Chapitre 3
Les grandes puissances du cyberespace

1. Introduction

Pour tout un chacun, mettre un pied dans la cybersécurité, c'est prendre le risque de se noyer dans un océan d'informations et de jargon sans savoir dans quelle direction nager pour rejoindre la rive. Les écosystèmes privés et publics à l'échelle des pays sont extrêmement complexes.

Au plan international, la suprématie sur le sujet peut se regarder de multiples manières et dépend des sources que l'on analyse, chaque jour sa nouvelle analyse, chaque jour son nouveau chiffre.

Commençons avec le rapport du MIT, *The Cyber Defense Index 2022/23*. Tel qu'il est présenté, « *ce rapport examine dans quelle mesure les institutions ont mis en œuvre les technologies et les pratiques numériques pour résister aux cyberattaques et dans quelle mesure les gouvernements et les cadres politiques favorisent des transactions numériques cybersécurisées.* »

1000 personnes – dont 43 % de responsables techniques – interrogées en nombre égal par pays (pays du G20, la Russie étant exclue et remplacée par la Pologne, seul biais de cette étude très fouillée). « *Les personnes interrogées ont évalué l'efficacité de l'adoption des technologies, de l'élaboration des politiques et des réglementations, ainsi que de leurs propres activités en matière de cybersécurité.* » L'étude est segmentée en quatre grandes parties : les infrastructures critiques, les ressources en cybersécurité, la capacité organisationnelle et enfin l'engagement politique.

Selon ce classement et la combinaison de ces critères, c'est l'Australie qui est première, suivie des Pays-Bas, de la Corée du Sud, des États-Unis et du Canada. La France se classe globalement huitième, juste derrière le Royaume-Uni. L'Allemagne est treizième d'un classement où la Turquie et l'Indonésie ferment la marche.

Comment en arrive-t-on là ?

L'Australie bénéficie de la part de son tissu économique d'une forte confiance dans une infrastructure numérique robuste, dans les moyens mis en œuvre par le gouvernement et dans la posture cybersécuritaire du gouvernement lui-même.

Concernant les Pays-Bas, la présence de nombreuses organisations internationales à La Haye joue pour beaucoup dans leur classement, de même que la qualité des ressources et bien entendu le bénéfice produit par le RGPD (Règlement général pour la protection des données) à l'échelle européenne.

La Corée du Sud et la Pologne (sixième du classement) ont pour elles leur géopolitique, qui les oblige à une vigilance accrue en matière cyber.

La Chine que l'on se serait attendue à trouver dans les leaders, figure dans la deuxième partie du classement, défavorisée en particulier par la qualité insuffisante de ses infrastructures et son contexte politique.

L'Allemagne est assez mal classée dans le rapport du MIT. Son tissu d'entreprises, avec un grand nombre de PME/PMI, lui est d'habitude très favorable notamment au plan économique. Ici, c'est l'inverse : il ne favorise pas l'adoption rapide des technologies nécessaires. La pénurie de main-d'œuvre dégrade elle aussi la note de l'Allemagne dans ce rapport.

Pour les pays européens de ce classement, ils bénéficient tous très positivement du RGPD, comme nous l'avons indiqué plus haut pour les Pays-Bas. C'est le cas de la France en particulier, une France qui est première au classement des ressources notamment par rapport aux réglementations mises en place (RGPD, successeur de la loi Informatique et Libertés du 6 janvier 1978) et aux organes de contrôle en particulier la CNIL.

L'Union Internationale des Télécommunications publie également un classement des pays en termes de cybersécurité : l'Index Mondial de Cybersécurité (GCI : *Global Cybersecurity Index*) dont c'est la quatrième édition.

194 pays sont évalués à travers 82 questions selon cinq grandes thématiques : mesures juridiques, mesures techniques, mesures organisationnelles, renforcement des capacités et mesures de coopération.

Le classement est cette fois dominé par les USA (note de 100/100), suivis du UK et de l'Arabie Saoudite. Une remarque toutefois sur cette note de 100/100 pour les USA qui nous laisse un peu perplexe car elle signifie que sur les critères évalués, les USA n'auraient pas d'amélioration envisageable et seraient donc parfaits dans les cinq dimensions analysées. En un mot, le Graal, ce qui est loin d'être le cas.

Voyons plutôt cela comme une valeur relative entre les pays passés au crible de l'enquête.

La France obtient la neuvième note du classement, en cohérence avec son classement du rapport MIT.

À la différence de ce dernier qui excluait la Russie, la Fédération russe obtient dans le GCI la cinquième note, ce qui reflète sans doute mieux son positionnement international sur le sujet.

Quatrième note pour la Corée du Sud, huitième pour le Canada, Australie douzième Allemagne treizième, Pays-Bas seizièmes et Chine trente-troisième… Sans surprise, la France doit sa très bonne place et sa très bonne note (97,6) notamment à ses mesures juridiques comme cela a été souligné aussi dans le rapport du MIT.

Une fois que l'on a regardé les classements internationaux et que l'on s'est familiarisé avec les grandes puissances du monde cyber, il est intéressant de prendre une perspective un peu différente, d'observer les choses sous un autre angle peut-être plus qualitatif, sans doute parfois orienté, cela pour approcher au plus près notre relation avec ces puissances cyber.

Sous quel angle ? Celui de la souveraineté numérique.

Dans une conférence de presse du 19 avril 1963, De Gaulle déclarait : « *Tout système qui consisterait à transmettre notre souveraineté à des aréopages internationaux serait incompatible avec les droits et les devoirs de la République française.* »

Si De Gaulle n'était pas le premier à se soucier de la souveraineté de la France, il l'a placée très haut sur l'échelle de nos valeurs et encore aujourd'hui, celle à laquelle nous faisons référence a beaucoup à voir avec celle que de Gaulle a promue.

De fait, il s'est toujours inquiété de protéger et développer la souveraineté de la France, principe qu'il disait « *intangible* », au cœur de sa pensée notamment quand il déclarait : « *toute ma vie, je me suis fait une certaine idée de la France* ».

Pour autant, il reconnaissait que la souveraineté avait des limites dans un monde d'interdépendances de plus en plus fortes.

La souveraineté numérique à laquelle nous voulons prétendre est justement une affaire de limites, autrement dit jusqu'où acceptons-nous de dépendre des autres ?

À ce propos, les experts et les sachants se gardent bien d'employer le terme de souveraineté numérique tant dans le cyberespace, elle reste utopique et dans l'état actuel des choses, inatteignable.

Autonomie stratégique est un terme bien plus approprié à la situation et qui donne des perspectives positives d'atteinte de résultats.

Dans les domaines qui nous concernent, le terme d'autonomie stratégique apparaît pour la première fois en 1994 dans le livre blanc de la Défense. Il était question à l'époque de définir les moyens dont la France devait disposer pour ne pas totalement dépendre de l'OTAN.

De notion nationale, elle est ensuite devenue européenne à l'occasion de multiples travaux, notamment en 2013 (notion d'une Base Industrielle et Technologique de DEfense, (BITDE) pour augmenter notre autonomie stratégique), puis en 2016 quand dans la stratégie globale pour la politique étrangère et de sécurité de l'Union européenne, on évoque « l'intensification de nos efforts en matière de défense, de lutte contre le terrorisme, d'énergie et de communications stratégiques ainsi que pour ce qui est du cyberespace… », puis dans le nouveau programme stratégique 2019-2024 du conseil européen où la dimension commerciale de l'autonomie stratégique est passée en revue.

À partir des années 2000, et par opposition à l'organisation des systèmes d'information précédente, on voit naître une nouvelle forme de gestion des données appelée cloud computing. Désormais, vu le volume de données produites et échangées sur les réseaux, il devient nécessaire de disposer d'une informatique évolutive à la fois au plan technologique et également au plan économique. Les systèmes précédents ne répondent pas à cette préoccupation et limitent les progrès que réalisent les entreprises sur leurs marchés. Et ce qui est vrai pour les entreprises va progressivement devenir vrai également pour les particuliers. Parallèlement à l'accroissement du volume des données, le coût de leur stockage baisse assez significativement. Ces deux facteurs permettent le développement de l'industrie du cloud computing, développement fondé sur le principe de l'efficacité.

Ce qui fait qu'en quelques années, le cloud computing est devenu le modèle d'organisation informatique de référence pour la flexibilité de gestion qu'il offre à ses utilisateurs en termes de stockage et d'accès aux données.

Et comme toujours en matière de tech, les USA dominent ce marché dans lequel ils sont omniprésents et dans lequel leurs géants (Google, Amazon, Microsoft, Oracle, etc.) mènent la danse.

Cela pose, entre autres, la question de la souveraineté du cloud pour les utilisateurs français et européens et de manière stratégique pour les services de l'état.

La prise de conscience politique des besoins de souveraineté du cloud (et donc le constat de la suprématie des USA sur le sujet) remonte à un peu plus de quatorze ans quand François Fillon, Premier ministre de l'époque, lance en 2009 le projet Andromède (tentative de cloud souverain regroupant Thalès, Dassault Systèmes et Orange) et déclare le 18 janvier 2010 : « *Mon souhait est que ce nouveau type d'infrastructure de service fasse l'objet d'un partenariat public-privé grâce aux fonds du programme pour les investissements d'avenir. Il faut absolument que nous soyons capables de développer une alternative française et européenne dans ce domaine, qui connaît un développement exponentiel […] Force est de constater que les Nord-Américains dominent ce marché, qui constitue pourtant un enjeu absolument majeur pour la compétitivité de nos économies, pour le développement durable et même, j'ose le dire, pour la souveraineté de nos pays* ».

Suite à des divergences entre les participants, le projet sera abandonné en 2015.

Le projet reprendre forme à partir de 2018 avec la présentation de la doctrine d'utilisation de l'informatique en nuage de l'État dans le cadre de la transformation numérique de l'état.

Il s'agit pour les administrations de se servir du potentiel du cloud pour développer de nouveaux services dans un contexte de protection maximal des données, avec le principe du cloud au centre.

Une circulaire du Premier ministre, datée du 5 juillet 2021, vient préciser les principes de la doctrine « Cloud au centre ».

On y trouve en particulier les indications suivantes : « *l'adoption du cloud ne doit pas entraver l'autonomie de prise de décision ni d'action de l'État, pas plus que sa sécurité numérique et la résilience de ses infrastructures, la maîtrise par l'État des données et des traitements qui lui sont confiés, le respect des règles européennes en matière de protection des données à caractère personnel, et ce alors que l'empreinte des acteurs extraeuropéens en matière de cloud est prédominante.* »

L'hébergement des données doit se faire soit sur les ressources de l'État (clouds interministériels) soit, auprès de prestataires qui satisfont aux principes de sécurité édictés par l'état.

Dans le cas de l'utilisation de clouds fournis par des prestataires extérieurs, ils doivent respecter la qualification SecNumCloud de l'ANSSI, de même qu'ils doivent être protégés contre les réglementations extracommunautaires.

L'état est-il en mesure de respecter sa doctrine ?

C'est sans doute une tout autre histoire. Raison pour laquelle il est intéressant de se pencher sur les influences étrangères qui pèsent sur nous, qu'elles aient des origines étatiques, technologiques ou commerciales voire criminelles.

Dans tous les cas, notre opinion est que l'autonomie stratégique ne doit pas devenir un concept banalisé ainsi que l'est devenue la souveraineté numérique qui a perdu son sens faute de pouvoir être atteinte. L'autonomie stratégique dans le cyberespace invite chacun, dans sa sphère privée comme professionnelle, à réfléchir aux moyens qu'il doit absolument garder sous son contrôle pour ne pas se mettre en situation de dépendance critique vis-à-vis d'une « puissance » facialement amie, mais qui peut devenir ennemie soit contextuellement, soit au fil du temps. En parallèle, il faudra aussi accepter de confier une partie de sa souveraineté à des tiers qui ne nous donnent pas de garanties absolues. À nous de faire notre analyse des risques et de leur atténuation.

Dans ce contexte d'autonomie stratégique et de développement des systèmes d'information en cloud computing, impossible de ne pas commencer par parler des USA.

Comme toujours dans la tech, les USA ont depuis un leadership important sur cette brique technologique centrale en matière d'organisation informatique. Et cela ne va pas sans poser problème en particulier vis-à-vis du cloud souverain.

2. Les USA

Photo de Saad Alfozan sur Unsplash

Cette question doit être abordée de deux manières : globalement et avec un focus sur les questions de cybersécurité.

Pourquoi et en quoi les USA sont un pays incontournable en matière de cybersécurité et de souveraineté numérique ?

Les Américains dominent le monde de la « tech » en général et de la cybersécurité en particulier.

L'avance technologique des compagnies américaines et leur empreinte mondiale est telle qu'aujourd'hui, il est quasi impossible de penser un système d'information sans a minima une composante US.