La France face au défi de la souveraineté numérique

Christophe AUGUSTIN

Colonel (terre), auditeur de la 69e session du CHEM.

Véritable lanceur d'alerte sur la *Souveraineté numérique*, notamment dans son ouvrage éponyme de 2014, Pierre Bellanger, président fondateur de la radio libre *Skyrock*, publie des articles et réalise régulièrement des conférences sur le sujet de la souveraineté numérique. Sa conférence au CHEM, à l'automne 2019, a d'ailleurs inspiré la rédaction de cet article qui a pour objet de réaliser un tour d'horizon complet sur la question. Après avoir été longtemps la *vox clamentis in deserto* (1), son appel a fini par induire une prise de conscience et atteindre les plus hauts sommets de l'État. En novembre 2017, la France a créé un poste quasi unique au monde d'ambassadeur pour le numérique (2). Il est occupé par Henri Verdier, un entrepreneur et spécialiste du numérique, depuis octobre 2018. Le Sénat français s'est également saisi de cette question stratégique à travers une commission d'enquête lancée en avril 2019. Pierre Bellanger, juste retour des choses, en fut la première personnalité auditée. De nombreuses pistes proposées dans cet article sont d'ailleurs issues des longues heures d'audition de cette commission au Palais du Luxembourg (3).

La révolution numérique transforme la société à une vitesse et dans une mesure sans précédent. Si elle ouvre d'immenses possibilités, elle présente aussi des défis redoutables. Alors que ce n'est – *a priori* – pas le cœur de son sujet, le président de la République Emmanuel Macron aborde ainsi la souveraineté numérique dans son discours du 7 février 2020 sur la stratégie de défense et de dissuasion : « Porteur d'innovations sans limite, le numérique innerve tous les milieux physiques. Devenu lui-même un champ de confrontation à part entière, sa maîtrise exacerbe les rivalités entre puissances, qui y voient un moyen d'acquérir la supériorité stratégique ». Il poursuit par une approche générale de la souveraineté que l'on peut élargir au numérique : « Pour que la France soit à la hauteur de son ambition européenne, à la hauteur aussi de son histoire, elle doit rester souveraine ou décider elle-même, sans les subir, les transferts de souveraineté qu'elle consentirait, tout comme les coopérations contraignantes dans lesquelles elle s'engagerait (4) ».

(1) « La voix de celui qui crie dans le désert ».
(2) L'Australie, l'Estonie ou le Danemark ont des postes équivalents avec des périmètres un peu différents.
(3) Commission d'enquête sur la souveraineté numérique (www.senat.fr/).
(4) MACRON Emmanuel, « Discours du président de la République sur la stratégie de défense et de dissuasion devant les stagiaires de la 27e promotion de l'École de Guerre », 7 février 2020 (www.elysee.fr/).

La conception classique de la souveraineté ébranlée par le numérique

La souveraineté est le pouvoir suprême reconnu à l'État, qui lui confère une compétence exclusive sur le territoire national et une indépendance absolue dans l'ordre international, où il n'est limité que par ses propres engagements [5]. L'État souverain est reconnu dans ses frontières par la communauté internationale et exerce un pouvoir d'administration et de juridiction sur sa population.

Au sens étymologique, est souverain ce – ou celui – qui est au-dessus de tous les autres et cet adjectif était donc originellement réservé à Dieu. L'époque moderne en Europe fut cependant marquée par la volonté des monarques de s'émanciper de l'autorité spirituelle du Pape. C'est ainsi que François Ier, incarnant le pouvoir temporel national face au pouvoir transnational de l'Église, promulgue l'ordonnance de Villers-Cotterêts en 1539 imposant l'usage du français de préférence au latin comme langue du droit et de l'administration. Au XVIIe siècle, les traités de Westphalie [6] donnent naissance au concept d'État-nation qui s'imposera comme référence pour définir l'État et la souveraineté qui en découle. Théorisée par Jean Bodin[7] au XVIe siècle puis Thomas Hobbes[8] au XVIIe, la souveraineté de l'État-nation se traduit par l'absolutisme royal en France tandis que l'Angleterre place le parlement au centre du jeu politique. Mais dès le XVIIIe siècle, Jean-Jacques Rousseau développe dans *Le Contrat social* (1762), l'idée que les hommes doivent être gouvernés par des lois découlant de la volonté générale exprimée par le peuple. Il confère ainsi la souveraineté au peuple et inspire la Déclaration des droits de l'Homme et du citoyen de 1789 : « Le principe de toute souveraineté réside essentiellement dans la Nation (…) [9] ». Cependant, l'État-nation est parfois remis en question par des acteurs qui ne le perçoivent pas comme le seul cadre possible de l'exercice de la souveraineté. Les compagnies des Indes, quelle que soit leur nationalité [10], régissaient souverainement leurs comptoirs ultramarins au XVIIe et XVIIIe siècles. Comment ne pas faire le parallèle avec les Gafam [11], dont la suprématie technologique, économique et normative s'étend par-delà les frontières et dont la valorisation boursière cumulée, dépassant les 5 000 milliards de dollars en janvier 2020, est supérieure aux produits intérieurs bruts des principales puissances européennes ?

L'exercice de la souveraineté se traduit par des prérogatives relevant *a priori* de la compétence des États. Les fonctions régaliennes sont variables d'un État à l'autre, mais recouvrent généralement la sécurité intérieure, la défense, le renseignement, la diplomatie, la justice et les finances, avec en particulier la politique monétaire et la perception de l'impôt. Cependant, la maîtrise de ces fonctions régaliennes est de plus

---

(5) Encyclopédie Larousse.

(6) En 1648, ces deux traités mettent fin à la guerre de Trente Ans qui a impliqué l'ensemble des puissances du continent dans un conflit entre le Saint Empire romain germanique et ses États allemands protestants en rébellion.

(7) Bodin Jean, *Les Six Livres de la République*, Paris, Jacques du Puys, 1576, 861 pages.

(8) Hobbes Thomas, *Léviathan ou Matière, forme et puissance de l'État chrétien et civil*, Gallimard, 2000, 1 024 pages.

(9) Déclaration des Droits de l'Homme et du Citoyen de 1789, article 3 (www.legifrance.gouv.fr/).

(10) Les plus connues sont les françaises, néerlandaises et britanniques, mais il y eut également des compagnies suédoises et danoise.

(11) Google, Apple, Facebook, Amazon et Microsoft, les géants américains du numérique.

en plus limitée aujourd'hui. L'emprise des États sur l'économie est modérée par la mondialisation et par les relations multilatérales qui limitent leur pouvoir par des traités. Certaines prérogatives peuvent aussi être transférées à des entités supranationales. Ainsi, l'Union européenne possède la compétence exclusive en matière douanière, de concurrence interne ou de politique monétaire pour les pays de la zone euro [12]. Enfin, des normes sont fixées par des organismes internationaux comme c'est le cas dans le domaine numérique afin de garantir l'interopérabilité entre systèmes.

Cette perte progressive de souveraineté des États est amplifiée par l'avènement du numérique. Ainsi, l'impact d'*Internet* sur la société s'est accéléré au cours des années 1990 pour devenir omniprésent aujourd'hui. « *Internet* ne vient pas s'ajouter au monde que nous connaissons. Il le remplace. [13] ». La révolution numérique a augmenté les capacités de communiquer, d'agir et de produire. Simultanément, elle remet en cause les fonctions régaliennes qui fondent la souveraineté au sens classique. Quelle loi et quelle fiscalité appliquer sur un réseau mondial qui abolit les frontières ? Que devient la souveraineté monétaire à l'heure des monnaies virtuelles ? Comment se protéger de la cybercriminalité menaçant la sécurité intérieure, les infrastructures vitales, les entreprises et les individus ? Comment protéger les citoyens des atteintes aux libertés individuelles ? Comment les armées doivent-elles prendre en compte ce nouveau domaine de conflictualité ? Eric Schmidt, alors président-directeur général de Google, écrivait en 2014 dans *The New Digital Age* : « les États sont devenus des monstres bureaucratiques inefficaces, les sociétés de l'*Internet* comme Google sont beaucoup plus efficaces, elles auront donc vocation à les remplacer [14] ». Sommes-nous prêts à passer de l'État-nation à l'État-entreprise ?

Avec l'omniprésence des Technologies de l'information et de la communication (TIC), leur maîtrise prend une importance considérable. Pour les armées, la supériorité opérationnelle est intimement liée à cette maîtrise. Ainsi, un État qui se veut souverain, doit être capable de concevoir et de réaliser des composants électroniques, des logiciels, des infrastructures de réseau, des moyens de chiffrement et d'analyse de données. Il doit être en mesure de se protéger des attaques informatiques tout en étant capable d'en mener. Il doit permettre à ses citoyens d'effectuer des transactions sécurisées. Il doit disposer de lois protégeant les individus et les entreprises sans pour autant freiner l'innovation. « La souveraineté numérique peut être entendue comme la capacité de la France d'une part, d'agir de manière souveraine dans l'espace numérique, en y conservant une capacité autonome d'appréciation, de décision et d'action, et d'autre part, de préserver les composantes les plus traditionnelles de la souveraineté vis-à-vis de menaces nouvelles tirant parti de la numérisation croissante de la société [15] ».

---

[12] Article 3 du Traité sur le fonctionnement de l'Union européenne, Traité de Lisbonne de 2007.

[13] Bellanger Pierre, *La souveraineté numérique*, Stock, 2014, p. 9.

[14] Schimdt Eric et Cohen Jared, *The New Digital Age: Reshaping the Future of People, Nations and Business*, Hodder & Stoughton Libri, 2014, 368 pages.

[15] Secrétaire général de la défense et de la sécurité nationale (SGDSN), *Revue stratégique de cyberdéfense*, février 2018, p. 93 (www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/).

Face aux puissances établies, la France a pris du retard mais elle possède des atouts qui lui permettront de relever ces deux défis : répondre aux menaces numériques sur sa souveraineté au sens classique et exercer sa souveraineté dans l'espace numérique.

La France face aux grandes puissances numériques : une situation contrastée

Seul espace stratégique créé de la main de l'homme, le cyberespace est un nouveau continent à conquérir. Après s'être affrontées sur terre et en mer, puis dans les airs, les grandes puissances luttent désormais pour la suprématie dans ce domaine immatériel. Dans cette lutte, les États-Unis sont en position dominante. Ils s'appuient sur un modèle libéral favorisant la concurrence et l'innovation, et sont dotés d'un complexe militaro-industriel puissant. La *DARPA* et la *NSF* [16], deux agences gouvernementales dont les budgets s'élèvent respectivement à 3,6 et 8,3 milliards de dollars en 2020, ont joué un rôle majeur dans le développement du numérique. La frontière entre l'État américain et les Gafam est poreuse, et le soutien des administrations successives ne se dément pas. Ainsi, convaincue de l'importance du numérique, l'administration Clinton a lancé une nouvelle dynamique dès 1993 et la Silicon Valley bénéficia alors d'un effort public considérable. Le *Patriot Act* [17], promulgué à la suite des attentats du 11 septembre 2001, renforce encore ces liens pour donner naissance à une véritable industrie du renseignement. En pleine crise entre la Chine et Google en janvier 2010, la secrétaire d'État Hillary Clinton, promet d'abattre le « rideau de fer numérique [18] » créé par le système de censure chinois.

Cependant, ce lien entre l'administration américaine et les géants du numérique n'empêche pas ces derniers de s'opposer parfois au gouvernement car leurs relations ambiguës nuisent à la confiance de leurs clients après les révélations d'Edward Snowden [19]. En 2015, Apple refuse ainsi de fournir les clés de chiffrement de l'*iPhone* d'un criminel [20]. En 2016, Microsoft refuse pour sa part de livrer au *FBI* les courriels d'un trafiquant de drogue hébergés sur des serveurs en Irlande [21]. En réaction, le *Cloud Act* [22] de 2018 offre aux autorités les outils juridiques pour obliger les entreprises américaines à fournir les données stockées sur leurs serveurs, y compris à l'étranger et quelle que soit la nationalité de leur propriétaire. En réaction aux projets européens de taxation des services numériques, Donald Trump menace de représailles les pays de

(16) *Defense Advanced Research Project Agency* ; *National Science Foundation*, l'équivalent du CNRS français.
(17) Cette loi renforce le pouvoir des agences gouvernementales dans la lutte antiterroriste. Elle autorise le *FBI* à épier les mails et à conserver les traces de navigation de toute personne suspectée de contact avec une puissance étrangère (www.congress.gov/bill/107th-congress/house-bill/03162).
(18) Rodham Clinton Hillary, Secrétaire d'État, Washington DC, 21 janvier 2010 (https://2009-2017.state.gov/).
(19) Mise sur la place publique des programmes américains et britanniques de surveillance de masse à l'été 2013.
(20) « Apple refuse d'aider à débloquer l'*iPhone* d'un des auteurs de la tuerie de San Bernardino », *Le Figaro*, 17 février 2016 (www.lefigaro.fr/).
(21) Cassini Sandrine, « Microsoft devant la Cour suprême pour défendre la protection des données », *Le Monde*, 17 octobre 2017.
(22) *Clarifying Lawful Overseas Use of Data Act* (www.congress.gov/bill/115th-congress/senate-bill/2383/text).

l'UE [23]. Il considère aussi la protection des données personnelles instaurée par le RGPD [24] comme un acte anticoncurrentiel freinant l'accès des petites et moyennes entreprises américaines au marché du numérique [25].

Par ailleurs, les Gafam ont bien compris l'importance stratégique des câbles sous-marins par lesquels transitent plus de 95 % des communications intercontinentales. Ils réalisent aujourd'hui 50 % des investissements du domaine [26], Google étant le plus actif. À titre d'exemple, le câble Marea posé en 2017 entre la Virginie et Bilbao dont Microsoft et Facebook sont propriétaires pour 25 % chacune, est le plus performant du monde avec une capacité de 160 térabits par seconde.

Face aux États-Unis qui aspirent à un *leadership* incontesté, la Chine a développé sa propre vision de la souveraineté numérique. Dopée par des investissements étrangers massifs au cours des années 1990, Pékin est rapidement montée en puissance. Alors que la Chine ne comptait que 22 millions d'internautes en 2000, ils étaient déjà 733 M en 2016. Par ailleurs, elle occupe aujourd'hui la deuxième place en matière de *cloud* [27]. Dans son dernier plan quinquennal [28], elle ambitionne l'autonomie dans de nombreux domaines dont le numérique, l'intelligence artificielle (IA) et le spatial. Ses grands opérateurs nationaux, les *BATX* [29], rivalisent avec leurs concurrents américains. Ils sont soutenus par un immense marché intérieur, un atout maître dans le jeu numérique. Sur le plan des équipements, la société Huawei, fondée seulement en 1987, est aujourd'hui le deuxième constructeur mondial de *smartphones*, un fournisseur de solutions réseaux et *cloud*, mais surtout un équipementier pour la 5G [30], technologie hautement stratégique. En matière de câbles sous-marins, Huawei Marine Networks se positionne à la quatrième place mondiale. Elle développe par exemple un projet de câble de 12 000 km reliant la Chine et la France *via* le Pakistan et Djibouti dans le cadre des nouvelles Routes de la soie [31].

Fondé sur un modèle autoritaire, l'espace numérique chinois est très contrôlé. Il possède peu de points de connexion avec l'*Internet* mondial, si bien qu'il est comparable à un *intranet* géant. La Chine conserve ainsi environ deux tiers du trafic sur son sol et impose depuis 2017 le stockage des données personnelles sur son territoire. Pour accompagner cette forme d'autoritarisme numérique, une armée d'opérateurs effectue

---

[23] « Taxe GAFA : Washington brandit la menace d'une imposition massive des produits français », *Capital*, 3 décembre 2019 (www.capital.fr/).

[24] Le Règlement général sur la protection des données adopté par l'UE en avril 2016, entré en vigueur en mai 2018, accroît la protection des personnes concernées par le traitement de leurs données et responsabilise les acteurs. Règlement UE 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679).

[25] Commission d'enquête, *La souveraineté numérique* (Rapport), Sénat, 2019, p. 19 (www.senat.fr/).

[26] Izambard Antoine, « Facebook, Google, Amazon… Pourquoi les géants du *Net* se ruent sur les câbles sous-marins ? », *Challenges*, 18 juillet 2019.

[27] L. Bastien, « Le marché du *cloud* chinois a crû de 67 % au dernier trimestre 2019 », *Le Big Data*, 20 mars 2020 (www.lebigdata.fr/marche-cloud-chinois-t4-2019).

[28] « *Made in China 2025*, l'ambition chinoise », *Portail de l'IE*, 15 septembre 2015.

[29] Baidu, Alibaba, Tencent, Xiaomi sont les équivalents chinois des Gafam.

[30] Après la voix (1G), les SMS (2G), le *Web* mobile (3G), la communication entre objets (4G), la 5G permettra de connecter 1 million d'objets par km² avec des débits 100 fois plus rapides qu'aujourd'hui.

[31] Huawei Marine Networks, « PEACE Cable Project Enters into Cable and Materiel Manufacturing Stage », 22 octobre 2018 (www.huaweimarine.com/en/News/2018/press-releases/pr20181022).

des contrôles destinés à empêcher l'émergence de critiques politiques et à asseoir la domination du Parti communiste. Ces contrôles vont jusqu'à instaurer un système attribuant à chaque individu un crédit social, qui fluctue selon son comportement et auquel sont corrélés des droits [32]. Combien de temps cette muraille de Chine numérique pourra encore tenir face aux aspirations de sa population ?

La Russie a également adopté une politique autoritaire dans le domaine. Ne disposant pas de champions mondiaux, elle a adapté ses ambitions et s'est concentrée sur la couche sémantique du cyberespace [33]. L'influence et la propagande ne datent pas d'hier, mais les nouvelles technologies permettent de toucher une audience plus large, parfois de manière individualisée. La vitesse de propagation d'informations mensongères rend ces actions difficiles à prévenir et à contrer. Elles permettent parfois de « soumettre l'ennemi sans combattre, art suprême de la guerre » selon Sun Tzu (*L'Art de la guerre*). Leur efficacité a été démontrée en 2014 et 2015 en Crimée et au Donbass par le soutien des velléités séparatistes [34]. Ces actions constituent une menace pour les démocraties. Après les opérations d'influence principalement orchestrées depuis la Russie lors des élections américaines de 2016, les réseaux sociaux ont lutté contre les faux comptes. Malgré cela, Facebook a encore bloqué en février 2020 des campagnes d'influence menées par des groupes soutenus par les services russes[35].

Même si la Russie ne dispose pas de géants du numérique, ses équivalents des Gafam développent leurs activités. Ainsi, Mail.ru, propriétaire du réseau social *Vkontakt* s'est allié avec le chinois Alibaba pour développer l'*e*-commerce russe. Le moteur de recherche Yandex se lance dans la vente de smartphones fabriqués en Chine. Enfin, Rostec, acteur majeur des technologies civiles et militaires de pointe, permet à la Russie d'être autonome pour ses systèmes sensibles. En parallèle, Moscou a mis en œuvre un arsenal juridique impressionnant pour protéger sa souveraineté. La censure d'*Internet* est organisée et le stockage des données de ses ressortissants doit être localisé sur le territoire russe. La loi « des blogueurs » de 2014, permet de censurer les pages dont l'influence est jugée néfaste [36]. La loi antiterroriste de 2016 impose la conservation de tout message pendant un an et oblige les messageries cryptées comme Telegram et WhatsApp à fournir les clés de chiffrement [37]. Enfin, une loi de novembre 2019 vise à créer un *Internet* russe indépendant avec des équipements permettant de l'isoler des serveurs mondiaux afin de permettre aux services vitaux de fonctionner en cas de guerre ou de cyberattaques massives [38]. Le trafic sera réorganisé de manière à réduire les flux de données venant d'autres pays. Cela permettra au gendarme russe des

[32] Croquet Pauline, « En Chine, un système de notation des citoyens encore flou mais aux ébauches effrayantes », *Le Monde*, 28 décembre 2018 (www.lemonde.fr/).
[33] Le cyberespace se compose de la couche matérielle (serveurs, routeurs, ordinateurs…), de la couche logique (logiciels), et de la couche sémantique (valeur ajoutée aux données transformées en informations utiles comme les réseaux sociaux).
[34] Nocetti Julien, « Guerre de l'information : le *Web* russe dans le conflit en Ukraine », *Russie.Nei.Reports* n° 20, Institut français des relations internationales (Ifri), septembre 2015, 36 pages (www.ifri.org/).
[35] *AFP*, « Facebook bloque 3 campagnes de manipulation liées à la Russie, l'Iran et la Birmanie », *Le Figaro*, 12 février 2020 (www.lefigaro.fr/).
[36] *AFP*, « Le parlement russe renforce le contrôle des blogs », *Le Monde*, 22 avril 2014 (www.lemonde.fr/).
[37] « *Russie, Poutine promulgue une série de lois antiterroristes controversées* », *Le Point*, 7 juillet 2016 (www.lepoint.fr/).
[38] *AFP*, « La Russie cherche à créer un *Internet* indépendant », *Le Figaro*, 12 février 2019 (www.lefigaro.fr/).

télécommunications, le *Roskomnadzor*, d'analyser le trafic et de le rediriger vers ses services. Tout en se protégeant, les Russes ont développé des capacités cyber d'espionnage et d'attaque. Ils affichent clairement leur volonté de souveraineté numérique en développant une vision autoritaire mais aussi agressive avec une capacité de nuisance accrue.

Alors que la France disposait d'atouts dans le domaine de l'informatique et des télécommunications, le poids relatif de son industrie du numérique a décliné au cours des trois dernières décennies. Le Plan Calcul, lancé en 1966 par de Gaulle, visait à assurer l'autonomie du pays dans ces technologies et à en faire la base d'une industrie informatique européenne [(39)]. Ce plan est à l'origine de la création de l'Institut national de recherche en informatique et automatique (Inria) et de la Compagnie internationale pour l'informatique (CII, qui fusionnera plus tard avec Bull) et a permis le développement de l'industrie des circuits intégrés (Thomson) tout en marquant un effort au profit de la formation. C'est à cette époque que le technopôle de Rennes [(40)] se développe avec un réseau d'écoles, de centres de recherche et d'industries, posant les bases de l'actuel pôle d'excellence cyber. L'ingénieur polytechnicien Louis Pouzin, considéré comme un pionnier d'*Internet*, invente en 1973 la segmentation des données en datagrammes et conçoit le réseau Cyclades. Il fut récompensé par de nombreux prix [(41)] pour cela, mais reste peu connu du grand public en France.

Malgré ces atouts, le manque de vision stratégique des années 1990 a entraîné le démantèlement de notre industrie d'informatique et d'électronique grand public. Elle a aussi entraîné le départ de nos meilleurs développeurs à l'étranger faute de les associer à des projets ambitieux. Thomson Multimédia échappe de justesse au rachat par le coréen Daewoo en 1996, alors qu'elle dispose de nombreux brevets sur la musique et la vidéo utilisés dans les *smartphones*. Sa branche grand public est vendue en 2004 au chinois TCL. Alcatel, autre fleuron français des télécommunications, après avoir transféré ses usines vers la Chine en 2002, fusionne avec l'américain Lucent en 2006 et perd de nombreux brevets à son profit. À cette époque, la France est pénalisée par un dispositif juridique inadapté en matière de « guerre économique ». La reprise d'Alcatel-Lucent par le finlandais Nokia en 2015 signe son arrêt de mort. Alors que les *smartphones* deviennent un succès mondial, la France qui était l'un des principaux fabricants perd ses capacités industrielles. Simultanément, les logiciels de la Silicon Valley inondent nos ordinateurs et sont utilisés dans toutes les sphères régaliennes. Cela alimente d'ailleurs un débat récurrent sur l'emploi des logiciels libres.

Cependant, la France possède encore aujourd'hui des entreprises performantes dans le secteur : Dassault Systèmes pour les logiciels, Atos, Orange et Thales pour la cybersécurité, Capgemini pour le conseil, Ubisoft pour les jeux, OVH pour le *cloud*, Veepee (ex-Vente-Privée) pour l'économie du *Net*, Acome et Nexans pour la fibre optique, Alcatel Submarine Networks pour les câbles sous-marins. Ces réussites ne

---

(39) Gaston-Breton Tristan, « Le plan Calcul, l'échec d'une ambition », *Les Échos*, 20 juillet 2012 (www.lesechos.fr/).

(40) Le début des années 1970 voit l'installation du Centre national d'études des télécommunications (Cnet), de Supélec, de l'École supérieure d'électronique de l'Armée de terre (ESEAT), du Centre d'électronique de l'armement (Célar) et de l'Institut national de recherche en informatique et automatique (Inria).

(41) *IEEE Internet Award* en 2001, *Queen Elizabeth Prize for Engineering* en 2013.

doivent pas masquer notre extrême dépendance et parfois notre résignation quant à la défense de nos libertés individuelles. Depuis l'avènement des réseaux sociaux, la quasi-totalité de nos données personnelles traversent l'Atlantique. Dès 2011, Pierre Bellanger alertait sur les risques pour notre souveraineté dans la revue *Le Débat* : « Les Français et les Européens transfèrent massivement leurs données personnelles sur le continent nord-américain. La France fait partie des premiers exportateurs mondiaux de vie privée [42] ». Deux ans plus tard, l'affaire Snowden en a démontré tous les risques.

Nos voisins européens sont dans une situation similaire. Ils possèdent des atouts mais pas de champion mondial. Sur les 465 licornes [43] recensées en avril 2020 par le cabinet d'analyse économique new-yorkais CB Insights, 223 sont américaines, 119 chinoises et seulement 54 européennes [44]. Pour développer son propre modèle de souveraineté numérique, la France devra pourtant favoriser l'émergence de champions en s'appuyant sur des partenariats européens. Une action de niveau européen sera donc nécessaire. Par ailleurs, ce modèle pourra s'inspirer du modèle américain dans lequel les armées jouent un rôle important.

Se défendre face aux menaces sur la souveraineté classique

Le pouvoir acquis par certaines entreprises remet en cause l'exercice par l'État de ses fonctions régaliennes en matière de sécurité, de défense, de normes, de fiscalité et de monnaie.

D'après la Cnuced [45], les exportations de services numériques en 2018 ont représenté 2 900 Md$, soit 50 % des exportations mondiales de services. Les États-Unis et la Chine cumulent plus de 90 % de la capitalisation boursière des 70 premières plateformes numériques alors que l'UE n'en détient que 4 %. Le modèle économique « biface » [46] a permis la constitution rapide de géants par la fourniture de services faussement gratuits, en échange de la collecte de données utilisées pour des publicités ciblées. L'effet réseau attire les utilisateurs vers les plateformes les plus populaires. Cela favorise des rendements d'échelle pour investir dans de nouveaux services et attirer ainsi de nouveaux utilisateurs. Le cercle vertueux pour les plus forts ou vicieux pour les autres est enclenché. On assiste à la création de monopoles puis de conglomérats avec le rachat de *start-up* performantes sur des produits de niche [47].

Non seulement cette situation défavorise les entreprises françaises, mais elle accroît aussi notre dépendance à ces groupes étrangers. Si cette puissance économique se mue en domination, c'est notre souveraineté économique qui est menacée. Déjà envisagé, le démantèlement des Gafam n'est pas réaliste et pourrait favoriser l'essor des

---

[42] Bellanger Pierre, *op. cit.*, p. 11.
[43] Une licorne est une *start-up* non cotée en Bourse mais valorisée à plus de 1 milliard de dollars.
[44] Site *Internet* du cabinet d'analyse économique new-yorkais CB Insights (cbinsights.com/).
[45] Conférence des Nations unies sur le commerce et le développement, *Rapport 2019 sur l'économie numérique*, 198 pages (https://unctad.org/fr/PublicationsLibrary/der2019_fr.pdf).
[46] Jean Tirole décrit comment le digital modifie la chaîne de création de valeur dans son livre *Économie du bien commun*.
[47] Google a racheté Android en 2005, Youtube en 2006, Waze en 2013 et DeepMind en 2014.

BATX. En revanche, il est souhaitable de renforcer l'arsenal législatif du droit de la concurrence et de lutte contre les acquisitions prédatrices. Forte de ses 450 M de consommateurs, l'UE est le bon niveau pour agir. La directive européenne « ECN + » de décembre 2018 [48], doit être transposée car elle permet aux autorités nationales de prononcer la cession d'une branche d'activité en cas de pratiques anticoncurrentielles. En outre, la Direction générale des entreprises (DGE) travaille à l'identification des règles qui pourraient être imposées au-delà de la simple concurrence [49]. Elles concernent la portabilité des données, l'interopérabilité des plateformes, l'obligation de partage de certaines données, le respect de la transparence introduit par la récente Loi pour une République numérique [50], et l'auditabilité. En effet, s'il n'est pas réaliste d'imposer la publication des algorithmes protégés par le secret des affaires, il faut en organiser l'auditabilité par la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) afin de garantir le respect des règles de la concurrence et la protection des données. Par ailleurs, la Commission européenne s'est dotée en 2018 d'un observatoire sur l'économie des plateformes numériques chargée de surveiller les pratiques abusives [51]. Il faut lui donner le rôle d'une véritable agence européenne d'évaluation.

Si le pétrole a été le carburant de l'industrie au XX^e^ siècle, les données seront celui du cyberespace au XXI^e^ siècle. La baisse des coûts de traitement permet la création de nouveaux services numériques et des gains d'efficacité dans la production de biens et de services des secteurs traditionnels. La localisation sur le territoire national des données particulièrement sensibles doit être imposée. Si cela semble évident pour les sujets de défense et de sécurité, cette pratique doit être étendue aux autres traitements publics et aux données commerciales stratégiques. Cela permettra un contrôle et une accessibilité renforcée tout en soutenant les acteurs français du *cloud*. En revanche, la relocalisation en France ou en Europe des données personnelles ne résoudrait pas, à elle, seule la problématique d'extraterritorialité posée par le *Cloud Act*. Le RGPD offre un cadre juridique renforçant le droit des personnes physiques dont les données sont utilisées et responsabilisant les acteurs du traitement. Il permet des sanctions dissuasives jusqu'à 20 M€ ou 4 % du chiffre d'affaires mondial. Son champ d'application est vaste et a vocation à s'appliquer en dehors de l'UE. Elle doit l'appliquer fermement et réfléchir à l'opportunité d'étendre ces sanctions aux données stratégiques des entreprises qui pourraient être transmises en dehors d'une procédure judiciaire. L'UE envisage aussi de se doter d'une législation à dimension extraterritoriale pour l'accès aux preuves électroniques, avec le projet *e-evidence*, en cours de négociation avec les États-Unis [52].

---

[48] Parlement européen et Conseil, Directive (UE) 2019/1 visant à doter les autorités de concurrence des États-membres des moyens de mettre en œuvre plus efficacement les règles de concurrence et à garantir le bon fonctionnement du marché intérieur, 11 décembre 2018 (https://eur-lex.europa.eu/).

[49] *La souveraineté numérique* (Rapport), *op. cit.*, p. 46.

[50] Cette loi du 7 octobre 2016, complétée par les décrets du 29 septembre 2017, oblige les opérateurs de plateformes à élaborer des bonnes pratiques pour renforcer la loyauté et la clarté des informations transmises et notamment les avis en ligne (www.legifrance.gouv.fr/).

[51] Commission européenne, « Plateformes en ligne : la Commission définit de nouvelles normes en matière de transparence et d'équité (Communiqué de presse) », 26 avril 2018 (https://ec.europa.eu/).

[52] Commission européenne, « Union de la sécurité : la Commission facilite l'accès aux preuves électroniques » (communiqué de presse), 17 avril 2018 (https://ec.europa.eu/commission/presscorner/detail/fr/IP_18_3343).

Par ailleurs, le droit à la portabilité, introduit par le RGPD, permet à toute personne de récupérer, dans un format structuré, les données personnelles fournies à un prestataire en vue de les transmettre à un autre. Cette pratique va encourager l'émergence d'acteurs concurrents aux géants du numérique. Il convient d'envisager désormais de passer à l'étape suivante avec l'obligation d'interopérabilité entre les plateformes. Cela permettrait de poursuivre une activité d'une plateforme à l'autre sans perdre les contacts ni les réseaux sociaux établis précédemment. La mise en œuvre de ces derniers points nécessite de renforcer en moyens humains les autorités de régulation. La Commission nationale de l'informatique et des libertés (Cnil) [53] ne compte que 215 employés fin 2019 alors que ses homologues allemands et britanniques sont environ 700 [54].

L'authentification des personnes est également une activité régalienne qui ne peut pas être abandonnée à Google dont les solutions d'identification ont déjà la primauté sur *Internet*. Si des instruments officiels comme FranceConnect existent, nous sommes encore loin d'offrir une identité numérique souveraine et nous accusons du retard face à l'Estonie ou la Belgique. Ces derniers fournissent déjà une carte d'identité électronique facilitant les démarches administratives en ligne, en bénéficiant d'une authentification forte [55].

La fiscalité est un autre domaine régalien remis en cause par le numérique. Alors que les multinationales profitent d'infrastructures financées par les impôts de leurs clients, elles mettent en œuvre des stratégies de contournement en utilisant les méthodes traditionnelles d'optimisation et en tirant profit des caractéristiques propres à ce secteur comme la difficulté à localiser la création de valeur ajoutée. Une étude de la Commission européenne de 2017 estimait que le différentiel d'imposition entre multinationales du numérique et traditionnelles était de 14 points (9,5 % contre 23,2 %) [56]. Ces entreprises bénéficient aussi du concours de pays au régime fiscal spécifique comme l'Irlande. Le projet français de taxe sur les services numériques adopté en juillet 2019 a fait l'objet de joutes musclées avec l'administration américaine. Son rendement annuel est estimé à 400 M€, mais cette taxe est susceptible de faire l'objet de représailles puis d'être répercutée sur le consommateur final. Même si l'UE a abandonné son projet de taxe, l'initiative française constitue une avancée significative. L'Italie a mis en œuvre un dispositif équivalent [57] et d'autres pays souhaitent faire de même (Espagne, Royaume-Uni, Autriche). L'Organisation de coopération et de développement économique (OCDE), qui est le bon niveau pour définir des bases solides et pérennes, encadre des négociations entre 129 pays pour lutter contre cette évasion fiscale. Il est donc important d'y défendre nos intérêts en promouvant le principe d'imposition de la valeur ajoutée en fonction du lieu de consommation des services et

[53] Autorité indépendante chargée de la protection des données personnelles et de veiller à ce que l'informatique ne porte pas atteinte à la vie privée et aux droits de l'Homme.
[54] *La souveraineté numérique* (Rapport), *op. cit.*, p. 63.
[55] Thales Group, « Identité numérique forte : le cas de la carte d'identité nationale électronique », 8 mai 2020 (www.thalesgroup.com/fr/europe/france/dis/gouvernement/identite).
[56] Commission européenne, « Questions et réponses sur un système d'imposition des entreprises juste et efficace au sein de l'Union pour le marché unique numérique » (Fiche d'information), 21 mars 2018 (https://ec.europa.eu/).
[57] *La souveraineté numérique* (Rapport), *op. cit.*, p. 84.

non plus celui de production. Cependant, la fiscalité ne doit pas être envisagée seulement sous l'angle des sanctions, elle peut aussi servir à augmenter l'attractivité du pays en capital humain et financier.

La première cryptomonnaie est apparue en 2009 au moment de la crise financière mondiale. Le Bitcoin est géré sans autorité centrale, ni administrateur unique. Ce nouveau moyen de paiement est accepté par un nombre croissant de commerçants, motivés par des frais de transaction très inférieurs à ceux des cartes de crédit. Les transactions sont enregistrées sur un registre virtuel appelé *blockchain*, technologie permettant le stockage et la transmission cryptée de données sans organe de contrôle. Il est possible d'acheter des Bitcoins en ligne sur des plateformes spécialisées qui permettent d'en suivre la valeur en temps réel par rapport aux autres monnaies. Cherchant à diversifier ses activités et à devancer ses concurrents, Facebook fort de ses 2,4 Md d'utilisateurs a annoncé sa volonté de créer une nouvelle monnaie, le Libra, en juin 2019 [58]. Contrairement au Bitcoin soumis à une relative volatilité, Facebook prétend avoir les moyens financiers d'en garantir la valeur. L'État risque de se voir dépassé dans ce domaine hautement régalien sur lequel son pouvoir régulateur sera affaibli. Les risques de blanchiment ou de financement du terrorisme ne doivent pas être négligés car les cryptoactifs permettent un quasi-anonymat. Il y a aussi des enjeux pour la stabilité du système financier et la protection des investisseurs. Il est donc urgent de s'emparer du sujet en imposant des règles similaires au secteur bancaire. À l'instar d'initiatives lancées par la Chine ou le Brésil, il faut encourager les banques centrales à développer des cryptomonnaies qui présenteraient des avantages similaires tout en offrant la garantie de la puissance publique. Ce type de monnaie offrirait par ailleurs une alternative au dollar dans le commerce international et pourrait servir de valeur refuge pour les pays émergents.

Affirmer sa souveraineté numérique

L'exercice de la souveraineté numérique nécessite de mettre en œuvre une politique industrielle volontariste. Dans chaque filière, il faut identifier notre positionnement et assumer des investissements publics vers celles qui seraient menacées ou trop dépendantes de fournisseurs étrangers critiques. Il ne s'agit pas nécessairement de tout faire dans un cadre strictement national, mais de se donner les moyens de conserver une autonomie suffisante et une liberté de choix. Aujourd'hui, il n'apparaît plus raisonnable de développer un système d'exploitation souverain. L'investissement nécessaire pour rattraper l'avance des géants du numérique dans une offre concurrente risquerait de ne pas trouver sa place sur le marché. En revanche, l'utilisation de solutions alternatives basées sur des logiciels libres [59] doit être développée au sein de l'État et élargie aux secteurs sensibles.

[58] Cassel Boris et Z. G., « Facebook va lancer sa propre monnaie », *Le Parisien*, 15 juin 2019 (www.leparisien.fr/).

[59] Système d'exploitation Clip OS développé par l'Agence nationale de la sécurité des systèmes d'information ou ANSSI (www.ssi.gouv.fr/) ; la messagerie instantanée sécurisée Tchap développée par la DINSIC, la Direction interministérielle du numérique et du système d'information et de communication de l'État (www.tchap.fr/), ou encore les solutions libres développées par la Gendarmerie nationale (système d'exploitation, outils bureautiques, messagerie).

Dans le domaine du chiffrement, la France dispose de capacités de conception et de réalisation de matériels et de logiciels. L'État, et notamment les armées, doivent les soutenir par la commande publique et inciter nos entreprises à faire de même. La *Revue stratégique de cyberdéfense* de 2018 constatait que les secteurs de la supervision de sécurité, de la détection d'attaques et d'analyse de codes malveillants étaient trop dépendants d'acteurs étrangers [60]. La délivrance de qualifications par l'ANSSI [61] doit permettre de soutenir les offres nationales émergentes. Les craintes générées par l'installation du futur réseau 5G par des fournisseurs comme Huawei ont entraîné la décision de soumettre tout déploiement à une autorisation préalable instruite par l'ANSSI concernant les équipements, les modalités de déploiement et d'exploitation. Cette approche pragmatique doit garantir la sécurité des futurs réseaux dont les nouveaux usages sont particulièrement critiques (usine du futur ou voiture connectée).

Nos capacités en matière de composants électroniques (STMicroelectronics) ou de supercalculateurs (Atos pour le programme de dissuasion du Commissariat à l'énergie atomique et aux énergies alternatives, CEA) pourront bénéficier du programme européen pour le calcul à haute performance (EuroHPC) lancé fin 2018 et doté d'un budget d'un milliard d'euros [62]. Dans les domaines du *cloud* ou de l'IA dominés par les Américains, il est essentiel d'adopter une stratégie de différenciation afin d'établir un avantage concurrentiel. La promotion de solutions respectueuses de la vie privée en fait partie. Après l'échec de la tentative de *cloud* souverain [63] lancée en 2010, la DGE pilote actuellement des travaux visant à faciliter l'émergence d'offres *cloud* se différenciant par leur niveau de confiance. Si la stratégie et les moyens alloués au domaine de l'IA ont émergé lentement, la dynamique est désormais lancée. Son développement est essentiel pour les systèmes autonomes ou le traitement de données en masse. Les applications sont nombreuses : véhicule autonome ou diagnostic santé dans le domaine civil, essaims de drones, systèmes d'aide à la décision pour les armées. Le rapport Villani sur l'IA de mars 2018 [64] a été suivi d'actions concrètes dans le domaine, notamment la définition d'une stratégie spécifique à la défense publiée en 2019 [65]. La Dinum [66] joue le rôle de coordonnateur d'un programme doté de 1,5 Md€ sur 5 ans. La partie recherche sera pilotée par l'Inria et prévoit un renforcement des coopérations au niveau européen.

Alors qu'aucun acteur n'est véritablement établi dans les domaines de la *blockchain* et de l'informatique quantique, il convient de développer sans tarder une stratégie industrielle. L'utilisation de l'informatique quantique pour la cryptanalyse, opération

---

[60] La *Revue stratégique de cyberdéfense*, *op. cit.*, p. 97.

[61] L'ANSSI est un service du Premier ministre rattaché au SGDSN. Créée en 2009, elle apporte son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des Opérateurs d'importance vitale (OIV). Elle assure la veille, la détection, l'alerte et la réaction aux attaques informatiques.

[62] Commission européenne, « La Commission propose d'investir 1 milliard d'euros dans des superordinateurs européens de niveau mondial » (communiqué de presse), 11 janvier 2018 (https://ec.europa.eu/).

[63] Les projets *Cloudwatt* par Orange et Thales, et *Numergy* par SFR et Bull.

[64] Villani Cédric, *Donner un sens à l'Intelligence artificielle*, mission parlementaire, 2018, 242 pages (www.enseignementsup-recherche.gouv.fr/).

[65] Ministère des Armées, *L'intelligence artificielle au service de la Défense*, septembre 2019, 40 pages (www.defense.gouv.fr/).

[66] La Direction interministérielle du numérique a succédé à la DINSIC par décret du 25 octobre 2019.

consistant à « casser » un message chiffré sans en connaître la clé, rendrait inopérant de nombreux systèmes de chiffrement. Il est donc nécessaire d'investir dans la recherche en informatique quantique tout en développant des algorithmes de chiffrement plus robustes. Quant à la *blockchain*, les applications possibles ne sont pas limitées au domaine monétaire. Cette technologie pourrait fournir aux armées des solutions de sécurité permettant de stocker et de traiter des informations de niveaux classification différents.

À rebours de la philosophie européenne sur la concurrence ayant empêché la fusion Alstom-Siemens en 2019, il faut favoriser l'émergence de champions mondiaux. Il faut améliorer le régime des aides d'État et recourir au levier de l'achat public. Alors que Google détient 95 % des parts de marchés des moteurs de recherche, il faut promouvoir le français Qwant, respectueux des données privées. Il faut favoriser la croissance d'OVH qui figure parmi les 10 premiers prestataires de *cloud*, mais aussi l'équipementier finlandais Nokia pour disposer d'une alternative européenne pour la téléphonie mobile. Enfin, il faut peser au sein des organismes de normalisation [67] en mobilisant les acteurs français et européens pour y promouvoir nos intérêts. Cet enjeu est crucial pour les domaines émergents que sont la 5G et l'IA.

Afin de soutenir une politique industrielle ambitieuse, il faut aussi être capable de mobiliser les capitaux indispensables à la croissance des *start-up*. Si les fonds d'investissement tels que Bpifrance ou France Invest sont bien placés au niveau mondial pour aider les entreprises en phase d'amorçage, leurs dispositifs doivent être complétés pour les aider en phase de développement. Ces fonds doivent être attractifs pour les capitaux étrangers désireux de financer des projets majeurs, notamment ceux atteignant plusieurs dizaines de millions d'euros. En effet, il ne faut pas confondre mobilisation de capitaux étrangers et perte de nos actifs matériels et immatériels. La création de French Tech Investissement est susceptible de répondre à cet enjeu et ainsi faciliter les levées de fonds pour l'introduction en Bourse de nos *start-up*. Par ailleurs, le dispositif de crédit impôt recherche doit être adapté. « Les entreprises ne se font plus tant concurrence sur la technologie que sur le *design*, l'expérience utilisateur, le modèle d'affaires et, surtout, leur capacité à faire alliance avec la multitude [68] ». L'innovation porte souvent sur de nouveaux usages, les critères d'éligibilité doivent donc être revus en ce sens. Enfin, pour se prémunir de la perte des brevets en cas de rachat étranger de pépites françaises, le ministère de l'Économie et des Finances s'est doté d'un service chargé d'identifier des repreneurs nationaux.

L'enjeu en matière de ressources humaines (RH) est également primordial. Des mesures sont nécessaires pour stimuler la recherche et prévenir la fuite des cerveaux. L'excellence de notre système de formation scientifique permet de disposer d'un vivier d'ingénieurs qualifiés. Cependant, les études scientifiques et techniques souffrent

---

[67] L'*Internet Engineering Task Force* (*IETF*), le *World Wide Web Consortium* (*W3C*), l'*Internet Corporation for Assigned Names and Numbers* (ICANN) et le *3rd Generation Partnership Poject* (*3GPP*) sont toutes basées aux États-Unis.

[68] Colin Nicolas et Verdier Henri, *L'âge de la multitude*, Armand Colin, 2e édition 2015, p. 7.

en France d'une forte désaffection [69]. Il faut donc inciter, au plus tôt, les jeunes à emprunter ces filières, notamment les femmes qui y sont encore très minoritaires. Des partenariats existent entre l'enseignement supérieur et l'industrie, à l'exemple de Cisco avec Polytechnique. Microsoft envisage aussi d'ouvrir une vingtaine d'écoles dans le domaine de l'IA d'ici 2021. L'État doit veiller à ne pas se retrouver débordé par ces initiatives. Les liens entre les organismes de recherche et les entreprises doivent être facilités. Ainsi, dans le domaine de l'informatique quantique, la mission parlementaire de 2019 recommande, entre autres, de créer trois pôles d'excellence rassemblant chercheurs et industriels à Paris, Saclay et Grenoble [70]. Les dispositifs existant de soutien à l'innovation sont souvent complexes et manquent de visibilité. Pour y remédier, la mise en place d'un guichet unique favoriserait les partenariats. Enfin, à l'instar du dispositif déployé au Royaume-Uni, des coupons innovation faciliteraient l'accès des TPE-PME aux établissements de recherche pour leurs projets. Les armées ont également un rôle essentiel à jouer pour la recherche. La Direction générale de l'armement (DGA) et l'Agence innovation de défense (AID) possèdent des compétences techniques et managériales reconnues et proposent des cas d'usage exigeants. Elles ont un budget pour la recherche duale et offrent des perspectives de marchés en France et à l'export. Le Fonds européen de défense (FED) doit aussi inscrire le numérique dans ses priorités afin d'acquérir une autonomie dans ce domaine.

L'émergence d'un tissu industriel performant nécessite de poursuivre le déploiement d'infrastructures adaptées. Bien positionnée dans le domaine des câbles sous-marins, la France doit veiller à ce que ces moyens stratégiques demeurent sous contrôle. En revanche, de nets progrès sont à faire dans l'offre de couverture très haut débit, fixe et mobile. En 2018, seuls 58 % des bâtiments disposent d'une connexion par fibre, classant la France en dernière position en Europe ! Sa 18e position pour la couverture mobile 4G est à peine meilleure. Par ailleurs, il convient de faciliter l'installation de centres de données sur notre territoire par une politique fiscale incitative et une taxation de la consommation électrique réduite. Cette action est essentielle en vue de la constitution de bases de données massives. Alors que les grandes plateformes américaines ont gagné la bataille du stockage des données personnelles, des mesures incitatives pour le partage de données privées sectorielles permettront de ne pas rater le virage de l'IA. Ainsi, depuis 2016, le Système national des données de santé (SNDS) rassemble les données des différentes caisses et professionnels du secteur.

Ayant pris conscience des enjeux de cyberdéfense dès le *Livre blanc* de 2008 [71], la France a donné une forte impulsion à ce domaine stratégique pour la résilience des systèmes vitaux de l'État et de ses acteurs économiques. L'autorité de référence, l'ANSSI a vu le jour en 2009 et le Commandement de la cyberdéfense des armées en 2017. La *Revue stratégique de cyberdéfense* de 2018 constitue un tournant décisif de cette montée en puissance. La France y affirme la volonté d'une autonomie

[69] Jeger François et Peraldi Olivier, *Appétence et désaffection pour les études scientifiques et techniques en France : où en sommes-nous ?*, Institut chiffres et citoyenneté, octobre 2018, p. 37-42 (www.chiffres-citoyennete.fr/).
[70] Forteza Paula, Herteman Jean-Paul et Kerenidis Iordanis, *Quantique : le virage technologique que ne ratera pas la France – 37 propositions pour une stratégie nationale ambitieuse*, mission parlementaire, 2020, p. 57 (https://forteza.fr/).
[71] *Livre blanc sur la Défense et la Sécurité nationale*, p. 53 (http://archives.livreblancdefenseetsecurite.gouv.fr/).

d'appréciation, de décision et d'action en matière de défense et de sécurité du cyberespace. Cela se traduit par des capacités souveraines de détection et d'attribution d'attaques, mais également des capacités offensives permettant de disposer d'options de réponse militaire comme dans les autres milieux. Une doctrine nationale de découragement des attaques adverses et de réaction a aussi été développée. La Loi de programmation militaire (LPM) 2019-2025 a doté la cyberdéfense de 1,6 Md€ et d'effectifs supplémentaires afin de disposer de 4 000 cybercombattants d'ici 2025 [72]. Ce dernier point constitue un véritable enjeu de recrutement, de formation et de fidélisation, car le domaine fait l'objet d'une concurrence sévère avec les entreprises.

La crise du Coronavirus a, entre autres, démontré à quel point la continuité du fonctionnement du pays était dépendante de systèmes d'information et de communication fiables lorsque des millions de Français doivent télétravailler. Que se passerait-il si, au même moment, nos systèmes informatiques, nos câbles sous-marins ou nos satellites de communication subissaient une attaque massive ? La crise de Mai 68, avait permis d'accélérer la mise en œuvre du réseau maillé *Ritter* [73] entre Paris et les commandements militaires régionaux par des liaisons hertziennes. Ce réseau offrait une redondance aux liaisons fixes stratégiques des armées, mais aussi de l'État, en cas de grève générale. Il est indispensable d'aller plus loin dans les capacités de résilience de la Nation dans ce domaine. Ainsi, le déploiement d'une constellation européenne de satellites en orbite basse, à l'instar des projets des milliardaires Elon Musk et Jeff Bezos offrirait une résilience plus forte à nos communications. Il faut prolonger cette réflexion au niveau interministériel et les armées possèdent les savoir-faire pour y contribuer.

⁂

En seulement deux décennies, le numérique est devenu un véritable enjeu géopolitique. La question de la souveraineté numérique représente pour la France et l'Europe un triple défi économique, sécuritaire et éthique. Malgré toutes les actions déjà réalisées, engagées ou projetées pour la restaurer, cette souveraineté souffre d'un manque de stratégie globale. Le rapport du Sénat préconise la création d'un forum institutionnel temporaire du numérique, associant tous les acteurs publics et privés concernés. Il faudrait lui confier l'élaboration d'un « Plan numérique », nouvelle « Œuvre commune [74] » mobilisant la puissance publique, les entreprises et les citoyens autour d'objectifs partagés. Ce plan devra favoriser la création d'un écosystème de laboratoires de recherche, de *start-up* et faciliter l'émergence de champions français et européens. On pourrait imaginer la création d'un Airbus de l'IA.

Les armées et l'industrie de défense y auront un rôle majeur à jouer. La crise du Coronavirus va laisser le pays financièrement exsangue, pourtant, la mise en œuvre d'un tel plan permettrait de mobiliser les énergies pour une relance économique

[72] Ministère des Armées, « Loi de programmation militaire 2019-2025 : textes officiels », 16 février 2018, p. 31 du rapport annexé (www.defense.gouv.fr/).
[73] *Réseau intégré des transmissions de l'Armée de terre*.
[74] Dénomination attribuée au chantier de construction de la dissuasion nucléaire française, « œuvre commune » entre les armées et le CEA.

salvatrice tout en garantissant notre indépendance technologique. Or, nous avons pu constater combien une dépendance trop forte pouvait être critique. Cette démarche nationale devra comporter un volet européen afin de bénéficier de l'effet de levier de l'UE à chaque fois que c'est nécessaire. Thierry Breton, ancien PDG d'Atos, nommé commissaire au Marché intérieur au sein de la Commission européenne, a reçu pour mandat d'exploiter la transition numérique et de renforcer la souveraineté technologique de l'Europe [75]. C'est une réelle opportunité à saisir pour relever le défi de notre souveraineté numérique et ainsi appliquer la solution préconisée par Pierre Bellanger face à notre situation de dépendance : « Comment gagner une guerre perdue ? En gagnant la suivante [76] ».

Éléments de bibliographie

Bellanger Pierre, *La souveraineté numérique*, Stock, 2014, 264 pages.

Colin Nicolas et Verdier Henri, *L'âge de la multitude – Entreprendre et gouverner après la révolution numérique*, Armand Colin, 2e édition 2015, 304 pages.

Commission d'enquête, *La souveraineté numérique* (Rapport), Sénat, 2019, 253 pages (www.senat.fr/).

Conférence des Nations unies sur le commerce et le développement (Cnuced), *Rapport 2019 sur l'économie numérique*, 2019, 223 pages (https://unctad.org/fr/PublicationsLibrary/der2019_fr.pdf).

Ganascia Jean-Gabriel, Germain Éric et Kirchner Claude, *La souveraineté à l'ère du numérique – Rester maîtres de nos choix et de nos valeurs*, Cerna (Commission de réflexion sur l'éthique de la recherche en science et technologies du numérique d'Allistene), 2018, 36 pages (www.allistene.fr/).

Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Revue stratégique de cyberdéfense*, 2018, 167 pages (www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/).

Tirole Jean, *Économie du bien commun*, Puf, 2e édition 2018, 672 pages.

Türk Pauline et Vallar Christian, *La souveraineté numérique : le concept, les enjeux*, Mare et Martin, 2018, 240 pages.

Villani Cédric, *Donner un sens à l'Intelligence artificielle*, mission parlementaire, 2018, 242 pages (www.enseignementsup-recherche.gouv.fr/).

[75] Commission européenne, « Lettre de mission de M. Thierry Breton, commissaire désigné au marché intérieur », 7 novembre 2019, p. 4 (https://ec.europa.eu/).

[76] Bellanger Pierre, « Comment gagner une guerre perdue ? », *Cahiers de l'INHESJ* n° 45, juin 2019, Institut national des hautes études de la sécurité et de la justice (https://inhesj.fr/articles/comment-gagner-une-guerre-perdue).