soi et sur l'adversaire. Dans le même temps, il faut se rendre le plus opaque à l'autre… Étonnant de voir que notre situation actuelle en est l'exact inverse. Car la guerre prédictive a déjà commencé par la préparation intensive de nos adversaires potentiels. La guerre, jadis, utilisait les informations du passé, lui provenant de toutes sources, pour agir, réagir et anticiper la suite, comme le joueur d'échecs estimant les arborescences de coups futurs et leur probabilité de succès au vu du jeu existant. Désormais, la machine fournit des informations directement sur les futurs possibles classés sur une échelle de probabilité et construit ses hypothèses à partir de cette modélisation la plus pertinente possible de l'avenir. La guerre moderne utilisera les informations sur le futur pour agir et non plus celles du passé.

Bien entendu, le ou les adversaires potentiels emploieront les mêmes méthodes. Il faut donc connaître leurs procédés et leurs algorithmes pour choisir d'agir selon un de leurs futurs improbables, afin de les surprendre. Là encore, le renseignement total est capital. Là encore la protection de nos processus, de nos processeurs et de nos réseaux est vitale. Nous sommes dans un monde ouvert qui ne sépare plus, comme avant, les domaines civils et militaires, désormais liés en une symbiose informationnelle intégrée à tous les réseaux.

Il faut avoir en tête aussi que la puissance cyber civile est supérieure à son équivalent militaire et qu'un État doit avoir la faculté d'en mobiliser l'ensemble. La guerre est l'état naturel du réseau. Il n'y a plus de défense sans attaque permanente pour maintenir le niveau technologique, pour se préparer à la suite. Qui veut la paix numérique fait la guerre numérique. Pourquoi la guerre cyber ne s'arrête jamais ? Pourquoi des milliers d'attaques dans le monde chaque jour ? Parce que nos adversaires n'attendent pas la guerre pour la faire, car, dans le monde cyber, cette attente, au vu de la vitesse de ce monde, est la garantie de la défaite.

Il est acquis aujourd'hui que le champ de bataille s'exprime sur cinq espaces : la terre, la mer, l'air, l'espace et le cyberespace. La réalité vers laquelle nous allons est différente. Il n'y a qu'un seul champ de bataille : le cyberespace qui s'exprime dans cinq environnements matériels différents parce que l'environnement neutre que nous connaissons disparaît. Lorsque j'arpente un chemin de forêt, les cailloux, la pente, les feuillages alentour sont les mêmes pour tous, du marcheur à l'écureuil. Il n'en est pas de même dans un environnement qui me reconnaît par ses capteurs, qui peut se modifier en fonction et interagir avec mes propres systèmes informatiques. En milieu urbain, demain, la signalisation, l'orientation, les accès, les publicités, les autorisations pourront être rectifiés en fonction de chacun.

Nous ferons demain la guerre dans un « monde conscient ». La position d'un objet et notre relation à cet objet ne résulteront pas d'un hasard aveugle, mais d'une décision prise en fonction de notre présence. La réalité

devient une matière première élaborée par l'intelligence informatique qui s'y superpose et l'intègre. Qui contrôle cette conscience de l'environnement s'assure de la victoire. Pour la déjouer, quelle que soit l'arme, quel que soit le milieu, la dimension cyber est la première. Il faut détecter, cartographier les capteurs, les réseaux, les robots, identifier les logiciels à l'œuvre, les neutraliser et mieux encore les tromper, les empoisonner avec des leurres.

Jadis, le champ de bataille était un hasard passif et partagé, minéral et organique, c'est demain une somme de décisions préméditées en attente d'action, et, à ce moment-là, probablement adverses. Pour reprendre la distinction de Cournot, nous passons d'un monde de causes dont l'origine est aléatoire à un monde de raisons qui répondent chacune d'une intention. Ce n'est plus le cyberespace, c'est le « cyber-réel ». Vont disparaître dans cette mutation : l'évidence, le bon sens, la vérité, le consensus, la raison, l'impossible… Car, tout ce qui fondait ces réflexions n'est désormais – peut-être – que simulacre et mystification. C'est la fin du réalisme naïf. C'est la fin de la confiance par défaut.

Il faudra toute la puissance des machines apprenantes et le génie du commandement humain alliés en un même effort, écrivant ainsi une nouvelle page de l'art militaire, pour vaincre dans ce monde paradoxal : celui de l'incertitude dans l'abondance de données. Évoquons ici, ce champ de guerre mutant, le premier champ de bataille où nous ne serons pas les créatures les plus intelligentes. Les machines en réseau dominent. Le volume des données et surtout le nombre de décisions prises par seconde par les machines dépassent la capacité et l'entendement humains. Les robots, les agents logiciels, les drones agissent de façon autonome. C'est le règne des réseaux neuronaux, des ordinateurs quantiques – saut révolutionnaire – et de ce qu'on nomme l'intelligence artificielle devenue le rythme et la représentation dynamique de la bataille. Seules les machines peuvent estimer l'arborescence des possibles en continu en y intégrant à chaque instant les événements inattendus, leurs combinaisons et leurs potentiels effets secondaires et tertiaires. Seules les machines peuvent anticiper le réel le plus probable. Sur le réseau, en accélération permanente, être en avance est la condition pour ne pas être en retard.

IL FAUT AVOIR EN TÊTE AUSSI QUE LA PUISSANCE CYBER CIVILE EST SUPÉRIEURE À SON ÉQUIVALENT MILITAIRE ET QU'UN ÉTAT DOIT AVOIR LA FACULTÉ D'EN MOBILISER L'ENSEMBLE. LA GUERRE EST L'ÉTAT NATUREL DU RÉSEAU. IL N'Y A PLUS DE DÉFENSE SANS ATTAQUE PERMANENTE POUR MAINTENIR LE NIVEAU TECHNOLOGIQUE, POUR SE PRÉPARER À LA SUITE. QUI VEUT LA PAIX NUMÉRIQUE FAIT LA GUERRE NUMÉRIQUE. POURQUOI LA GUERRE CYBER NE S'ARRÊTE JAMAIS ? POURQUOI DES MILLIERS D'ATTAQUES DANS LE MONDE CHAQUE JOUR ? PARCE QUE NOS ADVERSAIRES N'ATTENDENT PAS LA GUERRE POUR LA FAIRE, CAR, DANS LE MONDE CYBER, CETTE ATTENTE, AU VU DE LA VITESSE DE CE MONDE, EST LA GARANTIE DE LA DÉFAITE.

De la même manière que les transactions entre automates représentent plus de 90 % du volume des ordres boursiers sur les marchés financiers, la guerre devient une affaire de machines sur les premières strates d'affrontement. Les machines apprenantes sont capitales pour donner aux humains une représentation raisonnée de cette saturation d'informations et de cette effervescence de calcul qui nous seront devenues inaccessibles. L'intelligence et la décision seront partout en même temps et à chaque instant. Pour l'armée cela implique de devenir un « réseau conscient » qui appuie la prise de décision décentralisée, automatique ou humaine, par la contextualisation et le flux d'informations. Le commandement, aidé des machines, coordonne ces myriades de décisions instantanées.

La clé est la croissance exponentielle des flux bilatéraux de données entre toutes les parties engagées, du capteur, au soldat, aux unités et systèmes d'armes… et leur traitement massif, interactif et instantané. Ainsi, dans le domaine civil, la société britannique de logistique et de livraison *Ocado* échange dix fois par seconde avec chacun des milliers de robots de sa flotte. Pour les militaires, la communication directe entre les cerveaux des soldats abandonne le territoire de la science-fiction. Les premières expériences de communication de cerveau à cerveau par « stimulation magnétique transcrânienne » font désormais partie de l'horizon des neurosciences.

Paradoxalement, le modèle d'organisation de cette symbiose multiple personne-machine en réseau est

biologique. Il consiste à reproduire le fonctionnement du vivant, notamment dans sa capacité à gérer simultanément les autonomies d'action de ses composantes les plus discrètes : les cellules. Un corps humain est composé d'environ 30 000 milliards de cellules réparties en 7 500 parties différenciées, 78 organes et 13 systèmes, sans oublier un microbiote associé de 40 000 milliards de microbes. Nous pouvons choisir, simplement, de nous lever pour prendre un café sans avoir la connaissance des centaines de millions de décisions biologiques qui précèdent ce souhait ni comprendre la succession de myriades d'opérations qui vont devoir se coordonner pour que cette action ait lieu et qui ensuite influeront sur notre comportement à venir, chaque cellule, chaque entité corporelle émettant ses propres signaux. Tel est notre modèle. Notre univers sera machinique, mais notre principe organisationnel sera biologique.

Comment faire la différence dans cette compétition effrénée d'efficacité et de puissance de calcul ? Bien sûr le talent de ceux qui élaboreront ces processus sera en première ligne, mais le mimétisme concurrentiel rapprochera les adversaires et les progrès risquent de devenir asymptotiques au fil du temps. La faiblesse des machines provient de leur logique. Ce qui est absurde leur échappe. Le fait de résister est aberrant par exemple. Il leur faut des données en nombre considérable pour tenter par corrélation de cerner des comportements en apparence déraisonnables. Ce sera le rôle des humains que de fabriquer de l'incertitude, de l'inattendu, des exceptions, des folies, de l'artistique, de l'expérimental de mettre en œuvre des alternatives disjonctives, bref d'accomplir des actes ou de transmettre des informations que la machine adverse ne saura ni prévoir ni comprendre, sauf à les traiter comme des vulnérabilités ou des erreurs. L'essentiel de l'apport humain sera sa capacité à faire des erreurs pour la machine adverse. À Austerlitz, Napoléon démunit son flanc droit. Il prévoit que les coalisés saisiront cette faute pour y engager le combat, quittant ainsi leur position de force. Ce qu'ils firent. Ce qui permit à Napoléon de les attaquer au centre afin de scinder en deux leur armée, remportant ainsi la victoire.

Cette capacité au risque incongru, mais ultra-réfléchi, caractérisera les meilleurs commandements. Il sera impératif de préserver l'opacité de nos généraux pour qu'ils demeurent imprévisibles et que la vision globale qu'ils impulsent reste impénétrable. Ce secret sera une de nos meilleures armes de guerre. En contrepoint, quelles seront nos principales faiblesses ? Peut-on en dresser la carte ? C'est simple, nous serons attaqués sur nos évidences, pourtant mises à mal dans le monde cyber. Nous croyons à la différence entre l'état de paix et l'état de guerre. Nous croyons que nos alliés, comme nos ennemis, ne commettront pas toutes les actions qu'ils sont en capacité de faire. Nous croyons que les attaques informatiques sont l'expression principale de la guerre cyber. Nous croyons que nos systèmes sont fiables parce qu'ils fonctionnent à cet instant. Nous ne considérons pas les jeux, les jouets, les appareils grand public comme des armes. Nous pensons que nos données sont en sûreté à l'étranger. Nous pensons que nos données sont en sûreté sur des serveurs sur notre territoire, mais répondant de souverainetés étrangères. Nous pensons que le *Patriot Act* américain ne lutte que contre le terrorisme. Nous pensons que le renseignement et le commerce sont des mondes séparés. Nous pensons qu'il y a des services gratuits sans contrepartie.

Nous pensons que les Américains et les Chinois investissent des milliards dans les réseaux sociaux simplement pour gagner de l'argent. Nous pensons que la Silicon Valley est le paradis libertaire de jeunes entrepreneurs hors-sol, ignorant le soutien massif qui leur vient de l'armée et du renseignement. Nous croyons aux *business angels*. Nous rêvons aux « licornes » dont la valeur atteint des sommets alors qu'elles perdent des fortunes, mais collectent nos données. On nous a dit que le futur c'est le « nuage » et nous y transférons nos documents. Mais où est ce nuage ? Nous pensons qu'il y a une différence entre le monde civil et la dimension militaire. Nous ne voyons pas de danger à utiliser des messageries étrangères pour nos échanges les plus secrets. Nous ne pensons pas que la paix peut nous faire plus de mal que la guerre. Nous croyons que si l'on n'a rien à cacher, on ne craint rien à être espionné. Nous n'imaginons pas que les données qui sont collectées sur nous seront revendues au plus offrant, c'est-à-dire à celui qui peut nous faire le plus de mal. Nous pensons que le champ de la guerre est limité. Nous pensons que dans une guerre, il y a forcément des ennemis. Nous ne concevons pas que, sur le réseau, on est aussi en guerre avec ses amis. Et ce n'est pas grave si les haut-parleurs intelligents sont d'abord des microphones intelligents… Nous pensons que nous sommes protégés par des systèmes fermés et durcis. Nous croyons que si les autres font confiance, nous pouvons faire confiance aussi. Nous pensons, comme les petits enfants, que si nous ne voyons pas l'adversaire, c'est qu'il ne nous voit pas. Nous pensons disposer encore d'un rapport de force. Nous sommes sûrs que ce qui ne nous fait pas mal ne nous fait pas du mal. Nous croyons que les *smileys* nous sourient. Nous pensons qu'être modernes, c'est se soumettre. Nous pensons que si c'est en anglais, c'est *smart* et que, si c'est en français, c'est nul. Nous croyons que la guerre a un début et une fin. Nous pensons que la paix est l'état normal d'une nation. Nous pensons que le futur c'est demain et que demain c'est loin. Nous pensons, tout à la fois, qu'il est trop tard et qu'il sera toujours temps. Nous croyons que

notre capacité de frappe physique nous protège. Nous pensons enfin que nous sommes en sécurité.

Il s'agit d'un château de cartes, sans cartes en dessous.

Les élus et gouvernants pensent que si c'était vraiment grave, les militaires les saisiraient de la question. Les militaires pensent que, peut-être, si c'était aussi catastrophique, la classe politique serait alertée et prendrait les mesures qui s'imposent. Le public, enfin, voit que le système tourne et que le sujet n'est pas vraiment évoqué. Et tous de penser que, si les gens ne se sentent pas concernés, il n'y a pas de raison d'agir. Il suffira d'un choc pour que cet enchaînement de dénis et de reports de responsabilité s'effondre. Et le pays avec.

Il est temps de sortir de ce piège. L'évolution accélérée du monde doit faire évoluer nos perspectives à la même vitesse. Un tel changement s'est déjà produit. Rappelons-nous l'extraordinaire récit de Xénophon, *L'Anabase*, qui raconte le périple et les batailles d'une armée grecque de dix mille soldats en terre perse au V^e^ siècle avant notre ère. Il y décrit la supériorité des phalanges d'hoplites lors du choc avec la masse barbare. C'est ce choc qui détermine alors le sort de la bataille. L'infanterie légère, la cavalerie, y compris les frondeurs et les archers, certes parfois décisifs, ne remplacent pas cependant cette confrontation physique. Mais voici qu'apparaissent au XVI^e^ siècle les armes à feu et notamment l'artillerie. Pour la première fois, avec cette ampleur, les guerres d'Italie en sont un bon exemple, la résistance traditionnelle des piquiers est mise à mal. La guerre change. Au XVII^e^ siècle, les progrès de la mousqueterie sont tels que c'est le feu qui désormais domine le champ de bataille.

En un siècle, nous sommes passés du choc au feu. Voici que nous sommes en train de passer du feu au cyber. Théorisé notamment par l'armée chinoise au début du XXI^e^ siècle, ce mouvement est en cours et va en s'accélérant. Nous vivons une période mixte qui hybride le feu et le cyber. Comme jadis, le choc et le feu furent intimes. C'est là que Condé, Turenne ou encore Maurice de Nassau, Prince d'Orange, excellèrent. Tel est notre défi aujourd'hui. Le réseau est notre chance. Rien ne nous contraint d'en être les victimes. Prenons-en le contrôle. Inventons cette armée nouvelle pour ce monde nouveau.

Comment gagner une guerre perdue ? En gagnant la suivante ■