SOUVERAINETÉ NUMÉRIQUE ET AUTONOMIE STRATÉGIQUE EN EUROPE : DU CONCEPT AUX RÉALITÉS GÉOPOLITIQUES

Didier Danet, Alix Desforges

La Découverte | « Hérodote »

2020/2 N° 177-178 | pages 179 à 195

ISSN 0338-487X
ISBN 9782348060250

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-herodote-2020-2-page-179.htm

Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques

Didier Danet[1] *et Alix Desforges*[2]

En 2011, une tribune dans *Les Échos* de Pierre Bellanger, patron de la radio Skyrock, alerte sur un abandon de la « souveraineté numérique française » au profit de l'« impérialisme américain ». Il y définit la souveraineté numérique comme « la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques », et appelle à une « alliance entre les nations européennes » pour contrer la domination des États-Unis en matière numérique. Depuis cette tribune, les prises de position de Bellanger sur la question contribuent à populariser l'expression de souveraineté numérique, régulièrement reprise par les médias et par les responsables politiques français jusqu'à aujourd'hui. Le 6 décembre 2019, le ministre des Affaires étrangères Jean-Yves Le Drian appelle lui-même à « construire une souveraineté numérique européenne à la fois efficace et conforme à nos valeurs, c'est-à-dire ni isolationniste, ni dominatrice, mais en mesure de nous donner la capacité de décider librement notre destin ».

L'expression connaît un intérêt croissant à partir de 2013, suite aux révélations d'Edward Snowden sur la surveillance de masse opérée par les États-Unis. En réaction à ces révélations, de nombreux États européens appellent à mettre en œuvre des législations visant à garantir la « souveraineté technologique » de l'Europe [Maurer *et al.*, 2014]. L'expression « souveraineté numérique » est

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

1. Maître de conférences, pôle « Mutation des conflits », Écoles de Saint-Cyr Coëtquidan et centre de recherche Géopolitique de la datasphère (GEODE).

2. Post-doctorante GEODE, Institut français de géopolitique, université Paris 8.

ainsi d'abord mobilisée pour évoquer la volonté d'émancipation des États européens à l'égard des plateformes – plus connues sous l'acronyme de Gafam – et entreprises du numérique américaines ultra-dominantes sur le marché européen. Depuis, l'expression est également employée en réaction à la montée en puissance d'entreprises chinoises en matière d'intelligence artificielle et de technologie 5G [Nocetti, 2019]. Elle devient l'argument justifiant le développement de technologies conçues spécialement par des entreprises européennes (*cloud*, 5G, procédés cryptographiques).

Face à la défiance européenne à l'égard des entreprises du numérique américaines et aujourd'hui chinoises, la « souveraineté numérique » s'est imposée dans les discours des industriels de défense et des responsables politiques français, puis des autres dirigeants et responsables politiques européens. Toutefois, en France comme en Europe – contrairement à la Russie ou la Chine où le concept est assumé –, les documents officiels ne reprennent pas le concept de « souveraineté numérique » et lui préfèrent le concept d'« autonomie stratégique numérique ». La réticence à recourir au concept de souveraineté numérique dans les documents officiels s'explique d'abord par ses usages très divers. En effet, le concept est utilisé pour décrire un grand nombre d'enjeux d'ordres différents : économique, culturel, politique, militaire et stratégique. En outre, son utilisation est potentiellement embarrassante pour des démocraties tandis que la Chine et la Russie l'emploient aussi bien pour justifier des politiques visant à développer une industrie numérique nationale que pour limiter la liberté d'expression en ligne. Enfin, l'autonomie stratégique étant un concept clé de la politique de défense française, son réemploi par des acteurs de la sécurité et de la défense sur les questions numériques s'est imposé facilement. Mais, à l'échelle européenne, la popularité de ce concept, depuis 2016, masque en réalité de profondes divergences de vues sur ce qu'il recouvre et implique.

Portés par le président français Emmanuel Macron et la *Revue stratégique de défense et de sécurité nationale* de 2017 (RS2017), les discours politiques en faveur d'une autonomie stratégique voient en l'Union européenne (UE), alliance économique et politique, l'échelle pertinente et le cadre privilégié pour favoriser l'émergence d'entreprises compétitives sur le marché international. Avec plus de 500 millions d'utilisateurs potentiels, elle constitue d'ailleurs le premier marché des entreprises américaines du numérique tant à l'exportation qu'à l'importation. L'Union européenne apparaît comme la plus susceptible de porter cette industrie numérique « de confiance ». Mais a-t-elle les moyens de ses ambitions stratégiques ?

Cet article propose d'analyser les usages des concepts de souveraineté numérique et d'autonomie stratégique dans les discours politiques et la littérature stratégique ainsi que leurs traductions industrielles en France et en Europe, en croisant les approches géopolitiques et en sciences de gestion. Dans une première

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

partie, l'article montrera que la naissance et l'émergence de ces deux concepts, en France puis en Europe, résultent de facteurs géopolitiques. Puis la deuxième partie sera consacrée à l'analyse de leur traduction industrielle, tant en termes de capacités techniques et technologiques que de structuration de l'écosystème européen.

Souveraineté numérique et autonomie stratégique : des concepts révélateurs de conflits géopolitiques

La dépendance aux entreprises américaines du numérique : un risque géopolitique

L'affaire Snowden, et plus récemment celle de Cambridge Analytica, du nom de l'entreprise qui a exploité les données des Européens sur Facebook à des fins d'influence politique, ont joué le rôle de catalyseur dans la prise de conscience de la dépendance des États européens vis-à-vis des technologies et services d'entreprises américaines du numérique. Ces deux affaires ont révélé à la fois les abus des services de renseignement américains en matière de captation des données personnelles et de compromission de matériels informatiques, mais également ceux d'entreprises exploitant les données personnelles sur les plateformes numériques américaines à des fins d'influence politique dans les processus électoraux. La dépendance européenne vis-à-vis des plateformes américaines a également été visible à travers la question de la régulation des contenus. Qu'il s'agisse de combattre les discours de haine, de terrorisme ou encore des manipulations de l'information, les États européens rencontrent des difficultés à faire appliquer leurs législations à ces géants du Web qui ne partagent ni la même culture ni la même approche en matière d'accès à l'information.

Cette dépendance européenne, qui s'accompagne d'une défiance croissante à l'égard de l'allié américain et de ses entreprises, engendre des risques géopolitiques pour l'UE et ses États membres : déstabilisation politique et espionnage stratégique et économique. Ces menaces potentielles pour l'avenir politique, économique et démocratique de l'Union européenne poussent les États membres à prendre des mesures pour s'en prémunir, dans un contexte géopolitique tendu (élection de Donald Trump aux États-Unis, Brexit, déstabilisations russes aux frontières Est de l'Europe) [Lipper *et al*., 2019 ; Järvenpää *et al*., 2019].

En 2013, la prise de conscience de la vulnérabilité des États européens face à la domination des entreprises du numérique américaines avait favorisé des discours et propositions de législations en faveur d'une « souveraineté technologique » européenne. Pourtant la majorité de ces propositions, principalement axées sur la protection de la donnée et de la vie privée, ne permettaient pas de se protéger du cyberespionnage [Maurer *et al*., 2014].

En matière de protection des données et notamment des données personnelles, les révélations Snowden ont favorisé l'adoption du Règlement général sur la protection des données (RGPD) et du *Privacy Shield* en 2016, visant à définir des cadres légaux protecteurs de la vie privée notamment dans le cadre de transferts des données vers des entreprises américaines. Mais la mise en œuvre de ces outils n'a cependant pas écarté l'usage abusif des données des citoyens et des entreprises européens dans des contextes électoraux, comme en a témoigné l'affaire *Cambridge Analytica* en 2018. Et, en 2016, l'adoption du *CLOUD Act* aux États-Unis, loi qui vise à faciliter l'accès des données stockées à l'étranger par les services de sécurité américains, est à nouveau venue alimenter la défiance des Européens vis-à-vis des entreprises américaines du numérique en renforçant la portée extraterritoriale de la législation américaine.

Plus récemment, l'augmentation des attaques informatiques attribuées par plusieurs pays à l'État russe, les stratégies d'influence numérique de médias d'origine russe à la popularité croissante en Europe ou encore la montée en puissance des entreprises chinoises en matière d'IA et de technologies 5G sont également venues alimenter et renforcer les discours prônant une « souveraineté numérique » européenne.

Ainsi, face à un cyberespionnage qui ne connaît pas la crise, y compris entre alliés, et à la manipulation des données personnelles et des informations sur les grandes plateformes, les États européens ont pris conscience qu'ils ne pouvaient pas se fier aux technologies et services numériques étrangers. Cette défiance sert les discours qui prônent une souveraineté numérique européenne en s'appuyant sur le développement des capacités technologiques et des services numériques au sein des États membres de l'UE. Ces discours se font encore plus insistants lorsque cette dépendance touche à des capacités souveraines des États, notamment dans les domaines militaires et du renseignement. Toutefois avec sa popularité médiatique, le concept de souveraineté numérique a été galvaudé et les contours de ce qu'il revêt se sont brouillés.

En France, émergence d'un discours sur la souveraineté numérique aux contours flous

Mobilisée pour justifier une émancipation de la tutelle américaine, la « souveraineté numérique » présentée par les différents acteurs français depuis 2010 (institutionnels, académiques, militaires, parlementaires) recoupe en fait différents enjeux (stratégiques, économiques et culturels).

Du point de vue économique, la situation des entreprises américaines sur le marché européen interroge notamment sur les abus de positions dominantes

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

potentiels. Plusieurs d'entre elles, dont Google et Microsoft, ont d'ailleurs été lourdement sanctionnées par la Commission européenne. Cette domination marque également les questions de fiscalité des acteurs du numérique. En 2013, le rapport Collin et Colin pointe la grande disparité en matière de fiscalité du numérique en Europe notamment vis-à-vis des entreprises américaines. Le rapport estime même que cette asymétrie constitue un « enjeu d'une gravité et d'une urgence particulières pour les États de l'Union européenne » et cite Pierre Bellanger et son concept de souveraineté numérique. Des conclusions qui seront reprises par plusieurs rapports parlementaires français. L'expression « souveraineté numérique » a également été reprise dans une tribune de Nicolas Demorand, alors rédacteur en chef au journal *Libération*, pour évoquer le conflit opposant Google aux éditeurs de presse en matière de revenus en France, mais également en Europe avec le groupe Axel Springer. Ces enjeux économiques et fiscaux, bien que fondamentaux, sont éloignés des préoccupations en matière de sécurité et défense qui sont les plus sensibles pour les États.

Toutefois, l'emploi du terme souveraineté numérique pour aborder des questions stratégiques prête également à confusion. Il est en effet basé sur la représentation par les acteurs politiques d'une perte de souveraineté de l'État dans l'espace numérique et d'une volonté de réappropriation du cyberespace, perçu comme un territoire à conquérir [Desforges, 2018]. En 2015, la stratégie de l'Agence française de cybersécurité (ANSSI) notait par exemple que « les évolutions en cours tant au niveau des technologies que dans les modèles économiques, avec par exemple la multiplication des objets connectés ou la concentration des plateformes de service en ligne entre les mains de quelques acteurs seulement, sont de nature à amplifier cette perte de maîtrise du cyberespace national ». Or ce postulat est un non-sens du point de vue du droit international, puisque tout État indépendant est souverain. En revanche, la révolution numérique vient effectivement bouleverser les modalités de l'exercice de cette souveraineté parce qu'elle permet des activités transfrontières et aussi parce qu'elle offre des moyens d'action à distance pour espionner et saboter des réseaux en dissimulant son identité et en s'abritant derrière des juridictions multiples.

La chancelière allemande Angela Merkel a également souligné les problèmes potentiels de l'utilisation d'un concept flou à l'occasion du Forum de gouvernance de l'Internet en novembre 2019 : « Bien sûr, la souveraineté numérique est très importante. Mais il se peut que nous en soyons tous venus à comprendre quelque chose de différent, même si nous utilisons le même terme. »

Ainsi, face à un concept aux contours mal définis, la littérature stratégique française en matière de défense et de sécurité mobilise davantage le concept d'autonomie stratégique que celui de souveraineté pour évoquer les enjeux du numérique.

L'affirmation de l'autonomie stratégique numérique

L'expression « souveraineté numérique » n'est d'ailleurs pas présente dans les *Livres blancs sur la défense et la sécurité nationale* (LBDSN) de 2008 ou 2013, dans la RS2017 ni dans la stratégie de l'ANSSI de 2011. On trouve une occurrence de l'expression dans la stratégie de l'ANSSI de 2015, mais elle ne figure que dans un titre et le détail de l'objectif présenté se réfère, lui, au concept d'autonomie stratégique numérique.

Dans la littérature stratégique française, les concepts de souveraineté et d'autonomie stratégique sont fortement liés et ne sont jamais éloignés dans les textes. L'autonomie stratégique est perçue comme le moyen pour un État d'exercer sa souveraineté [RS2017 ; LBDSN 2008, 2013]. Elle vise à détenir une « capacité autonome d'appréciation, de décision et d'action » et est employée notamment pour évoquer le développement de capacités militaires permettant à la France d'assurer ses engagements militaires.

Dès le LBDSN de 2008, le lien discursif entre l'autonomie stratégique de la nation et le développement d'une stratégie de cyberdéfense est explicite. La cybersécurité fait alors une entrée remarquée dans la littérature stratégique française en étant présentée, au même titre que les éléments de la dissuasion nucléaire, comme une des « capacités nécessaires au maintien de l'autonomie stratégique et politique de la nation » [LBDSN, 2008, p. 318]. Les deux stratégies de l'ANSSI font référence à l'autonomie stratégique : en 2011, le deuxième objectif de la stratégie visait à « garantir la liberté de décision de la France » [ANSSI 2011, p. 5] ; en 2015, la stratégie estime qu'« un État qui ne disposerait pas de l'autonomie nécessaire dans le secteur du numérique verrait sa souveraineté menacée » [ANSSI 2015, p. 7].

L'analyse des discours institutionnels montre que le lien discursif entre autonomie stratégique et cyberdéfense s'élabore autour de trois arguments qui promeuvent le développement d'une base industrielle propre. Le premier argument est que la France doit faire preuve d'autonomie vis-à-vis des fournisseurs de matériels et de solutions informatiques étrangers. La stratégie de l'ANSSI de 2011 évoque à propos de la domination d'acteurs industriels non européens une « situation [n'est] ni souhaitable, ni tenable » [ANSSI 2011, p. 16].

Le deuxième argument vise la protection des informations stratégiques de l'État français. C'est d'ailleurs l'un des quatre objectifs définis par la stratégie de l'ANSSI de 2011. La volonté affichée est de « garantir la liberté de décision de la France pour la protection de l'information de souveraineté ». La stratégie prône alors le recours à des procédés cryptographiques au nom de l'autonomie stratégique : « Le maintien de notre autonomie stratégique repose sur notre capacité à maîtriser les techniques cryptographiques et les technologies clés nécessaires à la conception de produits de sécurité qui les utilisent. »

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

Le dernier argument relève davantage de l'action militaire puisqu'il concerne les possibilités d'entrave des capacités de défense et systèmes d'armes français. Ce dernier argument fait un écho évident à la politique de défense de la France depuis l'après-guerre puisqu'elle touche directement aux capacités militaires.

La *Revue stratégique de cyberdéfense* de 2018 est l'un des rares documents officiels à recourir au terme de souveraineté numérique. Pourtant la définition qu'elle en donne renvoie directement à l'autonomie stratégique : « 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 sa souveraineté vis-à-vis de menaces nouvelles tirant parti de la numérisation croissante de la société [RSCyber 2018, p. 93]. »

Le recours au terme d'autonomie stratégique dans les documents stratégiques français au détriment de celui de souveraineté numérique s'explique par son rôle dans la politique de défense française du général de Gaulle dans l'après-guerre et dans sa dimension opérationnelle, promouvant le développement de capacités technologiques et industrielles. Il a, en outre, l'avantage de ne pas exclure les coopérations indispensables entre États dans le secteur du numérique et s'applique ainsi aisément à l'échelle européenne.

Un concept stratégique opérationnel qui valorise l'échelle européenne

Dans la pure tradition de la stratégie de défense française des années 1960

Le concept d'autonomie stratégique a été l'un des principes fondateurs de la politique de défense française de l'après-guerre, fondée sur l'idée d'autonomie de décision de Poirier. Le concept, apparu pour la première fois dans le *Livre blanc sur la défense nationale* de 1994, fait en effet référence à l'« autonomie de décision » définie par Lucien Poirier, théoricien de la dissuasion nucléaire française, à savoir la « faculté pour un peuple de choisir librement, à l'abri de toute pression étrangère, le projet politique qu'il juge conforme à ses intérêts et à ses ressources » [Poirier, 1982]. La souveraineté en est l'objectif puisqu'elle est « le principe de droit international selon lequel un État indépendant [...] exerce un pouvoir éminent et exclusif sur son territoire » [Kempin et Kunz, 2017, p. 10]. Ainsi l'autonomie stratégique est le moyen de garantir la souveraineté française.

Contrairement à l'indépendance qui induit une action isolée, l'autonomie stratégique n'exclut pas les alliances dans l'esprit de Poirier. Au contraire elle les encourage, mais ces alliances doivent être explicitement désirées et surtout éclairées : « Si l'autonomie ne nie pas l'interdépendance, elle permet de choisir, selon

les conjonctures internes et externes, les relations que le projet politique entend privilégier. » C'est donc dans le choix « des modalités de l'interdépendance » [Poirier, 1982] que réside l'autonomie de décision.

En France, les discours politiques sur l'autonomie stratégique se construisent sous de Gaulle et sont repris par ses successeurs, comme une émancipation de la tutelle militaire américaine et le développement d'une base industrielle de défense française.

Un concept pour développer les capacités industrielles et technologiques à l'échelle européenne

Pour Charles de Gaulle, « il faut que la défense de la France soit française [...]. Un pays comme la France, s'il lui arrive de faire la guerre il faut que ce soit sa guerre. Il faut que son effort soit son effort ». Il justifie par ce biais le développement de capacités militaires propres et notamment celles relatives à la dissuasion nucléaire, pilier de la politique de défense française. Lors de sa conférence de presse du 21 février 1966, le général de Gaulle estime que les menaces militaires sur les États européens ne sont plus les mêmes que lorsque « le protectorat américain fut installé en Europe sous le couvert de l'Otan ». C'est pourquoi, en vertu de « la volonté de la France de disposer d'elle-même », il dénonce l'incompatibilité d'assurer la souveraineté française dans une alliance « dans laquelle elle est subordonnée » et annonce la sortie de la France du Commandement intégré de l'Otan – sans remettre en cause l'alliance stratégique de la France avec ses États membres. En 2003, cette autonomie stratégique de la France émancipée de la tutelle américaine a été louée dans les discours relatifs à la prise de position française au Conseil de sécurité de l'ONU sur une intervention militaire en Irak, lorsque Colin Powell a cherché à imposer au Conseil de sécurité, sur des preuves fallacieuses, une intervention militaire alliée en Irak.

Mais l'autonomie stratégique numérique ne peut se concevoir que dans l'interdépendance car l'interconnexion mondiale des réseaux numériques et la conception des technologies numériques, reposant sur de nombreux composants (*software* et *hardware*) et compétences, excluent par définition un raisonnement à la seule dimension nationale. Elle comprend donc un raisonnement à l'échelle nationale pour les technologies jugées les plus critiques mais impose un raisonnement à l'échelle européenne pour développer et faire émerger des technologies avec des partenaires de confiance. La dimension européenne de cette recherche d'autonomie stratégique numérique est affichée au plus haut niveau des objectifs stratégiques français. Elle figure ainsi parmi les objectifs de la stratégie de l'ANSSI en 2015 et de la stratégie internationale du numérique du Quai d'Orsay en 2017.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

Une popularité récente à l'échelle européenne qui masque des représentations divergentes

Depuis 2016, le concept d'autonomie stratégique a fait son entrée dans la politique européenne, y compris dans les documents d'orientation stratégique de l'UE en matière de sécurité et d'affaires étrangères. La prolifération des publications sur le sujet montre toutefois qu'il ne fait pas l'unanimité dans ce qu'il recouvre et ce qu'il implique. Cet intérêt récent pour le concept d'autonomie stratégique s'explique par son utilisation dans la *Stratégie globale pour la politique étrangère et de sécurité de l'Union européenne* de 2016.

Ce document, qui vise à orienter la politique étrangère et de sécurité de l'Union, a été porté par Federica Mogherini, haute représentante de l'Union européenne pour les Affaires étrangères et la politique de sécurité. Il présente l'autonomie stratégique comme un élément important de la « capacité de l'Europe à promouvoir la paix et la sécurité à l'intérieur et à l'extérieur de ses frontières » dans la mesure où « les Européens doivent prendre davantage de responsabilité pour leur sécurité » [UE, 2016, p. 9]. La *Stratégie globale* estime ainsi que les Européens doivent être « mieux équipés, entraînés et organisés pour contribuer de façon déterminante à l'effort collectif » visant à « dissuader, répondre et [se] protéger contre les menaces extérieures ». En 2017, la *Stratégie de cybersécurité de l'Union européenne* est présentée comme un élément concourant à son autonomie stratégique dans le cyberespace et des experts appellent à le repenser à la lumière des enjeux numériques [Timmers, 2018].

Il apparaît toutefois que le concept fait l'objet d'interprétations différentes selon les États membres de l'Union. Bien que de nombreuses publications issues de chercheurs de think tanks ou d'universités européennes reprennent les grandes lignes du concept d'autonomie stratégique, une étude du think tank European Council of Foreign Relations montre que les États membres ne soutiennent pas tous le développement d'une autonomie stratégique européenne et que ceux qui le font ne s'accordent ni sur ce qu'elle recouvre, ni « sur le niveau d'ambition géographique et fonctionnel qu'ils devraient adopter » pour la mettre en œuvre [Franke et Varma, 2019]. En effet, l'attitude à adopter vis-à-vis des États-Unis est au cœur des discussions sur l'autonomie stratégique européenne et constitue l'un des points de crispation quant aux risques qu'elle pourrait faire peser sur les relations transatlantiques, particulièrement en matière de défense. L'Estonie et la Lituanie considèrent même qu'une autonomie stratégique européenne pourrait être problématique, voire dangereuse, pour l'Otan.

Souveraineté numérique et autonomie stratégique : quels fondements économiques, industriels et scientifiques ?

Le degré de crédibilité du discours national ou européen sur l'autonomie stratégique numérique, et *a fortiori* sur la souveraineté numérique, s'apprécie au regard de la confrontation avec le réel, c'est-à-dire avec l'état du tissu scientifique, socio-économique et industriel qui le sous-tend. Sans organismes de recherche à la pointe des progrès scientifiques, sans un appareil industriel maîtrisant les technologies clés du numérique et sans un environnement socioéconomique prêt aux efforts et aux sacrifices en sa faveur, la volonté politique de construire une transition numérique autodéterminée ou de maîtriser les choix fondamentaux concernant notre sécurité dans le cyberespace se trouve dénuée de toute portée effective. À cet égard, des questions se posent tant pour ce qui est de la souveraineté nationale d'un pays comme la France que d'une éventuelle souveraineté européenne. La France ou l'Europe disposent-elles des moyens de leur ambition, c'est-à-dire du capital intellectuel, humain, technologique, financier, etc. propre à leur donner la maîtrise des trois couches du cyberespace ? Peuvent-elles mobiliser les acteurs capables d'appuyer leur volonté si celle-ci se heurte à un projet politique concurrent dans l'espace numérique ? Seraient-elles en mesure de faire face à une décision d'embargo analogue à celle prise par l'administration américaine à l'encontre des opérateurs chinois de la 5G ?

Une impossible souveraineté de l'Europe dans l'espace numérique ?

Plusieurs raisons nous conduisent à répondre par la négative à cette question des fondements socioéconomiques et industriels de la souveraineté numérique de la France et de l'Europe.

Un modèle politique indésirable : le Synétat

En ce qui concerne son incarnation politique et institutionnelle, le discours de la souveraineté numérique tel qu'il s'est développé en France se trouve très fortement associé aux propositions portées par l'un de ses chantres initiaux, Pierre Bellanger, qui tient un discours pour le moins belliciste – « lutter au niveau mondial avec toutes les armes nécessaires » [Bellanger, 2012] – et préconise l'instauration d'un « Synétat », sorte de gouvernement oligarchique intégrant l'intérêt général et les intérêts privés de quelques groupes industriels et financiers liés au numérique au sein d'une « macro-entreprise composite ». Ce type de proposition n'est pas pour surprendre tant elle s'inspire des canons de l'idéologie politico-économique des

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

années 1980-1990 : goût pour la métaphore militaire de la « guerre économique », critique systématique de l'action publique au nom du « New Public Management », idéalisation du modèle de l'entreprise privée...

Cette liaison très étroite de la forme institutionnelle du « Synétat » avec le concept de souveraineté numérique constitue la première source de faiblesse de celui-ci pour une double raison. Elle est tout d'abord politiquement inacceptable puisqu'elle revient à faire litière des libertés individuelles d'utilisateurs dont l'auteur ne cache pas qu'il faudra les « rééduquer ». « Par ailleurs, nous devons être aussi vigilants à défendre nos réseaux qu'à défendre la liberté de leurs utilisateurs. [...] La sécurité de nos réseaux, systèmes et machines informatiques est une clef de notre existence. » On ne saurait mieux dire que les utilisateurs de l'espace numérique, c'est-à-dire la population tout entière, seront soumis aux diktats des acteurs privés représentés dans le « Synétat ». Promotion d'un régime oligarchique, assujettissement des libertés individuelles à des considérations de sécurité définies par les plus grands groupes industriels et financiers, confusion de l'intérêt général et de certains intérêts particuliers ; le modèle du « Synétat » se présente comme un puissant repoussoir au concept de souveraineté numérique qui lui est malheureusement intimement associé.

Repoussoir, le « Synétat » l'est également au plan de son efficacité économique et managériale. Il consacre, en effet, sans nuance aucune les thèses du Nouveau Management Public, modèle de gestion qui a prévalu autour de 2010 et qui vise à combattre les méfaits d'un État dépensier et d'agents publics inefficients d'une double manière : la transposition dans l'ensemble de la fonction publique de techniques et d'outils de gestion issus de l'entreprise privée d'une part, et l'assujettissement de l'action publique aux impératifs du marché. Or les échecs répétés ou les limites désormais bien identifiées d'une formule comme le partenariat public-privé sur lequel serait construit le « Synétat » conduisent à affaiblir le discours sur la souveraineté numérique au sens où l'entend Pierre Bellanger.

L'échec du projet de cloud *souverain*

S'il ne fallait citer qu'un exemple peu convaincant de politique « synétatique » en action, il suffirait de rappeler l'expérience française du « *Cloud* souverain ». Les faits sont trop récents et trop connus pour qu'il soit nécessaire de les rappeler en détail[3]. En l'occurrence, l'expérience du *Cloud* souverain nous semble présenter un certain nombre des écueils qu'il faut s'attendre à rencontrer en pareil cas : primauté accordée à des « champions nationaux » qui n'ont pas forcément les compétences et l'expérience requises au détriment d'opérateurs moins en cour mais

3. Voir l'article de Bômont et Cattaruzza dans ce numéro.

plus dynamiques et plus innovants, difficulté pour des entreprises non spécialistes de monter en compétence dans un domaine aussi dynamique malgré le soutien administratif et financier de l'État, difficulté à trancher franchement entre des intérêts privés qui ont tous une forme de légitimité, risque de saupoudrage des crédits publics déjà anémiques par rapport aux investissements des champions mondiaux, etc. L'échec de la solution initiale fondée sur la concurrence entre deux groupes industriels nationaux était assez largement prévisible, ce qui n'a pas empêché l'administration de la retenir sous la pression des protagonistes. L'expérience semble mal augurer de ce que pourrait donner l'intégration de l'ensemble des acteurs dans une « macro-entreprise composite » gouvernée par une négociation entre pairs.

Une coopération européenne en échec : Quaero

Face à l'efficacité restreinte des politiques nationales de soutien à l'innovation régulièrement mises en œuvre par les États européens, la tentation est grande d'en rechercher la cause dans une question d'échelle : l'espace numérique serait incompatible avec des approches nationales balkanisées et ne pourrait avoir de succès qu'à l'échelle de l'Europe. Même si les effets positifs d'une action collective dans le domaine de l'économie numérique peuvent théoriquement se défendre, force est de constater que l'expérience ne plaide pas nécessairement en ce sens.

Le programme Quaero représente un exemple assez emblématique des difficultés que la coopération européenne dans le domaine du numérique est susceptible de rencontrer. Lancé en 2004 et interrompu de manière inopinée dix ans plus tard, ce programme répondait typiquement à un objectif de souveraineté : faire face à la montée en puissance des géants californiens, singulièrement de Google, en favorisant la maîtrise par les acteurs européens des technologies de recherches multilingues et multimédias. Malgré une volonté politique très affirmée, l'initiative s'est rapidement délitée. Sur le plan institutionnel, l'alliance européenne a explosé moins de deux ans après sa création, les partenaires allemands se retirant purement et simplement du projet ou demandant qu'il soit réorienté dans une direction totalement nouvelle. Quant aux résultats concrets du programme, la coopération scientifique et technique n'a jamais été en mesure de développer une application susceptible de rivaliser avec les leaders américains du domaine.

Un duopole sino-américain désormais établi dans les technologies critiques

Selon Julien Nocetti, dont nous partageons pleinement l'analyse, l'avenir de l'espace numérique souverain, notamment militaire, se joue principalement autour de trois technologies critiques : l'intelligence artificielle (qui révolutionne les

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

processus de prise de décision), l'informatique quantique (qui remet en cause les systèmes de chiffrement en vigueur dans les forces armées) et la 5G (qui permet de connecter l'ensemble des équipements et des soldats sur le champ de bataille) [Nocetti, 2019]. Sur cet ensemble de technologies critiques, un duopole sino-américain est constitué, la Chine cherchant à contester le leadership des États-Unis en s'appuyant sur les forces dont elle dispose. Malgré les avantages conférés par le caractère dictatorial du régime en place et les gigantesques programmes d'investissement que ce dernier lui consacre, les États-Unis conservent encore un leadership assez net. Ceci dit, quoi qu'il en soit du rapport de force actuel et de son évolution possible entre les deux leaders, le duopole sino-américain apparaît solidement établi et mutuellement dépendant : de nombreux liens ont été tissés entre les acteurs des deux camps. L'émergence d'un nouvel acteur capable de perturber significativement l'équilibre duopolistique qui s'est établi dans les technologies critiques de la souveraineté numérique semble donc fort peu réaliste au regard du « ticket d'entrée » requis (scientifique, technique, financier, commercial, etc.) et du comportement stratégique des acteurs déjà présents.

Finalement, le discours de la souveraineté numérique, très présent en Europe, témoigne d'une volonté politique forte mais dont la crédibilité est sujette à caution au regard de l'avance grandissante prise par le duopole sino-américain. Par ailleurs, les échecs récurrents des États européens et de l'Union elle-même dans les tentatives menées pour constituer une base scientifique, technique et industrielle susceptible de fonder cette souveraineté doivent inciter à ne pas ignorer les difficultés difficilement surmontables du projet.

Les conditions socioéconomiques de l'autonomie stratégique dans l'espace numérique

Faut-il en conclure que la France et l'Europe n'ont plus d'autre choix que de s'aligner sur le moins mauvais des deux membres du duopole et de renoncer à toute autonomie décisionnelle quant aux enjeux cruciaux de l'espace numérique ? La faiblesse relative de nos positions dans les sciences et les technologies critiques doit-elle nous conduire au renoncement sur les plans politique, économique, culturel, diplomatique ou militaire ?

La réponse est bien évidemment négative. Certes, l'affirmation d'une souveraineté numérique mal comprise – refus de toute interdépendance et recherche d'une totale maîtrise de l'espace numérique par des acteurs nationaux – n'apparaît pas soutenable pour un pays moyen comme la France ou pour un ensemble régional en tension comme l'Europe. Il est cependant possible de développer certaines formes d'autonomie stratégique, en matière militaire notamment, fondées sur le

développement d'écosystèmes numériques locaux engendrant innovation coopérative et compétitivité. Deux pistes semblent s'offrir à cet égard : premièrement revoir les dispositifs visant à mettre en synergie acteurs publics et privés en tenant compte des apports de la géographie économique contemporaine et deuxièmement mettre en œuvre un soutien aux écosystèmes d'innovation coopérative en privilégiant des structures et des modes de gouvernance insérés dans un environnement local propice.

Les apports de la géographie économique à la question de la synergie des acteurs du numérique

La logique générale des politiques visant à promouvoir la souveraineté numérique est de considérer qu'il n'est point de salut en dehors de l'articulation la plus étroite possible des acteurs publics et privés, l'intégration complète de ces acteurs dans le modèle du « Synétat » en étant le stade ultime. En soi, le principe de coopération des acteurs apparaît vertueux à plusieurs égards. Mais, il ne s'ensuit pas que l'intégration complète au sein d'une « macro-entreprise composite » correspond à un idéal en termes d'efficacité ni même que plus d'intégration signifie nécessairement plus d'efficacité. Ce constat est dressé par Ron Boschma qui montre que le succès des écosystèmes d'affaires repose sur un optimum en termes de proximité des acteurs et non sur leur totale intégration [Boschma, 2004]. Or les traits caractéristiques du monde numérique, en particulier celui de la cyberdéfense, laissent penser que le degré déjà atteint de proximité est particulièrement élevé sur l'ensemble des dimensions étudiées par Boschma : proximité cognitive (partage d'une culture technique forte au sein d'un réservoir limité de ressources humaines), organisationnelle (appartenance des principaux acteurs au champ très structuré de l'industrie de la défense), sociale (appartenance fréquente aux mêmes cercles, par exemple, d'alumni), institutionnelle (présence forte de normes juridiques et de valeurs partagées autour de l'intérêt national) et géographique (concentration des implantations étatiques et privées au sein de pôles de compétitivité ou de campus). Si l'ambition des politiques de soutien à l'écosystème du numérique est uniquement pensée sous l'angle du renforcement de l'intégration des acteurs, les avantages attendus en termes d'innovation et de compétitivité pourraient ne pas advenir et laisser la place à des effets plutôt négatifs : verrouillage de l'écosystème, rejet des innovations de rupture, incapacité à dépasser les visions purement techniciennes de l'espace numérique, etc.

La conclusion qui s'impose ici consiste à réviser l'ambition des politiques classiques de soutien à l'écosystème du numérique. Il ne suffit pas de réunir l'ensemble des parties prenantes du numérique au sein de structures coopératives

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

toujours plus intégrées pour obtenir les effets positifs d'un écosystème d'affaires comme celui de la Silicon Valley. L'ambition de rapprocher les différentes parties prenantes (organismes de recherche, entreprises, administrations locales, militaires...) doit s'accompagner d'une réflexion sur le degré optimal de proximité de ces acteurs et les modalités de leur coopération.

Les apports des sciences de gestion à la gouvernance des écosystèmes du numérique.

La littérature économique et managériale partage très largement la conclusion que la dynamique de l'innovation est plus particulièrement marquée dans les écosystèmes d'affaires qui ont réussi à développer des processus d'innovation coopérative auxquels contribuent l'ensemble des parties prenantes : entreprises industrielles et de service, administration, équipes de recherche, institutions de formation, acteurs financiers... Cette dynamique collective peut cependant revêtir des formes très diverses selon les contextes locaux, le domaine d'activité, la diversité des acteurs impliqués, etc. [Assens et Ensminger, 2015]. Ainsi, les trois modèles du district industriel, du cluster et du pôle de compétitivité se distinguent par des traits essentiels et leur réussite repose d'abord sur le respect de la logique générale du dispositif adopté.

	Moteur de confiance	**Type de coopération**	**Mode de gouvernance adapté**
District industriel	*Intuitu personae* (voisinage, histoire, règles informelles)	Principalement vertical, coopération au long de la chaîne de production	Accords implicites résultant des bons usages professionnels
Cluster	Répétition des transactions commerciales	Coopération verticale et horizontale, implique les acteurs publics et privés	Régulation fondée sur les conventions marchandes
Pôle de compétitivité	Institutionnalisation de la gouvernance (normes de coopération définies par l'État, règles démocratiques formelles)	Coopération verticale, horizontale et transverse	Gouvernance démocratique : règles de vote à la majorité

Dans le cas particulier de l'écosystème de la cyberdéfense, un possible conflit de gouvernance pourrait naître du fait de la structure même du secteur concerné. L'industrie de la défense est, en effet, traditionnellement organisée autour d'un lien privilégié entre l'agence qui transforme le besoin opérationnel en spécifications industrielles, d'une part, et le petit nombre des entreprises de premier rang qui sont susceptibles de piloter des programmes d'armement majeurs d'autre part.

Cette relation privilégiée donne aux grandes firmes du secteur un poids essentiel et elle leur confère un pouvoir d'organisation vis-à-vis des entreprises de second rang, des sous-traitants ou des petites entreprises porteuses d'innovation qui sont fondamentales dans le secteur du numérique. De ce fait, une contradiction se trouve en germe dans l'écosystème de la cyberdéfense. Son succès repose sur la mise en place d'une gouvernance démocratique sans laquelle la confiance indispensable à la coopération d'acteurs très hétérogènes ne peut pas s'établir. Mais il est difficile de faire totalement abstraction, dans le fonctionnement de cet écosystème, des rapports de pouvoir induits par la structure du marché qui se trouve largement dominée par les plus grands des protagonistes de la cyberdéfense. Ce conflit de logiques (démocratique *vs* économique) est susceptible de parasiter la gouvernance de l'écosystème et d'affaiblir la confiance des « petits » acteurs qui sont essentiels pour les processus d'innovation.

Conclusion

La domination du duopole sino-américain est probablement irréversible dans les technologies critiques qui seraient aujourd'hui nécessaires pour construire une souveraineté numérique au sens le plus fort du terme. En revanche, les compétences propres des acteurs européens dans certains domaines critiques du numérique ainsi que l'émergence de nouvelles technologies critiques (l'informatique quantique ou l'intelligence artificielle par exemple) devraient conduire à une politique sélective de soutien à des acteurs susceptibles de tenir leur rang dans la compétition avec leurs homologues américains ou chinois. De la sorte, l'Europe pourrait se doter d'une réelle autonomie stratégique sur la base de ces compétences limitées mais essentielles. Autant la conquête générale de la chaîne du numérique paraît exclue du fait du retard pris et de l'énormité du ticket d'entrée qu'il serait nécessaire d'acquitter, autant une politique ciblée concentrant les ressources limitées dont dispose l'Europe pourrait avoir une efficacité politique, économique et militaire suffisante pour lui permettre d'affirmer ses valeurs et ses préférences.

La mise en œuvre du concept d'autonomie stratégique européenne en matière de numérique s'avère possible mais complexe, tant dans sa dimension politique que dans sa dimension industrielle. Et l'usage croissant des termes « souveraineté numérique » par les politiques n'est pas de nature à faciliter l'émergence d'une compréhension commune entre les États membres. Pourtant, cette compréhension commune s'avère particulièrement cruciale au regard des enjeux du numérique, qu'ils soient technologiques, démocratiques, éthiques, économiques ou encore de sécurité.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

Bibliographie

AGENCE NATIONALE POUR LA SÉCURITÉ DES SYSTÈME D'INFORMATION (ANSSI) (2011), *Stratégie*.

– (2015), *Stratégie*.

ASSENS C. et ENSMINGER J. (2015), « Une typologie des écosystèmes d'affaires : de la confiance territoriale aux plateformes sur Internet », *Vie et sciences de l'entreprise*, n° 2, p. 77-98.

BELLANGER P. (2012), « De la souveraineté numérique », *Le Débat*, vol. 170, n° 3, p. 149-159.

BOSCHMA R. (2004), « Proximité et innovation », *Économie rurale*, vol. 280, n° 1, p. 8-24.

CHAMBÉRON J. (2019), « La coopération dans la "Cyber Vallée" », thèse professionnelle mastère spécialisé, Écoles de Saint-Cyr Coëtquidan.

DESFORGES A. (2018), « Approche géopolitique du cyberespace. Enjeux pour la défense et la sécurité nationale, l'exemple de la France », thèse de doctorat, soutenue le 27 août 2018.

FRANKE U. et VARMA T. (2019), « Independence play : Europe's pursuit of strategic autonomy » (Le jeu de l'indépendance : la poursuite de l'autonomie stratégique de l'Europe), ECFR.

JÄRVENPÄÄ P. (dir.) (2019), « European strategic autonomy : operationalising a buzzword » (Autonomie stratégique européenne : la mise en œuvre d'un mot à la mode), Tallinn, International Centre for Defence and Security

KEMPIN R. et KUNZ B. (2017), « France, Germany, and the Quest for European Strategic Autonomy » (France, Allemagne, et la quête d'une autonomie stratégique européenne), IFRI.

LIPPERT (dir.) (2019), « European strategic autonomy *:* Actors, issues, conflicts of interests » (Autonomie stratégique européenne : acteurs, problèmes, intérêts divergents), Berlin, SWP Research Paper.

MAURER T. (dir.) (2014), « Technological sovereignty : missing the point ? » (Souveraineté technologique : passer à côté de l'essentiel ?), Transatlantic Dialogues on Security and Freedom in the Digital Age.

MINISTÈRE DES ARMÉES (1994), *Livre blanc sur la défense et la sécurité nationale*.

– (2008), *Livre blanc sur la défense et la sécurité nationale*.

– (2013), *Livre blanc sur la défense et la sécurité nationale*.

MINISTRE DES ARMÉES (2017), *Revue stratégique de défense et de sécurité nationale*.

NICHOLSON J. et NOONAN R. (2014), « Digital economy and crossborder trade : the value of digitally-deliverable services » (L'économie numérique et le commerce transfrontalier : la valeur des services numériques), US Department of Commerce, Economics and Statistics Administration.

NOCETTI J. (2019), « Intelligence artificielle et politique internationale. Les impacts d'une rupture technologique », Études de l'Ifri, Institut français des relations internationales.

POIRIER L. (1982), *Essais de stratégie théorique I*, Fondation pour les Études de Défense Nationale.

TIMMERS P. (2019), « Strategic autonomy and cybersecurity » (Autonomie stratégique et cybersécurité), EU Cyber Direct.

UNION EUROPÉENNE (2016), *Global Strategy*.